在FMC管理的FTD上配置基於路由的站點到站點 VPN隧道

目錄		
 <u>簡介</u>		
<u>必要條件</u>		
<u>需求</u>		
<u>採用元件</u>		
<u>背景資訊</u>		
限制和限制		
<u>FMC的配置步驟</u>		
<u>驗證</u>		
<u>在FMC GUI上</u>		
<u>在FTD CLI上</u>		

簡介

本文檔介紹如何在由Firepower管理中心管理的Firepower威脅防禦上配置基於靜態路由的站點到站 點VPN隧道。

必要條件

需求

思科建議您瞭解以下主題:

- 對VPN隧道工作方式有基礎認識。
- 瞭解如何在FMC中導航。

採用元件

本檔案中的資訊是根據以下軟體版本:

- 思科Firepower管理中心(FMC)版本6.7.0
- Cisco Firepower威脅防禦(FTD)版本6.7.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

基於路由的VPN允許確定要加密或通過VPN隧道傳送的相關流量,並且使用流量路由而不是策略/訪問清單(如基於策略或基於加密對映的VPN中所示)。加密域設定為允許任何進入IPsec隧道的流量。IPsec本地和遠端流量選擇器設定為0.0.0/0.0.0.0。這表示路由到IPsec通道的任何流量都會被加密,無論其來源/目的地子網為何。

本檔案將重點介紹靜態虛擬通道介面(SVTI)組態。有關安全防火牆上的動態虛擬通道介面(DVTI)組 態,請參閱<u>本檔案</u>。

限制和限制

以下是FTD上基於路由的通道的已知限制和限制:

- 僅支援IPsec。不支援GRE。
- 僅支援IPv4介面,以及IPv4、受保護的網路或VPN負載(不支援IPv6)。
- 對VPN流量進行分類的VTI介面支援靜態路由和僅BGP動態路由協定(不支援其他協定,如 OSPF、RIP等)。
- 每個介面僅支援100個VTI。
- FTD叢集上不支援VTI。
- 這些策略不支援VTI:
 - · QoS
 - \cdot NAT
 - ·平台設定

新VPN通道的FMC/FTD 6.7.0版不再支援這些演演算法(FMC支援所有移除的密碼以管理FTD < 6.7):

- IKE策略不支援3DES、DES和NULL加密。
- DH組1、2和24在IKE策略和IPsec建議中不受支援。
- IKE策略不支援MD5完整性。
- IKE策略不支援PRF MD5。
- IPsec提議中不支援DES、3DES、AES-GMAC、AES-GMAC-192和AES-GMAC-256加密演算法。

注意:對於基於站點到站點路由和基於策略的VPN隧道,此情況適用。為了將舊版FTD從 FMC升級到6.7,它會觸發預驗證檢查,警告使用者有與封鎖升級的已移除密碼相關的變更。

通過FMC 6.7管理的FTD 6.7	配置可用	站點到站點VPN隧道
全新安裝	弱密碼可用,但無法用於配置 FTD 6.7裝置。	弱密碼可用,但無法用於配置 FTD 6.7裝置。
升級:FTD僅配置弱密碼	從FMC 6.7 UI升級,預驗證檢查 會顯示錯誤。在重新配置之前 ,升級被阻止。	進行FTD升級後,並假設對等點 的設定未變更,則通道會終止。
升級:FTD僅設定一些弱密碼和 強密碼	從FMC 6.7 UI升級,預驗證檢查 會顯示錯誤。在重新配置之前 ,升級被阻止。	FTD升級後,假設對等點具有強 密碼,然後通道重新建立。
升級:C類國家/地區(沒有強大 的加密許可證)	允許DES	允許DES

✤ 注意:無需其他許可,可在許可模式和評估模式下配置基於路由的VPN。 如果沒有加密合規 (啟用匯出控制功能),只有DES可用作加密演算法。

FMC的配置步驟

步驟 1.導航至Devices >VPN >Site To Site。

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 Collapse All	į	Remote Troubles	Access	D)	Warning (0)	Offline (0) N	ormal (1) Dep	loymer

步驟 2.按一下「Add VPN」,然後選擇「Firepower Threat Defense Device」,如下圖所示。



步驟 3.提供拓撲名稱並選擇VPN型別作為基於路由(VTI)。選擇IKE版本。

在本演示中:

拓撲名稱:VTI-ASA

IKE版本: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

步驟 4.選擇需要在其上配置隧道的Device,您可以選擇新增新的Virtual Template Interface(按一下 +圖示),或者從現有清單中選擇一個介面。

ndpoints	IKE	IPsec	Advanced			
	Node A			Node B		
Device:*			D	evice:*		
FTD		Y	E	Empty	*	
Virtual T	unnel Interface:*			irtual Tunnel Interface:*		
		*		Empty	~	\odot
U Tunne	I Source IP is Private	Edit V H		J Tunnel Source IP is Private	Edit VII	
Connect	ion Type:*		C	connection Type:*		
Bidirecti	onal	*	E	Bidirectional	*	
Tuppel I	P. Addrosec			uppel TD Address		
Tunnel	F Address Source Interface	1		unnel Source Interface		
Tunnel S	Source Interface IP	-	Ť	unnel Source Interface IP		

步驟 5.定義新虛擬通道介面的引數。按一下「OK」(確定)。

- 在本演示中:
- 名稱:VTI-ASA
- 說明(可選):使用外網ASA的VTI隧道
- 安全區域:VTI-Zone
- 通道ID:1
- IP地址:192.168.100.1/30
- 隧道源:GigabitEthernet0/0(外部)

Add Virtual Tunnel	Interface		?	
General				
Name *:	VTI-ASA	Enabled		
Description:	VTI Tunnel with Extranet ASA]		
Security Zone:	VTI-Zone 🗸]		
Tunnel ID *:	1	Range: 0 - 10413		
IP Address *:	192.168.100.1/30	0		
Tunnel Source *:	GigabitEthernet0/0 (Outside)	•		
		ок	ancel	Ī

步驟 6.點選彈出視窗中的OK,提示已建立新VTI。

				Node B
Virtual				
the VT	VTI has been of Please go to th Interfaces pag	crea ne D le to	ted successfully. evice > delete/update	erface:
			ок	is Priva
			Connection Typ	e:*

步驟 7.選擇新建立的VTI或虛擬隧道介面下存在的VTI。提供節點B(對等裝置)的資訊。

在本演示中:

裝置:Extranet

裝置名稱:ASA-Peer

終端IP地址:10.106.67.252

16	Create New VPN Topo	logy		? :	×
	Topology Name:*	VTI-ASA	to Map) 💿 Route B	Based (VTI)	
	Network Topology: IKE Version:*	Point to Point IKEv1 IKEv2	* Hub and Spoke	Full Mesh	
	Endpoints IKE	IPsec	Advance	ed	
	No Device:* FTD Virtual Tunnel Inte VTI-ASA Tunnel Source IP Connection Type:* Bidirectional	de A rface:* is Private		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 erface : Outside erface IP : 10.197. ration () e VTI : Routing : AC Polic	8.100.1 224.90 <u>Policy</u>		
Ľ				Save Cancel	

步驟 8.導航到IKE頁籤。您可以選擇使用預定義的Policy,或按一下Policy頁籤旁邊的+按鈕並建立 一個新策略。

IKEv2 Settings		_
Policy:*	AES-GCM-NULL-SHA-LATEST	▼
Authentication Type:	Pre-shared Automatic Key	~
Pre-shared Key Length:*	24 Characters (Range 1-1	.27)

步驟9.(可選,如果建立新的IKEv2策略。) 為策略提供名稱,並選擇要在策略中使用的演算法。 按一下「Save」。

在本演示中:

名稱:ASA-IKEv2-Policy

完整性演算法:SHA-512

加密演算法:AES-256

PRF演算法:SHA-512

Diffie-Hellman組:21

New IKEv2 Policy			? X
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	MDS SHA SHA512 SHA256 SHA384 SHA384	Add	
		Save Car	ncel

步驟 10.選擇新建立的策略或現有的Policy。選擇Authentication Type。如果使用預共用手動金鑰 ,請在金鑰和確認金鑰框中提供金鑰。

在本演示中:

策略:ASA-IKEv2-Policy

身份驗證型別:預共用手動金鑰

主要:cisco123

確認金鑰:cisco123

KEv1 Settings			
Policy:*	preshared_sha_aes256_dh14_3	~	\bigcirc
Authentication Type:	Pre-shared Automatic Key	~	
Pre-shared Key Length:*	24 Characters (Range 1-	127)	
KEv2 Settings			
KEv2 Settings	ASA-IKEv2-Policy	~	
KEv2 Settings Policy:*	ASA-IKEv2-Policy	*	0
KEv2 Settings Policy:* Authentication Type:	ASA-IKEv2-Policy Pre-shared Manual Key	*	0
KEv2 Settings Policy:* Authentication Type: Key:*	ASA-IKEv2-Policy Pre-shared Manual Key	×	0

≫ 注意:如果兩個終端在同一個FMC上註冊,則還可以使用預共用自動金鑰選項。

步驟 11.導航到IPsec選項卡。 您可以選擇使用預定義的IKEv2 IPsec建議或建立一個新的IKEv2 IPsec建議。點選IKEv2 IPsec Proposal選項卡旁的Edit按鈕。

Crypto Map Type:	Static Opynamic		
IKEv2 Mode:	Tunnel	~	
Transform Sets:	IKEv1 IPsec Proposals 🏑	2	IKEv2 IPsec Proposals* 🥜
	tunnel_aes256_sha		AES-GCM
Enable Security Ass	ociation (SA) Strength E	nforceme	int

步驟12.(可選,如果建立新的IKEv2 IPsec提議。) 提供建議書的名稱,並選擇建議書中要使用的 演算法。按一下「Save」。

在本演示中:

名稱: ASA-IPSec-Policy

ESP雜湊:SHA-512

ESP加密:AES-256

lew IKEv2 IPsec P	roposal		?
Name:* Description:	ASA-IPSec-Policy		
ESP Hash	Available Algorithms	Selected A	lgorithms
	AES-GCM-256 AES-GCM-192 AES-192 AES-GCM AES-GCM AES AES DES AES-GMAC-256	Add	56
		Save	Cancel

步驟 13. 從可用提案清單中選擇新建立的提案或提案。按一下「OK」(確定)。

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

步驟14。(可選)選擇Perfect Forward Secrecy設定。配置IPsec生存期和生存期大小。

在本演示中:

10 M

完全前向保密:模群21

生存時間:28800(預設)

生存期大小:	4608000 ((預設值)
--------	-----------	-------

L	Enable Security Ass	ociation (SA) Strength	Enforc	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)
	−▼ ESPv3 Settings			

步驟 15.檢查配置的設定。按一下「Save」,如下圖所示。

Topology Name:*	VTI-ASA		
	○ Policy Based (Cr	ypto Map) 🖲 Route Based (VTI)	
Network Topology	: Foint to Point	t 🔆 Hub and Spoke 💠 Full Mesh	
IKE Version:*	🗌 IKEV1 🗹 IKEV2	2	
Endpoints	IKE IPsec	Advanced	
Crypto Map Type:	Static Dynamic		
IKEv2 Mode:	Tunnel		
Transform Sets:	IKEv1 IPsec Proposals 🥜	IKEv2 IPsec Proposals* 🥜	
	tunnel_aes256_sha	ASA-IPSec-Policy	
Enable Security A	Association (SA) Strength Enfo	prcement	
Enable Perfect For Enable Per	orward Secrecy		
Modulus Group:	21		
Lifetime Duration*:	28800	Seconds (Range 120-2147483647)
Lifetime Size:	4608000	Kbytes (Range 10-2147483647)	
— ▼ ESPv3 Settin	gs		
			Save Cancel

步驟 16.配置訪問控制策略。導覽至Policies > Access Control > Access Control。編輯應用於 FTD的策略。

◆ 注意:sysopt connection permit-vpn不適用於基於路由的VPN隧道。需要為IN-> OUT區域和 OUT -> IN區域配置訪問控制規則。

在Zones頁籤中提供Source Zones和Destination Zones。

在Networks 選項卡中提供Source Networks和Destination Networks。按一下「Add」。

在本演示中:

源區域:內區域和外區域

目標區域:區外和區內

源網路:內聯網和遠端網路

目標網路:遠端網路和內聯網

Name						?
	VTI-Traffic		Enabled	Insert into Manda	tory	~
Action	🖋 Allow	- 00.a	tı I			
Time Range	None 🗸 🕥					
Zones N	Networks VLAN Tags A Lisers	Applications	Ports URLS SGT/ISE	Attributes	Inspection Logo	ing Comments
vailable Zon	es Ĉ	rippined circuit	Source Zones (2)		Destination Zones (2)	of the second second
Search by r	name		in-Zone	8	In-Zone	6
- In-Zone				6		6
Out-Zone		l l				
VTI-Zone		Add to	1			
		Source	J			
		Add to Destination				
			9			
ction	Allow	VUDA	en 🗔		,	
ction	Allow	V 🗆 🖌	ta 🕒			
ime Range	None 💙 📀					
Zones N	etworks VLAN Tags 🔺 Users	s Applications	Ports URLs SGT/IS	E Attributes	Inspection Logo	ing Comments
ailable Netw	vorks C 📀		Source Networks (2)		Destination Networks (2)	
			Source	Original Client	📻 In-Netwrk	
Networ	rks Geolocation		🚍 In-Netwrk	8	Remote-Network	
			Remote-Network	6		
IPv4-Private	e-172.16.0.0-12					
IPv4-Private	e-172.16.0.0-12 e-192.168.0.0-16	Add To Source	-			
IPv4-Private	e-172.16.0.0-12 e-192.168.0.0-16 e-All-RFC1918 Manned	Add To Source Networks				
IPv4-Private IPv4-Private IPv4-Private IPv6-IPv4-M IPv6-Link-Li	e-172.16.0.0-12 e-192.168.0.0-16 e-All-RFC1918 Mapped .ocal	Add To Source Networks Add to Destination				
IPv4-Private IPv4-Private IPv4-Private IPv6-IPv4-M IPv6-Link-Link-Link-Link-Link-Link-Link-Link	e-172.16.0.0-12 e-192.168.0.0-16 e-All-RFC1918 Mapped .ocal e-Unique-Local-Addresses	Add To Source Networks Add to Destination				
IPv4-Private IPv4-Private IPv4-Private IPv6-IPv4-N IPv6-Link-Li IPv6-Private IPv6-to-IPv	e-172.16.0.0-12 e-192.168.0.0-16 e-All-RFC1918 Mapped .ocal e-Unique-Local-Addresses r4-Relay-Anycast	Add To Source Networks Add to Destination				
IPv4-Private IPv4-Private IPv4-Private IPv6-IPv4-N IPv6-Inv4-N IPv6-Private IPv6-Private Remote-Net	e-172.16.0.0-12 e-192.168.0.0-16 e-All-RFC1918 Mapped .ocal e-Unique-Local-Addresses r4-Relay-Anycast twork	Add To Source Networks Add to Destination				

步驟 17.透過VTI通道新增路由。導覽至Devices > Device Management。編輯VTI隧道配置所在的 裝置。

導覽至Routing 索引標籤下的Static Route。按一下Add Route。

提供Interface,選擇Network,提供Gateway。按一下「OK」(確定)。

在本演示中:

介面:VTI-ASA

網路:遠端網路

網關:VTI-ASA — 隧道

Add Static Ro	ute Configuratio	n			? X
Type: Interface*	IPv4 O IPv6 VTI-ASA (Interface starting wi	ith this icon 👩	▼ signifies it is av	ailable for rout	e leak)
Available Net	twork C ③	Add	Selected I	Network xe-Network	
Gateway* Metric: Tunneled: Route Tracking:	VTI-ASA-Tunnel	fault Route)	 (1 - 254) (254) 		
				ок	Cancel

步驟 18.導航到部署>部署。選擇需要將組態部署到的FTD,然後按一下Deploy。

成功部署後配置推送到FTD CLI:

<#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 192.168.100.1 255.255.252
tunnel source interface Outside
tunnel destination 10.106.67.252
tunnel mode ipsec ipv4

tunnel protection ipsec profile FMC_IPSEC_PROFILE_1

驗證

在FMC GUI上

按一下Check Status選項以從GUI本身監控VPN隧道的即時狀態



其中包括從FTD CLI獲取的以下命令:

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

extranet : ASA-Peer		• FTD/VTI-ASA
> show crypto ipsec sa peer		> show crypto ipsec sa peer 10.106.67.252
Not applicable for extranet peer		<pre>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 compressed: 0, #pkts decrypt: 100, #pkts verify: 100 #pkts compressed: 0, #pkts decrypt: 100, #pkts verify: 100 #pkts not compressed: 100, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PTUs 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	i	> show vpn-sessiondb detail l2l filter ipaddress 10.106.67.252
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)AE5256 IPsec: (1)AE5256 Hashing : IKEV2: (1)SHA512 IPsec: (1)SHA512 Bytes Tx : 10000 Login Time : 03:54:57 UTC Thu Nov 12 2020 Duration : 0h:02m:12s Tunnel Zone : 0 IKEV2 Tunnels: 1 IPsec Tunnels: 1 IKEV2: [Duration : 04.1
		UDP Dst Port : 500 Rem Auth Mode: preSharedKeys Loc Auth Mode: preSharedKeys Encryption : AE5256 Rekey Int (T): 86400 Seconds PRF : SHA512 D/H Group : 21

在FTD CLI上

可從FTD CLI使用這些命令來檢視VPN通道的組態和狀態。

```
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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。