# 在FMC管理的FTD上配置基于路由的站点到站点 VPN隧道

# 简介

本文档介绍如何在由Firepower管理中心管理的Firepower威胁防御上配置基于静态路由的站点到站 点VPN隧道。

# 先决条件

### 要求

Cisco 建议您了解以下主题:

- 基本了解VPN隧道的工作方式。
- 了解如何在FMC中导航。

### 使用的组件

本文档中的信息基于以下软件版本:

- 思科Firepower管理中心(FMC)版本6.7.0
- 思科Firepower威胁防御(FTD)版本6.7.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

# 背景信息

基于路由的VPN允许确定要加密或通过VPN隧道发送的相关流量,并且使用流量路由而不是策略/访问列表,如基于策略或基于加密映射的VPN中所示。加密域设置为允许任何进入IPsec隧道的流量。IPsec本地和远程流量选择器设置为0.0.0/0.0.0。这意味着路由到IPsec隧道的所有流量都会被加密,无论源/目标子网如何。

本文档重点介绍静态虚拟隧道接口(SVTI)配置。有关安全防火墙上的动态虚拟隧道接口(DVTI)配置 ,请参阅此<u>文档</u>。

#### 限制和限制

以下是FTD上基于路由的隧道的已知限制和限制:

- 仅支持IPsec。不支持GRE。
- 仅支持IPv4接口以及IPv4、受保护的网络或VPN负载(不支持IPv6)。
- 为VPN流量分类的VTI接口支持静态路由和仅BGP动态路由协议(不支持其他协议,如 OSPF、RIP等)。
- 每个接口仅支持100个VTI。
- FTD集群不支持VTI。
- 以下策略不支持VTI:
  - · QoS

#### • NAT

·平台设置

对于新的VPN隧道,FMC/FTD 6.7.0版不再支持这些算法(FMC支持所有删除的密码以管理FTD < 6.7):

- IKE策略不支持3DES、DES和NULL加密。
- DH组1、2和24在IKE策略和IPsec建议中不受支持。
- IKE策略不支持MD5完整性。
- IKE策略不支持PRF MD5。
- IPSec提议中不支持DES、3DES、AES-GMAC、AES-GMAC-192和AES-GMAC-256加密算法。

注意:对于基于站点到站点路由和基于策略的VPN隧道而言,此情况均成立。为了将旧的 FTD从FMC升级到6.7,它会触发预验证检查,警告用户有关与阻止升级的删除密码相关的更 改。

FTD 6.7通过FMC 6.7管理	可用配置	站点到站点VPN隧道
全新安装	弱密码可用,但无法用于配置 FTD 6.7设备。	弱密码可用,但无法用于配置 FTD 6.7设备。
升级:FTD仅配置弱密码	从FMC 6.7 UI升级,预验证检查 显示错误。在重新配置之前,升 级会被阻止。	FTD升级后,假设对等体未更改 其设置,则隧道将终止。
升级:FTD仅配置了一些弱密码 和强密码	从FMC 6.7 UI升级,预验证检查 显示错误。在重新配置之前,升 级会被阻止。	FTD升级后,假设对等体具有强 密码,然后重建隧道。
升级:C类国家/地区(没有强加 密许可证)	允许DES	允许DES

\_\_\_\_

✤ 注意:无需额外许可,可在许可模式和评估模式下配置基于路由的VPN。 如果没有加密合规 (启用导出控制功能),只有DES可用作加密算法。

# FMC的配置步骤

步骤1:导航到设备>VPN >站点到站点。

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)   Dep	loymer

第二步:单击Add VPN,然后选择Firepower Threat Defense Device,如图所示。



第三步:提供拓扑名称并选择VPN类型作为基于路由(VTI)。选择IKE Version。

在本演示中:

拓扑名称:VTI-ASA

IKE版本: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				

第四步:选择需要在其上配置隧道的Device,您可以选择添加新的Virtual Template Interface(单击 +图标),或从现有列表中选择一个。

Indpoints	IKE	IPsec	Advanced	l		
	Node A			Node B		
Device:*			D	evice:*		
FTD		*	E	Empty		*
Virtual T	unnel Interface:*			irtual Tunnel Interface:*		<b>v</b> ()
Tunnel	Source IP is Private	Edit VI		Tunnel Source IP is Private	Edit V	<u>/TI</u>
Connecti	on Type:*		c	connection Type:*		
Bidirectio	onal	*	E	Bidirectional		*
Tunnel I Tunnel S Tunnel S	P Address ource Interface ource Interface IP	:	ТТТ	unnel IP Address unnel Source Interface unnel Source Interface IP	:	

第五步:定义新虚拟隧道接口的参数。Click OK.

在本演示中:

名称:VTI-ASA

说明(可选):具有外网ASA的VTI隧道

安全区域:VTI-Zone

隧道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	abled
Description:	VTI Tunnel with Extranet ASA	
Security Zone:	VTI-Zone 👻	
Tunnel ID *:	1 Range	: 0 - 10413
IP Address *:	192.168.100.1/30	
Tunnel Source *:	GigabitEthernet0/0 (Outside)	
	ſ	OK Cancel

第六步:点击弹出窗口中的OK,提示已创建新的VTI。

		No	de B
	Virtual Tunnel Interface A	dded	
	VTI has been created and Please go to the Device Interfaces page to delete the VTI.	successfully. e > ete/update	rface:
*****		ок	is Priva
		onnection Type:*	

步骤 7.选择Virtual Tunnel Interface下新创建的VTI或存在的VTI。提供节点B(对等设备)的信息。

在本演示中:

设备:外联网

### 设备名称:ASA-Peer

#### 终端IP地址:10.106.67.252

16	Create New VPN Topo	logy		? >
	Topology Name:*	VTI-ASA O Policy Based (Cry	pto Map) 💿 Route B	Based (VTI)
	Network Topology: IKE Version:*	Point to Point     IKEv1 IKEv2	Hub and Spoke	Full Mesh
	Endpoints IKE No Device:* FTD Virtual Tunnel Inte VTI-ASA VTI-ASA Connection Type:* Bidirectional Tunnel IP Address Tunnel Source Inte Tunnel Source Inte Additional Configur Route traffic to the Permit VPN traffic	IPsec de A rface :* is Private erface IP ration (1) e VTI : Routin : AC Pole	Advance	And Node B  Device:* Extranet  Device Name*: ASA-Peer  Endpoint IP Address*: 10.106.67.252
				Save Cancel

步骤 8导航到IKE选项卡。您可以选择使用预定义的Policy,或单击Policy选项卡旁边的+按钮并创建 一个新策略。

IKEv2 Settings		_	
Policy:*	AES-GCM-NULL-SHA-LATEST	<b>v</b> (	D
Authentication Type:	Pre-shared Automatic Key	~	
Pre-shared Key Length:*	24 Characters (Range 1-12	27)	

步骤9.(可选,如果创建新的IKEv2策略。) 为策略提供Name并选择要在策略中使用的算法。 Click Save.

在本演示中:

名称:ASA-IKEv2-Policy

完整性算法:SHA-512

加密算法:AES-256

PRF算法:SHA-512

Diffie-Hellman组:21

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

步骤 10选择新创建的策略或现有的Policy。选择身份验证类型。如果使用预共享手动密钥,请在密 钥和确认密钥框中提供密钥。

在本演示中:

策略:ASA-IKEv2-Policy

#### 身份验证类型:预共享手动密钥

密钥:cisco123

确认密钥:cisco123

Policy:*	preshared_sha_aes256_dh14_3	~	$\bigcirc$
Authentication Type:	Pre-shared Automatic Key	~	
Pre-shared Key Length:*	24 Characters (Range 1	-127)	
KEv2 Settings			
Policy:*	ASA-IKEv2-Policy	~	0
REv2 Settings Policy:* Authentication Type:	ASA-IKEv2-Policy Pre-shared Manual Key	× •	0
REv2 Settings Policy:* Authentication Type: Key:*	ASA-IKEv2-Policy Pre-shared Manual Key	* *	0

注意:如果两个终端在同一个FMC上注册,也可以使用预共享自动密钥选项。

步骤 11导航到IPsec选项卡。 您可以选择使用预定义的IKEv2 IPsec提议,也可以创建一个新的 IKEv2 IPsec提议。点击IKEv2 IPsec Proposal选项卡旁的Edit按钮。

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 Er	nforceme	nt

步骤12.(可选,如果创建新的IKEv2 IPsec提议。) 为建议书提供Name并选择要在建议书中使用 的算法。Click Save.

在本演示中:

名称:ASA-IPSec-Policy

ESP哈希:SHA-512

ESP加密:AES-256

New IKEv2 IPsec Pro	posal			? ×
Name:* Description.	ASA-IPSec-Policy			
ESP Hash ESP Encryption	Available Algorithms	_	Selected Algorithm	ıs
	AES-GCM-256 AES-GCM-192 AES-192 AES-GCM AES-GCM AES AES-GCM AES DES AES-GMAC-256	Add	🔅 AES-256	
			Save	Cancel

步骤 13 从可用提案列表中选择新创建的提案或提案。Click OK.

on:*	IKEv2 IPsec Proposal			? ×
D T:	Available Transform Sets C C Search AES-GCM AES-SHA		Selected Transform Sets	
Se	Image: Astronomy of the sector of the sec	Add		
Sec Peri s G				
ura ze:			ок	Cancel

步骤14.(可选)选择Perfect Forward Secrecy设置。配置IPsec Lifetime Duration和Lifetime Size。 在本演示中:

完全前向保密:模数组21

生存期:28800(默认)

生存期大小:	4608000 (	(默认)	)
--------	-----------	------	---

	Enable Security Ass	sociation (SA) Stre	nath Enforce	ement
L	Enable Perfect Forv	vard Secrecy		
L	Modulus Group:	21	*	
L	Lifetime Duration*:	28800		Seconds (Range 120-2147483647)
L	Lifetime Size:	4608000		Kbytes (Range 10-2147483647)
	-	-		

步骤 15检查配置的设置。单击Save,如下图所示。

Topology Name:*	VTI-ASA			
	O Policy Based (Cry	pto Map) 🖲 Route Based (VTI)		
Network Topology:	← Point to Point	* Hub and Spoke + Full Mes		
IKE Version:*	🗌 IKEv1 🗹 IKEv2			
Endpoints	IKE IPsec	Advanced		
Crypto Map Type:	Static Opynamic			
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 For	rward Secrecy			
Modulus Group:	21 👻			
Lifetime Duration*:	28800	Seconds (Range 120-2147483	547)	
Lifetime Size:	4608000	Kbytes (Range 10-214748364	)	
- 💌 ESPv3 Setting	gs			
				Save

步骤 16配置访问控制策略。导航到策略>访问控制>访问控制。编辑应用于FTD的策略。

✤ 注意:sysopt connection permit-vpn不适用于基于路由的VPN隧道。需要为IN-> OUT区域和 OUT -> IN区域配置访问控制规则。

在Zones 选项卡中提供Source Zones 和Destination Zones。

在Networks选项卡中提供Source Networks和Destination Networks。单击 Add。

在本演示中:

源区域:区内区与区外

目标区域:区外和区内

源网络:内部网络和远程网络

目的网络:远程网络和内部网络

						?
Name	VTI-Traffic		Enabled	Insert into Manda	tory	~
Action	Allow	V U D 2	115			
Time Range	None 🗸 🔾					
Zones	Networke VIAN Tans A Lisers	Applications	Porte LIPLE SCT/IS	E Attributes	Inspection Logo	aina Commente
vailable Zor	necificities vickit rogs as oscis	Applications	Source Zones (2)	L AITHUITES	Destination Zones (2)	ging comments
Search by	name		startes zones (2)	8	in-Zone	
- In. 7000			Out-Zone	6	Out-Zone	6
2 Out-Zone				-		-
VTI-Zone		Add to	1			
		Source				
		Add to				
		Destination				
ld Rule						?
lame	VTI-Traffic		Enabled	Insert into Manda	tory	
lame	VTI-Traffic		Enabled	Insert into Manda	itory	~
lame	VTI-Traffic	V U 0.8	Enabled	Insert into Manda	itory	~
lame ction ïme Range	VTI-Traffic	V U D 28	Enabled	Insert into Manda	itory	<b>v</b>
lame ction îme Range Zones	VTI-Traffic  VII-Traffic  VII-T	S Applications	Enabled     Ports URLs SGT/IS	Insert into Manda	Inspection Loge	qing Comments
ame ction ime Range Zones N vailable Netr	VTI-Traffic VTI-Traffic None None VLAN Tags Users works C Q	Applications	Enabled  Ports URLs SGT/I:  Source Networks (2)	Insert into Manda	Inspection Log Destination Networks (2)	ging Comments
lame ction îme Range Zones N vailable Netr	VTI-Traffic  VTI-Traffic  VIAN Tags  Users  VLAN Tags  Users  VLAN Tags  VLAN	Applications	Enabled  Ports URLs SGT/II  Source Networks (2)  Source	Insert into Manda SE Attributes Original Client	Inspection Log Destination Networks (2)	ging Comments
ame ction ime Range Zones N vailable Net	VTI-Traffic	Applications	Enabled  Ports URLs SGT/I:  Source Networks (2)  Source In-Netwrk	Insert into Manda	Inspection Log Destination Networks (2)	ging Comments
lame ction Time Range Zones N vailable Net Netwo	VTI-Traffic VII-Traffic VII-Traffic None VLAN Tags Users works C Geolocation te-172.16.0.0-12	Applications	Enabled  Ports URLs SGT/I3  Source Networks (2)  Source Remote-Network	Insert into Manda	Inspection Loge Destination Networks (2)	ging Comments
lame ction ime Range Zones N vailable Net Netwo i IPv4-Privat	VTI-Traffic  VII-Traffic  VII-Traffic  VIAN Tags Users VLAN Tags Users vorks C Geolocation te-172.16.0.0-12 te-192.168.0.0-16	Applications	Enabled  Ports URLs SGT/IS  Source Networks (2)  Source In-Netwrk Remote-Network	Insert into Manda	Inspection Log Destination Networks (2)	ging Comments
lame ction Time Range Zones N vailable Netwo Netwo IPv4-Privat IPv4-Privat IPv4-Privat IPv4-Privat	VTI-Traffic Allow None VLAN Tags A Users works C works C works Geolocation te-172.16.0.0-12 te-192.168.0.0-16 te-All-RFC1918 Magacia	Applications Applications	Enabled  Ports URLs SGT/IS  Source Networks (2)  Source Remote-Network	Insert into Manda	Inspection Log Destination Networks (2)	ging Comments
lame ction Time Range Zones N vailable Netwo IPv4-Privat IPv4-Privat IPv4-Privat IPv6-IPv4-	VTI-Traffic  VTI-Traffic  VII-Traffic  VIAN Tags VLAN Tags VLAN Tags VLAN Tags C VIAN Tags	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) In-Netwrk Remote-Network	ging Comments
lame ction Time Range Zones N vailable Net Post-Privat IPv4-Privat IPv4-Privat IPv4-Privat IPv6-IPv4- IPv6-Link- IPv6-Link-	VTI-Traffic	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 Comments
Iame ction Time Range Zones N vailable Net Protection IPv4-Privat IPv4-Privat IPv4-Privat IPv6-IPv4- IPv6-Link- IPv6-co-IP	VTI-Traffic VII-Traffic None None VLAN Tags Users works C C C C C C C C C C C C C	Applications Add To Source Networks Add to Destination	Enabled      Ports URLs SGT/I      Source Networks (2)      Source      In-Netwrk      Remote-Network	Insert into Manda	Inspection Loge Destination Networks (2)	ging Comments
Iame ction ime Range Zones N vailable Netwo IPv4-Prival IPv4-Prival IPv6-IPv4- IPv6-Inv- IPv6-Link- IPv6-c-IPv Remote-Netwo	VTI-Traffic Allow None VLAN Tags Users works C Geolocation te-172.16.0.0-12 te-192.168.0.0-16 te-All-RFC1918 Mapped Local te-Unique-Local-Addresses v4-Relay-Anycast etwork	Applications 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 Comments
Aame ction ime Range Zones N vailable Netwo i IPv4-Privat i IPv4-Privat IPv4-Privat IPv6-IPv4- i IPv6-Link-l IPv6-C-IPk Remote-Netwo VTI-ASA-T	VTI-Traffic VII-Traffic None None VLAN Tags Users works C C C C C C C C C C C C C	Applications Add To Source Networks Add to Destination	Enabled  Ports URLs SGT/IS  Source Networks (2)  Source In-Netwrk Remote-Network  Enter an IP address	Insert into Manda	Inspection Log Destination Networks (2)	ging Comments

步骤 17添加通过VTI隧道的路由。导航到设备>设备管理。编辑配置VTI隧道的设备。

导航到路由选项卡下的静态路由。单击Add Route。

提供接口,选择网络,提供网关。Click OK.

在本演示中:

接口:VTI-ASA

网络:远程网络

网关:VTI-ASA-Tunnel

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)	<ul> <li>(1 - 254)</li> <li>(254)</li> </ul>		
				ок	Cancel

步骤 18.导航到部署>部署。选择配置需要部署到的FTD,然后单击Deploy。

成功部署后推送到FTD CLI的配置:

<#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

# 验证

### 从FMC GUI

单击Check Status选项以从GUI本身监控VPN隧道的实时状态



这包括从FTD CLI获取的以下命令:

- 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

# 从FTD CLI

#### 可以从FTD CLI使用这些命令查看VPN隧道的配置和状态。

```
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

#### 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。