在由FMC管理的FTD上配置双ISP VTI

目录

<u>简介</u>		
<u>先决条件</u>		
基本要求		
使用的组件		
<u>FMC上的配置</u>		
<u>拓扑配置</u>		
<u>终端配置</u>		
<u>IKE 配置</u>		
<u>IPSec 配置</u>		
<u>路由配置</u>		

简介

本文档介绍在FMC管理的FTD设备上使用虚拟隧道接口部署双ISP设置。

先决条件

基本要求

- 对站点到站点VPN有基本了解将非常有益。此背景有助于掌握VTI设置过程,包括涉及的关键 概念和配置。
- 了解在Cisco Firepower平台上配置和管理VTI的基础知识至关重要。这包括了解VTI如何在 FTD中运行,以及如何通过FMC界面控制它们。

使用的组件

- 适用于VMware的思科Firepower威胁防御(FTD):版本7.0.0
- Firepower管理中心(FMC):版本7.2.4(内部版本169)

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。

FMC上的配置

拓扑配置

1. 导航到设备>VPN >站点到站点。



2.单击Add以添加VPN拓扑。

Deploy	ų	₩	?	aamin 🔻	cisc	SECU	RE
Last l	Jpdate	ed: 10:02 F	PM	Refresh		Add	
							×

3. 为拓扑命名,选择VTI和点对点,然后选择IKE版本(本例中为IKEv2)。

Create New VPN Topology	
Topology Name:* Dual-ISP-VTI	
 Policy Based (Crypto Map) (Route Based (VTI) Network Topology: 	
Point to Point Hub and Spoke Full Mesh	
IKE Version:* 🗌 IKEv1 🗹 IKEv2	

终端配置

1. 选择需要配置隧道的设备。

添加远程对等体详细信息。 您可以通过点击"+"图标添加新的虚拟模板接口,或从现有列表中选择一个虚拟模板接口。

Node A	Node B
)evice:*	Device:*
New_FTD 🔻	Extranet 👻
/irtual Tunnel Interface:*	Device Name*:
• +	VTI-Peer
Tunnel Source IP is Private Edit VTI	Endpoint IP Address*:
Send Local Identity to Peers	10.10.10.2
+ Add Backup VTI (optional)	

Cancel	Save

如果要创建新的VTI接口,请添加正确的参数,启用该接口,然后单击"确定"。

注意:这将成为主VTI。

Add Virtual Tunnel Interface

General	
Name:* VTI-1	
Enabled	
Description:	
This is the primary VTI tunnel. This VTI goes through ISP 1.	
Security Zone:	
OUT v	
Priority:	
0	(0 - 65535)
	·
Virtual Tunnel Interface Details	Turnel Course is a physical interface where VDN turnel terminates for the

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:*

1	(0 - 10413)	
Tunnel Source:*		
GigabitEthernet0/0 (outside1)	▼ 10.106.52.104	r

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

r	IPeee Tunnel Mede:*	
I	IPv4 O IPv6	
I	192.168.10.1/30	0
5		

3. 单击"+"。添加备份VIT"以添加辅助VIT。

0

Device:*

10.106.50.55 Virtual Tunnel Interface:* VTI-1 (IP: 192.168.10.1) Tunnel Source: outside1 (IP: 10.106.52.104)Edit VTI

Tunnel Source IP is Private Send Local Identity to Peers + Add Backup VTI (optional) Connection Type:* **Bidirectional** T Additional Configuration Route traffic to the VTI : <u>Routing Policy</u> Permit VPN traffic · AC Policy

T

V

4. 点击"+"添加辅助VTI的参数(如果尚未配置)。

Endpoints	IKE	IPsec	Advanced		
10.	106.50	.55		•	
Virtua	l Tunne	el Interfa	ce:*		
VTI	-1 (IP:	192.168	.10.1)	• +	
Tunne	el Sour unnel S	ce: outsi Source IP	de1 (IP: 10.1) is Private	06.52.10	94)Edit VTI
S	end Lo	cal Ident	tity to Peers		
Backu	ıp VTI:				Remove
Virtua	l Tunne	el Interfa	ce:*		–
				• +	
	unnel S	Source IP	is Private		Edit VTI
S	end Lo	cal Ident	ity to Peers		
Conn	ection	Type:*			

5. 如果要创建新的VTI接口,请添加正确的参数,启用该接口,然后单击"确定"。 注意:这将成为辅助VTI。

Add Virtual Tunnel Interface

General
VTI-2
C Enabled
Description:
This is the secondary VTI tunnel VTI goes through ISP 2.
Security Zone:
OUT 🔹
Priority:
0 (0 - 65535)
Virtual Tunnel Interface Details An interface named Tunnel <id> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI. Tunnel ID:*</id>
2 (0 - 10413)
Tunnel Source:*
GigabitEthernet0/1 (outside2) ▼ 10.106.53.10 ▼
IPsec Tunnel Details IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.
192.168.20.1/30

IKE 配置

1. 导航至IKE选项卡。您可以选择使用预定义的策略,也可以点击Policy选项卡旁边的铅笔按钮创建 新策略,或者根据需要选择其他可用策略。

0

Cancel

OK



Cancel	OK

2. 选择身份验证类型。如果使用预共享手动密钥,请在Key和Confirm Key框中提供密钥。

Endpo	ints IKE IPsec Ad	vanced				
	IKEv2 Settings					
	Policies:*	AES-GCM-NULL-SHA-LATEST				
	Authentication Type:	Pre-shared Manual Key 🔻]			
	Key:*]			I
	Confirm Key:*)			I
		Enforce hex-based pre-shared key	/ only	-		
						▼
					Cancel Save	

IPSec 配置

导航到IPsec选项卡。您可以点击proposal(建议)选项卡旁边的铅笔按钮选择使用预定义的建议创 建新建议,也可以根据需要选择另一个可用建议。

Endpoints	IKE IPsec	IPsec Advanced			
	IKEV2 Mode:	Tunnel	v		
	Transform Sets:	IKEv1 IPsec Proposals 💉	IKEv2 IPsec Proposals* 🖋		
		tunnel_aes256_sha	AES-GCM		
		Enable Security Association	n (SA) Strength Enforcement		
	\checkmark	Enable Reverse Route Injec	tion		
		Enable Perfect Forward Sec	crecy		

路由配置

1. 转至Device > Device Management,并单击铅笔图标编辑设备(FTD)。

Firewall Management Center Overview Analysis Devices / Device Management	Policies	Devices Objects Inte	gration		Deploy Q 💰	Carlos SECURE
View By: Group • All (4) • Error (2) • Warning (0) © Offline (2) • Normal (0) Collspace All • • • • •	 Deployme 	Device Management Device Upgrade NAT QoS	VPN Site To Site Remote Access Dynamic Access Policy	Troubleshoot File Download Threat Defense CLI Packet Tracer		Deployment History Q. Search Device Add
Name ✓ Ungrouped (4)	Model	Platform Settings FlexConfig Certificates	Troubleshooting Site to Site Monitoring	Packet Capture	Access Control Policy	Auto RollBack
Contraction of a stated	FTDv for VMware	7.0.0	N/A	Base, AnyConnect Plus	s (1 more) new_pol	N/A

2. 转至Routing(路由)> Static Route(静态路由),然后单击"+"按钮,将路由添加到主要和辅助 VTI。

注意:您可以配置适当的路由方法,让流量通过隧道接口。在本例中,使用了静态路由。

Device	Routing	Interface	s Inline S	ets DHO	CP				
Manage V	′irtual Ro	outers							+ Add Foute
Global	tor Droport	v	Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
Global Image: Complexity of the second sec		► IPv4 Routes							
OSPF		► IPv6 R	► IPv6 Routes						
OSPFv3									
EIGRP									
RIP									
BGP									
Static Rout	e								
[′] Multicast R	outing								

3. 为受保护网络添加两个路由,并为辅助路由设置更高的AD值(本例中为2)。

第一条 路由使用VTI-1接口,第二条路由使用VTI-2接口。

Network 🔺		Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	
Ŧ	IPv4 Routes						
	protected-network	VTI-1	Global	VTI-1-Gateway	false	1	
	protected-network	VTI-2	Global	VTI-2-Gateway	false	2	

验证

1. 转至Devices > VPN > Site to Site Monitoring。

	Devices	Objects	Integ	ration		
	Device	Management		VPN	Troubleshoot	
	Device	Upgrade		Site To Site	File Download	
	NAT			Remote Access	Threat Defense CLI	: 1
	QoS			Dynamic Access Policy	Packet Tracer	opo
	Platforn	n Settings	_	Troubleshooting	Packet Capture	G
	FlexCor	nfig		Site to Site Monitoring		
_	Certifica	ates				0.1
						ck

2. 单击眼睛查看有关隧道状态的更多详细信息。

	Dual-ISP-VTI	Active	2024-06-11 06:55:26
View ft II information	Dual-ISP-VTI	Active	2024-06-12 14:27:22

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)。