# 由FMC管理的FTD上的站点到站点VPN配置

## 目录

<u>简介</u>

<u>先决条件</u>

<u>要求</u>

<u>使用的组件</u>

#### <u>配置</u>

<u>步骤1:定义VPN拓扑。</u>

<u>第二步:配置IKE参数。</u>

<u> 第三步:配置 IPSec 参数.</u>

<u>第四步:绕过访问控制。</u>

<u>第五步:创建访问控制策略。</u>

<u>第六步:配置NAT免除。</u>

<u>步骤 7.配置ASA。</u>

#### <u>验证</u>

<u>故障排除和调试</u>

<u>初始连接问题</u>

<u>特定流量问题</u>

# 简介

本文档介绍如何在FMC管理的Firepower威胁防御(FTD)上配置站点到站点VPN。

# 先决条件

#### 要求

您应该了解以下主题:

- 对VPN的基本了解
- 使用Firepower管理中心的经验
- 使用ASA命令行体验

## 使用的组件

本文档中的信息基于以下软件和硬件版本:

- 思科FTD 6.5
- ASA 9.10(1)32
- IKEv2

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。

## 配置

首先在FTD上配置FirePower管理中心。

步骤1:定义VPN拓扑。

1.导航到设备> VPN >站点到站点。 在Add VPN下,点击Firepower Threat Defense Device,如下图 所示。



2.出现Create New VPN Topology(创建新VPN拓扑)框。为VPN提供一个易于识别的名称。

网络拓扑: 点对点

IKE版本:IKEv2

在本示例中,当您选择终端时,节点A是FTD,节点B是ASA。单击绿色的加号按钮将设备添加到拓 扑中,如图所示。

Create New VI	Create New VPN Topology ?					? ×
Topology Name:	* BTPVF	PN-ASA		]		
Network Topolog	y: ⊷ p	oint to Point 😽 Hub	and Spoke 🔶 Full	Mesh		
IKE Version:*	IKE	v1 🗹 IKEv2				
Endpoints	IKE	IPsec	Advanced			
Node A:						
Device Name		VPN Interface	e	Protected Network	s	
						-
Node B:						0
Device Name		VPN Interface	2	Protected Network	s	
						-
• Ensure the pro	otected network	s are allowed by acce	ess control policy o	f each device.		
					Save	Cancel

3.添加FTD作为第一个终端。

选择放置加密映射的接口。IP地址应该从设备配置中自动填充。

点击Protected Networks下的绿色加号(如图所示),选择此VPN中应加密哪些子网。

# Add Endpoint

Device:*	FTD	~
Interface:*	outside	~
IP Address:*	172.16.100.20	~
	This IP is Private	
Connection Type:	Bidirectional	~
Certificate Map:	<b>~</b>	٢
Protected Networks:*		
Subnet / IP Address (Net)	work) O Access List (Extended)	0
		_
	OK Cancel	

5.添加需要加密的FTD的所有本地子网。单击Add将其移动到Selected Networks。现在单击OK,如 图所示。

? ×

6

#### FTDSubnet = 10.10.113.0/24

Network Objects		
Available Networks 🖒	٩	Selected Networks
🔍 ftd	×	FTDSubnet
FTDSubnet		
	Add	J
		OK Cancel

节点A:(FTD)终端已完成。如图所示,点击节点B的绿色加号。

Create New VPN Topology ?						? ×				
Topology Name:	8	RTPVPN-	ASA							
Network Topolog	y:	++ Poin	t to Point	₩ Hub	and Spoke	💠 Full Mes	sh			
IKE Version:*		IKEv1	✓ IKEv2							
Endpoints	IKE		IPsec		Advanced	1				
Node A:										٢
Device Name			VPN In	terface			Protected Networks			
FTD			outside/	172.16.	100.20		FTDSubnet		🥜 🗓	* *
Node B:										
Device Name			VPN I	nterface	a		Protected Networks			
Ensure the protected networks are allowed by access control policy of each device										
and and and pro-	- leaved in			-,						
								Save	Canc	el

节点B是ASA。不受FMC管理的设备被视为外联网设备。

6.添加设备名称和IP地址。单击绿色加号以添加受保护的网络,如图所示。

# Edit Endpoint

Device:*	Extranet	~
Device Name:*	ASA	
IP Address:*	🖲 Static 🔍 Dynamic	
	192.168.200.10	
Certificate Map:	<b>~</b>	0
Protected Networks:*		
Subnet / IP Address (Net)	work) O Access List (Extended)	
		0
	OK Cancel	

7.如本图所示,选择需要加密的ASA子网,然后将其添加到所选网络。

### ASA子网= 10.10.110.0/24

Network Object	ts			? ×
Available Networks	Ċ (	D	Selected Networks	
🔍 ASAS	3	<	🚍 ASASubnet	5
ASASubnet				
		Add		
			ОК	Cancel

## 第二步:配置IKE参数。

现在,两个终端都已通过IKE/IPSEC配置。

1.在IKE选项卡下,指定用于IKEv2初始交换的参数。单击绿色加号可创建新的IKE策略,如图所示 。

Create	New	VPN	Topo	logy
--------	-----	-----	------	------

Topology Name:*	RTPVPN-ASA			
Network Topology:	↔ Point to Point 😽 Hu	b and Spoke 💠 Full Mesh		
IKE Version:*	🗌 IKEv1 🗷 IKEv2			
Endpoints IKE	IPsec	Advanced		
IKEv1 Settings				
Policy:*	preshared_sha_aes256_dh5_	_5 🗸 🔾		
Authentication Type:	Pre-shared Automatic Key	~		
Pre-shared Key Length:*	24 Characters	(Range 1-127)		
IKEv2 Settings				
Policy:*	AES-GCM-NULL-SHA	× 🔘		
Authentication Type:	Pre-shared Automatic Key	*		
Pre-shared Key Length:*	24 Characters	(Range 1-127)		
			Save Cancel	

2.在新的IKE策略中,指定连接的优先级编号和阶段1的生存期。本文档在初始交换中使用以下参数 :完整性(SHA256)、加密(AES-256)、PRF(SHA256)和Diffie-Hellman组(组14)

注意:无论所选策略部分中的内容如何,设备上的所有IKE策略都将发送到远程对等体。为 VPN连接选择与远程对等项匹配的第一个IKE策略。使用优先级字段选择首先发送的策略。优 先级1将首先发送。

Name:*	ASA	]		
Description:		]		
Priority:	1	(1-65535)		
Lifetime:	86400	seconds (120-214	47483647)	
Integrity Algorithms Encryption Algorithms PRF Algorithms Diffie-Hellman Group	Available Algorithms MD5 SHA SHA512 SHA256 SHA384 NULL	Add	elected Algorithn	ns
			Save	Cancel

Name:*	ASA	]		
Description:				
Priority:	1	(1-65535)		
Lifetime:	86400	seconds (120-2	2147483647)	
Integrity Algorithms	Available Algorithms		Selected Algorit	hms
PRF Algorithms Diffie-Hellman Group	AES-256 AES-256 AES-256 AES-192 AES-192 AES-GCM AES-GCM-192 AES-GCM-256 NULL	Add	🔅 AES-256	
		ſ	Save	Cancel

Name:* Description:	ASA	]		
Priority: Lifetime:	1 86400	(1-65535) seconds (120-2	2147483647)	
Integrity Algorithms Encryption Algorithms PRF Algorithms Diffie-Hellman Group	Available Algorithms MD5 SHA SHA512 SHA256 SHA384	Add	Selected Algorit	hms
		ĺ	Save	Cancel

Name:*	ASA	]	
Description:		]	
Priority:	1	(1-65535)	
Lifetime:	86400	seconds (120-2147483647)	
Integrity Algorithms	Available Groups	Selected Group	)S
PRF Algorithms Diffie-Hellman Group	Image: 1       ▲         Image: 2       Image: 5         Image: 14       Image: 15         Image: 16       Image: 16	Add	
		Save	Cancel

#### 3.添加参数后,选择此策略,然后选择验证类型。

4.选择pre-shared-key manual。本文档使用PSK cisco123。

Create New VPN Topol	ogy		? ×
Topology Name:*	RTPVPN-ASA		]
Network Topology:	↔ Point to Point 🛠 H	ub and Spoke 💠 Fu	ll Mesh
IKE Version:*	□ IKEv1 IKEv2		
Endpoints IKE	IPsec	Advanced	
IKEv1 Settings			
Policy:*	preshared_sha_aes256_dh	5_5 💙 🔾	
Authentication Type:	Pre-shared Automatic Key	Y	
Pre-shared Key Length:*	24 Characters	(Range 1-127)	
IKEv2 Settings			
Policy:*	ASA	¥ ()	
Authentication Type:	Pre-shared Manual Key	~	
Key:*	•••••		
Confirm Key:*	•••••		
	Enforce hex-based pre-s	hared key only	
			Save Cancel

# 第三步:配置 IPSec 参数.

1.在IPsec下,单击铅笔编辑转换集并创建新的IPsec提议,如下图所示。

Create New VPN	Topology	3	×
Topology Name:*	RTPVPN-ASA		
Network Topology:	++ Point to Point	* Hub and Spoke 💠 Full Mesh	
IKE Version:*	IKEv1 IKEv2		
Endpoints II	KE IPsec	Advanced	
Crypto Map Type:	Static      Dynamic		
IKEv2 Mode:	Tunnel		
Transform Sets:	IKEv1 IPsec Proposals 🥜	IKEv2 IPsec Proposals* 🥜	
	tunnel_aes256_sha	AES-GCM	
Enable Security As	sociation (SA) Strength Enfor	cement	
🗹 Enable Reverse Rou	ute Injection		
Enable Perfect Forv	vard Secrecy		
Modulus Group:	14 💙		
Lifetime Duration*:	28800	Seconds (Range 120-2147483647)	
Lifetime Size:	4608000	Kbytes (Range 10-2147483647)	
- ESPv3 Settings	;		_
		Save Cancel	

2.要创建新的IKEv2 IPsec提议,请单击绿色加号并输入阶段2参数。

选择ESP Encryption > AES-GCM-256。使用GCM算法加密时,不需要散列算法。使用GCM时,哈希函数是内置的。

## Edit IKEv2 IPsec Proposal

Name:*	ASA	
Description:		
ESP Hash	Available Algorithms	Selected Algorithms
ESP Encryption	AES-GCM-256 AES-256 AES-GCM-192 AES-192 AES-GCM AES DES AES-GMAC-25	Add
		Save Cancel

## 3.创建新的IPsec方案后,将其添加到选定的转换集。

IKEv2 IPsec Proposal				? ×
Available Transform Sets 🖒 💿		Selected Transfor	m Sets	
🔍 Search		ASA		ï
MAES-GCM				
AES-SHA				
ASA				
@ DES_SHA-1	Add			
			ОК	Cancel

新选择的IPsec建议现在列在IKEv2 IPsec建议下。

如果需要,可在此处编辑阶段2的有效期和PFS。在本例中,生命周期将被设置为默认值,PFS将被 禁用。

Create New VPN	Topology	? X
Topology Name:*	RTPVPN-ASA	
Network Topology:	Point to Point	
IKE Version:*	□ IKEv1  IKEv2	
Endpoints I	KE IPsec Advanced	
Crypto Map Type: IKEv2 Mode: Transform Sets:	<ul> <li>Static</li> <li>Dynamic</li> <li>Tunnel</li> <li>IKEv1 IPsec Proposals</li> <li>IKEv2 IPsec Proposals*</li> <li>IKEv2 IPsec Proposals</li> </ul>	
<ul> <li>Enable Security Ast</li> <li>Enable Reverse Rot</li> <li>Enable Perfect Forv Modulus Group:</li> <li>Lifetime Duration*:</li> <li>Lifetime Size:</li> <li>ESPv3 Setting:</li> </ul>	sociation (SA) Strength Enforcement ute Injection ward Secrecy 14 28800 Seconds (Range 120-2147483647) 4608000 Kbytes (Range 10-2147483647) s	
	Save Cano	el

可选 — 必须完成旁路访问控制选项或创建访问控制策略。

第四步:绕过访问控制。

或者,可以在Advanced > Tunnel下启用sysopt permit-vpn。

这消除了使用访问控制策略检查来自用户的流量的可能性。VPN过滤器或可下载ACL仍可用于过滤 用户流量。 这是全局命令,如果启用此复选框,该命令将应用于所有VPN。

Topology Name:* RTPVPN-ASA   Network Topology: Point to Point * Hub and Spoke * Full Mesh   IKE IKE Version:*   IKE IPsec   Advanced     IKE   IPsec   INAT Settings   Tunnel     Keepalive Messages Traversal   Interval:   20   Seconds   (Range 10 - 3600)     Access Control for VPN Traffic   Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)   Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN traffic.   Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN traffic.   Output:   Output:   Output:   Decrypted traffic (sysopt permit-vpn)   Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN traffic.   Output:	Create New VP	N Topology							? ×
Network Topology: <ul> <li>Point to Point</li> <li>Hub and Spoke</li> <li>Full Mesh</li> <li>IKE</li> <li>IKE IPsec</li> <li>IKE</li> <li>INAT Settings</li> <li>Keepalive Messages Traversal</li> <li>Interval:</li> <li>20</li> <li>Seconds (Range 10 - 3600)</li> <li>Access Control for VPN Traffic</li> <li>Ø Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)</li> <li>Decrypted Taffic is subjected to Access Control Policy by default. This ophion bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.</li> <li>Cettificate Map Settings</li> <li>Use the certificate OU field to determine the tunnel</li> <li>Ø Use the IKE identity to determine the tunnel</li> <li>Ø Use the per IP address to determine the tunnel</li> <li>Ø Use the per IP address to determine the tunnel</li> <li>Ø Use the per IP address to determine the tunnel</li> <li>Ø Use the per IP address to determine the tunnel</li> <li>Ø Use the per IP address to determine the tunnel</li> <li>Ø Use the per IP address to determine the tunnel</li> <li>Ø Use the per IP address to determine the tunnel</li> <li>Ø Use the per IP address to determine the tunnel</li> <li>Ø Use the per IP address to determine the tunnel</li> <li>Ø Use the per IP address to determine the tunnel</li> <li>Ø Use the per IP address to determine the tunnel</li> <li>Ø Use the per IP address to determine the tunnel</li> <li>Ø Use the per IP address to determine the tunnel</li> <li>Ø Use the per IP address to determine the tunnel</li> <li>Ø Use the per IP address to determine the tunnel</li> <li>Ø Use the per IP address to determine the tunnel</li> <li>Ø Use the per IP address to determine the tunnel</li> <li>Ø Use the per IP address to determine the</li></ul>	Topology Name:*	RTPVPN	ASA						
IKE Version:*       IKEv1 IKEv2         Endpoints       IKE       IPsec         IKE       IPsec       NAT Settings         Tunnel       Interval:       20         Seconds       (Range 10 - 3600)         Access Control for VPN Traffic       Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)         Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.         Certificate Map Settings       Use the certificate map configured in the Endpoints to determine the tunnel         Use the cificate OU field to determine the tunnel       Use the peer IP address to determine the tunnel         Use the peer IP address to determine the tunnel       Use the peer IP address to determine the tunnel	Network Topology	r: ⊷ Poir	it to Point	✤ Hub and Spoke	💠 Full Mes	h			
Endpoints       IKE       IPsec       Advanced         IKE       INAT Settings       Interval:       Interval:       Interval:       Seconds       (Range 10 - 3600)         Interval:       20       Seconds       (Range 10 - 3600)         Access Control for VPN Traffic       Bypass Access Control policy for decrypted traffic (sysopt permit-vpn) Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.         Certificate Map Settings       Use the certificate map configured in the Endpoints to determine the tunnel         I Use the certificate OU field to determine the tunnel       Use the IKE identity to determine the tunnel         I Use the peer IP address to determine the tunnel       Use the peer IP address to determine the tunnel	IKE Version:*	IKEv1	✓ IKEv2						
IKE       NAT Settings         Tunnel	Endpoints	IKE	IPsec	Advance	d				
	IKE IPsec Tunnel	NAT Settings Keepalive Interval: Access Control f Bypass Ac Decrypted but VPN F Certificate Map S Use the co Use the co Use the file Use the p	Messages Tr 20 or VPN Traffi cess Control l traffic is sub ilter ACL and Settings ertificate maj ertificate OU (E identity to eer IP addres	raversal S fic I policy for decrypted bjected to Access Control I authorization ACL dow p configured in the Er I field to determine the Er I field to determine the tunne iss to determine the tunne	econds (f traffic (sysop of Policy by de nloaded from idpoints to d tunnel innel	Range 10 - 3 ot permit-vp efault. This of AAA server a etermine the	n) ption bypasses are still applied	s the inspection, d to VPN traffic.	

如果未启用sysopt permit-vpn,则必须创建访问控制策略,以允许VPN流量通过FTD设备。如果 sysopt permit-vpn已启用,请跳过创建访问控制策略。

#### 第五步:创建访问控制策略。

在Access Control Policies下,导航到Policies > Access Control > Access Control,并选择针对 FTD设备的策略。要添加规则,请点击Add Rule,如图所示。

必须允许流量从内部网络传出到外部网络,以及从外部网络传到内部网络。创建一个规则以同时执 行这两个操作,或创建两个规则以将其分开。在本例中,创建一条规则来同时执行这两个操作。

Editing F	Rule - VP	N_Traffic
-----------	-----------	-----------

Name	VPN_Tra	ffic				🗹 Enabl	led		Mc	we							
Action	🖋 Allo	v			- 00.a	ù 8											
Zone	es Ne	tworks	VLAN Tags	🛆 Users	Applications	s Ports	URLs	SGT/I	ISE Attr	ibutes			1	Inspectio	on Logging	Comme	ents
Availab	le Netwo	rks C		0		Source N	Networks	(2)				Des	tinatio	n Netwo	rks (2)		
🔍 sub	net			×			Source		Orig	inal Clie	nt		ASASul	bnet			
	Network	5	Geolocat	on		R ASAS	Subnet				6	-	FTDSul	bnet			6
ASA	Subnet					FTDS	Subnet				8						
FTD	Subnet				Add To Source	1											
					Networks												
				1	Add to	1											
					Destination	1											
						Enter an	IP addres	15			Add	Ent	er an Ii	P address			Add
														6	Saure	Cance	
															Save	Cance	
Rules	Security I	Intelligence	HTTP Respon	ses Logging	Advanced												
曲 Filter b	y Device						🗌 🗆 Shor	w Rule Co	nflicts 🥹	0 A	Add Catego	ory	🔾 Add I	Rule 👳	Search Rules		×
ø Name	e	Source Z	on Dest Zon	es Sourc	e Networks De	est Networks	• VL	Us	Ap	So	De	URLs	50	De	• v 🔊 y		٢
👻 Manda	tory - FTC	Access-Cor	trol-Policy (1-1	)													
1 VPN_T	raffic	슈 Inside 슈 Outside	A Inside		54Subnet g	ASASubnet FTDSubnet	Any	Any	Any	Any	Any	Any	Any	Any	🗸 ANG 🖏 J	2 1	/ 6
👻 Defaul	lt - FTD-A	cess-Contro	I-Policy (-)														
There are i	no rules in	this section.	ldd Rule or Add C	itegory													
Default A	ction										Access O	ontrol: B	lock All 1	Traffic			× 1

## 第六步:配置NAT免除。

为VPN流量配置NAT免除语句。必须实施NAT免除,以防止VPN流量到达另一个NAT语句并错误地 转换VPN流量。

1.导航到设备> NAT,选择以FTD为目标的NAT策略。 点击Add Rule按钮时创建新规则。

Over	iew Analysis Nanagement	Policies NAT V	Devices Object	ts AMP Intellige atform Settings File	nce xCanfig Certificates					Deploy 🔍	System Help	r admin≁
Virt	alFTDNAT									A Show Warning	B E Save	Cancel
Rules	econgtren										🛃 Pole	y Assignments (1)
A rise	by Denvice										4	Add Rule
						Original Packet			Translated Packet		_	
•	Direction	Туре	Source Interface Objects	Destination Interface Objects	Oviginal Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options	
• ME	ules before											
♥ Auto	NAT Rules											

2.创建新的静态手动NAT规则。参考内部和外部接口。

#### Edit NAT Rule

NAT Rule: Type:	Manual NAT Rul Static	e ▼ ▼   € Ena	Insert: ble	In Category	NAT Rules Before	
Description: Interface Objects	Translation	PAT Pool Advar	nced			
Available Interface Obj	ects C		Source Interface Obje	ects (1)	Destination Interface Objects	(1)
୍କ୍ତ Inside ଲି Outside		Add to Source Add to Destination	inside	Ö	Dutside	

3.在转换选项卡下,选择源子网和目标子网。由于这是NAT免除规则,请使原始源/目标与转换后的 源/目标相同,如下图所示:

Add NAT Rule													? >
NAT Rule:	Manual NAT Rule	•	Ins	ert:			In Category	*	NAT Rules	Before	•		
Type:	Static	~	🗹 Enable										
Description:													
Interface Objects	ranslation	PAT Pool	Advanced										
Original Packet					7	- Translate	d Packet						
Original Source:"	FTDSubnet			× 0		Translated	Source:	Addr	ess			~	
Original Destination:	Address			~				FTDS	ubnet			~	٢
	ASASubnet			<b>~</b> O		Translated	Destination:	ASAS	Subnet			~	0
Original Source Port:				× 0		Translated	Source Port:					~	0
Original Destination Po	rt:			<b>~</b> O		Translated	Destination Port	t:				~	0
										0	< ) [	Cano	el

4.最后,转到Advanced选项卡并启用无代理arp和路由查找。

#### Add NAT Rule

12	Manual NAT	Rule 💙	Insert:	In Category	~	NAT Rules Before	~
	Static	~	Enable				
cription:							
terface Objects	Translation	PAT Pool	Advanced				
anslate DNS repli	es that match th	is rule					
allthrough to Inter	face PAT(Destina	ation Interface	:)				
<sup>1</sup> V6							
et to Net Mapping							
o not proxy ARP o	n Destination In	terface					
erform Route Look	up for Destination	on Interface					
Unidirectional							
						0	ĸ

#### 5.保存此规则并在NAT列表中查看最终结果。

(	Overview Ar	alysis Po	licies Devi	ces Object	s AMP Inte	elligence				Deploy	System	Help v	admin 🕯
C	Device Manager	nent NA	T VPN •	QoS Pk	atform Settings	FlexConfig	Certificates						
N	VirtualFTDNAT												
R	Rules												
63	Filter by Device											0	Add Rule
						Original Pac	ket			anslated Packet			
#	Direction	Туре	Source Interface	Destination Interface	Original Sources	Original Destinatio	Origin ons Servic	al es	Translated Sources	Translated Destinations	Translated Services	Options	
<ul> <li>NAT Rules Before</li> </ul>													
1	*	Static	🚠 Inside	🚠 Outside	💂 FTDSubnet	💂 ASASut	met		🚍 FTDSubnet	🚔 ASASubnet		Ons:fa Coute-l Cout	/ 8
٠	▼ Auto NAT Rules												
"	+	Dynamic	🚠 Inside	🚠 Outside	👳 any-obj			1	🝓 Interface			🍓 Dns:fa	/0
•	NAT Rules After												

6.完成配置后,保存配置并将其部署到FTD。

步骤 7.配置ASA。

1. 在ASA的外部接口上启用IKEv2:

Crypto ikev2 enable outside

2.创建定义在FTD上配置的相同参数的IKEv2策略:

Encryption aes-256 Integrity sha256 Group 14 Prf sha256 Lifetime seconds 86400

3.创建允许ikev2协议的组策略:

Group-policy FTD\_GP internal Group-policy FTD\_GP attributes Vpn-tunnel-protocol ikev2

4.创建对等FTD公有IP地址的隧道组。引用组策略并指定预共享密钥:

Tunnel-group 172.16.100.20 type ipsec-121
Tunnel-group 172.16.100.20 general-attributes
Default-group-policy FTD\_GP
Tunnel-group 172.16.100.20 ipsec-attributes
 ikev2 local-authentication pre-shared-key cisco123
 ikev2 remote-authentication pre-shared-key cisco123

5.创建定义要加密的流量的访问列表: (FTDSubnet 10.10.113.0/24)(ASASubnet 10.10.110.0/24)

Object network FTDSubnet Subnet 10.10.113.0 255.255.255.0 Object network ASASubnet Subnet 10.10.110.0 255.255.255.0 Access-list ASAtoFTD extended permit ip object ASASubnet object FTDSubnet

6.创建一个引用FTD上指定的算法的ikev2 ipsec-proposal:

Crypto ipsec ikev2 ipsec-proposal FTD Protocol esp encryption aes-gcm-256

7.创建将配置关联在一起的加密映射条目:

Crypto map outside\_map 10 set peer 172.16.100.20 Crypto map outside\_map 10 match address ASAtoFTD Crypto map outside\_map 10 set ikev2 ipsec-proposal FTD Crypto map outside\_map 10 interface outside 8.创建NAT免除语句,阻止防火墙NAT传输VPN流量:

Nat (inside,outside) 1 source static ASASubnet ASASubnet destination static FTDSubnet FTDSubnet no-

#### 验证

#### ≫ 注:此时无法从FMC查看VPN隧道状态。此功能<u>CSCvh77603</u>有一个增强请求。

尝试通过VPN隧道发起流量。通过访问ASA或FTD的命令行,可以使用packet tracer命令完成此操作。使用packet-tracer命令启动VPN隧道时,必须运行两次以验证隧道是否启动。首次发出该命令时,VPN隧道关闭,因此packet-tracer命令在VPN加密DROP时将会失败。请勿将防火墙的内部 IP地址用作Packet Tracer中的源IP地址,因为此操作始终会失败。

firepower# packet-tracer input inside icmp 10.10.113.10 8 0 10.10.110.10 Phase: 10 Type: VPN Subtype: encrypt Result: DROP Config: Additional Information: firepower# packet-tracer input inside icmp 10.10.113.10 8 0 10.10.110.10 Phase: 1 Type: ROUTE-LOOKUP Subtype: Resolve Egress Interface Result: ALLOW Config: Additional Information: found next-hop 172.16.100.1 using egress ifc outside Phase: 2 Type: UN-NAT Subtype: static Result: ALLOW Config: nat (Inside, outside) source static FTDSubnet FTDSubnet destination static ASASubnet ASASubnet no-proxy-Additional Information: NAT divert to egress interface outside Untranslate 10.10.110.10/0 to 10.10.110.10/0 Phase: 3 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group CSM\_FW\_ACL\_ global access-list CSM\_FW\_ACL\_ advanced permit ip ifc Inside object-group FMC\_INLINE\_src\_rule\_268436483 ifc ou access-list CSM\_FW\_ACL\_ remark rule-id 268436483: ACCESS POLICY: FTD-Access-Control-Policy - Mandatory access-list CSM\_FW\_ACL\_ remark rule-id 268436483: L7 RULE: VPN\_Traffic object-group network FMC\_INLINE\_src\_rule\_268436483 description: Auto Generated by FMC from src of UnifiedNGFWRule# 1 (FTD-Access-Control-Policy/mandatory) network-object object ASASubnet network-object object FTDSubnet object-group network FMC\_INLINE\_dst\_rule\_268436483 description: Auto Generated by FMC from dst of UnifiedNGFWRule# 1 (FTD-Access-Control-Policy/mandatory) network-object object ASASubnet network-object object FTDSubnet Additional Information: This packet will be sent to snort for additional processing where a verdict will be reached Phase: 5 Type: NAT Subtype: Result: ALLOW Config: nat (Inside, outside) source static FTDSubnet FTDSubnet destination static ASASubnet ASASubnet no-proxy-Additional Information: Static translate 10.10.113.10/0 to 10.10.113.10/0 Phase: 10 Type: VPN Subtype: encrypt Result: ALLOW Config: Additional Information: Result: input-interface: Inside input-status: up input-line-status: up output-interface: outside output-status: up output-line-status: up Action: allow 要监控隧道状态,请导航到FTD或ASA的CLI。 在FTD CLI中,使用以下命令验证第1阶段和第2阶段: Show crypto ikev2 sa <#root> > show crypto ikev2 sa IKEv2 SAs: Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local 9528731 172.16.100.20/500 Remote 192.168.200.10/500

#### READY

INITIATOR

Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK Life/Active Time: 86400/118 sec Child sa: local selector

10.10.113.0/0 - 10.10.113.255/65535

remote selector

10.10.110.0/0 - 10.10.110.255/65535

ESP spi in/out:

0x66be357d/0xb74c8753

## 故障排除和调试

初始连接问题

构建VPN时,需要双方协商隧道。因此,当您排除任何类型的隧道故障时,最好让对话双方都参与 进来。 有关如何调试IKEv2隧道的详细指南位于:<u>如何调试IKEv2 VPN</u>

隧道故障的最常见原因是连接问题。确定这一点的最佳方法是在设备上捕获数据包。 使用此命令获 取设备上的数据包捕获:

Capture capout interface outside match ip host 172.16.100.20 host 192.168.200.10

捕获到位后,尝试通过VPN发送流量并检查数据包捕获中的双向流量。

#### 使用以下命令检查数据包捕获:

show cap capout

firepower# show cap capout

4 packets captured

1: 11:51:12.059628	172.16.100.20.500 > 192.168.200.10.500:	udp 690
2: 11:51:12.065243	192.168.200.10.500 > 172.16.100.20.500:	udp 619
3: 11:51:12.066692	172.16.100.20.500 > 192.168.200.10.500:	udp 288
4: 11:51:12.069835	192.168.200.10.500 > 172.16.100.20.500:	udp 240

#### 特定流量问题

您遇到的常见流量问题包括:

- FTD后的路由问题 内部网络无法将数据包路由回分配的IP地址和VPN客户端。
- 访问控制列表阻止流量。
- VPN流量未绕过网络地址转换。

有关FMC管理的FTD上的VPN的详细信息,您可以在此处找到完整配置指南:<u>FMC管理的FTD配置</u> <u>指南</u>

#### 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)。