在FDM管理的FTD上配置VRF感知路由的站点到 站点VPN

目录			
<u>简介</u>			
<u>先决条件</u>			
<u>要求</u>			
<u>使用的组件</u>			
<u>背景信息</u>			
<u>配置</u>			
<u>网络图</u>			
<u>配置FTD</u>			
<u>配置 ASA</u>			
<u>验证</u>			
<u>故障排除</u>			
<u>参考</u>			

简介

本文档介绍如何在FDM管理的FTD上配置VRF感知路由的站点到站点VPN。

先决条件

要求

Cisco 建议您了解以下主题:

- 对VPN的基本了解
- 基本了解虚拟路由和转发(VRF)
- 使用FDM的经验

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FTDv版本7.4.2
- 思科FDM版本7.4.2
- 思科ASAv版本9.20.3

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

通过Firepower设备管理器(FDM)上的虚拟路由和转发(VRF),您可以在单个Firepower威胁防御 (FTD)设备上创建多个隔离路由实例。每个VRF实例都作为单独的虚拟路由器运行,具有自己的路 由表,从而实现网络流量的逻辑分离,并提供增强的安全性和流量管理功能。

本文档说明如何使用VTI配置VRF感知IPSec VPN。VRF红色网络和VRF蓝色网络位于FTD之后。 VRF红色网络中的Client1和VRF蓝色中的Client2将通过IPSec VPN隧道与ASA后面的客户端3通信 。

配置

网络图



拓扑

配置FTD

步骤1.必须确保节点间的IP互联初步配置已经适当完成。Client1和Client2使用FTD内部IP地址作为 网关。 Client3使用ASA内部IP地址作为网关。

步骤2.创建虚拟隧道接口。登录FTD的FDM GUI。导航到设备>接口。单击View All Interfaces。

Firewall Device Manager Monitoring Policies Obje	ets Device: ftdv742 Software VDB Intrusion Rule at Defense for KVM 7.4.2-172 376.0 20231011-1	Update Cloud Services High Aveilability Sta Connected fangni Not Configure	admin Administrator CISCO SECURE
trad	OZ Cisco Firepower Threat Defense for KVM 0/0 0/1 0/2 0/4 0/5 0/6 Image: Cisco Firepower Threat Defense for KVM Image: Cisco Firepower Threat Defense for KVM		Internet DNS Server YTP Server Smart Lice
Interfaces Management: Merged () Enabled 4 of 9 View All Interfaces	Routing 6 static routes View Configuration >	Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration	System Settings Management Access Logging Settings DHCP Servier / Relay DDNS Service DNS Service

FTD_View_Interfaces

步骤2.1.单击Virtual Tunnel Interfaces选项卡。单击+按钮。

Firewall Device Mana	iger Monitoring	Policies	証 Objects	Device: ftdv742	\odot		?	:	admin Administrator	~	cisco SECURE
	Device Summary Interfaces										
	Cisco Firepower Threat D 0/0 0/1 0/2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	0/3 0/4 0/5	0/6 0/7								
	Interfaces Virtual Tu	nnel Interfaces)								
:	2 tunnels					▼ Fi	ter				+

FTD_Create_VTI

步骤2.2.提供必要信息。单击OK按钮。

- 名称 : demovti
- 隧道ID:1
- 通道来源:外部(GigabitEthernet0/0)
- IP 地址和子网掩码:169.254.10.1/24
- 状态:单击滑块到"已启用"位置

Name demovti	atus
Most features work with named interfaces only, although some require unnamed interfaces. Description	
	h
Tunnel ID Tunnel Source 1 outside (GigabitEthernet0/0)	
IP Address and Subnet Mask	
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0	

CANCEL

FTD_Create_VTI_Details

步骤3.导航到Device > Site-to-Site VPN。单击View Configuration按钮。

Firewall Device Manager	Monitoring Policies Obje	E Devic	e: ftdv742			?) : admin Administrator ~ "livili" SECURE
	Model Cisco Firep	oower Threat De	Software VDB fense for KVM 7.4.2-172 376.0	Intrusion Ru 20231011-	ale Update Cloud Services High Av 1536 ▲ Issues Unknown Not Cor	allability 🕢 CONFIGURE
		C Inside Netwo	Cisco Firspower Threat Defense Q10 Q/1 Q/2 Q/3 Q10 Q/1 Q/2 Q/3	o for KVM () 0/4 0/5 0/6	0/7 CONSOLE	Child Server
	Interfaces		Routing		Updates	System Settings
						Management Assess
	Management: Merged () Enabled 4 of 9 View All Interfaces	>	1 static route View Configuration	>	Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration	Management Access Logging Settings DHCP Server / Relay DDNS Service
	Management: Merged (*) Enabled 4 of 9 View All Interfaces Smart License Registered Ter: FTDx50 - 10 Gbps	>	1 static route View Configuration Backup and Restore	>	Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration > Troubleshoot No files created yet	Management Access Logging Settings DHCP Server / Relay DDNS Service DNS Server Hostname Time Services SSL Settings
	Management: Merged (*) Enabled 4 of 9 View All Interfaces Smart License Registered Tier: FTDv50 - 10 Gbps View Configuration	>	1 static route View Configuration Backup and Restore View Configuration	>	Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration Troubleshoot No files created yet REQUEST FILE TO BE CREATED	Management Access Logging Settings DHCP Server / Relay DDNS Service DNS Server Hostname Time Services SSL Settings See more
	Management: Merged () Enabled 4 of 9 View All Interfaces Smart License Registered Tier: FTDv50 - 10 Gbps View Configuration Site-to-Site VPN There are no connections yet	> >	1 static route View Configuration Backup and Restore View Configuration Remote Access VPN Requires Secure Client License No connections 1 Group Policy	>	Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration	Management Access Loging Settings DHCP Server / Relay DNS Service DNS Service Not Services SSL Settings See more Device Administration Audit Events, Deployment History, Download Configuration

步骤3.1.开始创建新的站点到站点VPN。单击CREATE SITE-TO-SITE CONNECTION 按钮。或点击+按钮。

Firewall Device Manager	500 Monitoring	Policies	i‡≟ Objects	Device: ftdv742		(Σ)	۲ 🕲 🗎	admin Admin	nistrator V	cisco SEC	CURE
	Device Summa Site-to-S	Site VPN									
							T Filter				+
							Preset filters: Route J	lased (VO), Polic;	.Based		
	# NAME		LOCAL INT	RFACES	LOCAL NETWORKS	REMOTE NETWORKS	NAT EXEMPT				
					There are no Site	-to-Site connections yet.					
					Start by creating the	first Site-to-Site connection.					
					CREATE SITE-	TO-SITE CONNECTION					

FTD_Create_Site2Site_Connection

第 3.2 步: 提供 必要信息。单击NEXT按钮。

- 连接配置文件名称: Demo_S2S
- type:基于路由(VTI)
- 本地VPN访问接口:demovti(在第2步中创建)
- 远程 IP 地址:192.168.40.1 (这是外部IP地址的对等ASA)

New Site-to-site VPN	1 Endpoints	2 Configuration	3 Summary	
Local Network	FTDV742	N TUNNEL	OUTSIDE INTERFACE	Remote Network
Identify the in the loca	nterface on this device, and the remote p al and remote networks that can use the	Define Endpoints beer's interface IP address, that form connection. Traffic between these	n the point-to-point VPN connection. networks is protected using IPsec enc	Then, identify ryption.
(Connection Profile Name Demo_S2S	Type	e Policy Based	
	Sites Configuration	DEMOTE SITE		
(Local VPN Access Interface demovti (Tunnel1)	Remote IP Addre 192.168.40.1	ess	
		CANCEL		

FTD_站点到站点_VPN_终端

第3.3步:导航到IKE Policy。单击EDIT按钮。

Firewall Device Manager Monitoring Poli	Device: ftdv742	() (i) (i) (i) (i) (i) (i) (i) (i) (i) (
New Site-to-site VPN	1 Endpoints 2 Configuration	3 Summary
C Local Network	VPN TUNNEL FTDV742	OUTSIDE 123.1.1 I III PEER ENDPOINT
Select the	Privacy Configuration Internet Key Exchange (IKE) policy and enter the preshared keys needed to IPsec proposals to use for encrypting tra	authenticate the VPN connection. Then, select the offic.
	IKE Policy IKE policies are global, you cannot configure different policies per VPN. Any ena connections.	ibled IKE Policies are available to all VPN
	IKE VERSION 2	
	IKE Policy Globally applied EDIT	
	IPSec Proposal None selected EDIT	

FTD_Edit_IKE_Policy

第 3.4 步: 对于IKE策略,可以使用预定义,也可以通过单击创建一个新策略 创建新的IKE策略. 在本示例中,切换现有IKE策略名称AES-SHA-SHA。单击OK按钮保存。



Create New IKE Policy

FTD_Enable_IKE_Policy

步骤3.5.导航至IPSec建议书。单击EDIT按钮。

þ	Firewall Device Manager	Monitoring	Ø Policies	註 Objects	Device: ftdv742	_		e admin e Administrator ✓	cisco SECURE
	New Site-to-	site VPN	(1 Endpoints		2 Configuration	3 Summary		
		C Local Netwo	rk	FTDV742	VPN TI	INTERNET	OUTSIDE 123.1.1.1 PEER ENDPOINT	Remote Network	
		Sele	ect the Interne	rt Key Exchange	Pr (IKE) policy and ente IPsec pr	ivacy Configura r the preshared keys need oposals to use for encrypt	tion ed to authenticate the VPN connection. ing traffic.	Then, select the	
			IKE I	Policy IKE policies are glo connections.	bal, you cannot configu	re different policies per VPN. /	any enabled IKE Policies are available to all VPI	N	
			IKE VE IKE Pi Globa IPSec None	ERSION 2	EDIT	IKE VERSIC	N 1 ()		

FTD_Edit_IPSec_Proposal

第3.6步:对于IPSec提议,您可以使用预定义,也可以通过点击创建新IPSec提议来创建一个新 IPSec提议。

在本示例中,切换现有IPSec建议名称AES-SHA。点击 确定 按钮进行保存。

Select IPSec Proposals

	+		
	Y Filter	SET DEFAULT	
	AES-GCM in Default Set	0	^
	🥪 🐴 AES-SHA	0	
yo	DES-SHA-1	0	✓ olicie:
	Create new IPSec Proposal	CANCEL	

0 X

FTD_Enable_IPSec_Proposal

步骤3.7.向下滚动页面并配置预共享密钥。单击NEXT按钮。

请记下此预共享密钥,稍后在ASA上配置它。

1	Firewall Device Manager	Monitoring	Policies	objects	Device: ftdv742		(Σ_{-})		(2)) :	admin Administrator	~	cisco SEC	UR
				FTDV742		INTERNET		PEE	R ENDPOINT					
		Sel	lect the Intern	et Key Exchange	Pr e (IKE) policy and ente IPsec pr	r the preshared keys nee posals to use for encryp	ded to authentica ting traffic.	ite the VP	N connection	n. Then,	select the			
				Policy IKE policies are g connections.	jlobal, you cannot configu	re different policies per VPN.	Any enabled IKE Po	licies are av	vailable to all V	PN				
			IKE V	ERSION 2		IKE VERSI	ION 1							
			IKE I Glob	Policy Dally applied	EDIT									
			IPSe Cust	tom set selected	d EDIT									
			Auth	entication Type Pre-shared Man	nual Key 🔵 Certifi	cate								
			Loca	al Pre-shared Ke	BY .									
			Rem	ote Peer Pre-sh	ared Key									
			10.000	rie kirrhûne		BACK								

FTD_Configure_Pre_Shared_Key

步骤3.8.检查VPN配置。如果需要修改任何内容,请单击BACK按钮。如果一切正常,请单击 FINISH按钮。

nterface	
IKE V2	aes,aes-192,aes-256-sha512,sha384,sha,sha256-sha512,sha384,sha,sha256-21,20,16,15,14
PSec Proposal Authentication Type	Pre-shared Manual Key
IKE V1: DISABLED	l
IKE V1: DISABLED	
IKE V1: DISABLED IPSEC SETTINGS Lifetime Duration	28800 seconds

步骤3.9.创建访问控制规则以允许流量通过FTD。在本示例中,允许所有内容用于演示目的。请根据您的实际需求修改您的策略。

ewall	Device Manager	Monitor	ing Policies	Dbjects	Device: ftdv742			۵ 🖨		adr Ad	min ministrator	cisco SECU
	🕏 Security Po	licies										
	$\square \rightarrow \bigcirc SSL$	Decryptic	on \rightarrow \bigcirc Ide	entity \rightarrow C) Security Intelligence	-> 📀 N	AT $ ightarrow$ Acc	ess Control 🔿	S Intrusion			
1 rule			T Filter				☆' @ +					
			SOURCE			DESTINATION						
	# NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS	APPLICATIONS	URLS	USERS	ACTION
	> 1 Demo_allow	Allow	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	¶ C₀

FTD_ACP_示例

第3.10步。(可选)如果为客户端访问互联网配置了动态NAT,请为FTD上的客户端流量配置 NAT豁免规则。在本示例中,无需配置NAT免除规则,因为FTD上未配置动态NAT。

FTD_Review_VPN_Configuration

步骤3.11.部署配置更改。

	þ	Firewall Device Manager	Monitoring	Ø Policies	Objects	Device: ftdv742			?	:	admin Administrator	cisco	SECURE
--	---	-------------------------	------------	---------------	---------	-----------------	--	--	---	---	------------------------	-------	--------

FTD_Deployment_Changes

步骤4.配置虚拟路由器。

步骤4.1.为静态路由创建网络对象。导航到对象>网络,单击+按钮。

Firewall Device Manager	Monitoring Policies	HE Objects	Device: ftdv742	() () () () () () () () () () () () () (SECURE
Object Types ←	Network (Objects a	nd Groups		_
C Networks	9 objects			¥ Filter	+ 🔍
S Ports				Preset filters: System defined, User defined	\Box

FTD_Create_NetObjects

步骤4.2.提供每个网络对象的必要信息。单击OK按钮。

- 名称: local_blue_192.168.20.0
- type : 网络
- 网络:192.168.20.0/24

Add Network Object



Name	
local_blue_192.168.20.0	
Description	
	Ø.
Type Network Host	
Network	
192.168.20.0/24	
e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60	

CANCEL

FTD_VRF_Blue_Network

- 名称:local_red_192.168.10.0
- type : 网络
- 网络:192.168.10.0/24

Add Network Object



OK

CANCEL

Name local_red_192.168.10.0	
Description	
	li.
Type Network Host 	
Network	
192.168.10.0/24 e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60	

FTD_VRF_Red_Network

- 名称:remote_192.168.50.0
- type:网络
- 网络:192.168.50.0/24

Add Network Object

Name		
remote_192.168.50.0		
Description		
		lli.
Type Network O Host O FQDN	O Range	
Network		
192.168.50.0/24		
e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60		

 \times

OK

CANCEL

FTD_Remote_Network

步骤4.3.创建第一个虚拟路由器。导航到设备>路由。单击View Configuration。



FTD_View_Routing_Configuration

步骤4.4.单击添加多个虚拟路由器。

注意:在FDM初始化期间,已配置通过外部接口的静态路由。如果您没有此功能,请手动配置。

Ę	Firewall Device Manager Monitoring	Policies O	bjects Device	e: ftdv742	۵.		admin Administrator
Devic ROL Ac	dd Multiple Virtual Routers	raffic Zapas				~	>_ Commands ~
otatio		Tanio Londo					
1 rou	te					T Filter	
ан) Т	NAME		IP TYPE		GATEWAY IP		SLA MONITOR
1	StaticRoute_IPv4	outside	IPv4	0.0.0/0	192.168.30.3		

FTD_Add_First_Virtual_Router1

步骤4.5.单击CREATE FIRST CUSTOM VIRTUAL ROUTER。

Firewall Device Manager Monitoring Policie	es Objects	Device: ftdv742	(b.) (admin Administrate	or
Device Summary Routing						
Virtual Route Forwarding (Virtual Routing) Description	ł	How Multiple Virtual Route	ers Work	^	>_ Commands ~	
You can create multiple virtual routing and forwarding instances, called virtual routers, to maintain separate routing tables for groups of interfaces. Because each virtual router has its own routing table, you can provide clean separation in the traffic flowing through the device. Thus, you can provide support to two or more distinct customers over a common set of networking equipment. You can also use virtual routers to provide more separation for elements of your own network, for example, by isolating a development network from your general-purpose corporate network.	CUSTOMER A NETWORK 1	I Router mode is enabled au least one custom Virtual R THREAT DEFENSE	Custor	MER A MER A MER B MER B MER B		
	CUSTOMER N NETWORK 1	VIRTUAL ROUTER N		MER N RK 2		

FTD_Add_First_Virtual_Router2

步骤4.6.提供第一台虚拟路由器的必要信息。单击OK按钮。首次创建虚拟路由器后,将自动显示vrf名称Global。

- 名称:vrf_red
- 接口:inside_red(GigabitEthernet0/1)

Firewall Device Manager	Add Virtual Router	• ×		3 i admin Administrate
Device Summary Routing	Name vrf_red			
Virtual Route Forwarding (Virtual Route You can create multiple virtual routing and instances, called virtual routers, to mainta tables for groups of interfaces. Because of has its own routing table, you can provide the traffic flowing through the device. Thus, you can provide support to two or r customers over a common set of network can also use virtual routers to provide mo	Description Interfaces	A	e is at	>_ Commands ~
development network from your general-; network.	NET		ER N K 2	

FTD_Add_First_Virtual_Router3

步骤4.7.创建第二个虚拟路由器。导航到设备>路由。单击View Configuration。单击+按钮。



FTD_Add_Second_Virtual_Router

步骤4.8.提供第二台虚拟路由器的必要信息。单击OK按钮

- 名称:vrf_blue
- 接口:inside_blue(GigabitEthernet0/2)

Monitoring Policies	Add Virtual Router		admin Administrator
	Name vrf_blue		✓ BGP Global Settings
		Å	+
inside_bi managen outside	Interfaces + Inside_blue (GigabitEthernet0/2)		ACTIONS
inside_re		CANCEL)

FTD_Add_Second_Virtual_Router2

步骤5.创建从vrf_blue到Global的路由泄漏。此路由允许192.168.20.0/24网络上的终端发起将穿过站 点到站点VPN隧道的连接。在本示例中,远程终端正在保护192.168.50.0/24网络。

导航到设备>路由。单击查看配置,然后单击查看图标 虚拟路由器vrf_blue的Action单元格中。

þ	Firewall Device Manager Monitoring Policies	Device: ftdv742	() (i) (i) (i) (i) (i) (i) (i) (i) (i) (diala SECURE
	Device Summary Virtual Routers			
	How Multiple Virtual Routers Work		×	BGP Global Settings
	3 virtual routers		Y Filter	+
	H NAME	INTERFACES	SHOW/TROUBLESHOOT	ACTIONS
	1 Global	management outside	>_ Routes >_ Iovo_routes >_ BOP >_ GSPF	
	2 vrf_blue	inside_blue	>_Routes >_Ipvg_routes >_Rop >_copp	⊘ ∎ View
	3 vrf_red	inside_red	>_Routes >_Ipv6_routes >_B0P >_oSPF	

FTD_View_VRF_Blue

步骤5.1.单击静态路由选项卡。单击+按钮。

Firewall Device Manager Monitoring	Policies Objects	Device: ftdv742	2 1	admin Administrator	 diale SECURE
Device Summary / Virtual Routers ∽ Vrf_blue ~ 音					
How Multiple Virtual Routers Work				~	>_ Commands ~
Virtual Router Properties Static Routing	BGP OSPF ECM	P Traffic Zones			
			T Filter		+

FTD_Create_Static_Route_VRF_Blue

步骤5.2.提供必要信息。单击OK按钮。

- 名称 : Blue_to_ASA
- 接口:demovti(Tunnel1)
- 网络:remote_192.168.50.0
- 网关:将此项目留空。

Name Blue_to_ASA		
Description		
		A
Interface	Belongs to c	urrent Router
demovti (Tunnel1) ~	-+ [†] + N/A	
Protocol		
● IPv4 ○ IPv6		
Networks +		
C remote_192.168.50.0		
Gateway		Metric
Please select a gateway	~	1
SLA Monitor Applicable only for IPv4 Protocol type		
Please select an SLA Monitor		~
	CANCEL	OX

FTD_Create_Static_Route_VRF_Blue_Details

步骤6.创建从vrf_red到Global的路由泄漏。此路由允许192.168.10.0/24网络上的终端发起将穿过站 点到站点VPN隧道的连接。在本示例中,远程终端正在保护192.168.50.0/24网络。

导航到设备>路由。单击查看配置,然后单击查看图标 虚拟路由器vrf_red的操作单元格中。

Firewall Device Manag	er	Monitoring Policies	会社 Objects	Device: ftdv742	6			?	:	admin Administrator	 ∽ ci 	SECURE
	Devi Vir	ce Summary tual Routers										
	How Multiple Virtual Routers Work									~	BGP 0	ilobal Settings
		tual routers					T Fib	er				+
	•	NAME		INTERFACES	SHOW/TROU	BLESHOOT 📥						ACTIONS
	1	Global		management outside	>_ Routes >_ Inv6 ro >_ mor >_ oser	utes						
	2	vrf_blue		inside_blue	X_Routes X_Tav6.rc X_BSP X_OSPF	utes						
	3	vrf_red		inside_red	X_ Routes X_ Igv6 ro X_ RoP X_ OSPF	utes						View

FTD_View_VRF_Red

步骤6.1.单击静态路由选项卡。单击+按钮。

Firewall Device	Manager Monitoring	Policies Objects	Device: ftdv742		admin	istrator 👻 discle SECURE
	Device Summary / Vi ← vrf_red ~ 音	rtual Routers				
	How Multiple Virtual	Routers Work				✓ >_ Commands ✓
	Virtual Router Properties	Static Routing BG	P OSPF ECMP Traffic Zones			
				T	r Filter	+

FTD_Create_Static_Route_VRF_Red

步骤6.2.提供必要信息。单击OK按钮。

- 名称 : Red_to_ASA
- 接口:demovti(Tunnel1)
- 网络:remote_192.168.50.0
- 网关:将此项目留空。

vrf_red Add Static Route

0 ×

Name Red_to_ASA		
Description		
		h.
Interface	Belongs to co	urrent Router
demovti (Tunnel1) ~	-++++ N/A	
Protocol		
IPv4 O IPv6		
Networks +		
C remote_192.168.50.0		
Gateway		Metric
Please select a gateway	~	1
SLA Monitor Applicable only for IPv4 Protocol type		
Please select an SLA Monitor		~
	GANCEL	ok

FTD_Create_Static_Route_VRF_Red_Details

步骤7.创建从全局到虚拟路由器的路由泄漏。这些路由允许受站点到站点VPN的远程终端保护的终端访问vrf_red虚拟路由器中的192.168.10.0/24网络和vrf_blue虚拟路由器中的192.168.20.0/24网络

导航到设备>路由。单击View Configuration,然后单击Global虚拟路由器的Action单元格中的 View图标。

Firewall Device Manager Monitoring Policie	s Objects Device: ftdv742	(C)	 diale SECURE
Device Summary Virtual Routers			
How Multiple Virtual Routers Work		×	BGP Global Settings
3 virtual routers		Y Filter	+
N NAME	INTERFACES	SHOW/TROUBLESHOOT	ACTIONS
1 Global	management outside	>_ Routes >_ Inve routes >_ BeP >_ OSPF	⊘ View
2 vrf_blue	inside_blue	>_ Routes >_ Toys routes >_ BeP >_ OSPF	
3 vrf_red	inside_red	>_Routes >_Ipvs_routes >_Bop >_ospf	

FTD_View_VRF_Global

步骤7.1.单击静态路由选项卡。单击+按钮。

Firewall Device N	Manager 🕅 🎯 🌐 Monitoring Policies Objects Devi	ce: ftdv742				admin Administrator	 alialia SECURE
	Device Summary / Virtual Routers ← Global ~ !: 音						
	How Multiple Virtual Routers Work					~	>_ Commands ~
	Virtual Router Properties Static Routing BGP	OSPF EIGRP	ECMP Traffic	c Zones			
	3 routes				T Filter		+
	# NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC ACTIONS
	1 StaticRoute_IPv4	outside	IPv4	0.0.0/0	192.168.30.3		1

FTD_Create_Static_Route_VRF_Global

步骤7.2.提供必要信息。单击OK按钮。

- 名称:S2S_leak_blue
- 接口:inside_blue(GigabitEthernet0/2)
- 网络:local_blue_192.168.20.0
- Gateway:将此项目留空。

Global Add Static Route



Name S2S_leak_blue		
Description		4
The selected interface belongs to a different virtual in the route will cross virtual router boundaries, with the router will leak into another virtual router. Proceed will	outer. If you creat r fait, that traffic t th caution.	te this static route, form this virtual
Interface	Belongs to d	ifferent Router
inside_blue (GigabitEthernet0/2) v	🖉 - 💠 vrt_bi	ue .
Protocol		
() IPv6		
Networks +		
C tocal_blue_192.168.20.0		
Gateway		Metric
Please select a gateway	~	1
SLA Monitor Applicable only for IPv4 Protocol type		
Please select an SLA Monitor		~
	C44/2/10	
	and the life	

encryption aes-256 aes-192 aes integrity sha512 sha384 sha256 sha group 21 20 16 15 14 prf sha512 sha384 sha256 sha lifetime seconds 86400

步骤10.创建定义在FTD上配置的相同参数的IKEv2 ipsec-proposal。

<#root>

crypto ipsec ikev2 ipsec-proposal

AES-SHA

protocol esp encryption aes-256 aes-192 aes protocol esp integrity sha-512 sha-384 sha-256 sha-1

步骤11.创建 ipsec配置文件,引用 第10步中创建的IPSec提议。

<#root>

crypto ipsec profile

demo_ipsec_profile

set ikev2 ipsec-proposal

AES-SHA

set security-association lifetime kilobytes 4608000 set security-association lifetime seconds 28800

步骤12.创建允许IKEv2协议的组策略。

<#root>

group-policy

demo_gp_192.168.30.1

```
internal
group-policy demo_gp_192.168.30.1 attributes
vpn-tunnel-protocol ikev2
```

步骤13.参考步骤12中创建的组策略,为对等FTD外部IP地址创建隧道组,然后 使用FTD配置相同 的预共享密钥(在步骤3.7中创建)。

<#root>

tunnel-group 192.168.30.1 type ipsec-121 tunnel-group 192.168.30.1 general-attributes default-group-policy

demo_gp_192.168.30.1

tunnel-group 192.168.30.1 ipsec-attributes ikev2 remote-authentication pre-shared-key ***** ikev2 local-authentication pre-shared-key *****

步骤14.在外部接口上启用IKEv2。

crypto ikev2 enable outside

步骤15.创建虚拟隧道。

<#root>

```
interface Tunnel1
nameif demovti_asa
ip address 169.254.10.2 255.255.255.0
tunnel source interface outside
tunnel destination 192.168.30.1
tunnel mode ipsec ipv4
tunnel protection ipsec profile
```

demo_ipsec_profile

步骤16.创建静态路由。

route demovti_asa 192.168.10.0 255.255.255.0 169.254.10.1 1
route demovti_asa 192.168.20.0 255.255.255.0 169.254.10.1 1
route outside 0.0.0.0 0.0.0.0 192.168.40.3 1

验证

使用本部分可确认配置能否正常运行。

第1步:通过控制台或SSH导航到FTD和ASA的CLI,通过命令show crypto ikev2 sa和show crypto ipsec sa验证第1阶段和第2阶段的VPN状态。

> system support diagnostic-cli Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach. Type help or '?' for a list of available commands. ftdv742# ftdv742# show crypto ikev2 sa IKEv2 SAs: Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1 Tunnel-id Local Remote 32157565 192.168.30.1/500 192.168.40.1/500 Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK Life/Active Time: 86400/67986 sec Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535 remote selector 0.0.0.0/0 - 255.255.255.255/65535 ESP spi in/out: 0x4cf55637/0xa493cc83 ftdv742# show crypto ipsec sa interface: demovti Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.30.1 Protected vrf (ivrf): Global local ident (addr/mask/prot/port): (0.0.0.0/0.0.0/0/0) remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0/0/0) current_peer: 192.168.40.1 #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30 #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 30, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs 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.: 192.168.30.1/500, remote crypto endpt.: 192.168.40.1/500 path mtu 1500, ipsec overhead 94(44), media mtu 1500 PMTU time remaining (sec): 0, DF policy: copy-df ICMP error validation: disabled, TFC packets: disabled current outbound spi: A493CC83 current inbound spi : 4CF55637 inbound esp sas: spi: 0x4CF55637 (1291146807) SA State: active transform: esp-aes-256 esp-sha-512-hmac no compression in use settings ={L2L, Tunnel, IKEv2, VTI, } slot: 0, conn_id: 13, crypto-map: __vti-crypto-map-Tunnel1-0-1 sa timing: remaining key lifetime (kB/sec): (4055040/16867) IV size: 16 bytes replay detection support: Y Anti replay bitmap: 0x0000000 0x0000001 outbound esp sas:

C.

FTD:

```
spi: 0xA493CC83 (2761149571)
         SA State: active
         transform: esp-aes-256 esp-sha-512-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, VTI, }
         slot: 0, conn_id: 13, crypto-map: __vti-crypto-map-Tunnel1-0-1
         sa timing: remaining key lifetime (kB/sec): (4285440/16867)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x0000000 0x0000001
ASA :
ASA9203# show crypto ikev2 sa
IKEv2 SAs:
Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id Local
                                                              Remote
26025779 192.168.40.1/500
                                                              192.168.30.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/68112 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0xa493cc83/0x4cf55637
ASA9203#
ASA9203# show cry
ASA9203# show crypto ipsec sa
interface: demovti_asa
    Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.40.1
      Protected vrf (ivrf): Global
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0/0/0)
      current_peer: 192.168.30.1
      #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
      #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 30, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs 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.: 192.168.40.1/500, remote crypto endpt.: 192.168.30.1/500
      path mtu 1500, ipsec overhead 94(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 4CF55637
      current inbound spi : A493CC83
    inbound esp sas:
      spi: 0xA493CC83 (2761149571)
         SA State: active
```

transform: esp-aes-256 esp-sha-512-hmac no compression in use settings ={L2L, Tunnel, IKEv2, VTI, } slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-1 sa timing: remaining key lifetime (kB/sec): (4101120/16804) IV size: 16 bytes replay detection support: Y Anti replay bitmap: 0x0000000 0x0000001 outbound esp sas: spi: 0x4CF55637 (1291146807) SA State: active transform: esp-aes-256 esp-sha-512-hmac no compression in use settings ={L2L, Tunnel, IKEv2, VTI, } slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-1 sa timing: remaining key lifetime (kB/sec): (4055040/16804) IV size: 16 bytes replay detection support: Y Anti replay bitmap: 0x0000000 0x0000001

步骤2.检验FTD上VRF和全局的路由。

ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, + - replicated route SI - Static InterVRF, BI - BGP InterVRF Gateway of last resort is 192.168.30.3 to network 0.0.0.0 S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.30.3, outside С 169.254.10.0 255.255.255.0 is directly connected, demovti L 169.254.10.1 255.255.255.255 is directly connected, demovti SI 192.168.10.0 255.255.255.0 [1/0] is directly connected, inside_red SI 192.168.20.0 255.255.255.0 [1/0] is directly connected, inside_blue С 192.168.30.0 255.255.255.0 is directly connected, outside L 192.168.30.1 255.255.255.255 is directly connected, outside ftdv742# show route vrf vrf blue Routing Table: vrf_blue Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, + - replicated route SI - Static InterVRF, BI - BGP InterVRF

Gateway of last resort is not set

L 192.168.20.1 255.255.255 is directly connected, inside_blue SI 192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti

ftdv742# show route vrf vrf_red

Routing Table: vrf_red Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, + - replicated route SI - Static InterVRF, BI - BGP InterVRF Gateway of last resort is not set
C 192.168.10.0 255.255.255.0 is directly connected, inside_red L 192.168.10.1 255.255.255.255 is directly connected, inside_red

SI 192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti

步骤3.检验ping测试。

在ping之前,请检查show crypto ipsec sa的计数器 | inc接口:|encap|decap on FTD。

在本示例中,Tunnel1显示封装和解封的30个数据包。

ftdv742# show crypto ipsec sa | inc interface:|encap|decap interface: demovti #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30 #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 ftdv742#

Client1成功ping Client3。

Client1#ping 192.168.50.10 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 5/299/620 ms

Client2成功ping Client3。

Client2#ping 192.168.50.10 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds: 检查的计数器 show crypto ipsec sa | inc interface:|encap|decap 在FTD上, ping成功。

在本例中,Tunnel1在成功ping后显示封装和解封的40个数据包。此外,两个计数器增加10个数据 包,匹配10个ping回应请求,表示ping流量成功通过IPSec隧道。

ftdv742# show crypto ipsec sa | inc interface:|encap|decap interface: demovti #pkts encaps: 40, #pkts encrypt: 40, #pkts digest: 40 #pkts decaps: 40, #pkts decrypt: 40, #pkts verify: 40 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0

故障排除

本部分提供了可用于对配置进行故障排除的信息。

可以使用这些debug命令对VPN部分进行故障排除。

debug crypto ikev2 platform 255 debug crypto ikev2 protocol 255 debug crypto ipsec 255 debug vti 255

您可以使用这些debug命令对路由部分进行故障排除。

debug ip routing

参考

<u>思科安全防火墙设备管理器配置指南,版本7.4</u>

<u>思科安全防火墙ASA VPN CLI配置指南,9.20</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)。