在FDM管理的FTD上配置基于路由的VPN上的 BGP

目录	ł			
<u>简介</u>				
<u>先决条</u>	<u>件</u>			
<u>要求</u>	<u>1</u>			
<u>使用</u>	<u> 的组件</u>			
<u>配置</u>				
<u>网络</u>	<u>图</u>			
VPN	<u>1上的配置</u>			
BGF	<u> 上的配置</u>			
<u>验证</u>				
<u>故障排</u>	<u>除</u>			

简介

本文档介绍如何在FirePower设备管理器(FDM)管理的FTDv上配置基于路由的站点到站点VPN上的 BGP。

先决条件

要求

Cisco 建议您了解以下主题:

- VPN基本知识
- FTDv上的BGP配置
- 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

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





Торо

VPN上的配置

步骤1:确保节点之间的IP互联准备就绪且稳定。FDM上的智能许可证成功注册到智能帐户。

第二步: Site1客户端的网关配置有Site1 FTD (192.168.70.1)的内部IP地址。Site2客户端的网关配 置有Site2 FTD的内部IP地址(192.168.50.1)。此外,请确保在FDM初始化后正确配置两个FTD上的 默认路由。

登录每个FDM的GUI。导航到Device > Routing。单击。View Configuration单击Static Routing选项卡以验证默认 静态路由。

Firew	vall Device Manager Monitoring Policies	Objects Device: fr	itdv742			admin Administ	trator Y cisco SEC	URE
	Device Summary Routing							
	Add Multiple Virtual Routers					✓ ≻- Commands ✓	BGP Global Settin	ngs
	Static Routing BGP OSPF EIGRP	ECMP Traffic Zones						
	1 route				۲	Y Filter		+
	# NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC ACTIN	DNS
	1 StaticRoute_IPv4	outside	IPv4	0.0.0.0/0	192.168.30.3		1	
站点1_FT	D_网关							
站点1_FT	D_网关 rall Device Manager	The second secon	itdv742		(). 🗎 (? : admin Adminis	strator × "thethe SEC	URE
站点1_FT	D_网关 vall Device Manager Monitoring Policies Device Summary Routing	하고: Objects Device: f	itdv742		۵ 🖨 ((?) : admin Adminis	strator V shulli SEC	URE
站点1_FT	D_网关 vall Device Manager Monitoring Policies Device Summary Routing Add Multiple Virtual Routers	하고: Objects Device: f	ttdv742		> 🗎	 admin Adminis >- Commands 	strator Cisco SEC	URE
站点1_FT	D_网关 rall Device Manager 國 Policies Device Summary Routing Add Multiple Virtual Routers Static Routing BGP OSPF EIGRP	Objects Device: f	tdv742			 admin Adminis Commands 	strator V the SEC	URE
站点1_FT	TD_网关 vall Device Manager Monitoring Policies Device Summary Routing Add Multiple Virtual Routers Static Routing BGP OSPF EIGRP 1 route	Objects Device: f	tdv742			 admin Adminis Commands Filter 	strator Cisco SEC	URE
站点1_FT	D_网关 vall Device Manager Monitoring Policies Device Summary Routing Add Multiple Virtual Routers Static Routing BGP OSPF EIGRP 1 route NAME	Cobjects Device: f	IP TYPE	NETWORKS		 i admin Adminis >- Commands Filter SLA MONITOR 	strator Cisco SEC	URE ngs +

第三步: 配置基于路由的站点到站点VPN。 在本示例中,首先配置Site1 FTD。

步骤 3.1 登录到Site1 FTD的FDM GUI。为Site1 FTD的内部网络创建新的网络对象。 导航至Objects > Networks,点击+按钮。



Create_Network_Object

步骤 3.2提供必要信息。单击 按钮。OK

- 名称:inside_192.168.70.0
- 类型:网络
- 网络: 192.168.70.0/24

Add Network Object

Name

inside_192.168.70.0	
Description	
	11.
Type Network Host FQDN	N O Range
Network	
192.168.70.0/24	
e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60	2
	CANCEL OK

Site1_Inside_Network

步骤 3.3导航到Device > Site-to-Site VPN。单击。View Configuration



查看站点到站点VPN

步骤 3.4开始创建新的站点到站点VPN。单击。CREATE SITE-TO-SITE CONNECTION

Firewall Device Manager	500 Monitoring	Policies	다. Objects	Device: ftdv742		E		admir Admi	nistrator ~	cisco SE	CURE
	Device Summa Site-to-S	Site VPN									
							T Filter				+
							Preset filters: Rost	te Based (VO), Polic	y.Based		
	# NAME		LOCAL INTE	ERFACES	LOCAL NETWORKS	REMOTE NETWORKS	NAT EXEMPT			ACTIONS	
					There are	no Site-to-Site connections yet.					
					Start by creat	Ing the first Site-to-Site connection.					

Create_Site-to-Site_Connection

步骤 3.5提供必要信息。

- 连接配置文件名称: Demo_S2S
- 类型:基于路由(VTI)
- 本地VPN访问接口:点击下拉列表,然后点击Create new Virtual Tunnel Interface。



Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name	Туре
Demo_S2S	Route Based (VTI) Policy Based
Sites Configuration	
LOCAL SITE	REMOTE SITE
Local VPN Access Interface	Remote IP Address
Please select	✓
▼ Filter	
	NEXT
Nothing found	
	~
Create new Virtual Tunnel Interface	

Create_VTI_in_VPN_Wizard

步骤 3.6提供创建新VTI所需的信息。 单击 OK 按钮。

- 名称 : demovti
- 隧道ID:1
- 隧道源:外部(GigabitEthernet0/0)
- IP地址和子网掩码:169.254.10.1/24
- 状态:点击滑块至"已启用"位置

Name demovti Most features work with named int	erfaces only, although some require unnamed interfaces.		Status
Description			
			li.
Tunnel ID () 1 0 - 10413	Tunnel Source () outside (GigabitEthernet0/0)	~	
IP Address and Subnet Mask			
169.254.10.1 / e.g. 192.168.5.15/17 or 192.168.5	24		

VCEL OK	CANCEL

创建_VTI_详细信息

步骤 3.7继续提供必要信息。 单击 Next 按钮。

- •本地VPN访问接口:demovti(在步骤3.6中创建。)
- 远程IP地址:192.168.10.1

New Site-to-site VPN	1 Endpoints	2 Configuration	3 Summary	
Local Network	FTDV742	VPN TUNNEL INTERNET	OUTSIDE	
Identify the I	e interface on this device, and the r ocal and remote networks that can	Define Endpoints remote peer's interface IP address, that use the connection. Traffic between the	form the point-to-point VPN connection. Then, identify ese networks is protected using IPsec encryption.	
	Connection Profile Name	1	Туре	

Demo_S2S		Route Based (VTI)	Policy Based
Sites Configuration			
LOCAL SITE	REMO	TE SITE	
Local VPN Access Interface	Remo	te IP Address	
demovti (Tunnel1)	✓ 193	2.168.10.1	
demovti (Tunnel1)	~ [192	2.168.10.1	
	CANCEL	NEXT	

VPN_Wizard_Endpoints_Step1

步骤 3.8导航至IKE Policy。单击 Edit 按钮。

þ	Firewall Device Manager Monito	oring Policies	Objects Device: ftdv	742	> 7	admin Administrator
	New Site-to-site VP	N (1 Endpoints	2 Configuration	3 Summary	
	€ Loc	al Network	FTDV742	VPN TUNNEL	OUTSIDE 123.1.1 PEER ENDPOINT	Fig. Remote Network
		Select the Internet	t Key Exchange (IKE) policy an IP:	Privacy Configuratio d enter the preshared keys needed sec proposals to use for encrypting	n to authenticate the VPN connection. traffic.	Then, select the
		IKE P	Policy			
		0	IKE policies are global, you cannot o connections.	configure different policies per VPN. Any	enabled IKE Policies are available to all VPN	4
		IKE VEI	RSION 2	IKE VERSION 1		
		IKE Po	blicy	h		
		Globa	Illy applied EDIT	J		
		IPSec	Proposal selected EDIT	0		

Edit_IKE_Policy

步骤 3.9 对于IKE策略,您可以使用预定义策略,也可以通过单击Create New IKE Policy创建新策略。

在本示例中,切换现有IKE策略AES-SHA-SHA,并创建一个新策略用于演示。单击OK按钮以保存

- 名称 : AES256_DH14_SHA256_SHA256
- 加密:AES、AES256
- DH组:14

o

- 完整性哈希: SHA、SHA256
- PRF散列:SHA、SHA256
- 生存期:86400(默认值)

			Add IKE v2 Policy	0 ×
Y Filter			Priority 1 AES256_DH14_SHA256_SHA256	State
AES-GCM-NULL-SHA	0	^	Encryption AES × AES256 ×	~
AES-SHA-SHA	0		Diffie-Hellman Group	
DES-SHA-SHA	0		14 ×	~
			Integrity Hash SHA × SHA256 ×	~
		~	Pseudo Random Function (PRF) Hash	~
Create New IKE Policy	ок		Lifetime (seconds) 86400 Between 120 and 2147483647 seconds.	
			CANCEL	ок

Add_New_IKE_Policy

▼ Filter		
AES-GCM-NULL-SHA	0	^
AES-SHA-SHA	0	
DES-SHA-SHA	0	
AES256_DH14_SHA256_SHA256	0	
		~
Create New IKE Policy	ок	

Enable_New_IKE_Policy

步骤 3.10 导航到IPSec提议。单击 Edit 按钮。

다	Firewall Device Manager	ionitoring I	Policies	₩ Objects	Device: ftdv742			admin Administrator	 cisco SECURE
	New Site-to-site	VPN	C	Endpoints		2 Configuration	3 Summary		
	e	g Local Network	-	FTDV742	VPN T	INNEL	OUTSIDE 123.1.1.1 PEER ENDPOINT	F Remote Network	
		Select	the Internet	Key Exchange (Pri IKE) policy and enter IPsec pro	vacy Configuratio	n to authenticate the VPN connection traffic.	ion. Then, select the	
			IKE P	olicy					
				KE policies are glo connections.	bal, you cannot configur	e different policies per VPN. Any e	anabled IKE Policies are available to all	VPN	
			IKE VER	ISION 2		IKE VERSION 1			
			IKE Pol	licy					
			Global	ly applied	EDIT				
			IPSec	Proposal					
			None s	selected	EDIT				

Edit_IKE_Proposal

步骤 3.11 对于IPSec提议,您可以使用预定义的,也可以通过单击Create new IPSec Proposal来创 建一个新的。在本例中,创建一个新的用于演示目的。提供必要的信息。单击OK按钮以保存。

- 名称: AES256_SHA256
- 加密: AES、AES256
- 完整性哈希: SHA1、SHA256

+			→ Add IKE v2 IPSec Proposal	Ø	×
▼ Filter	SET DEFAULT		Name AES256_SHA256		
AES-GCM in Default Set	0	^	Encryption		
AES-SHA	0	olicies	AES × AES256 ×		~
DES-SHA-1	0		Integrity Hash SHA1 × SHA256 ×		~
Create new IPSec Proposal	CANCEL	ř		CANCEL	

Add_New_IPSec_Proposal

	+		
	Y Filter	SET DEFAULT	
-	AES-GCM in Default Set	0 ^	
, yo	AES-SHA	0	olicie
	DES-SHA-1	0	
	AES256_SHA256	0.	
	Create new IPSec Proposal	CANCEL OK	

Enable_New_IPSec_Proposal

步骤 3.12配置预共享密钥。单击 Next 按钮。

记下此预共享密钥,稍后在Site2 FTD上配置它。

Firewall Device Manager	يين Monitoring	Policies Objects	Device: ftdv742	(>)		? :	admin Administrator	 diale SECUR
		FTDV742	IN	ITERNET	PEER ENDPOIL	۰r ۲		
	Selec	t the Internet Key Exchange	Privacy (e (IKE) policy and enter the presh IPsec proposals to	Configuration ared keys needed to authentici use for encrypting traffic.	ate the VPN connec	tion. Then,	select the	
		IKE Policy IKE policies are g connections.	global, you cannot configure different p	olicies per VPN. Any enabled IKE Pc	plicies are available to	all VPN		
		IKE VERSION 2)	IKE VERSION 1				
		IKE Policy Globally applied	EDIT					
		IPSec Proposal Custom set selecte	ed EDIT					
		Authentication Type Pre-shared Man	anual Key 🔵 Certificate					
		Local Pre-shared Ke	ey					
		Remote Peer Pre-sh	hared Key					
		Thicker's Problem	BACK	NEXT				

Configure_Preshared_Key

步骤 3.13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。

Demo_S2S (Connection Profile
Peer endpoi	int needs to be configured according to specified below configuration.
VPN Access Interface	0 demovti (169.254.10.1) Peer IP Address 192.168.10.1
IKE V2	aes,aes-192,aes-256-sha512,sha384,sha,sha256-sha512,sha384,sha,sha256-21,20,16,15,14, aes,aes-256- sha,sha256-sha,sha256-14
IPSec Proposal Authentication Type	aes,aes-256-sha-1,sha-256 Pre-shared Manual Key
IKE V1: DISABLED	
Lifetime Duration	28800 seconds
Lifetime Size	4608000 kilobytes
ADDITIONAL OPT	IONS
Diffie-Heliman Information is	Copied to the clipboard when you click Finish. You must allow the browser to access your clipboard for the copy to be successful. BACK FINISH
PN_Wizard_Com	plete

步骤 3.14创建访问控制规则以允许流量通过FTD。在本例中,为了演示目的,全部允许。 根据实际 需求修改策略。

ai Device Manager	Monitor	ing Polici	ies Objects	Device: ftdv74	2				• Ad	ministrator	cisco SECURE
🕏 Security Po	olicies										
$\square \rightarrow \bigcirc ss$	L Decryptic	an → O	Identity \rightarrow O	Security Intelligent	ce 🔶 🥑 N	AT $ ightarrow$ Acc	ess Control 🌙	Intrusion			
1 rule						۲	Filter			<	⊁ @. +
		SOURCE			DESTINATION						
# NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS	APPLICATIONS	URLS	USERS	ACTIONS
> 1 Demo_allow	€	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	€

Access_Control_Rule_Sample

第3.15步(可选)如果为客户端配置了动态NAT以访问互联网,请在FTD上配置客户端流量的 NAT豁免规则。在本示例中,无需配置NAT免除规则,因为每个FTD上均未配置动态NAT。

步骤 3.16部署配置更改。

Firewall Device Manager Monitoring Po	licies Objects	Device: ftdv742		0 0	e admin • Administr	ator	-11-11- cisco	SECURE
Device Summary Site-to-Site VPN								
1 connection profile				Filter Preset filters: Route Re	Filter reset filters: Route Resed (VTI), Policy Resed			+
# NAME		LOCAL INTERFACE	IS LOCAL NETWORKS	REMOTE NETWORKS	NAT EXEMPT			ACTIONS
1 Demo_S2S	Route Ba	ased (VTI) demovti					~	

Deploy_VPN_Configuration

BGP上的配置

第四步: 导航到设备>路由。单击View Configuration。

Firewall Device Manager Monitoring Policies	Device: ftdv742	> 🖨 🙆 ?	admin Administrator
Tip Inside Netwo	01 Clisco Firepower Threat Defense for KVM ● 0/0 0/1 0/2 0/3 0/4 0/5 0 € ● ● ● ● ● ● ● ●		Internet DNS Server NTP Server
Interfaces Management: Merged Enabled 4 of 9 View All Interfaces	Routing 1 static route View Configuration	Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration	System Settings Management Access Logging Settings DHCP Server / Relay DDNS Service
Smart License Registered Tier: FTDv50 - 10 Gbps	Backup and Restore	Troubleshoot No files created yet	Hostname Time Services SSL Settings
View Configuration >	View Configuration	REQUEST FILE TO BE CREATED	See more

View_Routing_Configuration

第五步:单击BGP选项卡,然后单击CREATE BGP OBJECT。

]	Firewall Device Manager Monito	ring Policies Objects	Device: ftdv742	Administrator	SECURE
	Device Summary Routing				
	Add Multiple Virtual Routers	3		✓ >- Commands ✓ 🎄 BGP	Global Settings
	Static Routing BGP OSPF	EIGRP ECMP Traffic Z	ones		
					+
	N NAME	DE	SCRIPTION	ACTIONS	
			There are no BGP of Start by creating the fir	bjects yet. st BGP object.	

Create_BGP_Object

第六步:提供对象的名称。 导航到模板并进行配置。单击OK按钮保存。

名称:demobgp

第1行:配置AS编号。单击as-number。手动输入本地AS编号。在本示例中,Site1 FTD的AS编号 65511。

第2行:配置IP协议。单击ip-protocol。选择ipv4。

Add New BGP Object	0 ×
Name demobgp	Description
Template 1 router bgp 65511 2 configure address-family ip-protocol v	Show disabled Reset
ipv4	
ipv6	CANCEL OK

Create_BGP_Object_ASNumber_Protocol

第4行:配置更多设置。单击settings,选择general,然后单击Show disabled。

Add New BGP Object							
Name	Description						
demobgp			11.				
Template	Show disabled	\$	Reset				
⊖ 1	router bgp 65511						
⊖ 2	configure address-fan Address Family IPV4 Settings						
Θ 3	address-family ipv4 unicast						
••• 🗇 4	configure address-family ipv4 <mark>settings ></mark>						
-	general						
	advanced CANCEL	ОК					

Create_BGP_Object_AddressSetting

第6行:点击+图标可允许该行配置BGP网络。单击network-object。您可以查看现有可用对象并选择一个。在本示例中,选择对象name inside_192.168.70.0(在步骤3.2中创建)。

Add	Ne	w BGP Object 🔹 😵 🛛 😨 🕹
Name		Description
demo	obgp	
Templa	te	We Hide disabled
Θ	1	router bgp 65511
Θ	2	configure address-family ipv4 v
Θ	з	address-family ipv4 unicast
Θ	4	configure address-family ipv4 general ~
Θ	5	distance bgp 20 200 200
€	6	network network-object ~
€	7	network network-object v route-map map-tag v
Ð	8	bgp inject-map inject-map v exist-map exist-map v options v
Ð	9	configure aggregate-address map-type v
Ð	10	configure filter-rules direction ~
÷	11	configure neighbor neighbor-address remote-as as-number config-options ~
€	12	configure ipv4 redistribution protocol v identifier none
€	13	bgp router-id router-id

Create_BGP_Object_Add_Network

Add New BGP Object

Name	han				Description						
demo	bbgh										11.
Templa	te							Ø H	ide disabled	φ	Reset
Θ	1	router bgp 65513	L .								
Θ	2	configure addr	ess-fami	ly ipv4∨							
Θ	з	address-fami	ly ipv4	unicast							
Θ	4	IPV4 Network	address	family ipv4 gene	al 🗸						
••• (-)	5	network	- or - o-								
œ €	7	network		l		~	^				
⊙	8	bgp inje	🔁 Out	sidelPv4DefaultRoute Ne	twork	0	otion				
€	9	configur	도 Out	sidelPv4Gateway Host		6					
Ð	10	configur				~					
€	11	configur	🔁 any	-ipv4 Network		0	mber	config-c	options 🗸		
€	12	configur	🕤 anv	-ipv6 Network		6	none				
Ð	13	bgp router-i	÷.,			~					
-			5	inside_192.168.70.0 /	letwork	Ð	~				
		L		ins	ide_192.168.70.0	J					

0

Create_BGP_Object_Add_Network2

第11行:点击+图标可启用该行以配置BGP邻居相关信息。单击neighbor-address,然后手动输入 对等体BGP邻居地址。在本示例中,它是169.254.10.2(Site2 FTD的VTI IP地址)。单击asnumber,然后手动输入对等体AS编号。在本示例中,65510用于站点2FTD。单击config-options 并 选择properties。

Add New BGP Object

Name		Description		
demo	obgp			
Templa	te	We disabled ↓ Reset		
Θ	1	router bgp 65511		
Θ	2	configure address-family ipv4 ~		
Θ	3	address-family ipv4 unicast		
Θ	4	configure address-family ipv4 general ~		
Θ	5	distance bgp 20 200 200		
Θ	6	network inside_192.168.70.0 v		
Ð	7	network network-object v route-map map-tag v		
Ð	8	<pre>bgp inject-map inject-map v exist-map exist-map v options v</pre>		
Ð	9	configure aggregate-address map-type > Select Configuration Option		
Ð	10	configure filter-rules direction ~		
•••	11	configure neighbor 169.254.10.2 remote-as 65510 config-options -		
Ð	12	configure ipv4 redistribution protocol v identitien properties		
€	13	bgp router-id router-id		

Create_BGP_Object_NeighborSetting

第14行:单击+图标可启用该行以配置邻居的某些属性。单击activate-options并选择properties。

Add Ne	ew BGP Object $ eal$ $ ightarrow imes$		
Name	Description		
demobgp			
Template	We Hide disabled		
⊖ 1	router bgp 65511		
⊖ 2	configure address-family ipv4 ~		
⊖ 3	address-family ipv4 unicast		
Θ 4	configure address-family ipv4 general ~		
⊖ 5	distance bgp 20 200 200		
Θ 6	network inside_192.168.70.0 v		
⊕ 7	network network-object v route-map map-tag v		
⊕ 8	bgp inject-map inject-map v exist-map exist-map v options v		
⊕ 9	configure aggregate-address map-type ~		
① 10	configure filter-rules direction ~		
⊖ 11	configure neighbor 169.254.10.2 remote-as 65510 properties v		
Θ 12	neighbor 169.254.10.2 remote-as		
① 13	configure neighbor 169.254.10.2 remote-as setting or		
⊖ 14	configure neighbor 169.254.10.2 activate activate-options		
⊕ 15	configure ipv4 redistribution protocol v ide properties		
	bgp router-id		

第13行:点击+图标可让行显示高级选项。单击设置并选择高级。

Add N	lev	v BGP Object	8	×	
Name		Description			
demo	bgp			11	
Templat	te	💐 Hide disabled	¢F	leset	
Θ	1	router bgp 65511			
Θ	2	configure address-family ipv4 v			
Θ	3	address-family ipv4 unicast			
Θ	4	configure address-family ipv4 general∽			
Θ	5	distance bgp 20 200 200			
Θ	6	network inside_192.168.70.0 v			
Ð	7	network network-object v route-map map-tag v			
\odot	8	<pre>bgp inject-map inject-map ~ exist-map exist-map ~ options ~</pre>			
Ð	9	configure aggregate-address map-type 🗸			
€	10	configure filter-rules direction ~			
Θ	11	configure neighbor 169.254.10.2			
Θ	12	neighbor 169.254.10.2 remote- 25 635510			
••• Θ	13	configure neighbor 169.254.10.2 remote-as settings -			
Θ	14	configure neighbor 169.254.10.2 activate general			
Θ	15	neighbor 169.254.10.2 activate			
€	16	configure neighbor 169.254.10.2 activate advanced			
Ð	17	configure ipv4 redistribution protocol v iden			
€	18	bgp router-id migration			
		ha-mode		_	
		CANCEL	ОК		

Create_BGP_Object_NeighborSetting_Properties_Advanced

第18行:点击选项并选择禁用以禁用路径MTU发现。

Add New BGP Object

Name		Description
demo	obgp	
Templa	te	🐼 Hide disabled 🗘 Reset
Θ	1	router bgp 65511
Θ	2	configure address-family ipv4 v
Θ	3	address-family ipv4 unicast
Θ	4	configure address-family ipv4 general ∽
Θ	5	distance bgp 20 200 200
Θ	6	network inside_192.168.70.0 v
€	7	network network-object v route-map map-tag v
€	8	<pre>bgp inject-map inject-map ~ exist-map exist-map ~ options ~</pre>
€	9	configure aggregate-address map-type v
€	10	configure filter-rules direction ~
Θ	11	configure neighbor 169.254.10.2 remote-as 65510 properties v
Θ	12	neighbor 169.254.10.2 remote-as 65510
Θ	13	configure neighbor 169.254.10.2 remote-as advanced ~
Θ	14	neighbor 169.254.10.2 password secret 🗸
Θ	15	configure neighbor 169.254.10.2 hops options v
Θ	16	neighbor 169.254.10.2 version version options (optional)
Θ	17	neighbor 169.254.10.2 transport connection-mode options
Θ	18	neighbor 169.254.10.2 transport path-mtu-discovery options -
Θ	19	configure neighbor 169.254.10.2 activate properties
Θ	20	neighbor 169.254.10.2 activate disable
€	21	configure neighbor 169.254.10.2 activate settings
Ð	22	configure ipv4 redistribution protocol v identifier none
Ð	23	bgp router-id router-id

Х

Create_BGP_Object_NeighborSetting_Properties_Advanced_PMD

第14、15、16、17行:点击-按钮以禁用这些行。然后,单击OK 按钮保存BGP对象。

Add New BGP Object

Name		Description
demo	bgp	
Templat	e	🐼 Hide disabled 🗘 Reset
Θ	1	router bgp 65511
Θ	2	configure address-family ipv4 ~
Θ	3	address-family ipv4 unicast
Θ	4	configure address-family ipv4 general ~
Θ	5	distance bgp 20 200 200
Θ	6	network inside_192.168.70.0 v
⊙	7	network network-object v route-map map-tag v
⊙	8	<pre>bgp inject-map inject-map v exist-map v options v</pre>
•	9	configure aggregate-address map-type v
•	10	configure filter-rules direction v
Θ	11	configure neighbor 169.254.10.2 remote-as 65510 properties v
Θ	12	neighbor 169.254.10.2 remote-as 65510
Θ	13	configure neighbor 169.254.10.2 remote-as advanced v
Θ	14	neighbor 169.254.10.2 password secret ∨
Θ	15	configure neighbor 169.254.10.2 hops options v
Θ	16	neighbor 169.254.10.2 version version-number
Θ	17	neighbor 169.254.10.2 transport connection-mode options v
Θ	18	neighbor 169.254.10.2 transport path-mtu-discovery disable v
Θ	19	configure neighbor 169.254.10.2 activate properties 🗸
Θ	20	neighbor 169.254.10.2 activate
•	21	configure neighbor 169.254.10.2 activate settings v
•	22	configure ipv4 redistribution protocol v identifier none
O	23	bgp router-id router-id

CANCEL

к

Create_BGP_Object_DisableLines

以下是此示例中的BGP设置的概述。您可以根据实际需求配置其他BGP设置。

X

Name	Description
demobgp	

Templat	te	№ Hide disabled
Θ	1	router bgp 65511
	2	configure address-family ipv4 v
Θ	3	address-family ipv4 unicast
Θ	4	configure address-family ipv4 general ~
Θ	5	distance bgp 20 200 200
Θ	6	network inside_192.168.70.0 v
€	7	network network-object v route-map map-tag v
€	8	bgp inject-map inject-map v exist-map exist-map v options v
€	9	configure aggregate-address map-type ~
€	10	configure filter-rules direction v
Θ	11	configure neighbor 169.254.10.2 remote-as 65510 properties v
Θ	12	neighbor 169.254.10.2 remote-as 65510
Θ	13	configure neighbor 169.254.10.2 remote-as advanced v
€	14	neighbor 169.254.10.2 password secret
\odot	15	configure neighbor 169.254.10.2 hops options v
€	16	neighbor 169.254.10.2 version version-number
€	17	neighbor 169.254.10.2 transport connection-mode options v
Θ	18	neighbor 169.254.10.2 transport path-mtu-discovery disable -
Θ	19	configure neighbor 169.254.10.2 activate properties
Θ	20	neighbor 169.254.10.2 activate
€	21	configure neighbor 169.254.10.2 activate settings v
€	22	configure ipv4 redistribution protocol v identifier none
€	23	bgp router-id router-id

CI	 10	

ОК

Create_BGP_Object_Final_Overview

步骤 7.部署BGP配置更改。

þ	Firewall Device Manager Monitoring	Policies Objects Device: ftdv742	() () () () () () () () () () () () () (
	Device Summary Routing		
	Add Multiple Virtual Routers		V V- Commands V & BGP Global Settings
	Static Routing BGP OSPF	EIGRP ECMP Traffic Zones	
	1 object		+
	H NAME	DESCRIPTION	ACTIONS
	1 demobgp		

部署_BGP_配置

步骤 8现在,Site1 FTD的配置已完成。

要配置Site2 FTD VPN和BGP,请使用相应的Site2 FTD参数重复第3步到第7步。

CLI中Site1 FTD和Site2 FTD的配置概述。

站点1 FTD	站点2 FTD
NGFW版本7.4.2	NGFW版本7.4.2
interface GigabitEthernet0/0 nameif outside cts manual (cts手册) propagate sgt preserve-untag 策略静态sgt已禁用,受信任 security-level 0 ip address 192.168.30.1 255.255.255.0 interface GigabitEthernet0/2 nameif内部 security-level 0	interface GigabitEthernet0/0 nameif outside cts manual (cts手册) propagate sgt preserve-untag 策略静态sgt已禁用,受信任 security-level 0 ip address 192.168.10.1 255.255.255.0 interface GigabitEthernet0/2 nameif内部 security-level 0
ip address 192.168.70.1 255.255.255.0	ip address 192.168.50.1 255.255.255.0
interface Tunnel1 nameif demovti ip address 169.254.10.1 255.255.255.0 隧道源接口外部 隧道目标192.168.10.1 隧道模式ipsec ipv4 隧道保护ipsec配置文件ipsec_profile]e4084d322d 对象网络外部IPv4网关	interface Tunnel1 nameif demovti25 ip address 169.254.10.2 255.255.255.0 隧道源接口外部 隧道目标192.168.30.1 隧道模式ipsec ipv4 隧道保护ipsec配置文件ipsec_profile e4084d322d 对象网络外部IPv4网关 host 192.168.10.3
object network inside_192.168.70.0 子网地址为192.168.70.0 255.255.255.0	object network inside_192.168.50.0 子网地址为192.168.50.0 255.255.255.0
access-group NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL remark rule-id 268435457:访问策略:NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5规则:Inside_Outside_Rule access-list NGFW_ONBOX_ACL advanced trust object- group acSvcg-268435457 ifc inside any ifc outside any rule-id 268435457 event-log both access-list NGFW_ONBOX_ACL remark rule-id 268435458:访问策略:NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458:L5规则:Demo_allow	access-group NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL remark rule-id 268435457:访问策略:NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5规则:Inside_Outside_Rule access-list NGFW_ONBOX_ACL advanced trust object- group acSvcg-268435457 ifc inside any ifc outside any rule-id 268435457 event-log both access-list NGFW_ONBOX_ACL remark rule-id 268435458:访问策略:NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5规则:Demo_allow access-list NGFW_ONBOX_ACL advanced permit object-

access-list NGFW_ONBOX_ACL advanced permit object-	group acSvcg-268435458 any any rule-id 268435458
group acSvcg-268435458 any any rule-id 268435458	event-log both
event-log both	access-list NGFW_ONBOX_ACL remark rule-id 1:访问策
access-list NGFW_ONBOX_ACL remark rule-id 1:访问策	略:NGFW_Access_Policy
略:NGFW_Access_Policy	access-list NGFW_ONBOX_ACL remark rule-id 1: L5规则
access-list NGFW_ONBOX_ACL remark rule-id 1: L5规则	:默认操作规则
:默认操作规则	access-list NGFW_ONBOX_ACL advanced deny ip any any
access-list NGFW_ONBOX_ACL advanced deny ip any any	rule-id 1
rule-id 1	
	router bgp 65510
router bgp 65511	bgp log-neighbor-changes
bgp log-neighbor-changes	bgp router-id vrf auto-assign
bgp router-id vrf auto-assign	address-family ipv4 unicast
address-family ipv4 unicast	neighbor 169.254.10.1 remote-as 65511
neighbor 169.254.10.2 remote-as 65510	邻居169.254.10.1 transport path-mtu-discovery disable
邻居169.254.10.2 transport path-mtu-discovery disable	neighbor 169.254.10.1 activate
neighbor 169.254.10.2 activate	network 192.168.50.0
network 192.168.70.0	no auto-summary
no auto-summary	无同步
无同步	exit-address-family
exit-address-family	
	route outside 0.0.0.0 0.0.0.0 192.168.10.3 1
route outside 0.0.0.0 0.0.0.0 192.168.30.3 1	
	crypto ipsec ikev2 ipsec-proposal AES256_SHA256
crypto ipsec ikev2 ipsec-proposal AES256_SHA256	protocol esp encryption aes-256 aes
protocol esp encryption aes-256 aes	protocol esp integrity sha-256 sha-1
protocol esp integrity sha-256 sha-1	
	crypto ipsec profile ipsec_profile e4084d322d
crypto ipsec profile ipsec_profile e4084d322d	set ikev2 ipsec-proposal AES256_SHA256
set ikev2 ipsec-proposal AES256_SHA256	set security-association lifetime kilobytes 4608000
set security-association lifetime kilobytes 4608000	set security-association lifetime seconds 28800
set security-association lifetime seconds 28800	
	crypto ipsec security-association pmtu-aging infinite
crypto ipsec security-association pmtu-aging infinite	
	crypto ikev2 policy 1
crypto ikev2 policy 1	加密aes-256 aes
加密aes-256 aes	integrity sha256 sha
integrity sha256 sha	第 14 组
第 14 组	prf sha256 sha
prf sha256 sha	lifetime seconds 86400
lifetime seconds 86400	
	crypto ikev2 policy 20
crypto ikev2 policy 20	加密aes-256 aes-192 aes
加密aes-256 aes-192 aes	lintegrity sha512 sha384 sha256 sha
integrity sha512 sha384 sha256 sha	第21组20 16 15 14
第21组20 16 15 14	prf sha512 sha384 sha256 sha
prf sha512 sha384 sha256 sha	lifetime seconds 86400

lifetime seconds 86400	
	crypto ikev2 enable outside
crypto ikev2 enable outside	
	组策略 s2sGP 192.168.30.1内部
组策略 s2sGP 192.168.10.1内部	组策略 s2sGP 192.168.30.1属性
组策略 s2sGP 192.168.10.1属性	vpn-tunnel-protocol ikev2
vpn-tunnel-protocol ikev2	
	tunnel-group 192.168.30.1 type ipsec-l2l
tunnel-group 192.168.10.1 type ipsec-l2l	tunnel-group 192.168.30.1 general-attributes
tunnel-group 192.168.10.1 general-attributes	default-group-policy s2sGP 192.168.30.1
default-group-policy s2sGP 192.168.10.1	
	隧道组192.168.30.1 ipsec属性
隧道组192.168.10.1 ipsec属性	ikev2 remote-authentication pre-shared-key *****
ikev2 remote-authentication pre-shared-key *****	ikev2 local-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****	

验证

使用本部分可确认配置能否正常运行。

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

站点1 FTD	站点2 FTD
ftdv742# show crypto ikev2 sa	
IKEv2 SA :	ftdv742# show crypto ikev2 sa
Session-id:134, Status:UP-ACTIVE, IKE count:1, CHILD count:1 隧道ID本地远程fvrf/ivrf状态角色	IKEv2 SA: Session-id:13, Status:UP-ACTIVE, IKE count:1, CHILD count:1
563984431 192.168.30.1/500 192.168.10.1/500全局/全球就绪型响应器 Encr:AES-CBC,密钥大小:256,散列	隧道ID本地远程fvrf/ivrf状态角色 339797985 192.168.10.1/500 192.168.30.1/500全局/全局就绪发起程序 Encr:AES-CBC,密钥大小:256,散列
:SHA256,DH组:14,身份验证签名 :PSK,身份验证验证:PSK	:SHA256,DH组:14,身份验证签名 :PSK,身份验证验证:PSK
寿命/活动时间:86400/5145秒	寿命/活动时间:86400/74099秒 子sa:本地选择器0.0.0.0/0 -
子sa:本地选择器0.0.0.0/0 -	255.255.255.255/65535
255.255.255.255/65535	远程选择器0.0.0.0/0 - 255.255.255.255/65535
远程选择器0.0.0.0/0 - 255.255.255.255/65535	ESP spi输入/输出:0xb7b5b38b/0xf0c4239d
ESP spi输入/输出: 0xf0c4239d/0xb7b5b38b	

ftdv742# show crypto ipsec sa	ftdv742# show crypto ipsec sa
 	 垶口:demovti25
加密映射标记:	加密映射标记: vti_crvpto_man_Tunnel1_0_
□ 加否联初你记:Vii-Ciypto-map-Tuinter-0-	□ 加否联初你记:VII-Crypto-Inap-Tullier-0-
,序列与:05200,平地地址:192.100.50.1 	1,序列与:05200,平地地址:192.100.10.1
	│ 受保护的vrf (ivrf):全球
本地ident(地址/掩码/端口):	本地ident(地址/掩码/端口):
(0.0.0.0/0.0.0.0/0/0)	(0.0.0.0/0.0.0.0/0/0)
远程ident(地址/掩码/端口):	远程ident(地址/掩码/端口):
(0.0.0/0.0.0.0/0/0)	(0.0.0/0.0.0.0/0/0)
current_peer : 192.168.10.1	current_peer : 192.168.30.1
#pkts encaps: 5720,#pkts encrypt:	#pkts encaps : 5721、#pkts encrypt : 5721、
5720,#pkts digest: 5720	#pkts digest: 5721
#pkts decap:5717,#pkts	#pkts decap:5721,#pkts
decrypt:5717,#pkts verify:5717	decrypt:5721,#pkts verify:5721
#pkts压缩:0,#pkts解压缩:0	#pkts压缩:0,#pkts解压缩:0
#pkts未压缩: 5720,#pkts comp失败:	#pkts未压缩: 5721,#pkts comp失败:
0,#pkts decomp失败: 0	0,#pkts decomp失败: 0
#pre-frag成功:0,#pre-frag失败	#pre-frag成功:0,#pre-frag失败
:0,#fragments已创建:0	:0,#fragments已创建:0
发送#PMTUs:0,#PMTUs rcvd:0,需要重组	发送#PMTUs:0,#PMTUs rcvd:0,需要重组
的#decapsulated frg:0	的#decapsulated frg:0
#TFC rcvd:0,#TFC发送:0	#TFC rcvd:0,#TFC发送:0
#Valid ICMP错误rcvd:0,#Invalid ICMP错误	#Valid ICMP错误rcvd:0,#Invalid ICMP错误
rcvd : 0	rcvd : 0
#send错误: 0,#recv错误: 0	#send错误: 0,#recv错误: 0
本地加密终端:192.168.30.1/500,远程加密终	本地加密终端:192.168.10.1/500,远程加密终
端:192.168.10.1/500	端:192.168.30.1/500
路径mtu 1500、ipsec开销78(44)、媒体mtu 1500	路径mtu 1500、ipsec开销78(44)、媒体mtu 1500
PMTU剩余时间(秒):0,DF策略:copy-df	PMTU剩余时间(秒):0,DF策略:copy-df
ICMP错误验证:禁用,TFC数据包:禁用	ICMP错误验证:禁用,TFC数据包:禁用
当前出站spi:B7B5B38B	当前出站spi:F0C4239D
当前入站spi:F0C4239D	当前入站spi:B7B5B38B
) 入站esp sa ·	│ \入站esp sa ·
spi · 0xE0C4239D (4039386013)	spi · 0xB7B5B38B (3082138507)
SA状态:活动	[SA状态:活动
转换:esp-aes-256 esp-sha-256-hmac无压缩	转换:esp-aes-256 esp-sha-256-hmac无压缩
使用中的设置={L2L Tunnel IKEv2 VTL }	使用中的设置={L2L Tunnel IKEv2 VTL }
插槽:0.conn id:266.加密映射 · vti-	插槽:0.conn id:160.加密映射· vti-
crypto-map-Tunnel1-0-1	crypto-map-Tunnel1-0-1
sa计时:剩余密钥生存期(kB/秒	sa计时:剩余密钥生存期(kB/秒
) : (4285389/3722)	(3962829/3626)
/ ↓ ()==================================	/ / / ()

重播检测支持:Y	重播检测支持:Y
反重播位图:	反重播位图:
0xFFFFFFF 0xFFFFFFF	0xFFFFFFF 0xFFFFFFF
出站esp sa :	出站esp sa :
spi:0xB7B5B38B (3082138507)	spi:0xF0C4239D (4039386013)
SA状态:活动	SA状态:活动
转换:esp-aes-256 esp-sha-256-hmac无压缩	转换:esp-aes-256 esp-sha-256-hmac无压缩
使用中的设置={L2L, Tunnel, IKEv2, VTI, }	使用中的设置={L2L, Tunnel, IKEv2, VTI, }
插槽:0,conn_id:266,加密映射:vti-	插槽:0,conn_id:160,加密映射:vti-
crypto-map-Tunnel1-0-1	crypto-map-Tunnel1-0-1
sa计时:剩余密钥生存期(kB/秒	sa计时:剩余密钥生存期(kB/秒
) : (4147149/3722)) : (4101069/3626)
Ⅳ大小:16字节	Ⅳ大小:16字节
重播检测支持:Y	重播检测支持:Y
反重播位图:	反重播位图:
0x0000000 0x0000001	0x0000000 0x0000001

ſ

第二步: 使用命令show bgp neighbors和show route bgp通过控制台或SSH导航到每个FTD的 CLI以验证BGP状态。

站点1 FTD	站点2 FTD
ftdv742# show bgp neighbors	ftdv742# show bgp neighbors
BGP邻居是169.254.10.2, vrf single_vf, 远程AS 65510, 外部链路 BGP版本4, 远程路由器ID 192.168.50.1 BGP状态=已建立, 持续1d20h 上次读取时间为00:00:25, 上次写入时间为 00:00:45, 保持时间为180, 保持连接间隔为 60秒 邻居会话: 1个活动,不支持多会话(已禁用) 邻居功能: 路由刷新:已通告和已接收(新) 四组八位组的ASN功能:已通告和已接收 地址系列IPv4单播:通告和接收 多会话功能:	BGP邻居是169.254.10.1,vrf single_vf,远程AS 65511,外部链路 BGP版本4,远程路由器ID 192.168.70.1 BGP状态=已建立,持续1d20h 上次读取时间为00:00:11,上次写入时间为 00:00:52,保持时间为180,保持连接间隔为 60秒 邻居会话: 1个活动,不支持多会话(已禁用) 邻居功能: 路由刷新:已通告和已接收(新) 四组八位组的ASN功能:已通告和已接收 地址系列IPv4单播:通告和接收 各会活功能:
 多会话切能: 邮件统计信息: InQ深度为0 OutQ深度为0 发送的Rcvd 打开:11 通知:00 	 岁会话切能: 邮件统计信息: InQ深度为0 OutQ深度为0 发送的Rcvd 打开:11 通知:00
更新:22	更新:22

Keepalive : 2423 2427	Keepalive : 2424 2421
路由刷新:0.0	路由刷新:0.0
合计:2426 2430	合计:2427 2424
诵告运行之间的默认最短时间为30秒	通告运行之间的默认最短时间为30秒
」 对于地址系列:IPv4单播	│ 对于地址系列:IPv4单播
会话:169.254.10.2	会话:169.254.10.1
BGP表版本3 邻居版本3/0	BGP表版本9 邻居版本9/0
输出队列大小 · 0	输出队列大小 · 0
索引1	索引4
1个更新组成员	4个更新组成品
发送的Royd	发送的Revd
前缀活动:	前缀活动:
的	的级13%; 当前前缀:11(消耗80字节)
的观心妖,口。	的观心妖
业式撤捐,00 田佐昌住败汉,太洋田1	业式撤捐,00 田佐昌住败役,不适田4
用作多路径:N/a U	用作多哈侄:N/a U
出站入站	出站入站
来白此对笑设条的最佳路径 · 1 n/a	来白此对笔设备的最佳路径:1 n/a
ロロ・ロー 安洋的百新山的NI DI粉・是ナ1 - 是小0	日口:「O 出送的百新山的NI DI粉:是大1 是小0
及区的更新中的NENI级:取八1,取10	
 启用了地址跟踪,RIB确实具有到169.254.10.2的	│ 启用了地址跟踪,RIB确实具有到169.254.10.1的
路由	路由
已建立连接1:已丢弃0	已建立连接4:已丢弃3
上次重置从不	上次重置1d21h,由于会话1的接口摆动
	传输(tcp) path-mtu-discovery已禁用
Graceful-Restart已禁用	Graceful-Restart已禁用
ftdv742# show route bgp	ftdv742# show route bgp
	代码:L-平地,C-已连接,S-静态,R-
RIP,M-修动,B-BGP	RIP,M-修动,B-BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA -	D - EIGRP, EX - EIGRP external, O - OSPF, IA -
USPF Inter area	USPF Inter area
N1 - USPF NSSA external type 1, N2 - USPF	N1 - USPF NSSA external type 1, N2 - USPF
NSSA external type 2	NSSA external type 2
E1 - OSPF外部类型1,E2 - OSPF外部类型2,V	E1 - OSPF外部类型1,E2 - OSPF外部类型2,V
- VPN	- VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1,	i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1,
L2 - IS-IS level-2	L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U -	ia - IS-IS inter area, * - candidate default, U -

per-user static route o - ODR,P -定期下载的静态路由,+ -复制路由 SI -静态InterVRF、BI - BGP InterVRF Gateway of last resort is 192.168.30.3 to	per-user static route o - ODR,P -定期下载的静态路由,+ -复制路由 SI -静态InterVRF、BI - BGP InterVRF Gateway of last resort is 192.168.10.3 to
B 192.168.50.0 255.255.255.0 [20/0](通过 169.254.10.2,1d20h)	B 192.168.70.0 255.255.255.0 [20/0](通过 169.254.10.1,1d20h)

第三步:Site1客户端和Site2客户端相互之间成功ping通。

站点1客户端:

Site1_Client#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/56/90 ms

站点2客户端:

Site2_Client#ping 192.168.70.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.70.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/39/71 ms

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
```

可以使用这些debug命令对BGP部分进行故障排除。

ftdv742# debug ip bgp ?

BGP neighbor address A.B.C.D address families all All events BGP events BGP path import across topologies, VRFs or AFs in BGP Inbound information import Address family ipv4 ipv6 Address family keepalives BGP keepalives BGP Outbound information out BGP dynamic range range rib-filter Next hop route watch filter events updates BGP updates Address family vpnv4 Address family vpnv6 vrf VRF scope <cr>

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)。