在FDM管理的FTD上,透過路由型VPN設定BGP

目錄

<u>簡</u> :	<u>ት</u>
必	<u>要條件</u>
	<u>採用元件</u>
<u>設</u>)	
	<u>網路圖表</u>
	<u>VPN上的配置</u>
	<u>BGP上的配置</u>
驗	
<u>疑</u>	

簡介

本檔案介紹在FirePower裝置管理員(FDM)管理的FTDv上,透過路由型站台對站台VPN設定BGP。

必要條件

需求

思科建議您瞭解以下主題:

- 對VPN的基本瞭解
- FTDv上的BGP組態
- 使用FDM的經驗

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Cisco FTDv版本7.4.2
- Cisco FDM 7.4.2版

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

設定

網路圖表



托波

VPN上的配置

步驟 1.確保節點之間的IP互連就緒且穩定。FDM上的智慧型授權已順利註冊至智慧帳戶。

步驟 2. Site1客戶端的網關配置有Site1 FTD的內部IP地址(192.168.70.1)。Site2客戶端的網關配置 有Site2 FTD的內部IP地址(192.168.50.1)。此外,請確保在FDM初始化後,正確設定兩個FTD上的 預設路由。

登入每個FDM的GUI。導航到Device > Routing。按一下View Configuration。按一下Static Routing頁籤以驗證預 設靜態路由。

Firewall Device Manager Monitoring Policies	Objects Device: ft	dv742				e admin Administrator	, ∼ °¦	sco SECURE
Device Summary Routing								
Add Multiple Virtual Routers					~	>_ Commands ~	BGP (Global Settings
Static Routing BGP OSPF EIGRP E	CMP Traffic Zones							
1 route					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	

站點1_FTD_網關

Firewall	Device Manager Monitoring	Policies	Objects Device:	ftdv742) admin Administr	rator v cisc	SECURE
	Device Summary Routing									
	Add Multiple Virtual Routers						~	>_ Commands ~	BGP GI	obal Settings
	Static Routing BGP OSPF	EIGRP	ECMP Traffic Zones							
	1 route						F ilter			+
	# NAME		INTERFACE	IP TYPE	NETWORKS	GATEWAY IP		SLA MONITOR	METRIC	ACTIONS
	1 StaticRoute_IPv4		outside	IPv4	0.0.0/0	192.168.10.3			1	

站點2_FTD_網關

步驟 3.配置基於路由的站點到站點VPN。 在本範例中,首先設定Site1 FTD。

步驟 3.1. 登入Site1 FTD的FDM GUI。為Site1 FTD的內部網路建立新網路對象。 導航到Objects > Networks,按一下+按鈕。

Firewall Device N	lanager Monitoring	Ø Policies	∷ Objects	Device: ftdv742	\odot	۵) (?)	:	admin Administrator	~	cisco SE	CURE
Object Types ← Network Objects and Groups												
C Networks	9	objects				Y Filter					+	1
S Ports					P	reset filters: S	rstem define	d, User d	eficed			,

Create_Network_Object

步驟 3.2.提供必要資訊。按一下OK 按鈕。

- 名稱:inside_192.168.70.0
- 型別:網路
- 網路: 192.168.70.0/24

Add Network Object	0	×
Name inside_192.168.70.0		
Description		
		li.
Type Network Host FQDN Range 		
Network		
192.168.70.0/24		
e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60		
CANCEL	ок	

步驟 3.3.導航到Device > Site-to-Site VPN。點選View Configuration。

Firewall Device Manager	國 愛 詳 Monitoring Policies Objects	Device: ftdv742			admin Administrator
	Model Cisco Firepower Th	software VDB reat Defense for KVM 7.4.2-172 376.0	Intrusion Ru 20231011-	le Update Cloud Services High Availabilit 1536 Alssues Unknown Not Configure	ty Configure
	S max	Cisco Firepower Threat Defense f Cisco	for KVIM () /4 0/5 0/6	0/7 CONSOLE	DNS Sever NTP Sever
	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 Tie: FTDv50 - 10 Gbps View Configuration	Backup and Restore	,	Troubleshoot No files created yet REQUEST FILE TO BE CREATED	DNS Server Hostname Time Services SSL Settings See more
	Site-to-Site VPN There are no connections yet	Remote Access VPN Requires Secure Client License No connections 1 Group Policy		Advanced Configuration Includes: FlexConfig, Smart CLI	Device Administration Audit Events, Deployment History, Download Configuration
	View Configuration >	Configure	>	View Configuration >	View Configuration >

檢視站點到站點VPN

步驟 3.4.開始建立新的站點到站點VPN。點選CREATE SITE-TO-SITE CONNECTION。

Firewall Device Manager	500 Monitoring	Policies	Objects	Device: ftdv742) 🛛	admir Admir	n nistrator	cisco SEC	CURE
	Device Summ Site-to-S	ary Site VPN									
							T Filter				+
	-						Preset filters: Route	Based (VO), Polic	y.Based		
	# NAME		LOCAL INTE	RFACES	LOCAL NETWORKS	REMOTE NETWORKS	NAT EXEMPT			ACTIONS	
					There are no Site	e-to-Site connections yet.					
					Start by creating the	first Site-to-Site connection.					
					CREATE SITE	-TO-SITE CONNECTION					

Create_Site-to-Site_Connection

步驟 3.5.提供必要資訊。

- 連線配置檔名稱: Demo_S2S
- 型別:基於路由(VTI)
- 本地VPN訪問介面:按一下下拉選單,然後按一下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 Demo_S2S	Type Route Based (VTI) Policy Based
Sites Configuration	
Local VPN Access Interface	Remote IP Address
Please select	~
▼ Filter	^
Nothing found	NEXT
	~
Create new Virtual Tunnel Interface	

Create_VTI_in_VPN_Wizard

步驟 3.6.提供必要資訊以建立新的VTI。 按一下OK按鈕。

- 名稱:demovti
- 通道ID:1
- 隧道源:外部(GigabitEthernet0/0)
- IP地址和子網掩碼: 169.254.10.1/24
- 狀態:按一下滑杆至「已啟用」位置

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

CAN	CEL	0
	_	

建立_VTI_細節

步驟 3.7.繼續提供必要資訊。 按一下NEXT按鈕。

- 本地VPN訪問介面:demovti(在步驟3.6中建立。)
- 遠端IP地址: 192.168.10.1



	Туре	
	Route Based (VTI)	Policy Based
REMO	TE SITE	
Remo	te IP Address	
✓ 192	2.168.10.1	
CANCEL	NEXT	
	× Remo V CANCEL	Type Route Based (VTI) REMOTE SITE CANCEL

VPN_Wizard_Endpoint_Step1

步驟 3.8.導航到IKE Policy。按一下EDIT按鈕。

þ	Firewall Device Manager	Monitoring	Ø Policies	Objects Device:	tdv742		۶.))	?	e admin • Administrato	r	cisco SECURE
	New Site-to-s	ite VPN	1	Endpoints	2 Con	figuration	3	Summary				
		Cocal Networ	k	FTDV742	VPN TUNNEL	ITERNET	0	DUTSIDE 23.1.1.1 PEER ENDI	POINT	Remote Networ	3	
	Privacy Configuration Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection.											
			IKE Poli	icy								
			IKE conr	policies are global, you can nections.	ot configure different p	policies per VPN. Any enable	ed IKE Polic	cies are available	e to all VPN			
			IKE VERSIO	ON 2		IKE VERSION 1	\supset					
			IKE Policy	y								
			Globally	applied EDIT								
			IPSec Pro	oposal								
			None sel	EDIT	θ							

Edit_IKE_Policy

步驟 3.9. 對於IKE策略,您可以使用預定義策略,或者按一下Create New IKE Policy建立新策略。

在本示例中,切換現有IKE策略AES-SHA-SHA,並建立一個新策略用於演示。按一下OK按鈕進行 儲存。

- 名稱: AES256_DH14_SHA256_SHA256
- 加密:AES、AES256
- DH組:14
- 完整性雜湊:SHA、SHA256
- PRF雜湊:SHA、SHA256
- 存留期:86400 (預設)

			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	

啟用_新建_IKE_策略

步驟 3.10. 導航到IPSec建議。按一下EDIT按鈕。

다	Firewall Device Manager Moni	toring Polic	ies Objects	Device: ftdv742		> 🔊 ?	e admin ● Administrator	cisco SECURE	
	New Site-to-site VI	PN	1 Endpoints		2 Configuration	3 Summary			
	رې برې مې	ocal Network	FTDV742	VPN TI	INTERNET	OUTSIDE	Remote Network		
Privacy Configuration Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.									
			IKE Policy						
			IKE policies are gla connections.	obal, you cannot configur	e different policies per VPN. Any	enabled IKE Policies are available to all VPN			
			IKE VERSION 2		IKE VERSION	1			
			IKE Policy						
			Globally applied	EDIT					
			IPSec Proposal						
			None selected	EDIT					

Edit_IKE_Proposal

步驟 3.11. 對於IPSec提議,您可以使用預定義或者按一下建立新的IPSec提議建立一個新提議。在 此範例中,建立用於示範的新範例。請提供必要資訊。按一下OK按鈕進行儲存。

- 名稱: AES256_SHA256
- 加密:AES、AES256
- 完整性雜湊: SHA1、SHA256

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

增加_新建_IPSec_提議

Ŧ	Filte	er	SET DEFAULT	
	4	AES-GCM in Default Set	0	^
	4	AES-SHA	0	0
	4	DES-SHA-1	0	
	4	AES256_SHA256	0	~

啟用_新建_IPSec_提議

步驟 3.12.配置預共用金鑰。按一下NEXT按鈕。

記下這個預共用金鑰,稍後在Site2 FTD上配置它。

Firewall Device Manager Monitoring	g Policies Objects Device: ftdvi	742	() 🖨 🎒 🔄	admin · · · · · · · · · · · · · · · · · · ·
	FTDV742	INTERNET	PEER ENDPOINT	
	Select the Internet Key Exchange (IKE) policy an IP	Privacy Configuration ad enter the preshared keys needed to aut sec proposals to use for encrypting traffic	henticate the VPN connection. Th	en, select the
	IKE Policy IKE policies are global, you cannot connections.	configure different policies per VPN. Any enabled	IKE Policies are available to all VPN	
	IKE VERSION 2	IKE VERSION 1		
	IKE Policy Globally applied EDIT			
	IPSec Proposal Custom set selected EDIT.			
	Authentication Type Pre-shared Manual Key	Certificate		
	Local Pre-shared Key			
	Remote Peer Pre-shared Key			
	(Balace eleveritore	BACK		

Configure_Pre_Shared_Key

步驟 3.13.檢視VPN配置。如果需要修改任何內容,請按一下BACK按鈕。如果一切正常,請按一下 FINISH按鈕。

/PN Access nterface	0 demovti (169.254.10.1) Peer IP Address 192.168.10.1
IKE V2 KE Policy	aes,aes-192,aes-256-sha512,sha384,sha,sha256-sha512,sha384,sha,sha256-21,20,16,15,14, aes,aes-256-
PSec Proposal	aes,aes-256-sha-1,sha-256
uthentication ype	Pre-shared Manual Key
IPSEC SETTINGS	28800 seconds
uration	4608000 kilobytes
ADDITIONAL OPT	IONS

步驟 3.14.建立存取控制規則,以允許流量透過FTD。在本例中,允許全部用於演示目的。 根據您 的實際需求修改策略。

I Device Manager	Monitor	ring Policie	s Objects	Device: ftdv742			۵ 🖨		adi Ad	min ministrator	cisco SECURE
🛷 Security Po	olicies										
$\square \rightarrow \bigcirc$ ss	L Decryptic	on \rightarrow \bigcirc k	dentity \rightarrow C) Security Intelligence	• -> 📀 N.	AT $ ightarrow$ Acc	ess Control 🔿	S Intrusion			
1 rule						۲	Filter			4	₽ ₽ ● . +
		SOURCE			DESTINATION						
# NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS	APPLICATIONS	URLS	USERS	ACTIONS
> 1 Demo_allow	Allow	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	Ф C ₀

Access_Control_Rule_Example

步驟3.15. (可選)如果為客戶端配置了動態NAT以訪問網際網路,請在FTD上為客戶端流量配置 NAT免除規則。在本範例中,不需要設定NAT豁免規則,因為每個FTD上都沒有設定動態NAT。

步驟 3.16.部署配置更改。

Firewall Device Manager Monitoring Policies	Objects Device: ftdv742	_			admin Administr	rator ~	cisco	SECURE
Device Summary Site-to-Site VPN								
1 connection profile				Filter Preset filters: Route Bas	ed (VTI), Policy Ba	sed		+
# NAME	TYPE	LOCAL INTERFACES	LOCAL NETWORKS	REMOTE NETWORKS	NAT EXEMPT	IKE V1	IKE V2	ACTIONS
1 Demo_S2S	Route Based (VTI)	demovti					~	
	Pricewall Device Manager Monitoring Policies Device Summary Site-to-Site VPN 1 connection profile MAKE 1 Demo_\$2\$	Firewall Device Manager Monitoring Policies Objects Device: ftdv742 Device Summary Site-to-Site VPN 1 connection profile 1 TYPE 1 Demo_S2S Route Based (VTI)	Firewall Device Manager Monitoring Policies Objects Device: ftdv742 Device Summary Site-to-Site VPN 1 connection profile Image: Connection profile Image: Connection profile Image: NAME TYPE LOCAL INTEGRACES 1 Demo_S2S Route Based (VTI)	Firewall Device Manager Monitoring Policies Objects Device: ftdv742 Device Summary Site-to-Site VPN 1 connection profile NAME TYPE LOCAL INTERFACES 	Firewall Device Manager Monitoring Policies Objects Device: ftdv742 Device Summary Site-to-Site VPN 1 connection profile Image: Connection profile I connection profile Image: Connection profile Image: Connection profile I number Type LOCAL INTERFACES LOCAL NETWORKS I Demo_S2S Route Based (VTI) demovti	Firewall Device Manager Monitoring Policies Objects Device: ftdv742 Device Summary Site-to-Site VPN 1 connection profile	Firewall Device Manager Monitoring Policies Objects Device: ftdv742 Device Summary Site-to-Site VPN I connection profile Image: Connection profile Image: Connection profile I connection profile TYPE LOCAL INTERFACES LOCAL INTERFACES LOCAL INTERFACES I Demo_S2S Route Based (VTI) demovti demovti	FireWall Device Manager Monitoring Policies Objects Device: ftdv742 Device Summary Site-to-Site VPN 1 connection profile

部署_VPN_配置

BGP上的配置

步驟 4. 導航到裝置>路由。按一下View Configuration。

Firewall Device Manager Monitoring	Policies Objects	Device: ftdv742	۵ 🖨 🔊	admin Administrator
	For Inside Network	0/1 ower Threat Defense for KVM 0/1 0/2 0/3 0/4 0/5 0/0 0/0 0/0	0/6 0/7 CONSOLE DISPWAN/Gateway	DNS Server DNS Server NTP Server NTP Server Smart Lice
Interfaces Management: Merged Enabled 4 of 9 View All Interfaces	Routing 1 static route	ation >	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	Backup and	d Restore	Troubleshoot No files created yet	Hostname Time Services SSL Settings
Tier: FTDv50 - 10 Gbps				

檢視_路由_組態

步驟 5.按一下BGP頁籤,然後按一下CREATE BGP OBJECT。

3	Firewall Device Manager	Monitoring	Policies Objects	Device: ftdv742	E	0	e admin Administrato	or Y cisco SECURE
	Device Summary Routing							
	Add Multiple Virtu	al Routers				× >.	Commands 🗸	BGP Global Settings
	Static Routing BGP	OSPF EIGRF	ECMP Traffic Zo	nes				
								+
	•	NAME	DESC	RIPTION		ACTIONS		
				There are Start by creat	e no BGP objects yet. titing the first BGP object.			
				CRE	SATE BGP OBJECT			

Create_BGP_Object

步驟 6.提供物件的名稱。 導航到模板並進行配置。按一下OK按鈕進行儲存。

名稱:demobgp

第1行:配置AS編號。按一下as-number。手動輸入本地AS編號。在本例中,Site1 FTD的AS編號 65511。

第2行:配置IP協定。按一下ip-protocol。選擇ipv4。

Add New BGP Object	0 ×
Name demobgp	Description
Template	Show disabled C Reset
ipv4	
ipv6	CANCEL

Create_BGP_Object_ASNumber_Protocol

第4行:配置更多設定。按一下settings,選擇general,然後按一下Show disabled。

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

Create_BGP_Object_AddressSetting

第6行:點選+圖示可允許該行配置BGP網路。按一下network-object。您可以檢視現有的可用物件 ,然後選擇一個物件。在本示例中,選擇對象name inside_192.168.70.0(在步驟3.2中建立)。

Add New BGP Object				
Name		Description		
demo	bgp			
Templat	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		
⊙	6	<pre>network network-object v</pre>		
€	7	<pre>network network-object v route-map map-tag v</pre>		
€	8	bgp inject-map inject-map ∨ exist-map exist-map ∨ options ∨		
⊙	9	configure aggregate-address map-type v		
€	10	configure filter-rules direction ~		
€	11	configure neighbor neighbor-address remote-as as-number config-options v		
€	12	configure ipv4 redistribution protocol v identifier none		
€	13	bgp router-id router-id		

Create_BGP_Object_Add_Network

Add New BGP Object

Name					Description					
demo	obgp									//
										///.
Templa	te							8	Hide disabled	\$ Reset
Θ	1	router bgp 65511	1							
Θ	2	configure addr	ess-fa	mily ipv4∨						
Θ	3	address-fami	ly ipv	4 unicast						
Θ	4	IPV4 Network	addres	s-family ipv4 general	~					
Θ	5	distance	- or	a 200 200 - 1						
•••	6	network								
€	7	network	100		10 M	~	^			
Ð	8	bgp inje	5	OutsidelPv4DefaultRoute Netwo	ork	0	otions			
Ð	9	configur	5	OutsidelPv4Gateway Host		6	a an			
€	10	configur	~			-				
Ð	11	configur	Ģ.	any-ipv4 Network		0	mber	config-	options 🗸	
€	12	configur	5	anv-ipv6 Network		6	none			
⊕	13	bgp router-i	~			-				
			6	inside_192.168.70.0 Net	work	Ð	~			
		L		insid	e_192.168.70.0					

0

Create_BGP_Object_Add_Network2

第11行:點選+圖示可允許該行配置BGP鄰居相關資訊。按一下neighbor-address,然後手動輸入 對等體BGP鄰居地址。在本例中,它是169.254.10.2(站點2 FTD的VTI IP地址)。按一下asnumber,然後手動輸入對等體AS編號。在本例中,65510用於站點2 FTD。按一下config-options 並選擇properties。

Add New BGP Object

Name		Description
demob	gp	
Template	Ŀ.,	We disabled ↓ Reset
Θ	1	router bgp 65511
Θ	2	configure address-family ipv4 ~
Θ	з	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 ~ route-map map-tag ~
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
⊕ 1	10	configure filter-rules direction v
••• 🖸 1	11	configure neighbor 169.254.10.2 remote-as 65510 config-options
⊕ 1	12	configure ipv4 redistribution protocol v identitien properties
⊕ 1	13	bgp router-id router-id

Create_BGP_Object_NeighborSetting

第14行:點選+圖示以啟用該行以配置鄰居的某些屬性。按一下activate-options並選擇properties。

Add New BGP Object ${old on X}$				
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	<pre>bgp inject-map inject-map ~ exist-map exist-map ~ options ~</pre>			
⊕ 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 Select Configuration Option			
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:點選+圖示以顯示該行的高級選項。按一下設定並選擇高級。

Add N	Vev	v BGP Object	8	×	
Name		Description			
demo	obgp			1	
				///.	
Templa	te	🐼 Hide disabled	\$	Reset	
Θ	1	router bgp 65511			
Θ	2	configure address-family ipv4v			
Θ	3	address-family ipv4 unicast			
Θ	4	configure address-family ipv4 general v			
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	bgp inject-map inject-map v exist-map exist-map v options v			
Ð	9	configure aggregate-address map-type 🗸			
\odot	10	configure filter-rules direction v			
Θ	11	configure neighbor 169.254.10.2			
Θ	12	neighbor 169.254.10.2 remote- 25 635510			
•••	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			
Ð	16	configure neighbor 169.254.10.2 activate advanced			
Ð	17	configure ipv4 redistribution protocol v iden			
Ð	18	bgp router-id migration			
		ha-mode	_	_	
		CANCEL	ОК		

Create_BGP_Object_NeighborSetting_Properties_Advanced

第18行:點選選項並選擇停用以停用路徑MTU發現。

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

Create_BGP_Object_NeighborSetting_Properties_Advanced_PMD

明細行14、15、16、17:按一下-按鈕以停用明細行。然後,按一下OK按鈕以儲存BGP對象。

Add New BGP Object

Name		Description		
demo	bgp			
Templa	te	🐼 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	<pre>network inside_192.168.70.0 v</pre>		
۲	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∨		
€	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 v		
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		
۲	23	bgp router-id router-id		

CANCEL

ок

Create_BGP_Object_DisableLine

以下是此範例中BGP設定的概觀。您可以根據實際需求配置其他BGP設定。

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
€	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 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 ~
€	22	configure ipv4 redistribution protocol v identifier none
€	23	bgp router-id router-id

CANCEL

ОК

Create_BGP_Object_Final_Overview

步驟 7.部署BGP配置更改。

Firewa	all Device Manager Monitoring	Policies Objects Device: ftdv742	Administrator v viluelle SECURE
	Device Summary Routing		
	Add Multiple Virtual Routers		✓ ➤ Commands ➤ ∯ BGP Global Settings
	Static Routing BGP OSPF	EIGRP ECMP Traffic Zones	
	1 object		+
	и ламе	DESCRIPTION	ACTIONS
	1 demobgp		

部署_BGP_配置

步驟 8.現在,Site1 FTD的配置已完成。

若要設定Site2 FTD VPN和BGP,請對Site2 FTD的對應引數重複步驟3.到步驟7。

Site1 FTD和Site2 FTD在CLI中的配置概述。

站點1 FTD	站點2 FTD
NGFW版本7.4.2	NGFW版本7.4.2
interface GigabitEthernet0/0 nameif outside cts手冊 propagate sgt preserve-untag 策略靜態sgt已停用受信任 安全性層級0 ip address 192.168.30.1 255.255.255.0 interface GigabitEthernet0/2 nameif inside	interface GigabitEthernet0/0 nameif outside cts手冊 propagate sgt preserve-untag 策略靜態sgt已停用受信任 安全性層級0 ip address 192.168.10.1 255.255.255.0 interface GigabitEthernet0/2 nameif inside 安全性層級0
安全性層級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 隧道源介面外部 隧道目標192.168.10.1 通道模式ipsec ipv4 通道保護ipsec設定檔ipsec_profile]e4084d322d	interface Tunnel1 nameif demovti25 ip address 169.254.10.2 255.255.255.0 隧道源介面外部 隧道目標192.168.30.1 通道模式ipsec ipv4 通道保護ipsec設定檔ipsec_profile e4084d322d
對象網路OutsidelPv4網關 主機192.168.30.3 object network inside_192.168.70.0 子網192.168.70.0 255.255.255.0	對象網路OutsidelPv4網關 主機192.168.10.3 object network inside_192.168.50.0 子網192.168.50.0 255.255.255.0
access-group NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL advanced trust object- group 任何ifc內268435457任何rule-id268435457事件日誌 兩者之外的acSvcg-inter any ifc access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5 RULE: Demo_allow	access-group NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL advanced trust object- group 任何ifc內268435457任何rule-id268435457事件日誌 兩者之外的acSvcg-inter any ifc access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5 RULE: 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:訪問策
access-list NGFW_ONBOX_ACL remark rule-id 1:訪問策	略:NGFW_Access_Policy
略:NGFW_Access_Policy	access-list NGFW_ONBOX_ACL remark rule-id 1: L5
access-list NGFW_ONBOX_ACL remark rule-id 1: L5	RULE : DefaultActionRule
RULE : DefaultActionRule	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	neighbor 169.254.10.1 transport path-mtu-discovery disable
neighbor 169.254.10.2 transport path-mtu-discovery disable	鄰居169.254.10.1啟用
鄰居169.254.10.2啟用	網路192.168.50.0
網路192.168.70.0	no auto-summary
no auto-summary	無同步
無同步	exit-address-family
exit-address-family	
	0.0.0.0 0.0.0.0 192.168.10.3 1外部的路由
0.0.0.0 0.0.0.0 192.168.30.3 1外部的路由	
	crypto ipsec ikev2 ipsec-proposal AES256_SHA256
crypto ipsec ikev2 ipsec-proposal AES256_SHA256	協定esp加密aes-256 aes
協定esp加密aes-256 aes	協定esp完整性sha-256 sha-1
協定esp完整性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	完整性sha256 sha
完整性sha256 sha	群組14
群組14	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	integrity sha512 sha384 sha256 sha
integrity sha512 sha384 sha256 sha	組21 20 16 15 14
組21 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	
	組策略 s2sGP 192.168.30.1內部
組策略 s2sGP 192.168.10.1內部	組策略 s2sGP 192.168.30.1屬性
組策略 s2sGP 192.168.10.1屬性	vpn隧道協定ikev2
vpn隧道協定ikev2	
	tunnel-group 192.168.30.1 type ipsec-I2I
tunnel-group 192.168.10.1 type ipsec-l2l	tunnel-group 192.168.30.1一般屬性
tunnel-group 192.168.10.1一般屬性	default-group-policy s2sGP 192.168.30.1
default-group-policy s2sGP 192.168.10.1	
	隧道組192.168.30.1 ipsec屬性
隧道組192.168.10.1 ipsec屬性	ikev2遠端身份驗證預共用金鑰*****
ikev2遠端身份驗證預共用金鑰*****	ikev2本地身份驗證預共用金鑰*****
ikev2本地身份驗證預共用金鑰*****	

驗證

使用本節內容,確認您的組態是否正常運作。

步驟 1.透過控制檯或SSH導航到每個FTD的CLI,透過show crypto ikev2 sa和show crypto ipsec sa命令驗證階段1和階段2的VPN狀態。

站點1 FTD	站點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	IKEv2 SA: Session-id:13, Status:UP-ACTIVE, IKE
隧道ID本地逸端tvrf/ivrf苏悲角色	count:1, CHILD count:1
563984431 192.168.30.1/500 192.168.10.1/500 Global/Global READY RESPONDER	隧道ID本地遠端fvrf/ivrf狀態角色 339797985 192.168.10.1/500
加密:AES-CBC,金鑰大小:256,雜湊 :SHA256,DH組:14,身份驗證簽名 :PSK,身份驗證驗證:PSK	192.168.30.1/500全局/全局就緒啟動器 加密:AES-CBC,金鑰大小:256,雜湊 :SHA256,DH組:14,身份驗證簽名 :PSK,身份驗證驗證:PSK 壽命/活動時間:86400/74099秒 子sa:本地選擇器0.0.0.0/0 -
壽命/活動時間:86400/5145秒	
子sa:本地選擇器0.0.0.0/0 -	255.255.255.255/65535
255.255.255.255/65535	遠端選擇器0.0.0.0/0 - 255.255.255.255/65535
遠端選擇器0.0.0.0/0 - 255.255.255.255/65535	-SP Spi軸入/軸古: 0xb7b5b38b/0xf0c42390
ESP spi輸入/輸出: 0xf0c4239d/0xb7b5b38b	

ftdv742# show crypto ipsec sa	ftdv742# show crypto ipsec sa
介面:demovti	介面:demovti25
加密對映標籤:vti-crypto-map-Tunnel1-0-	加密對映標籤:vti-crypto-map-Tunnel1-0-
1、seq num: 65280、local addr:	1,序列號為65280,本地地址:192.168.10.1
192.168.30.1	受保護的vrf (ivrf):全球
受保護的vrf (ivrf):全球	本地ident (addr/mask/prot/port):
本地ident (addr/mask/prot/port):	(0.0.0.0/0.0.0.0/0/0)
(0.0.0.0/0.0.0.0/0/0)	遠端ident
遠端ident	(addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
(addr/mask/prot/port):(0.0.0.0/0.0.0.0/0/0)	current_peer: 192.168.30.1
current_peer: 192.168.10.1	#pkts encaps: 5721 #pkts encrypt: 5721
<pre>#pkts encaps: 5720, #pkts encrypt: 5720, #pkts digest: 5720 #pkts decap: 5717, #pkts decrypt: 5717, #pkts verify: 5717 #pkts壓縮: 0, #pkts解壓縮: 0 未#pkts壓縮: 5720, #pkts comp失敗: 0, #pkts解壓縮失敗: 0 #pre-frag成功: 0, #pre-frag失敗 : 0, #fragments建立: 0 已傳送#PMTUs: 0, #PMTUs rcvd: 0, 需要重 組的#decapsulated frgs: 0 #TFC rcvd: 0, #TFC傳送: 0 #Valid ICMP錯誤rcvd: 0, #Invalid ICMP錯誤 rcvd: 0 #send錯誤: 0, #recv錯誤: 0 本地加密端點: 192.168.30.1/500, 遠端加密端 點: 192.168.10.1/500</pre>	<pre>#pkts encaps : 3721, #pkts encrypt : 3721, #pkts digest : 5721 #pkts decap : 5721, #pkts decrypt : 5721, #pkts verify : 5721 #pkts壓縮 : 0, #pkts解壓縮 : 0 #pkts乘壓縮 : 5721, #pkts comp失敗 : 0, #pkts解壓縮失敗 : 0 #pre-frag成功 : 0, #pre-frag失敗 : 0, #fragments建立 : 0 已傳送#PMTUs : 0, #PMTUs rcvd : 0, 需要重 組的#decapsulated frgs : 0 #TFC rcvd : 0, #TFC傳送 : 0 #Valid ICMP錯誤rcvd : 0, #Invalid ICMP錯誤 rcvd : 0 #send錯誤 : 0, #recv錯誤 : 0 本地加密端點 : 192.168.10.1/500, 遠端加密端 點 : 192.168.30.1/500 路徑mtu 1500, ipsec開銷78(44), 媒體mtu 1500</pre>
路徑mtu 1500,ipsec開銷78(44),媒體mtu 1500 剩餘PMTU時間(秒):0,DF策略:copy-df ICMP錯誤驗證:已停用,TFC資料包:已停用 當前出站spi:B7B5B38B 當前入站spi:F0C4239D	A EINIG 1900, ipsee(用動10(44), 媒語ING 1900 剩餘PMTU時間(秒):0, DF策略:copy-df ICMP錯誤驗證:已停用,TFC資料包:已停用 當前出站spi:F0C4239D 當前入站spi:B7B5B38B 入站esp sa ⁻
入站esp sa :	spi: 0xB7B5B38B (3082138507)
spi : 0xF0C4239D (4039386013)	SA狀態:活動
SA狀態 : 活動	轉換:esp-aes-256 esp-sha-256-hmac無壓縮
轉換 : esp-aes-256 esp-sha-256-hmac無壓縮	使用中的設定={L2L,隧道,IKEv2,VTI,}
使用中的設定={L2L,隧道,IKEv2,VTI, }	插槽:0,conn_id:160,加密對映:vti-
插槽 : 0,conn_id : 266,加密對映 :vti-	crypto-map-Tunnel1-0-1
crypto-map-Tunnel1-0-1	sa計時:剩餘金鑰存留期(kB/秒):
sa計時 : 剩餘金鑰存留期(kB/秒) :	(3962829/3626)
(4285389/3722)	IV大小:16位元組

IV大小:16位元組	重新執行偵測支援:Y
重新執行偵測支援:Y	防重播點陣圖:
防重播點陣圖:	0xFFFFFFF 0xFFFFF
0xFFFFFFF 0xFFFFF	出站esp sa :
出站esp sa :	spi: 0xF0C4239D (4039386013)
spi: 0xB7B5B38B (3082138507)	SA狀態:活動
SA狀態:活動	轉換:esp-aes-256 esp-sha-256-hmac無壓縮
轉換:esp-aes-256 esp-sha-256-hmac無壓縮	使用中的設定={L2L,隧道,IKEv2,VTI, }
使用中的設定={L2L,隧道,IKEv2,VTI, }	插槽:0,conn_id:160,加密對映:vti-
插槽:0,conn_id:266,加密對映:vti-	crypto-map-Tunnel1-0-1
crypto-map-Tunnel1-0-1	sa計時:剩餘金鑰存留期(kB/秒):
sa計時:剩餘金鑰存留期(kB/秒):	(4101069/3626)
(4147149/3722)	Ⅳ大小:16位元組
Ⅳ大小:16位元組	重新執行偵測支援:Y
重新執行偵測支援:Y	防重播點陣圖:
防重播點陣圖:	0x0000000 0x0000001
0x0000000 0x0000001	

步驟 2. 使用命令show bgp neighbors和show route bgp透過控制檯或SSH導航到每個FTD的CLI以 驗證BGP狀態。

站點1 FTD	站點2 FTD
ftdv742# show bgp neighbors	ftdv742# show bgp neighbors
BGP鄰居是169.254.10.2,vrf single_vf,遠端AS	BGP鄰居是169.254.10.1,vrf single_vf,遠端AS
65510,外部鏈路	65511,外部鏈路
BGP版本4,遠端路由器ID 192.168.50.1	BGP版本4,遠端路由器ID 192.168.70.1
BGP狀態=已建立,持續1d20h	BGP狀態=已建立,持續1d20h
上次讀取00:00:25,上次寫入00:00:45,保持時	上次讀取00:00:11,上次寫入00:00:52,保持時
間為180,保持連線間隔為60秒	間為180,保持連線間隔為60秒
鄰居會話:	鄰居會話:
1個使用中,不支援多重作業階段(停用)	1個使用中,不支援多重作業階段(停用)
鄰居功能:	鄰居功能:
路由刷新:已通告和已接收(新)	路由刷新:已通告和已接收(新)
四八位組ASN功能:已通告和已接收	四八位組ASN功能:已通告和已接收
地址系列IPv4單播:已通告和接收	地址系列IPv4單播:已通告和接收
多會話功能:	多會話功能:
訊息統計資料:	訊息統計資料:
InQ深度為0	InQ深度為0
OutQ深度為0	OutQ深度為0
傳送的Rcvd	傳送的Rcvd
開啟:11	開啟:11
通知:00	通知:0.0
更新:22	更新:22

Keepalive: 2423 2427	Keepalive: 2424 2421
路由刷新:0 0	路由刷新:0 0
合計:2426 2430	合計:2427 2424
通告運行之間的預設最短時間為30秒	通告運行之間的預設最短時間為30秒
對於地址系列:IPv4單播	對於地址系列:IPv4單播
會話:169.254.10.2	會話:169.254.10.1
BGP表版本3,鄰居版本3/0	BGP表版本9,鄰居版本9/0
輸出隊列大小:0	輸出隊列大小:0
索引1	索引4
1個更新組成員	4個更新組成員
傳送的Rcvd	傳送的Rcvd
字首活動:	字首活動:
用作多重路徑:n/a 0	用作多重路徑:n/a 0
出站入站	出站入站
本地策略拒絕的字首:	本地策略拒絕的字首:
來自此對等體的最佳路徑:1 n/a	來自此對等體的最佳路徑:1 n/a
合計:10	合計:10
傳送的更新中的NLRI數:最大1,最小0	傳送的更新中的NLRI數:最大1,最小0
已啟用地址跟蹤,RIB確實具有到169.254.10.2的	已啟用地址跟蹤,RIB確實具有到169.254.10.1的
路由	路由
已建立連線1;已丟棄0	已建立連線4;已丟棄3
上次重設永不	上次重置1d21h,由於會話1的介面抖動
Transport(tcp) path-mtu-discovery is disabled	Transport(tcp) path-mtu-discovery is disabled
Graceful-Restart已停用	Graceful-Restart已停用
ftdv742# show route bgp	ftdv742# show route bgp
代碼:L -本地,C -已連線,S -靜態,R -	代碼:L -本地,C -已連線,S -靜態,R -
RIP,M -移動,B - BGP	RIP,M -移動,B - BGP
D - EIGRP、EX - EIGRP外部、O - OSPF、IA -	D - EIGRP、EX - EIGRP外部、O - OSPF、IA -
OSPF區域間	OSPF區域間
N1 - OSPF NSSA外部型別1,N2 - OSPF	N1 - OSPF NSSA外部型別1,N2 - OSPF
NSSA外部型別2	NSSA外部型別2
E1 - OSPF外部型別1、E2 - OSPF外部型別2、V	E1 - OSPF外部型別1、E2 - OSPF外部型別2、V
- VPN	- VPN
i - IS-IS, su - IS-IS摘要, L1 - IS-IS級別1, L2	i - IS-IS,su - IS-IS摘要,L1 - IS-IS級別1,L2
- IS-IS級別2	- IS-IS級別2
ia - IS-IS內部區域, * -候選預設值, U -每使用	ia - IS-IS內部區域,* -候選預設值,U -每使用

者靜態路由	者靜態路由
o - ODR, P -定期下載的靜態路由, + -複製路	o - ODR, P -定期下載的靜態路由, + -複製路
由	由
SI -靜態InterVRF、BI - BGP InterVRF	SI -靜態InterVRF、BI - BGP InterVRF
最後選用網關是192.168.30.3到網路0.0.0.0	最後選用網關是192.168.10.3到網路0.0.0.0
B 192.168.50.0 255.255.255.0 [20/0](透過	B 192.168.70.0 255.255.255.0 [20/0](透過
169.254.10.2,1d20h)	169.254.10.1,1d20h)

步驟 3.Site1客戶端和Site2客戶端相互之間成功ping通。

站點1客戶端:

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

站點2客戶端:

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

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

可使用這些debug命令對VPN部分進行故障排除。

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

可使用這些debug命令排除BGP部分故障。

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>

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。