## FDMによって管理されるFTDでのVRF対応ルー トベースのサイト間VPNの設定

内容
<u>はじめに</u>
前提条件
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>設定</u>
<u>ネットワーク図</u>
<u>FTDの設定</u>
<u>ASA の設定</u>
トラブルシュート
<u>参考</u>

### はじめに

このドキュメントでは、FDMによって管理されるFTDでVRF対応のルートベースのサイト間 VPN(VPN)を設定する方法について説明します。

#### 前提条件

要件

次の項目に関する知識があることが推奨されます。

- VPNの基本的な知識
- ・ Virtual Routing and Forwarding(VRF)の基本的な知識
- FDMの経験

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco FTDvバージョン7.4.2
- ・ Cisco FDMバージョン7.4.2
- Cisco ASAvバージョン9.20.3

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

#### 背景説明

Firepower Device Manager(FDM)のVirtual Routing and Forwarding(VRF)を使用すると、単一の Firepower Threat Defense(FTD)デバイス上に複数の隔離されたルーティングインスタンスを作成 できます。各VRFインスタンスは、独自のルーティングテーブルを持つ別個の仮想ルータとして 動作し、ネットワークトラフィックの論理的な分離を可能にし、拡張されたセキュリティおよび トラフィック管理機能を提供します。

このドキュメントでは、VTIを使用してVRF対応IPSec VPNを設定する方法について説明します。 FTDの背後には、VRF RedネットワークとVRF Blueネットワークがあります。VRF Redネットワ ークのClient1とVRF BlueネットワークのClient2は、IPSec VPNトンネル経由でASAの背後にある Client 3と通信します。

#### 設定

ネットワーク図



トポロジ

#### FTDの設定

ステップ1:ノード間のIP相互接続の事前設定が正常に完了していることを確認することが不可 欠です。Client1とClient2には、ゲートウェイとしてFTDの内部IPアドレスが設定されています。 Client3には、ゲートウェイとしてASA内部IPアドレスが設定されています。

ステップ2: 仮想トンネルインターフェイスを作成します。 FTDのFDM GUIにログインします。 Device > Interfacesの順に移動します。View All Interfaces をクリックします。

Firewall Device Manager Monitoring Policies Objects Model Cisco Firepower Threat Defense	Device: ftdv742 Software VDB Intrusion Rule Update Ci for KVM 7.4.2-172 376.0 20231011-1536 S	Connected   fangni     High Aveilability     Connected   fangni     High Aveilability     Not Configured     Convergure
Tesido Network	02 Cisco Firepower Threat Defense for KV/M © 	AGNT ISP/WAN/Gateway MGOLE Sport Smart Lloo
Interfaces Management: Merged Enabled 4 of 9 View All Interfaces	Routing Update: 6 static routes Geolocatic Security In View Configuration > View Confi	ES System Settings ion, Rule, VDB, System Upgrade, Intelligence Feeds Logging Settings DHCP Server / Relay DDNS Service DNS Service

ステップ 2.1: Virtual Tunnel Interfacesタブをクリックします。+ボタンをクリックします。

Firewall Device Ma	inager Monitori	ng Policies	₩E Objects	Device: ftdv742	$(\Sigma_{-})$		?	:	admin Administrator	~	cisco SECURE
	Device Summary Interfaces										
	Cisco Firepower 11 0/0 0/1	0/2 0/3 0/4 0/!	5 0/6 0/7								
	Interfaces Virtu	al Tunnel Interface:	\$			T Fi	iter				+

FTD\_Create\_VTI(仮想トンネルエンドポイント)

#### ステップ 2.2:必要な情報を提供します。OKボタンをクリックします。

- 名前: demovti
- ・トンネルID:1
- トンネル送信元:外部(GigabitEthernet0/0)
- IPアドレスとサブネットマスク: 169.254.10.1/24
- ステータス:スライダをクリックして有効の位置にします。

FTD\_View\_インターフェイス

Name demovti Most features work with named interfaces only, although some require unnamed	interfaces.	Status
Description		di.
Tunnel ID  Tunnel Source Tunnel Source Outside (GigabitEthernet0/0)	¥	
IP Address and Subnet Mask 169.254.10.1 / 24 e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0		
	CANCEL	ск

FTD\_Create\_VTI\_Details

ステップ 3:Device > Site-to-Site VPNの順に移動します。View Configurationボタンをクリック します。



FTD\_Site-to-Site\_VPN\_View\_設定

## ステップ 3.1: 新しいサイト間VPNの作成を開始します。CREATE SITE-TO-SITE CONNECTIONボタンをクリックします。または、+ボタンをクリックします。

Firewall Device Manager	题 Monitoring	Policies	objects	Device: ftdv742		6		* admi * Adm	in inistrator	cisco SE	CURE
	Device Summa Site-to-S	ary Site VPN									
							<b>T</b> Filter				+
							Preset filters: Rout	e Based (VCO), Polis	cy.Based		
	# NAME		LOCAL INTE	RFACES	LOCAL NETWORKS	REMOTE NETWORKS	NAT EXEMPT			ACTIONS	
					There are	no Site-to-Site connections yet.					
					Start by crea	ting the first Site-to-Site connection.					

FTD\_Create\_Site2Site\_Connection(サイト接続)

ステップ 3.2: 提供 必要な情報NEXTボタンをクリックします。

- 接続プロファイル名:Demo\_S2S
- タイプ:ルートベース(VTI)
- ・ ローカルVPNアクセスインターフェイス:demovti(ステップ2で作成)
- リモートIPアドレス: 192.168.40.1(これはピアASA外部IPアドレスです)

New Site-to-site VPN	1 Endpoints	2 Configuration	3 Summary
Local Network	FTDV742	PN TUNNEL INTERNET	OUTSIDE INTERFACE
		Define Endpoints	
Identify the the loc	interface on this device, and the remote cal and remote networks that can use the	peer's interface IP address, that for e connection. Traffic between these	m the point-to-point VPN connection. Then, identify networks is protected using IPsec encryption.
(	Connection Profile Name Demo_S2S	Typ	e Ioute Based (VTI) Policy Based
	Sites Configuration		
	LOCAL SITE	REMOTE SITE	
	Local VPN Access Interface demovti (Tunnel1)	Remote IP Addr ✓ 192.168.40.1	ess
· · · · · · · · · · · · · · · · · · ·			
		CANCEL	)

FTD\_Site-to-Site\_VPN\_エンドポイント

#### ステップ 3.3: IKE Policyに移動します。EDIT ボタンをクリックします。

L F	Firewall Device Manager	Monitoring	Ø Policies	註 Objects	Device: ftdv742		()_		:	admin Administrator	cisco SECURE
	New Site-to-sit	te VPN	(1	Endpoints	2	Configuration	3	Summary			
		C Local Network			VPN TUNN	INTERNET		OUTSIDE	©	Remote Network	
		Selec	t the Internet K	(ey Exchange (	Priva IKE) policy and enter the IPsec propo	cy Configuration preshared keys needed to a sals to use for encrypting traff	uthenticat fic.	te the VPN connection.	Then, sele	ect the	
			IKE Po	E policies are glot	bal, you cannot configure di	ferent policies per VPN. Any enab	led IKE Poli	icies are available to all VPI	N		
			IKE VERS	HON 2		IKE VERSION 1					
			IKE Polic	cy y applied	EDIT						
			IPSec Pr None se	roposal	EDIT						

FTD\_Edit\_IKE\_Policy(ポリシーの編集)

ステップ 3.4: IKEポリシーの場合は、事前に定義したポリシーを使用するか、 新しいIKEポリ シーの作成. この例では、既存のIKEポリシー名をAES-SHA-SHA に切り替えます。OK ボタンをクリックして 保存します。



FTD\_Enable\_IKE\_ポリシー

ステップ 3.5: IPSec Proposalに移動します。EDIT ボタンをクリックします。

þ	Firewall Device Manager Monito	ring Polic	ies Objects	Device: ftdv742		> 🖨 🙆 ?	e admin e Administrator ✓	cisco SECURE
	New Site-to-site VP	Ν	1 Endpoints		2 Configuration	3 Summary		
	fig Los	al Network	FTDV742	VPN TI	INTERNET	OUTSIDE	Fin Remote Network	
		Select the I	nternet Key Exchange	Pr (IKE) policy and ente IPsec pr	ivacy Configurations of the preshared keys needed apposals to use for encrypting to use for encrypting to the presence of the	DN d to authenticate the VPN connection. g traffic.	Then, select the	
			IKE Policy					
			IKE policies are glo connections.	bal, you cannot configu	re different policies per VPN. An	y enabled IKE Policies are available to all VPN	a	
			IKE VERSION 2		IKE VERSION	1		
			IKE Policy Globally applied	EDIT				
			IPSec Proposal None selected	EDIT				

FTD\_Edit\_IPSec\_Proposal(提案)

ステップ 3.6: IPSecプロポーザルの場合は、事前に定義されたパスワードを使用するか、 Create new IPSec Proposal をクリックして新しいパスワードを作成できます。

次の例では、既存のIPSecプロポーザル名をAES-SHAに切り替えます。[保存( OK ボタンをク リックします。

## Select IPSec Proposals

	+		
	<b>T</b> Filter	SET DEFAULT	
	AES-GCM in Default Set	6	^
	🥪 🐴 AES-SHA	0	
yo	DES-SHA-1	0	✓ olicie:
	Create new IPSec Proposal	CANCEL	

8

FTD\_Enable\_IPSec\_Proposal(提案)

ステップ 3.7: ページを下にスクロールし、事前共有キーを設定します。NEXTボタンをクリックします。

この事前共有キーをメモし、後でASAで設定してください。

1	Firewall Device Manager	Monitoring	Policies	-=== Objects	Device: ftdv742		(>_)			?	:	admin Administrator	~	cisco	SECUR
				FTDV742		INTERNET		PEE	R ENDPOI	NT					
		Se	lect the Intern	et Key Exchang	Privat e (IKE) policy and enter the IPsec propos	cy Configuratic preshared keys needed als to use for encrypting	DN to authentica traffic.	ite the VP	N conne	ction. Tì	hen, se	elect the			
				Policy IKE policies are a connections.	global, you cannot configure diff	erent policies per VPN. Any	enabled IKE Po	licies are av	vailable to	all VPN					
			IKE	ERSION 2		IKE VERSION									
			IKE I Glob	Policy Dally applied	EDIT										
			IPSe Cus	c Proposal tom set selecte	d EDIT										
			Auth	entication Type Pre-shared Mar	nual Key O Certificate										
			Loca	el Pre-shared Ke	<sup>9</sup> Y										
			Rem	ote Peer Pre-si	hared Key										
			19535	rie kirkliche -	BA	CK NEXT									

FTD\_Configure\_Pre\_Shared\_Keyを設定します。

ステップ 3.8: VPN設定を確認します。変更が必要な場合は、BACK(戻る)ボタンをクリック します。問題がなければ、FINISH ボタンをクリックします。

nterface	0 demovti (169.254.10.1) Peer IP Address 192.168.40.1
IKE V2	aes,aes-192,aes-256-sha512,sha384,sha,sha256-sha512,sha384,sha,sha256-21,20,16,15,14
PSec Proposal	Pre-shared Manual Key
Туре	
IVPE	▶
IKE V1: DISABLE	
IKE V1: DISABLE IPSEC SETTINGS lifetime Duration	28800 seconds

FTD\_Review\_VPN\_設定

ステップ 3.9: アクセスコントロールルールを作成して、トラフィックがFTDを通過できるよう にします。この例では、デモ用にすべて許可します。実際のニーズに基づいてポリシーを変更し てください。

wall Device Manager	Monitor	ring Policies	註 Objects	Device: ftdv742			۵. 🗳	0 ()	* admin * Admin	v	cisco SECURE	
🕏 Security Po	licies											
$\square \rightarrow \bigcirc SSL$	Decryptio	on $\rightarrow$ $\bigcirc$ Iden	tity $\rightarrow$ () s	ecurity Intelligence	ightarrow 📀 NAT	→ 🖌 Acc	cess Control 🔿	Intrusion				
1 rule						۲	Filter			\$	• • @. +	
		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	<b>€</b> C₀	
	wolte	Black (										

FTD\_ACP\_例

ステップ3.10:(オプション)クライアントがインターネットにアクセスできるようにダイナミッ

クNATが設定されている場合は、FTDでクライアントトラフィックのNAT免除ルールを設定しま す。この例では、FTDにダイナミックNATが設定されていないため、NAT免除ルールを設定する 必要はありません。

ステップ3.11:設定変更を導入します。

þ	Firewall Device Manager	Monitoring	© Policies	∰. Objects	Device: ftdv742	$\otimes$	e.	0	?	:	admin Administrator	×	cisco SECURE	
---	-------------------------	------------	---------------	---------------	-----------------	-----------	----	---	---	---	------------------------	---	--------------	--

FTD\_Deployment\_Changes

ステップ4:仮想ルータを設定します。

ステップ 4.1:スタティックルートのネットワークオブジェクトを作成します。 Objects > Networks の順に移動し、+ボタンをクリックします。

Firewall Device Manager	Monitoring Polici	s Objects	Device: ftdv742	(> (*) (*) (*) (*) (*) (*) (*) (*) (*) (*)	cisco SECURE
Object Types ←	Netwo	k Objects a	and Groups		_
C Networks	9 objects			<b>T</b> Filter	+
S Ports				Preset filters: System defined, User defined	

FTD\_Create\_NetObjects

ステップ 4.2:各ネットワークオブジェクトに必要な情報を提供します。OKボタンをクリックします。

- 名前: local\_blue\_192.168.20.0
- タイプ:ネットワーク
- ネットワーク: 192.168.20.0/24

## Add Network Object



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

CANCEL	ок

FTD\_VRF\_Blue\_Network

- 名前: local\_red\_192.168.10.0
- タイプ:ネットワーク
- ネットワーク: 192.168.10.0/24

## Add Network Object



OK

CANCEL

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

FTD\_VRF\_Red\_ネットワーク

- 名前: remote\_192.168.50.0
- タイプ:ネットワーク
- ・ ネットワーク: 192.168.50.0/24

## Add Network Object

Name remote 192,168,50.0			
Description			
			11
Network O Host	) FQDN	O Range	
Network			
192.168.50.0/24			
e.g. 192.168.2.0/24 or 2001:DB8:0:0	CD30::/60		

X

FTD\_Remote\_Network

ステップ 4.3:最初の仮想ルータを作成します。Device > Routing の順に移動します。View Configuration をクリックします。

CANCEL

ОК

Firewall Device Manager Monitoring Po	Ilicies         Objects	> 🖨 🙆 ?	admin Administrator
inside	0/1 Cisco Firepower Threat Defense for KVM ( 0/0 0/1 0/2 0/3 0/4 0/5 ( 0/0 ()/1 0/2 0/3 0/4 0/5 ( 0/0 ()/1 0/2 0/3 0/4 0/5 () 0/0 ()/1 0/2 0/3 0/4 0/5 ()		Internet DNS Server NTP Server Smart Lice
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

FTD\_View\_Routing\_設定

ステップ 4.4 : Add Multiple Virtual Routers をクリックします。

## 注意: Outsideインタフェースを経由する静的ルートは、FDMの初期化中にすでに構成されています。もしなければ、手動で設定してください。

Firewall Device Manager Monitoring	Ø Policies	Objects Devi	ice: ftdv742	۵. 🔄		) admin Admin	istrator
Device Summary Routing Add Multiple Virtual Routers Static Routing BGP OSPF EIGRP ECI	MP Traffic Zones				۲	>_ Commands	*
1 route					<b>T</b> Filter		
H NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP		SLA MONITOR	
1 StaticRoute_IPv4	outside	IPv4	0.0.0/0	192.168.30.3			

FTD\_Add\_First\_Virtual\_Router1

ステップ 4.5: CREATE FIRST CUSTOM VIRTUAL ROUTER をクリックします。

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

ステップ 4.6:最初の仮想ルータに関する必要な情報を提供します。OK ボタンをクリックします 。最初の仮想ルータを作成した後、vrf名Globalが自動的に表示されます。

- 名前 : vrf\_red
- ・ インターフェイス: inside\_red(GigabitEthernet0/1)

Firewall Device Manager	Add Virtual Router	0 ×	2	? : admin Administrat
Device Summary Routing Virtual Route Forwarding (Virtual Rou	Name vrf_red Description		is at	► Commands ➤
instances, called virtual routers, to maintai tables for groups of interfaces. Because e has its own routing table, you can provide the traffic flowing through the device. Thus, you can provide support to two or n customers over a common set of network can also use virtual routers to provide mor elements of your own network, for examp development network from your general-t	nterfaces + Inside_red (GigabltEthernet0/1)	Å	ER A C2 ER B	
network.			JER N JRK 2	

FTD\_Add\_First\_Virtual\_Router3

ステップ 4.7:2番目の仮想ルータを作成します。 Device > Routing の順に移動します。View

Configuration をクリックします。+ボタンをクリックします。

Firewall Device Manag	er Monitoring	Policies	ite: Objects	Device: ftdv742	$(\Sigma_{-})$	۲	?	:	admin Administrator	×	cisco SECUI	RE
	Device Summary Virtual Router	S										
	How Multiple Vir	tual Routers	Work						~	<b>Ø</b> 6	BGP Global Settings	s
	10. T					<b>Y</b> Fib	er				-	+

FTD\_Add\_Second\_Virtual\_ルータ

ステップ 4.8: 2番目の仮想ルータに関する必要な情報を提供します。OK ボタンをクリックしま す

- 名前:vrf\_blue
- インターフェイス: inside\_blue(GigabitEthernet0/2)

Name vrf_blue Description ↓ Interfaces ↓ manager outside_re Inside_blue (GigabitEthernet0/2) Inside_re	Monitoring Policies	Add Virtual Router	 @ ×	admin Administrator
BGP Global Settings  Description  Interfaces  inside_bl managen outside  inside_re  CANCEL OK		Name vrf_blue		
INTERFACES inside_bl manager outside inside_re CANCEL OK	:	Description		BGP Global Settings
inside_re	INTERFACES inside_bl managen outside	Interfaces	, An	ACTIONS
	inside_re		CANCEL	)

FTD\_Add\_Second\_Virtual\_Router2に追加します。

ステップ 5:vrf\_blueからGlobalへのルートリークを作成します。 このルートにより、 192.168.20.0/24ネットワーク上のエンドポイントは、サイト間VPNトンネルを通過する接続を開 始できます。この例では、リモートエンドポイントが192.168.50.0/24ネットワークを保護してい ます。

Device > Routing の順に移動します。View Configuration をクリックし、View アイコンをクリッ クします 仮想ルータvrf\_blueのActionセル

Ę,	Firewall Device Manager Monitori	ng Policies Objects Device: ftdv742	Admin Administration	tor v cisco SECURE
	Device Summary Virtual Routers			
	How Multiple Virtual Routers Work		×	BGP Global Settings
	3 virtual routers		<b>F</b> ilter	+
	# NAME	INTERFACES	SHOW/TROUBLESHOOT	ACTIONS
	1 Global	management outside	>_Routes >_Ipys_routes >_BoP >_OSFF	
	2 vrf_blue	inside_blue	>_Routes >_Ipvd_routes >_Rop >_OSPF	<b>⊘</b> ₀ View
	3 vrf_red	inside_red	>_ Routes >_ Tyvs routes >_ Bop >_ OSPF	

FTD\_View\_VRF\_Blue

#### ステップ 5.1 : Static Routing タブをクリックします。+ボタンをクリックします。

Firewall Device Manage	er Monitoring	Policies O	bjects Device: ftdv742	$(\Sigma)$	۲	?:	admin Administrator	<ul> <li>cisco SECURE</li> </ul>
Device Summary / Virtua ∽ vrf_blue ~   亩	al Routers							
How Multiple Virtual Rou	uters Work						~	>_ Commands ~
Virtual Router Properties	Static Routing	BGP OSPF	ECMP Traffic Zones					
					T FB	ter		+

#### ステップ 5.2: 必要な情報を提供します。OK ボタンをクリックします。

- 名前:Blue\_to\_ASA
- インターフェイス: demovti(Tunnel1)
- ・ ネットワーク: remote\_192.168.50.0
- ゲートウェイ:この項目は空白のままにします。

FTD\_Create\_Static\_Route\_VRF\_青

Name Blue to ASA			
Description			
Interface	Belongs to	current 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			v
		_	_
	CANCEL	OK	

FTD\_Create\_Static\_Route\_VRF\_Blue\_Details

手順 6: vrf\_redからGlobalへのルートリークを作成します。 このルートにより、 192.168.10.0/24ネットワーク上のエンドポイントは、サイト間VPNトンネルを通過する接続を開 始できます。この例では、リモートエンドポイントが192.168.50.0/24ネットワークを保護してい ます。

Device > Routing の順に移動します。View Configuration をクリックし、View アイコンをクリックします 仮想ルータvrf\_redのActionセル内。

Firewall Device Manag	er Monitoring	Policies	Cobjects	Device: ftdv742		90?	e admin Administrator	<ul> <li>diale SECURE</li> </ul>
	Device Summary Virtual Route	rs						
	How Multiple Vi	rtual Routers	Work				× 4	BGP Global Settings
	3 virtual routers					<b>T</b> Filter		+
	# NAME			INTERFACES	SHOW/TROUBLESHOO	π 📥		ACTIONS
	1 Global			management outside	>_Routes >_Igv6_routes >_BCP >_OSPF			
	2 vrf_blue			inside_blue	2 - Routes 2 - Invis, routes 2 - 999 2 - 989			
	3 vrf_red			inside_red	>_ Routes >_ Ipro.routes >_ GGP >_ OSPF			<b>O</b> View

FTD\_View\_VRF\_Red

#### ステップ 6.1: Static Routing タブをクリックします。+ボタンをクリックします。

þ	Firewall Device Manager	Monitoring	Policies	Dbjects	Device: ftdv742	()		?	:	admin Administrator	Ŷ	cisco SECI	URE
	vrf_	e Summary / Virtu _red ~   盲	al Routers										
	How M	ultiple Virtual Ro	uters Work							~	>	- Commands	~
	Virtual Rou	ter Properties	Static Rout	ing BGP	OSPF ECMP Traffic Zones								
							<b>Y</b> File	er				(	+

FTD\_Create\_Static\_Route\_VRF\_赤

ステップ 6.2: 必要な情報を提供します。OK ボタンをクリックします。

- 名前:Red\_to\_ASA
- インターフェイス: demovti(Tunnel1)
- ・ ネットワーク: remote\_192.168.50.0
- ゲートウェイ:この項目は空白のままにします。

# Add Static Route

0 X

Name Red_to_ASA		
Description		
		h.
Interface	Belongs to cu	ment Router
demovti (Tunnel1) v	-i_a <sup>t</sup> ⊢ 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	ок

FTD\_Create\_Static\_Route\_VRF\_Red\_Details

手順7:グローバルルータから仮想ルータへのルートリークを作成する。このルートにより、サイト間VPNのリモートエンドによって保護されているエンドポイントは、vrf\_red仮想ルータ内の

192.168.10.0/24ネットワークおよびvrf\_blue仮想ルータ内の192.168.20.0/24ネットワークにアク セスできます。

Device > Routing の順に移動します。View Configuration をクリックします。グローバル仮想ルー タのActionセルにあるView アイコンをクリックします。

þ	Fire	ewall Device Manager	Monitoring	Policies	Objects	Device: ftdv742		2	?	:	admin Administrat	or	cisco SECURE	
	Device Virte	e Summary Ual Routers												
	Но	w Multiple Virtual Routers \	Work								~	ф в	GP Global Settings	
	3 virtu	ual routers						T	Filter				+	
		NAME			TERFACES		SHOW/TROUBLESHOO	от 🔔					ACTIONS	
	1	Global		n	nanagement utside		>_ Routes >_ Ipy6 routes >_ BGP >_ OSPF	ŝ					<b>⊘</b> Vie	w
	2	vrf_blue		l	nside_blue		>_ Routes >_ Ipv6 routes >_ BGP >_ OSPF							
	3	vrf_red		İ	nside_red		>_ Routes >_ Ipv6 routes >_ BGP >_ OSPF							

FTD\_View\_VRF\_グローバル

#### ステップ 7.1: Static Routing タブをクリックします。+ボタンをクリックします。

þ	Firewall Device Manag	ər	500 Monitoring	Policies	Objects	Device: ftdv742				$\odot$			:	admin Administrator	×	cisco S	ECURE	
		¢	Device Summar Global ~	y / Virtual Roo	uters													
		н	low Multiple Vir	tual Routers	Work									~	>_	Comma	ands 🗸	
		Virtu	ual Router Propert	ies	Static Routing	BGP OSPF	EIGRP	ECMP Traffic	c Zones									
		3 roi	utes								٦	Filter					+	J
		•	NAME			INTERFA	CIE	IP TYPE	NETWORKS		GATEWAY	(IP	1	SLA MONITOR	METR	с	ACTIONS	
		-1	StaticRoute_IP	v4		outside		IPv4	0.0.0.0/0		192.16	8.30.3			1			

FTD\_Create\_Static\_Route\_VRF\_グローバル

ステップ 7.2: 必要な情報を提供します。OK ボタンをクリックします。

- 名前: S2S\_leak\_blue
- インターフェイス: inside\_blue(GigabitEthernet0/2)
- ・ ネットワーク: local\_blue\_192.168.20.0
- ゲートウェイ:この項目は空白のままにします。

## 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

ステップ 10: FTDで設定されているものと同じパラメータを定義するIKEv2 ipsec-proposalを作成します。

<#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

ステップ 11新しい ipsecプロファイル、参照 ipsec-proposalはステップ10で作成します。

#### <#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

ステップ 12 IKEv2プロトコルを許可するグループポリシーを作成します。

#### <#root>

group-policy

demo\_gp\_192.168.30.1

internal group-policy demo\_gp\_192.168.30.1 attributes vpn-tunnel-protocol ikev2

ステップ 13 ステップ12で作成したグループポリシーを参照して、ピアFTDのOutside IPアドレス

のトンネルグループを作成します。 ftdで同じ事前共有鍵を設定します(ステップ3.7で作成)。

#### <#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 \*\*\*\*\*

ステップ14: 外部インターフェイスでIKEv2を有効にします。

crypto ikev2 enable outside

ステップ15:仮想トンネルを作成します。

#### <#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

#### ステップ16:スタティックルートを作成します。

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

#### 確認

ここでは、設定が正常に機能しているかどうかを確認します。

ステップ1:コンソールまたはSSHを使用してFTDとASAのCLIに移動し、show crypto ikev2 saコマンドとshow crypto ipsec saコマンドを使用してフェーズ1とフェーズ2のVPNステータスを 確認します。

FTD :

> 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)

G

IV size: 16 bytes replay detection support: Y Anti replay bitmap: 0x00000000 0x0000001 outbound 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: 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: 0x00000000 0x00000001

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): (0.0.0.0/0.0.0.0/0/0) 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

G

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

#### ステップ2:FTDでVRFとグローバルのルートを確認します。

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 С 192.168.20.0 255.255.255.0 is directly connected, inside\_blue 192.168.20.1 255.255.255.255 is directly connected, inside\_blue L 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 С 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

ステップ3:pingテストを確認します。

pingを実行する前に、FTDでshow crypto ipsec sa | inc interface:|encap|decapのカウンタを確認し ます。

この例では、Tunnel1でカプセル化とカプセル化解除の両方について30個のパケットが示されています。

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 ping Client3が正常に実行されました。

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 ping Client3が正常に実行されました。

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: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 11/297/576 ms

次のカウンタを確認します。 show crypto ipsec sa | inc interface:|encap|decap FTDで確認しま す。

この例では、pingが成功した後、Tunnel1はカプセル化とカプセル化解除の両方について40個の パケットを示しています。さらに、どちらのカウンタも10パケット増加し、10個のpingエコー要 求に一致しています。これは、pingトラフィックがIPSecトンネルを正常に通過したことを示して います。

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

### トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

これらのdebugコマンドを使用して、VPNセクションのトラブルシューティングを行うことがで きます。

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

これらのdebugコマンドを使用して、ルートセクションのトラブルシューティングを行うことが できます。

debug ip routing

### 参考

Cisco Secure Firewall Device Managerコンフィギュレーションガイド、バージョン7.4

<u>Cisco Secure Firewall ASA VPN CLIコンフィギュレーションガイド9.20</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。