

# 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

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[FTDの設定](#)

[ASAの設定](#)

[確認](#)

[トラブルシューティング](#)

[参考](#)

---

## 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。

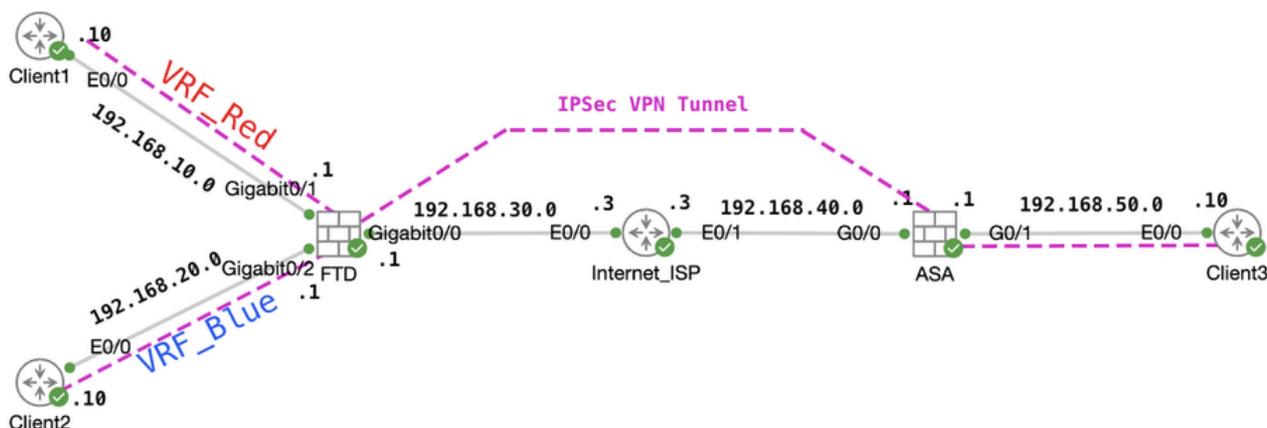
## 背景説明

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

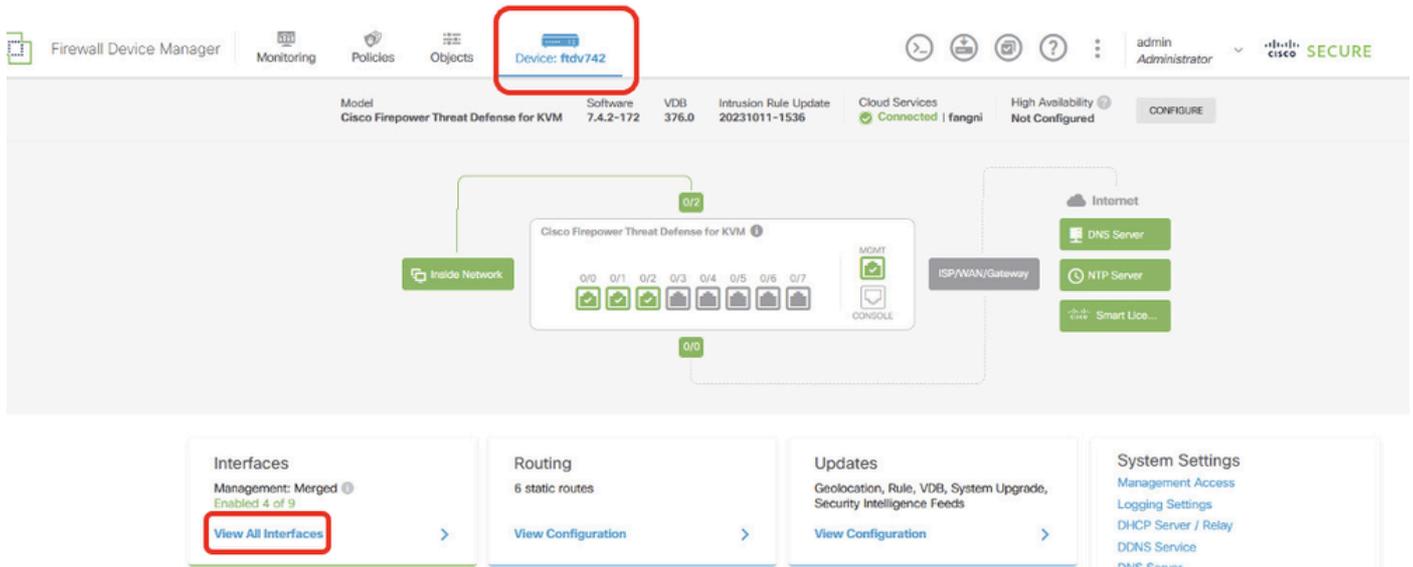


トポロジ

### FTDの設定

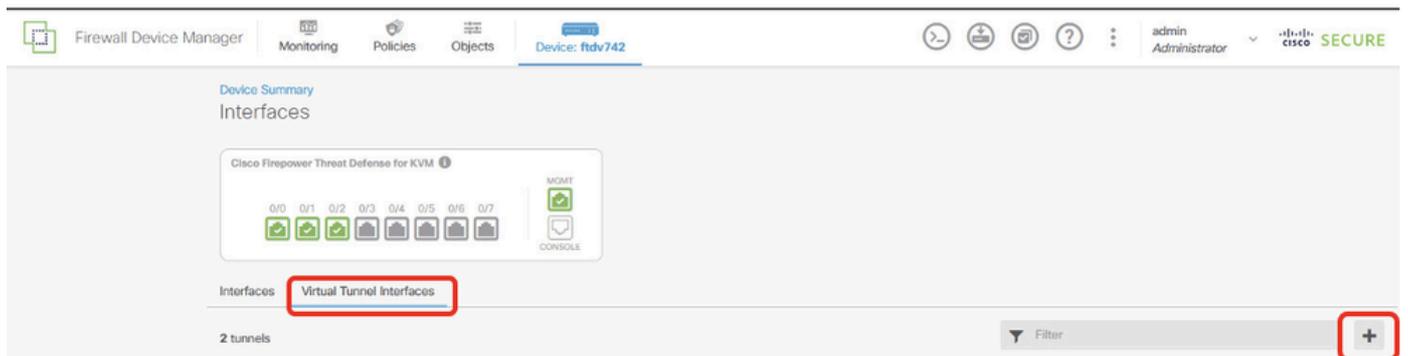
ステップ 1：ノード間のIP相互接続の事前設定が正常に完了していることを確認することが不可欠です。Client1とClient2には、ゲートウェイとしてFTDの内部IPアドレスが設定されています。Client3には、ゲートウェイとしてASA内部IPアドレスが設定されています。

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。



FTD\_View\_インターフェイス

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。



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 : スライダーをクリックして有効の位置にします。

Name

demovti

Status



Most features work with named interfaces only, although some require unnamed interfaces.

Description

Tunnel ID ⓘ

1

0 - 10413

Tunnel Source ⓘ

outside (GigabitEthernet0/0)



IP Address and Subnet Mask

169.254.10.1

/

24

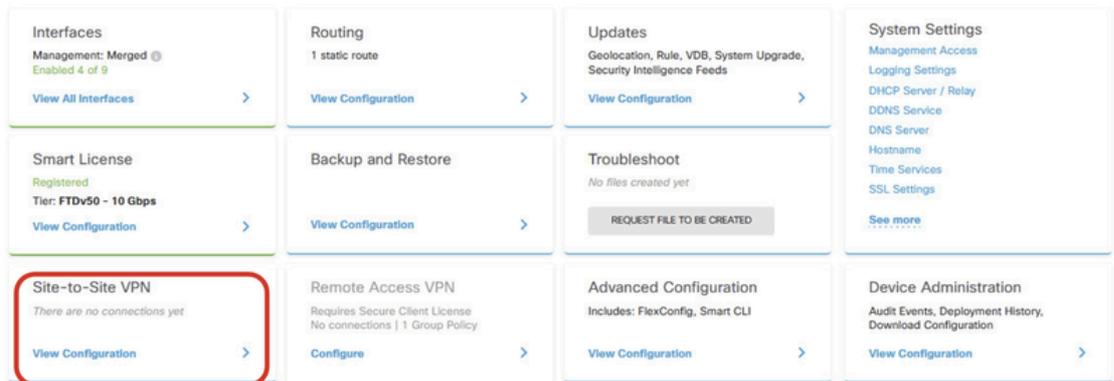
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

CANCEL

OK

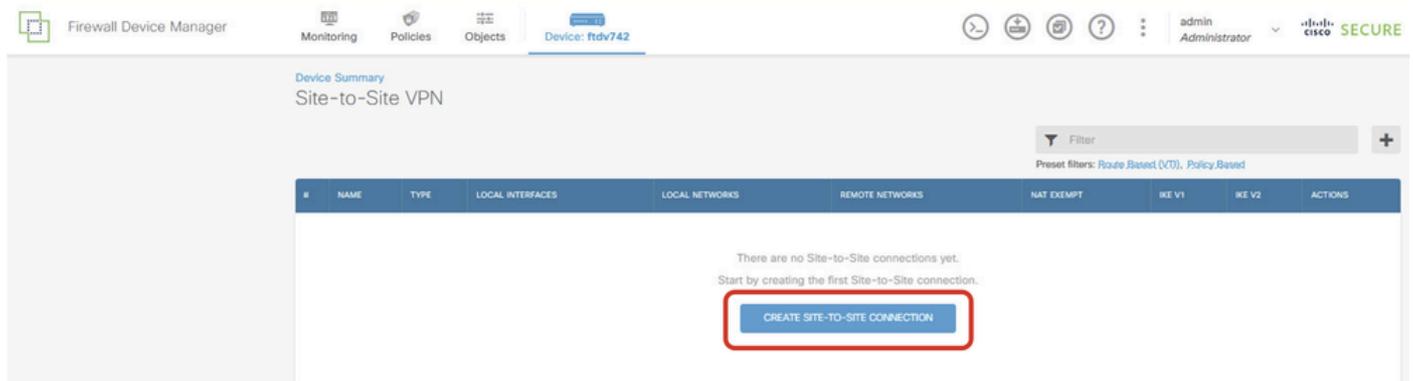
FTD\_Create\_VTI\_Details

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。



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。

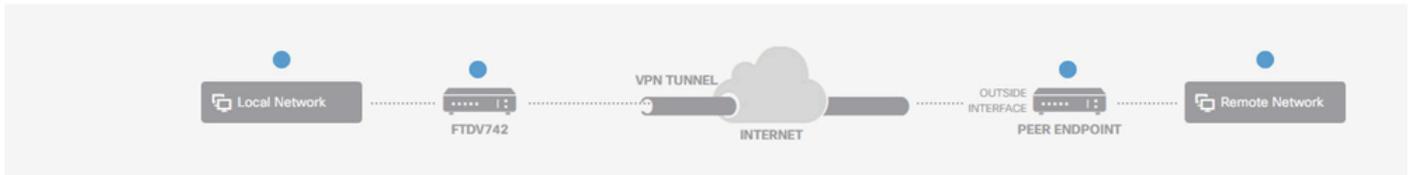
- 接続プロファイル名 : Demo\_S2S
- タイプ : ルートベース(VTI)
- ローカルVPNアクセスインターフェイス : demovti ( ステップ2で作成 )
- リモートIPアドレス : 192.168.40.1 ( これはピアASA外部IPアドレスです )

## New Site-to-site VPN

1 Endpoints

2 Configuration

3 Summary



### 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 SITE	REMOTE SITE
Local VPN Access Interface: demovti (Tunnel1)	Remote IP Address: 192.168.40.1

CANCEL NEXT

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。

Firewall Device Manager | Monitoring | Policies | Objects | Device: ftdv742 | admin Administrator | CISCO SECURE

New Site-to-site VPN

1 Endpoints 2 Configuration 3 Summary

The diagram illustrates the Site-to-site VPN configuration. It shows a Local Network connected to a device labeled FTDV742. This device is connected to a VPN TUNNEL, which is connected to the INTERNET. The INTERNET is connected to a PEER ENDPOINT, which is connected to a Remote Network. The VPN TUNNEL and PEER ENDPOINT are connected to the OUTSIDE INTERFACE of the FTDV742 device.

### 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

1 IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

IKE VERSION 2  IKE VERSION 1

IKE Policy

Globally applied

IPSec Proposal

None selected

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。

Filter

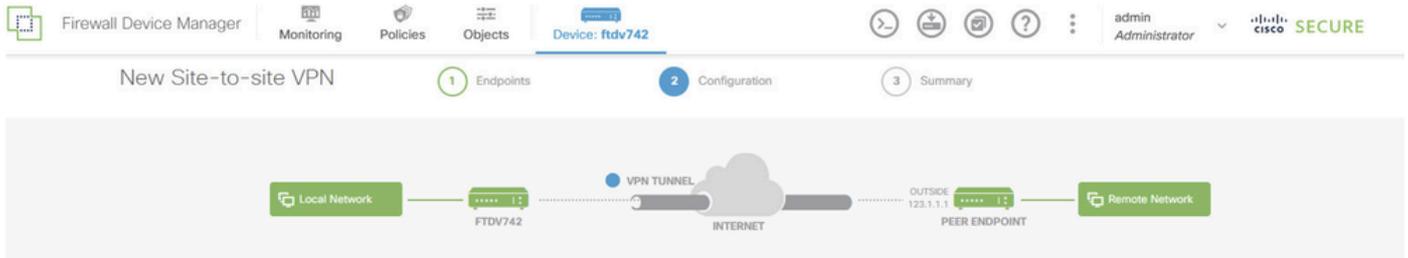
<input type="checkbox"/>	AES-GCM-NULL-SHA	i
<input checked="" type="checkbox"/>	AES-SHA-SHA	i
<input type="checkbox"/>	DES-SHA-SHA	i

Create New IKE Policy

OK

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。



### 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

1 IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

IKE VERSION 2

IKE VERSION 1

#### IKE Policy

Globally applied

#### IPSec Proposal

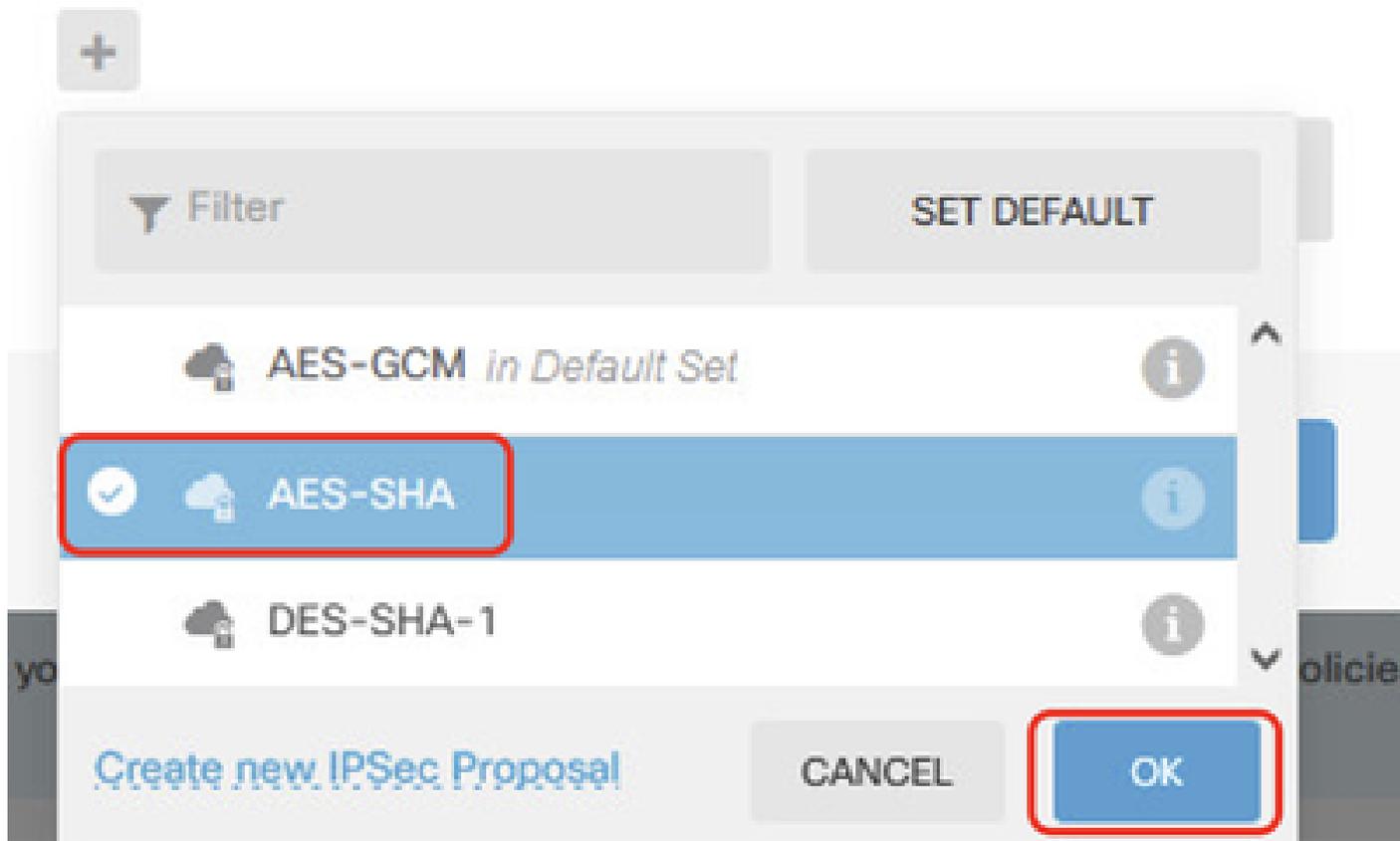
None selected  1

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



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。

Firewall Device Manager | Monitoring | Policies | Objects | Device: ftdv742 | admin Administrator | CISCO SECURE

FTDV742 | INTERNET | PEER ENDPOINT

### 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

**i** IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

IKE VERSION 2  | IKE VERSION 1

IKE Policy  
Globally applied

IPSec Proposal  
Custom set selected

Authentication Type  
 Pre-shared Manual Key  Certificate

Local Pre-shared Key  
\*\*\*\*\*

Remote Peer Pre-shared Key  
\*\*\*\*\*

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。

### Demo\_S2S Connection Profile

**Peer endpoint needs to be configured according to specified below configuration.**

**VPN Access Interface** demovti (169.254.10.1) ↔ **Peer IP Address** 192.168.40.1

**IKE V2**

**IKE Policy** aes,aes-192,aes-256-sha512,sha384,sha,sha256-sha512,sha384,sha,sha256-21,20,16,15,14

**IPSec Proposal** aes,aes-192,aes-256-sha-512,sha-384,sha-256,sha-1

**Authentication Type** Pre-shared Manual Key

**IKE V1: DISABLED**

**IPSEC SETTINGS**

**Lifetime Duration** 28800 seconds

**Lifetime Size** 4608000 kilobytes

**ADDITIONAL OPTIONS**

Diffie-Hellman Group: Null (not selected)

BACK FINISH

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。

Firewall Device Manager | Monitoring | Policies | Objects | Device: ftdv742 | admin Administrator | CISCO SECURE

### Security Policies

SSL Decryption → Identity → Security Intelligence → NAT → Access Control → Intrusion

1 rule

#	NAME	ACTION	SOURCE			DESTINATION			APPLICATIONS	URLS	USERS	ACTIONS
			ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS				
1	Demo_allow	Allow	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY		

Default Action: Access Control Block

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。

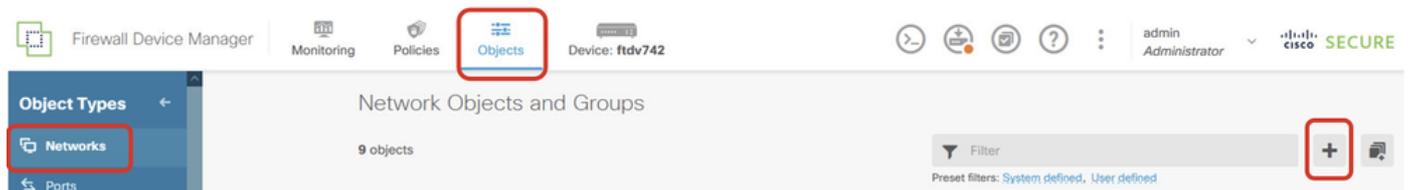
ステップ 3.11 : 設定変更を導入します。



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。



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

Type



Network



Host

Network

192.168.20.0/24

e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

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



Name

local\_red\_192.168.10.0

Description

Type

Network

Host

Network

192.168.10.0/24

*e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60*

CANCEL

OK

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

Type



Network



Host



FQDN



Range

Network

192.168.50.0/24

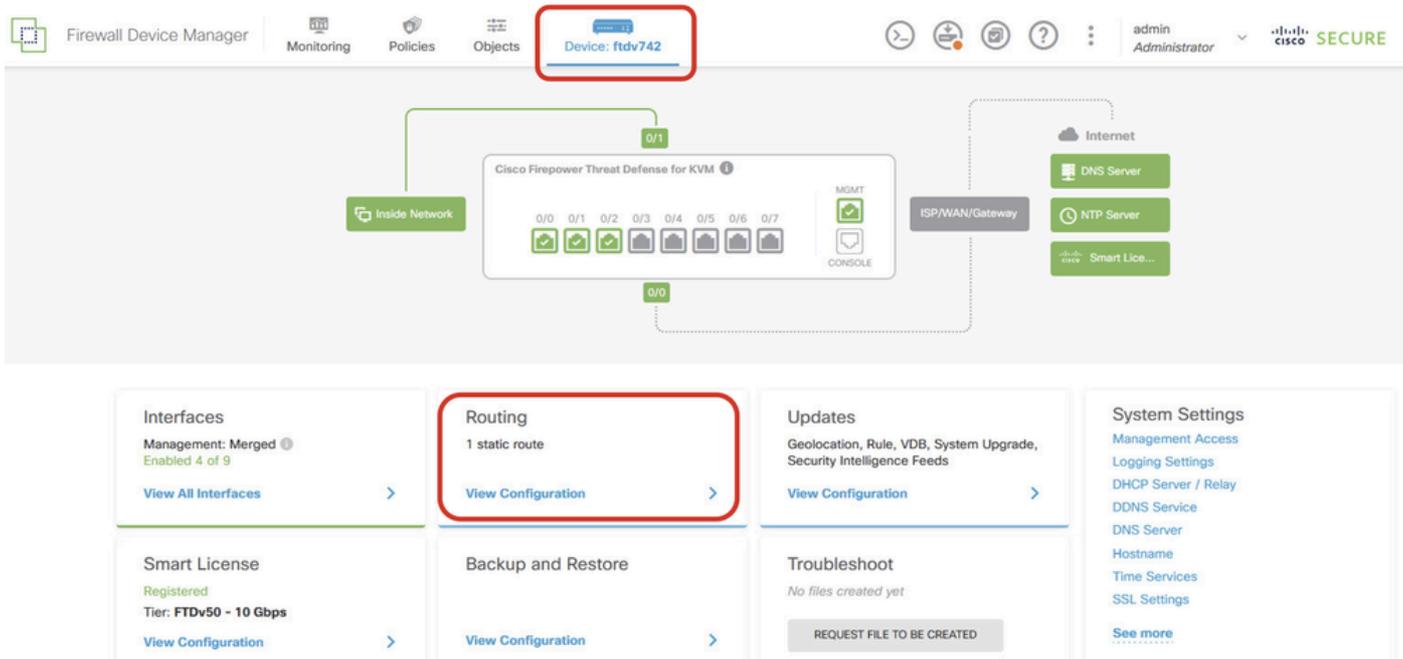
*e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60*

CANCEL

OK

FTD\_Remote\_Network

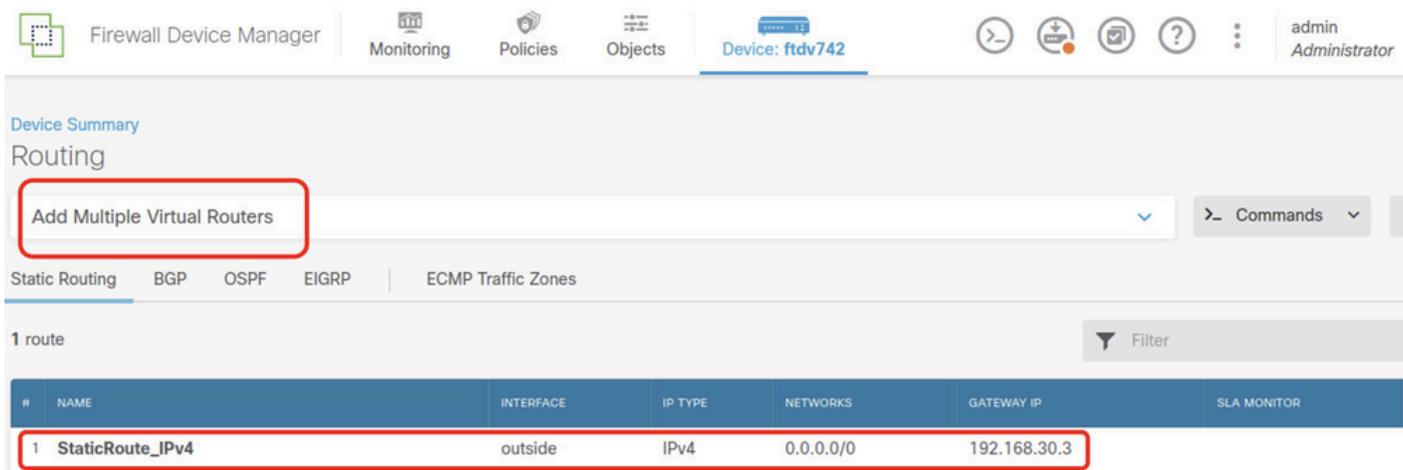
ステップ 4.3 : 最初の仮想ルータを作成します。Device > Routing の順に移動します。View Configuration をクリックします。



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 インター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。



FTD\_Add\_First\_Virtual\_Router1

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

Virtual Route Forwarding (Virtual Routing) Description

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.

How Multiple Virtual Routers Work

Multiple Virtual Router mode is enabled automatically if there is at least one custom Virtual Router.

CREATE FIRST CUSTOM VIRTUAL ROUTER

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)

Add Virtual Router

Name  
vrf\_red

Description

Interfaces  
+  
inside\_red (GigabitEthernet0/1)

CANCEL OK

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

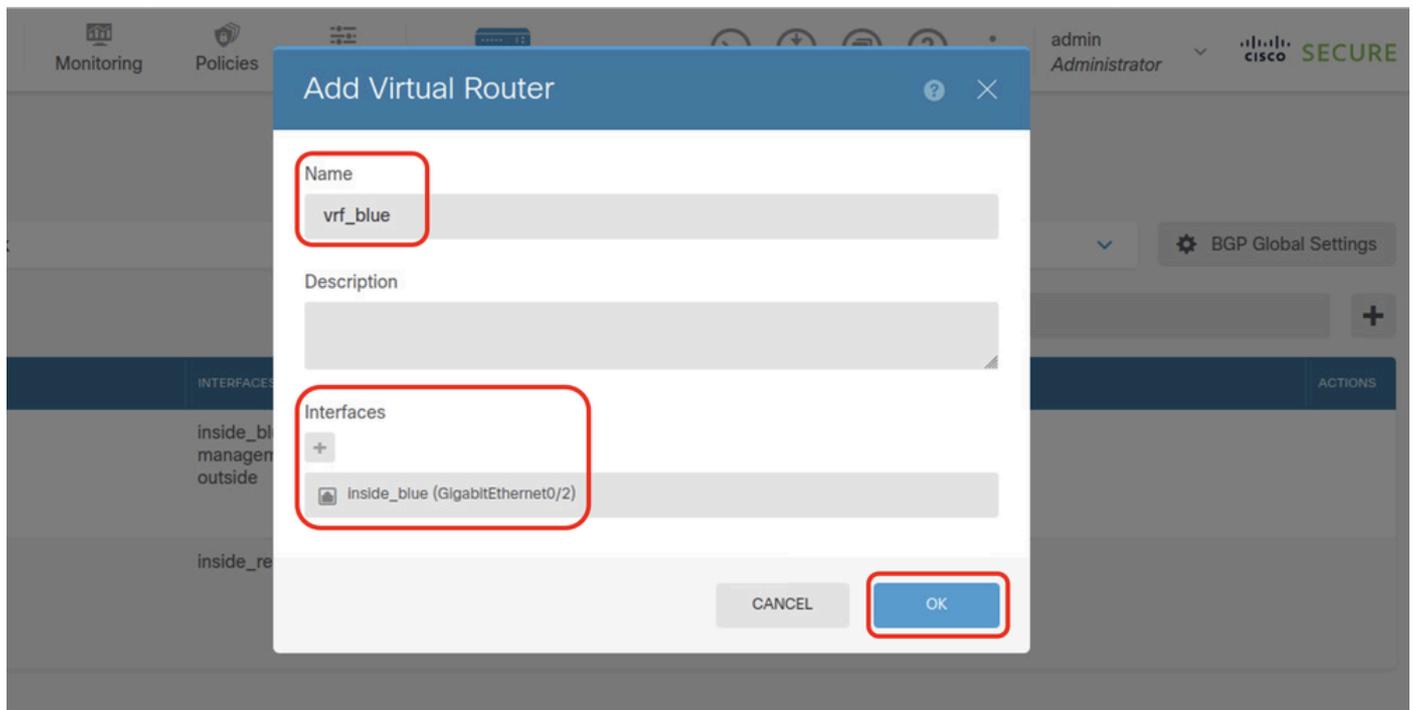
Configuration をクリックします。+ボタンをクリックします。



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)



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

Device Summary  
Virtual Routers

How Multiple Virtual Routers Work

3 virtual routers

#	NAME	INTERFACES	SHOW/TROUBLESHOOT	ACTIONS
1	Global	management outside	<a href="#">Routes</a> <a href="#">Ipv6 routes</a> <a href="#">BGP</a> <a href="#">OSPF</a>	
2	vrf_blue	inside_blue	<a href="#">Routes</a> <a href="#">Ipv6 routes</a> <a href="#">BGP</a> <a href="#">OSPF</a>	View
3	vrf_red	inside_red	<a href="#">Routes</a> <a href="#">Ipv6 routes</a> <a href="#">BGP</a> <a href="#">OSPF</a>	

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。

Device Summary / Virtual Routers  
vrf\_blue

How Multiple Virtual Routers Work

Virtual Router Properties | **Static Routing** | BGP | OSPF | ECMP Traffic Zones

Filter +

FTD\_Create\_Static\_Route\_VRF\_青

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。

Name  
Blue\_to\_ASA

Description

Interface  
demovti (Tunnel1) Belongs to current Router  
N/A

Protocol  
 IPv4  IPv6

Networks  
+  
remote\_192.168.50.0

Gateway  
Please select a gateway Metric  
1

SLA Monitor *Applicable only for IPv4 Protocol type*  
Please select an SLA Monitor

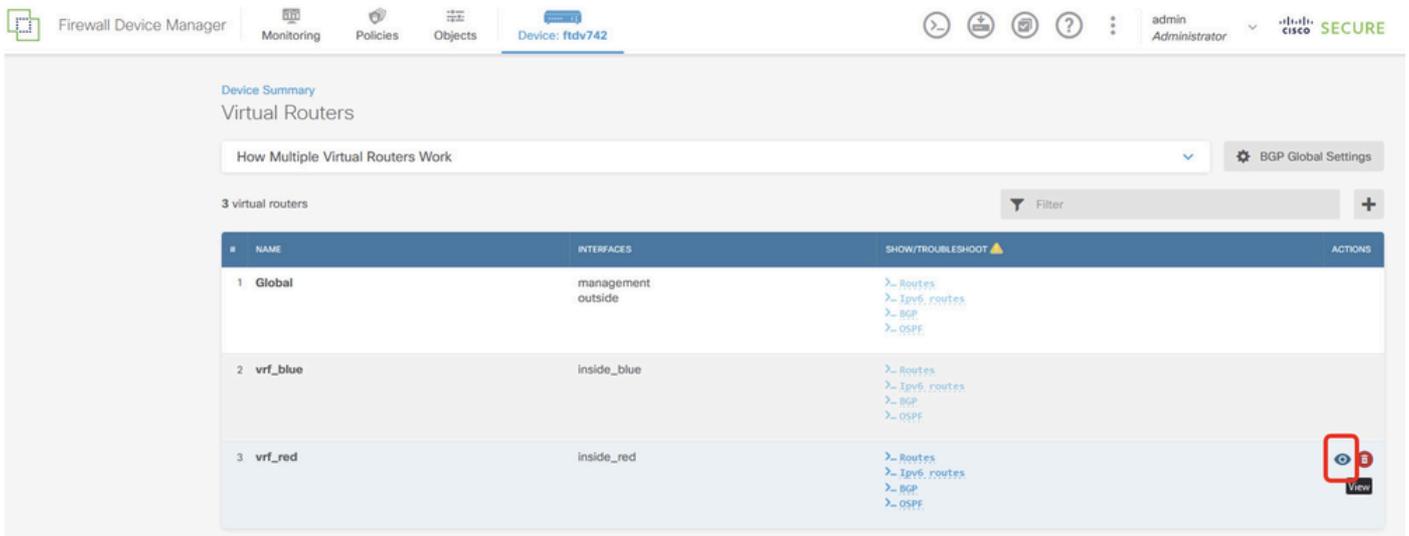
CANCEL OK

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

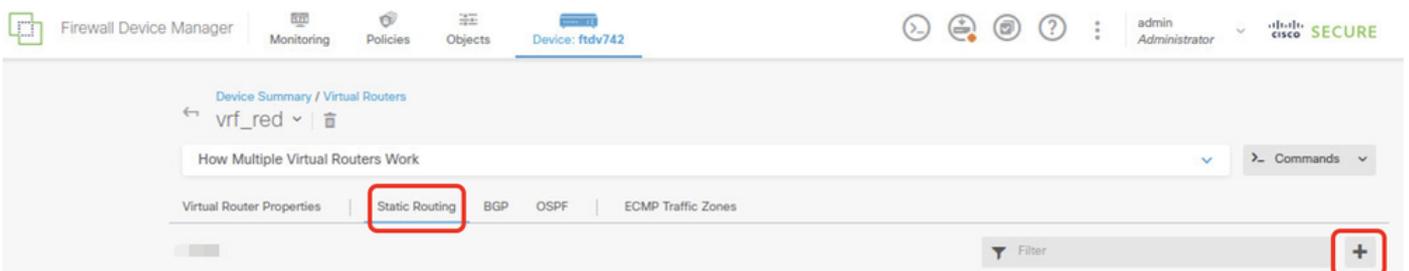
始できます。この例では、リモートエンドポイントが192.168.50.0/24ネットワークを保護しています。

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。



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。



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。

vrf\_red

## Add Static Route



Name

Red\_to\_ASA

Description

Interface

demovti (Tunnel1)

Belongs to current Router

N/A

Protocol



IPv4



IPv6

Networks



remote\_192.168.50.0

Gateway

Please select a gateway

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

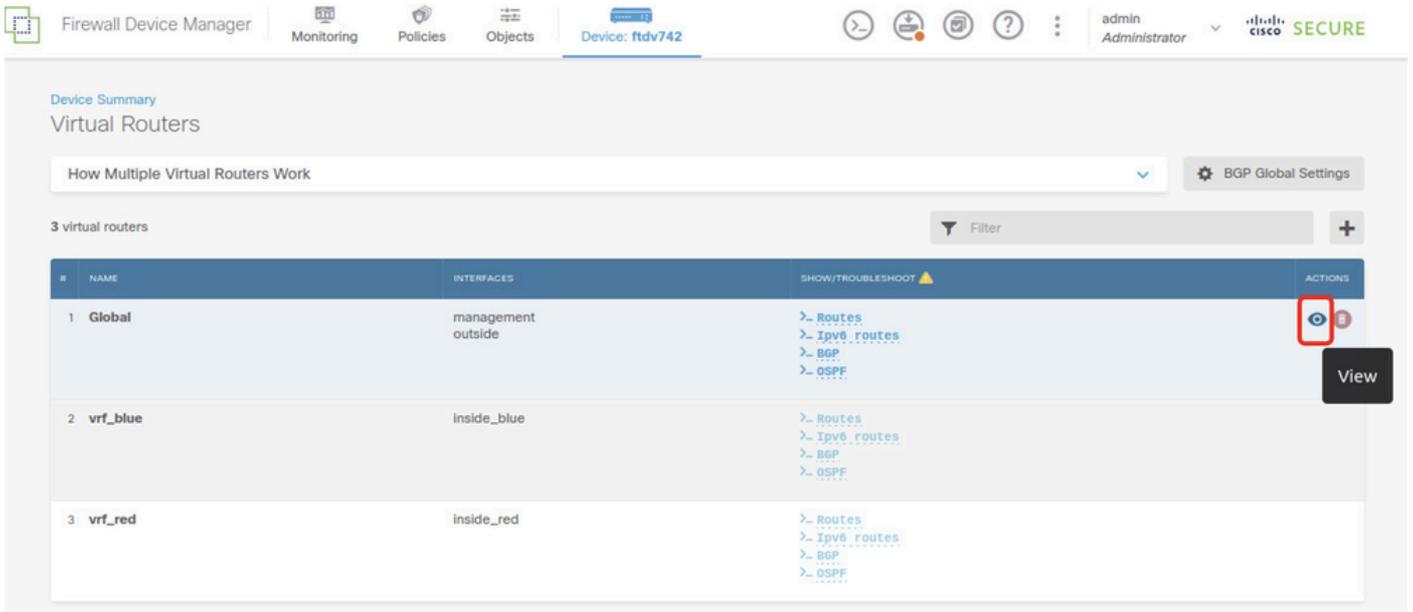
OK

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。



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。



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

S25\_leak\_blue

Description

 The selected interface belongs to a different virtual router. If you create this static route, the route will cross virtual router boundaries, with the risk that traffic from this virtual router will leak into another virtual router. Proceed with caution.

Interface

inside\_blue (GigabitEthernet0/2)

Belongs to different Router

vt\_blue

Protocol

IPv4  IPv6

Networks

+

local\_blue\_192.168.20.0

Gateway

Please select a gateway

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

OK

```
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-l2l  
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): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 192.168.40.1
```

```
#pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
#pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 30, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 192.168.30.1/500, remote crypto endpt.: 192.168.40.1/500
path mtu 1500, ipsec overhead 94(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: A493CC83
current inbound spi : 4CF55637
```

```
inbound esp sas:
spi: 0x4CF55637 (1291146807)
SA State: active
transform: esp-aes-256 esp-sha-512-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, VTI, }
slot: 0, conn_id: 13, crypto-map: __vti-crypto-map-Tunnel1-0-1
sa timing: remaining key lifetime (kB/sec): (4055040/16867)
```

```
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
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): (0.0.0.0/0.0.0.0/0/0)
```

```
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
```

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:

0x00000000 0x00000001

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:

0x00000000 0x00000001

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
C 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
C 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
```

```
C      192.168.20.0 255.255.255.0 is directly connected, inside_blue
L      192.168.20.1 255.255.255.255 is directly connected, inside_blue
SI     192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti
```

```
ftdv742# show route vrf vrf_red
```

```
Routing Table: vrf_red
```

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

```
C      192.168.10.0 255.255.255.0 is directly connected, inside_red
L      192.168.10.1 255.255.255.255 is directly connected, inside_red
SI     192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti
```

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 packets 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
```

## トラブルシューティング

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](#)

[Cisco Secure Firewall ASA VPN CLIコンフィギュレーションガイド9.20](#)

## 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。