

FDMによって管理されるFTD上のPBRを使用したデュアルアクティブルートベースサイト間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](#)

[VPNでの設定](#)

[Site1 FTD VPNの設定](#)

[Site2 FTD VPNの設定](#)

[PBRでの設定](#)

[Site1 FTD PBRの設定](#)

[Site2 FTD PBRの設定](#)

[SLAモニタの設定](#)

[Site1 FTD SLAモニタの設定](#)

[Site2 FTD SLAモニタの設定](#)

[スタティックルートの設定](#)

[Site1 FTDスタティックルートの設定](#)

[Site2のFTDスタティックルートの設定](#)

[確認](#)

[ISP1とISP2の両方が正常に動作します](#)

[VPN](#)

[ルート](#)

[SLAモニタ](#)

[ping テスト](#)

[ISP2が正常に動作している間、ISP1に割り込みが発生する](#)

[VPN](#)

[ルート](#)

[SLAモニタ](#)

[ping テスト](#)

[ISP1が正常に動作している間に、ISP2で中断が発生する](#)

[VPN](#)

[ルート](#)

[SLAモニタ](#)

[ping テスト](#)

[トラブルシューティング](#)

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上でPBRを使用してデュアルアクティブルートベースのサイト間VPN(DVVPN)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
- ポリシーベースルーティング(PBR)の基本的な知識
- Internet Protocol Service Level Agreement (IP SLA ; インターネットプロトコルサービスレベル契約) 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

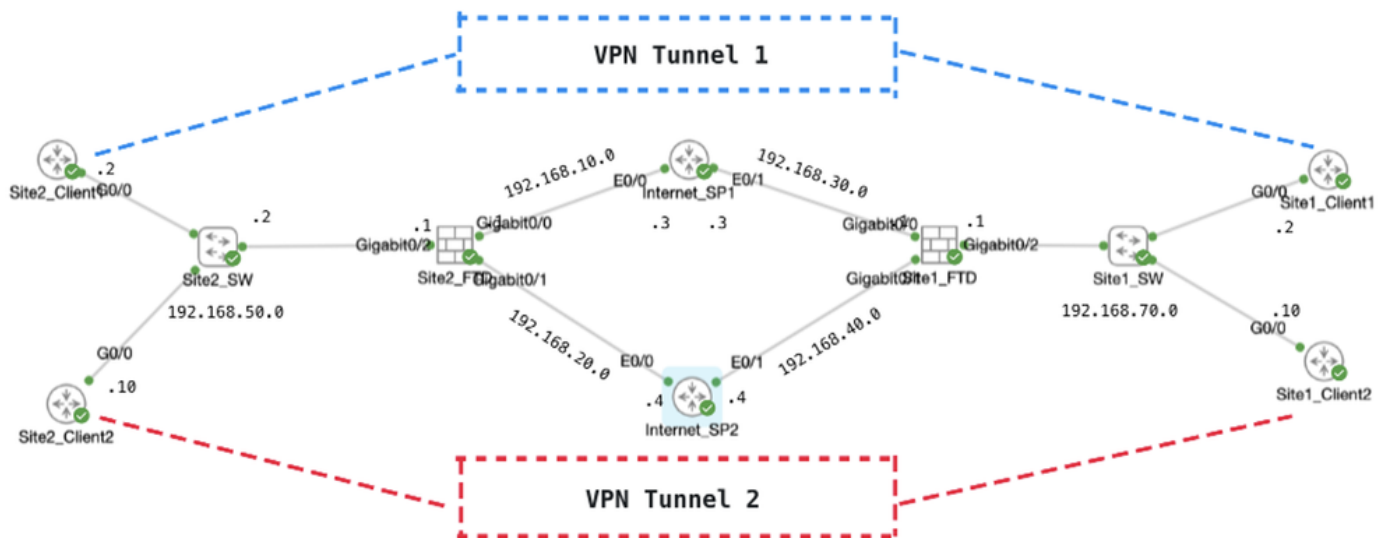
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントでは、FTDでデュアルアクティブルートベースのサイト間VPNを設定する方法について説明します。この例では、Site1とSite2の両方のFTDに、両方のISPとのサイト間VPNを同時に確立するデュアルアクティブISP接続があります。デフォルトでは、VPNトラフィックはISP1経由でTunnel 1（青い線）を通過します。特定のホストでは、トラフィックはISP2（赤い線）を介してトンネル2を通過します。ISP1で中断が発生すると、トラフィックはバックアップとしてISP2に切り替わります。逆に、ISP2で中断が発生すると、トラフィックはバックアップとしてISP1に切り替わります。この例では、これらの要件を満たすために、ポリシーベースルーティング(PBR)とインターネットプロトコルサービスレベル契約(IP SLA)を使用しています。

設定

ネットワーク図



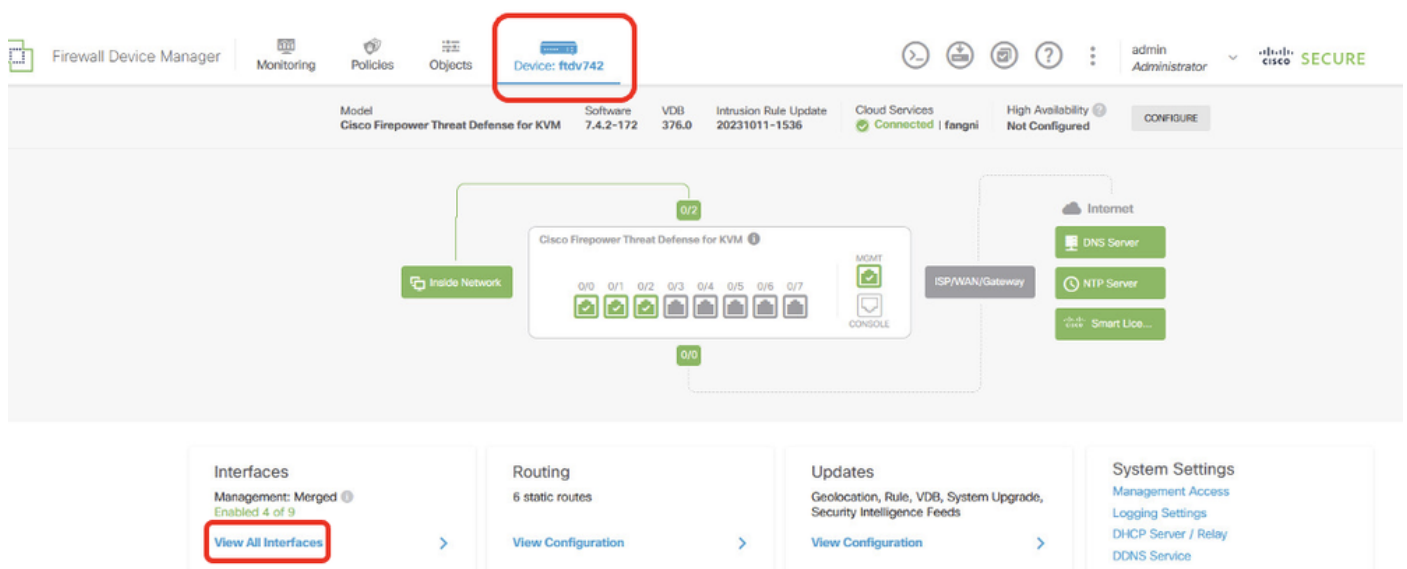
トポロジ

VPNでの設定

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。Site1とSite2の両方のクライアントが、ゲートウェイとしてFTDの内部IPアドレスを使用しています。

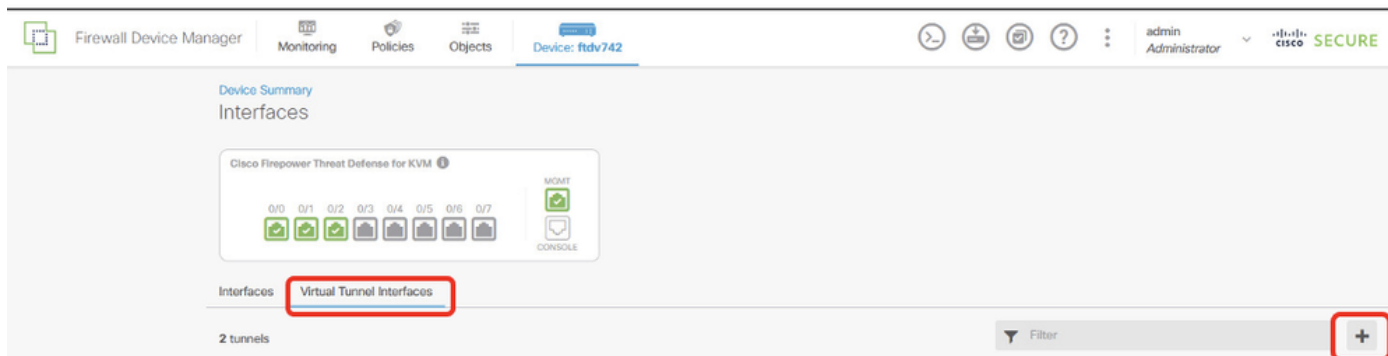
Site1 FTD VPNの設定

ステップ 1 : ISP1とISP2の仮想トンネルインターフェイスを作成します。Site1 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。



Site1FTD_View_All_インターフェイス

ステップ 2 : Virtual Tunnel Interfacesタブをクリックし、次に+ボタンをクリックします。



サイト1FTD_作成_VTI

ステップ 3 : VTIの詳細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 : 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。

Name Status

demovti ☒

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

Site1FTD_VTI_Details_Tunnel1_ISP1

- 名前 : demovti_sp2
- トンネルID:2

- トンネル送信元 : outside2(GigabitEthernet0/1)
- IPアドレスとサブネットマスク : 169.254.20.11/24
- 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。

The screenshot shows a configuration window for a Site-to-Site VPN. The following fields are highlighted with red boxes:

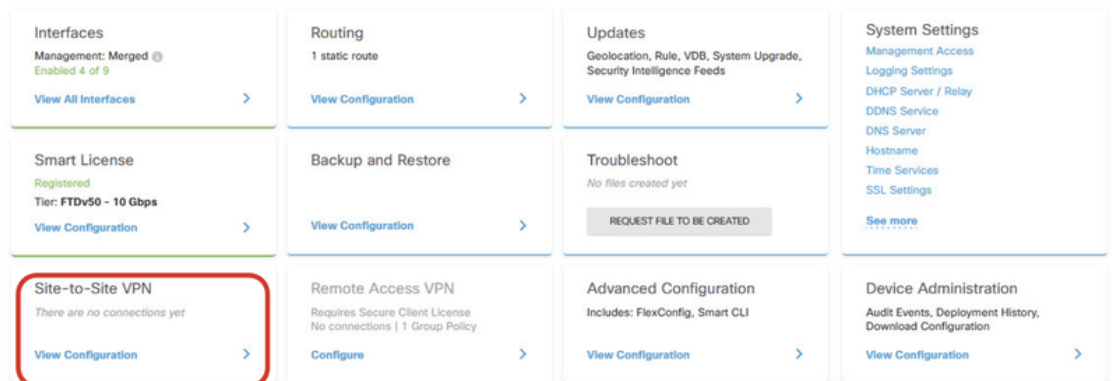
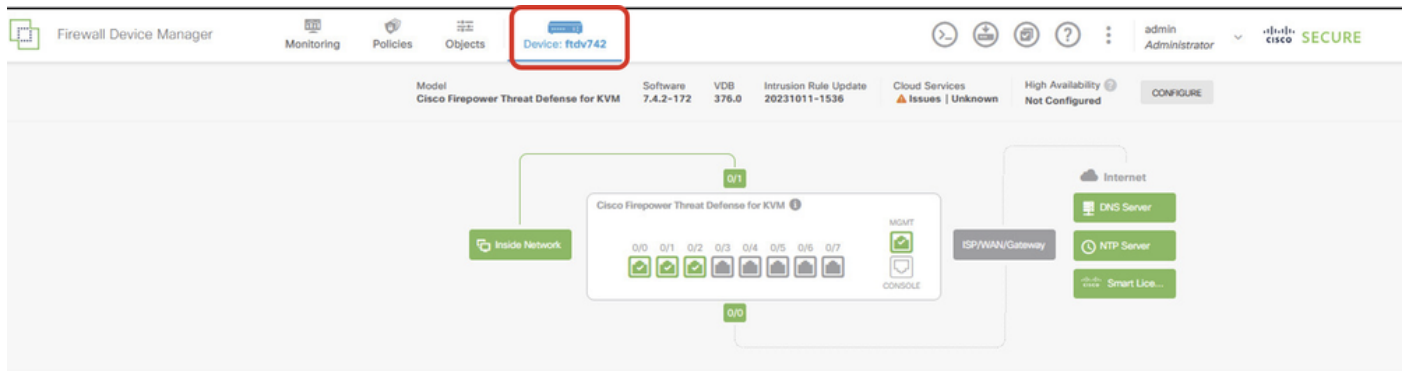
- Name:** demovti_sp2
- Status:** A toggle switch is turned on.
- Tunnel ID:** 2
- Tunnel Source:** outside2 (GigabitEthernet0/1)
- IP Address and Subnet Mask:** 169.254.20.11 / 24

Below the IP Address and Subnet Mask field, there is a note: *e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0*

At the bottom right, there are two buttons: **CANCEL** and **OK**. The **OK** button is highlighted with a red box.

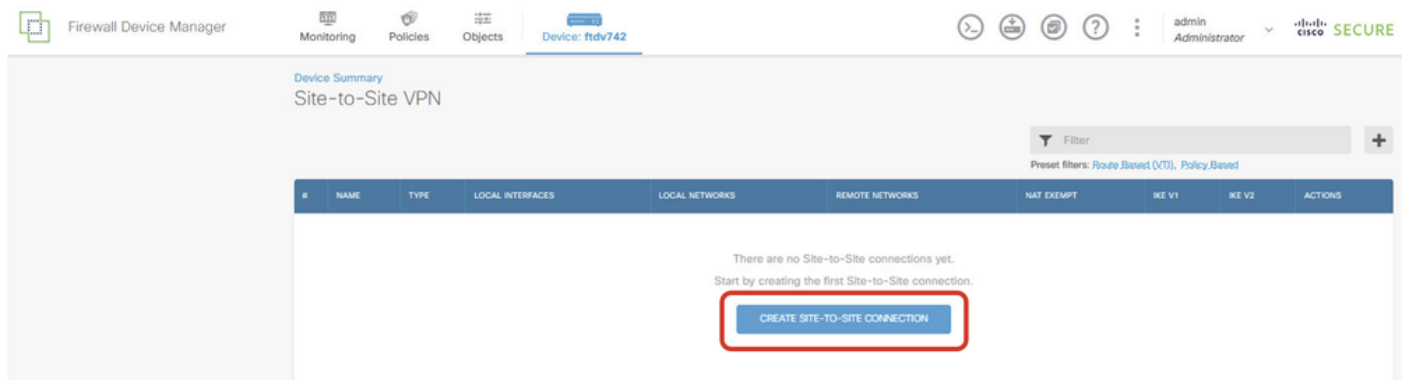
Site1FTD_VTI_Details_Tunnel2_ISP2

ステップ 4 : 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。



サイト1FTD_View_サイト2サイト_VPN

ステップ 5：ISP1経由の新しいサイト間VPNの作成を開始します。CREATE SITE-TO-SITE CONNECTIONボタンをクリックするか、+ボタンをクリックします。



サイト1FTD_作成_サイト間_接続

ステップ 5.1：エンドポイントに関する必要な情報を提供します。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3で作成)
- リモートIPアドレス：192.168.10.1 (これはSite2 FTD ISP1の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: 192.168.10.1

CANCEL **NEXT**

サイト1FTD_ISP1_サイト間_VPN_定義_エンドポイント

ステップ 5.2 : 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

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

EDIT...

IPSec Proposal

None selected

EDIT...

Site1FTD_Edit_IKE_Policy (ポリシー)

ステップ 5.3 : 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、Create New IKE Policyをクリックして新しいポリシーを作成できます。

この例では、既存のIKEポリシーAES-SHA-SHAを切り替え、デモ用に新しいIKEポリシーを作成します。OKボタンをクリックして保存します。

- 名前 : AES256_DH14_SHA256_SHA256
- 暗号化 : AES、AES256
- DHグループ : 14
- 整合性ハッシュ : SHA、SHA256
- PRFハッシュ : SHA、SHA256
- ライフタイム : 86400 (デフォルト)

The screenshot shows the 'Add IKE v2 Policy' configuration window. The left pane displays a list of policies with a filter bar. The 'AES-SHA-SHA' policy is selected, and the 'Create New IKE Policy' button is highlighted. The right pane shows the configuration for the selected policy, with fields for Priority, Name, State, Encryption, Diffie-Hellman Group, Integrity Hash, Pseudo Random Function (PRF) Hash, and Lifetime. Red boxes highlight the 'Create New IKE Policy' button, the 'AES-SHA-SHA' policy, and the configuration fields.

Add IKE v2 Policy

Filter

☐ AES-GCM-NULL-SHA

☒ AES-SHA-SHA

☐ DES-SHA-SHA

Create New IKE Policy

OK

Priority: 1

Name: AES256_DH14_SHA256_SHA256

State: ☒

Encryption: AES x AES256

Diffie-Hellman Group: 14

Integrity Hash: SHA x SHA256

Pseudo Random Function (PRF) Hash: SHA x SHA256

Lifetime (seconds): 86400

Between 120 and 2147483647 seconds.

CANCEL

OK

サイト1FTD_Add_New_IKE_Policy

Filter

AES-GCM-NULL-SHA

i

AES-SHA-SHA

i

DES-SHA-SHA

i

AES256_DH14_SHA256_SHA256

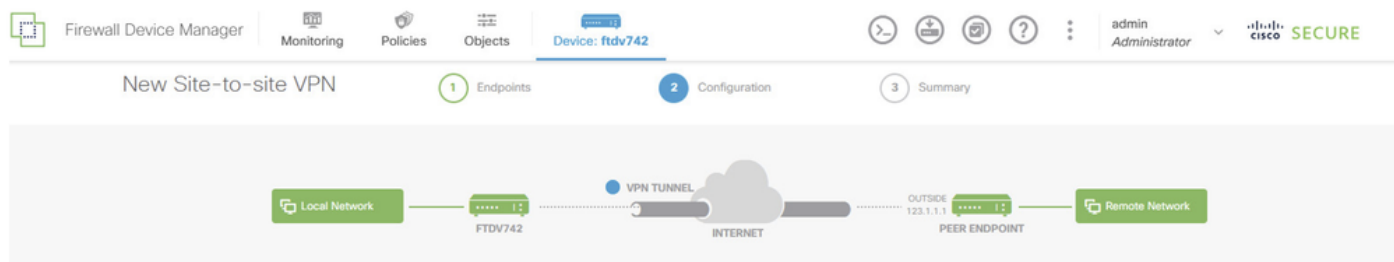
i

Create New IKE Policy

OK

Site1FTD_Enable_New_IKE_Policy (ポリシー)

ステップ 5.4 : 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

EDIT...

IPSec Proposal

None selected

EDIT...

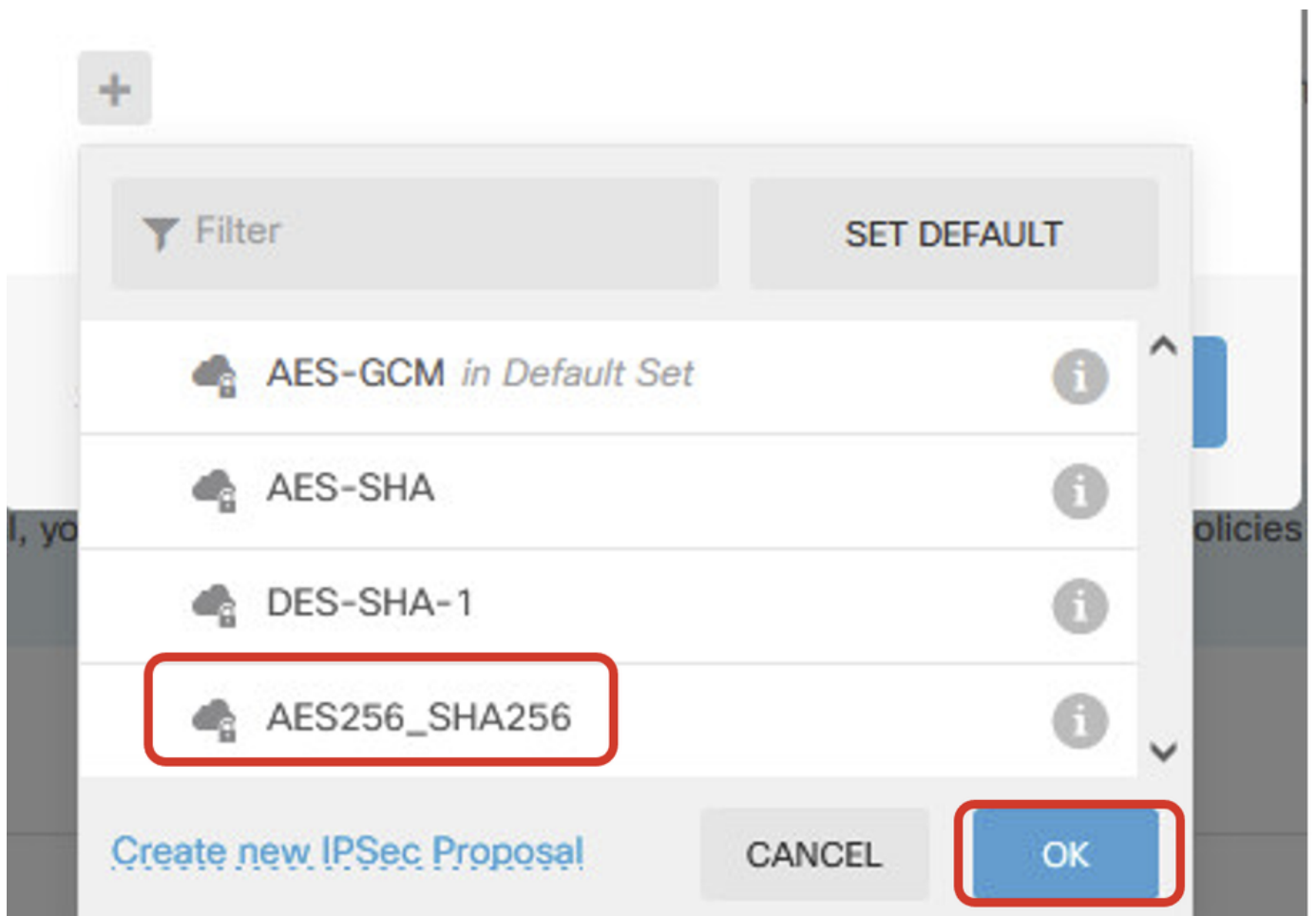


Site1FTD_Edit_IKE_Proposal (提案)

ステップ 5.5 : IPSecプロポーザルの場合は、事前に定義されているプロトコルを使用するか、Create new IPSec Proposalをクリックして新しいプロトコルを作成できます。この例では、デモ用に新しいプロファイルを作成します。OKボタンをクリックして保存します。

- 名前 : AES256_SHA256
- 暗号化 : AES、AES256
- 整合性ハッシュ : SHA1、SHA256

Site1FTD_Add_New_IKE_Proposal



Site1FTD_Enable_New_IKE_Proposal

ステップ 5.6 : ページを下にスクロールして、事前共有キーを設定します。NextButtonをクリックします。

この事前共有キーをメモし、後でSite2 FTDで設定します。

Firewall Device Manager

MonitoringPoliciesObjectsDevice: ftdv742

FTDV742INTERNETPEER ENDPOINT

adminAdministrator

CISCOSECURITY

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 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

EDIT...

IPSec Proposal

Custom set selected

EDIT...

Authentication Type

Pre-shared Manual Key

Certificate

Local Pre-shared Key

Remote Peer Pre-shared Key

BACK

NEXT

サイト1FTD_Configure_Pre_Shared_Key

ステップ 5.7：VPN設定を確認します。変更する必要がある場合は、BACK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

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

VPN Access
Interface

 demovti (169.254.10.1)



Peer IP Address

192.168.10.1

IKE V2

IKE Policy

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

IPSec Proposal

aes,aes-256-sha-1,sha-256

Authentication
Type

Pre-shared Manual Key

IKE V1: DISABLED

IPSEC SETTINGS

Lifetime
Duration

28800 seconds

Lifetime Size

4608000 kilobytes

ADDITIONAL OPTIONS

Diffie-Hellman

Null (not selected)

i Information is copied to the clipboard when you click Finish. You must allow the browser to access your clipboard for the copy to be successful.

BACK

FINISH

Site1FTD_ISP1_Review_VPN_Config_サマリー

手順 6 : ISP2を経由して新しいサイト間VPNを作成するには、ステップ5. を繰り返します。

Demo_S2S_SP2 Connection Profile

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

VPN Access Interface

demovti_sp2 (169.254.20.11)



Peer IP Address

192.168.20.1

IKE V2

IKE Policy

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

IPSec Proposal

aes,aes-256-sha-1,sha-256

Authentication Type

Pre-shared Manual Key

IKE V1: DISABLED

IPSEC SETTINGS

Lifetime Duration

28800 seconds

Lifetime Size

4608000 kilobytes

i Information is copied to the clipboard when you click Finish. You must allow the browser to access your clipboard for the copy to be successful.

Diffie-Hellman

Null (not selected)

BACK

FINISH

Site1FTD_ISP2_Review_VPN_Config_サマリー

手順 7: トラフィックがFTDを通過できるようにアクセスコントロールルールを作成します。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ます。

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	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS	APPLICATIONS	URLS	USERS	ACTIONS
1	Demo_allow	Allow	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	

Default Action: Access Control Block

Site1FTD_Allow_Access_Control_Rule_Example

ステップ8: (オプション) インターネットにアクセスするためにクライアントにダイナミック NATが設定されている場合、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。

デモ目的で、この例ではインターネットにアクセスするためにクライアント用にダイナミック NATを設定します。したがって、NAT免除ルールが必要です。

Policies > NATの順に移動します。+ボタンをクリックします。詳細を入力して、OKをクリックします。

- タイトル：NAT免除
- 配置：自動NATルールの前
- タイプ：スタティック
- 送信元インターフェイス：内部
- 宛先：任意
- 元の送信元アドレス：192.168.70.0/24
- 変換後の送信元アドレス：192.168.70.0/24
- 元の宛先アドレス：192.168.50.0/24
- 変換後の宛先アドレス：192.168.50.0/24
- ルートルックアップが有効な場合

The screenshot shows the 'Add NAT Rule' dialog box in the Cisco Secure Firewall Device Manager. The dialog is titled 'Add NAT Rule' and has a close button (X) in the top right corner. The 'Title' field is set to 'NAT Exempt'. The 'Create Rule for' dropdown is set to 'Manual NAT'. The 'Status' toggle is turned on. The 'Placement' dropdown is set to 'Before Auto NAT Rules'. The 'Type' dropdown is set to 'Static'. The 'Packet Translation' tab is selected, showing the 'ORIGINAL PACKET' and 'TRANSLATED PACKET' sections. In the 'ORIGINAL PACKET' section, the 'Source Interface' is 'inside', 'Source Address' is 'inside_192.168.70', 'Source Port' is 'Any', 'Destination Address' is 'peer_192.168.50.0', and 'Destination Port' is 'Any'. In the 'TRANSLATED PACKET' section, the 'Destination Interface' is 'Any', 'Source Address' is 'inside_192.168.70', 'Source Port' is 'Any', 'Destination Address' is 'peer_192.168.50.0', and 'Destination Port' is 'Any'. The 'Show Diagram' toggle is turned off. The 'OK' button is highlighted with a red box.

Site1FTD_Nat_Exempt_Rule

Add NAT Rule

Title
NAT Exempt

Create Rule for
Manual NAT

Status
☒

Manual NAT rules allow the translation of the source as well as the destination address of a network packet. Destination and port translation are optional. You can place manual NAT rules either before or after Auto NAT rules and insert the rules at a specific location.

Placement
Before Auto NAT Rules

Type
Static

Packet Translation **Advanced Options**

☐ Translate DNS replies that match this rule

☐ Falthrough to Interface PAT (Destination Interface)

☒ Perform route lookup for Destination interface

☐ Do not proxy ARP on Destination Interface

Show Diagram ☐

CANCEL **OK**

サイト1FTD_Nat_Exempt_Rule_2

Firewall Device Manager | Monitoring | Policies | Objects | Device: ftdv742

admin Administrator | cisco SECURE

Security Policies

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

3 rules

#	NAME	TYPE	INTERFACES	ORIGINAL PACKET				TRANSLATED PACKET				ACTIONS
				SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	
Manual NAT Rules												
1	NAT Exempt	STATIC	Inside Any	inside_192.1...	peer_192.16...	ANY	ANY	inside_192.1...	peer_192.16...	ANY	ANY	
Manual NAT Rules (After)												
1	ISP1NatRule	DYNAMIC	Inside outside	any-ipv4	ANY	ANY	ANY	Interface	ANY	ANY	ANY	
3	ISP2NatRule	DYNAMIC	Inside outside2	any-ipv4	ANY	ANY	ANY	Interface	ANY	ANY	ANY	

Site1FTD_Nat_Rule_の概要

ステップ 9： 設定変更を導入します。

Firewall Device Manager | Monitoring | Policies | Objects | **Device: ftdv742**

admin Administrator | cisco SECURE

Site1FTD_Deployment_Changes

Site2 FTD VPNの設定

ステップ 10 : Site2 FTDの対応するパラメータで、ステップ1からステップ9を繰り返します。

DemoS2S Connection Profile

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

VPN Access Interface

demovti25 (169.254.10.2)

Peer IP Address

192.168.30.1

IKE V2

IKE Policy

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

IPSec Proposal

aes,aes-256-sha-1,sha-256

Authentication Type

Pre-shared Manual Key

IKE V1: DISABLED

IPSEC SETTINGS

Lifetime Duration

28800 seconds

Lifetime Size

4608000 kilobytes

Information is copied to the clipboard when you click Finish. You must allow the browser to access your clipboard for the copy to be successful.

Diffie-Hellman Group

Null (not selected)

BACK

FINISH

Site2FTD_ISP1_Review_VPN_Config_サマリー

Demo_S2S_SP2 Connection Profile

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

VPN Access Interface demovti_sp2 (169.254.20.12)



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, aes,aes-256-sha,sha256-sha,sha256-14

IPSec Proposal aes,aes-256-sha-1,sha-256

Authentication Type Pre-shared Manual Key

IKE V1: DISABLED

IPSEC SETTINGS

Lifetime Duration 28800 seconds

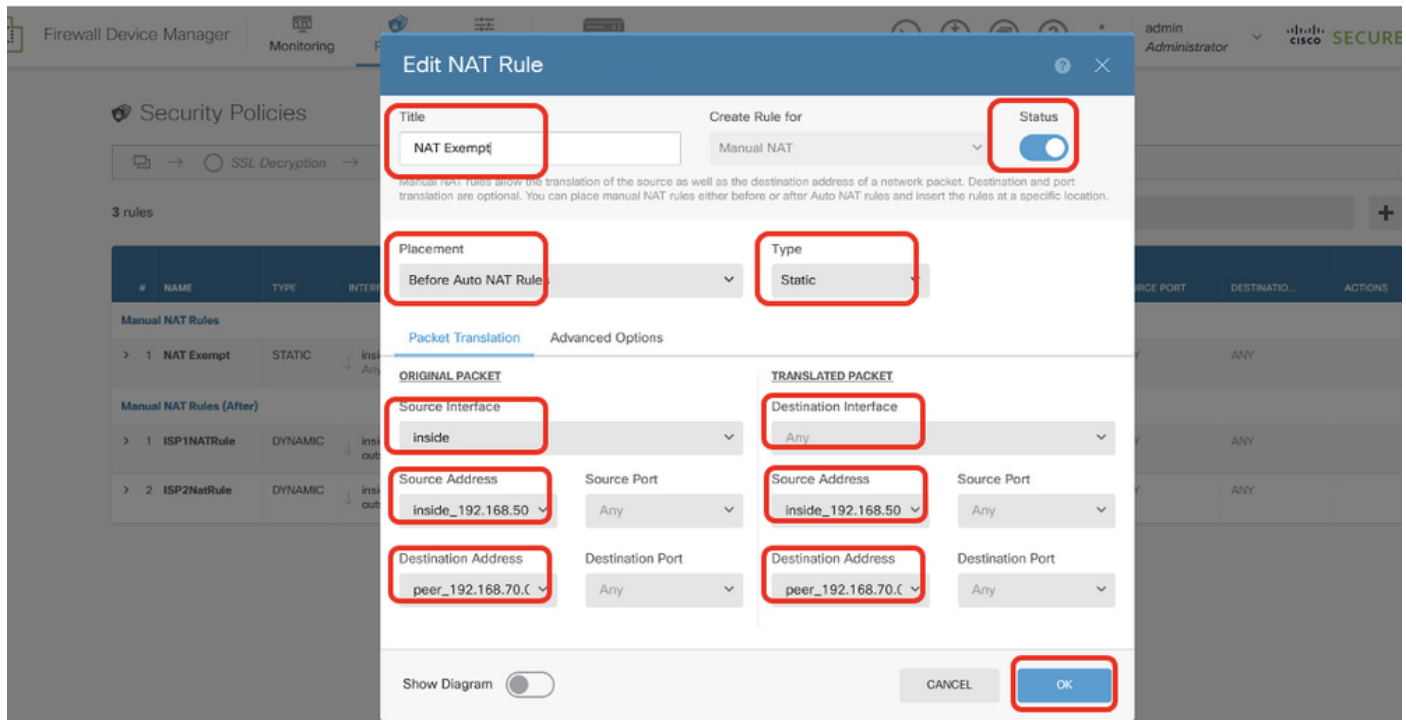
Lifetime Size 4608000 kilobytes

Information is copied to the clipboard when you click Finish. You must allow the browser to access your clipboard for the copy to be successful.

Diffie-Hellman Group Null (not selected)

BACK

FINISH

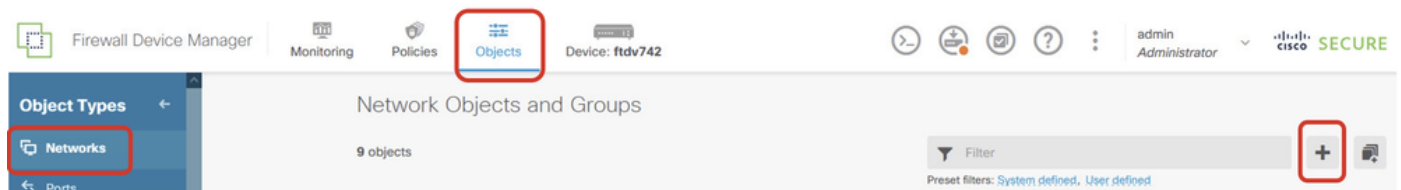


Site2FTD_Nat_Exempt_Rule

PBRでの設定

Site1 FTD PBRの設定

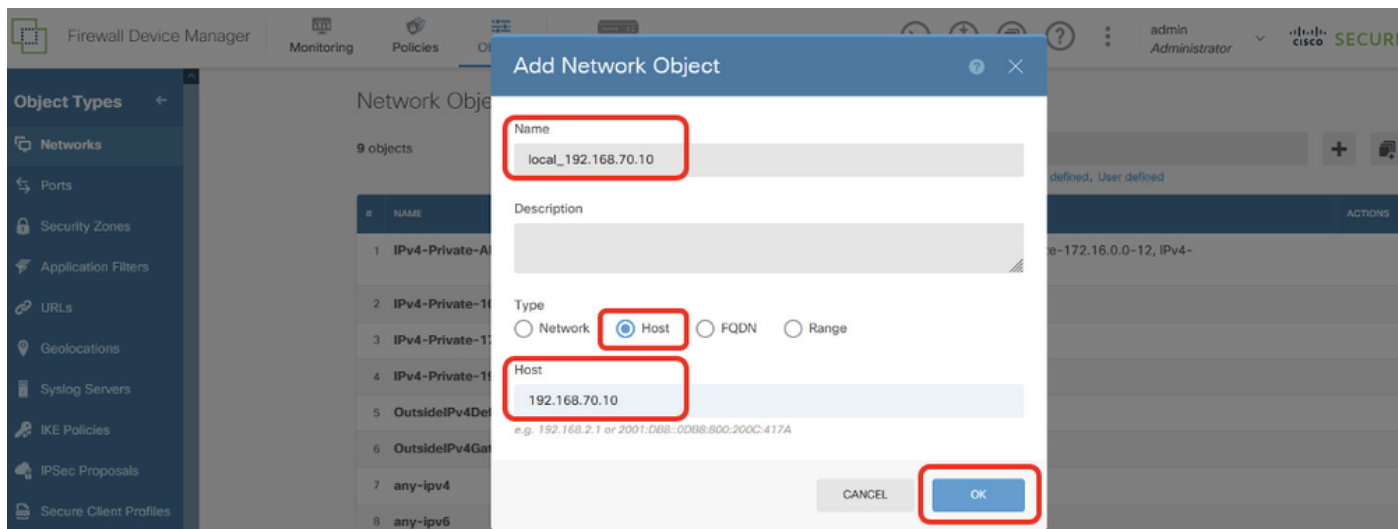
ステップ 11 Site1 FTDのPBRアクセスリストで使用する新しいネットワークオブジェクトを作成します。 Objects > Networksに移動し、+ボタンをクリックします。



Site1FTD_Create_Network_オブジェクト

ステップ11.1: Site1 Client2のIPアドレスのオブジェクトを作成します。 必要な情報を提供します。 [OK] ボタンをクリックします。

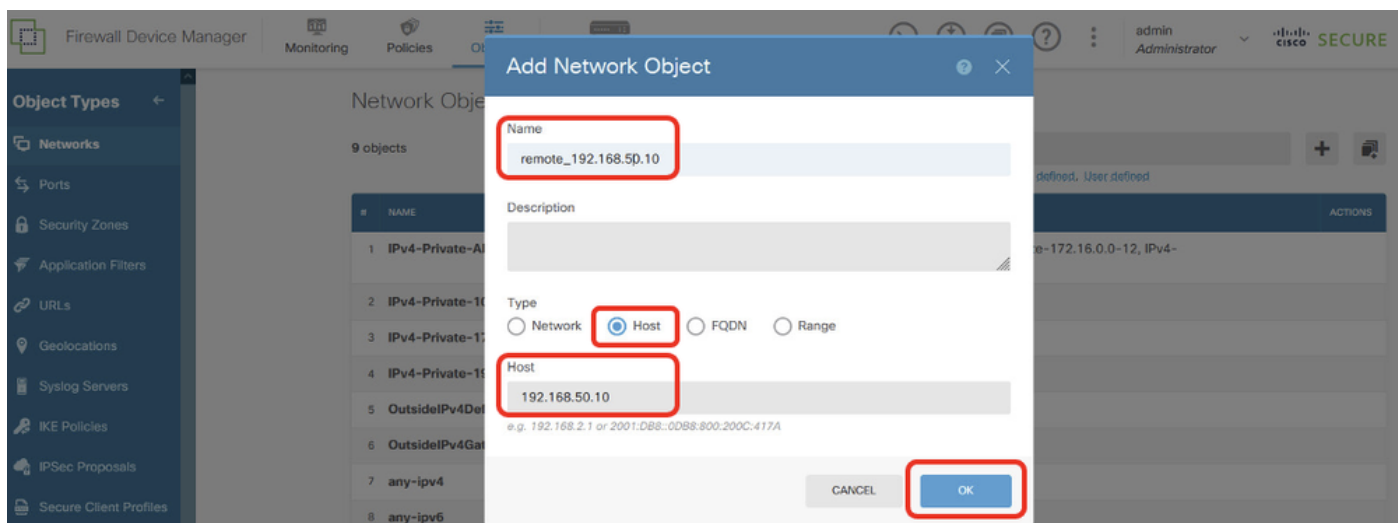
- 名前 : local_192.168.70.10
- タイプ : ホスト
- ホスト : 192.168.70.10



サイト1FTD_サイト1FTD_PBR_LocalObject

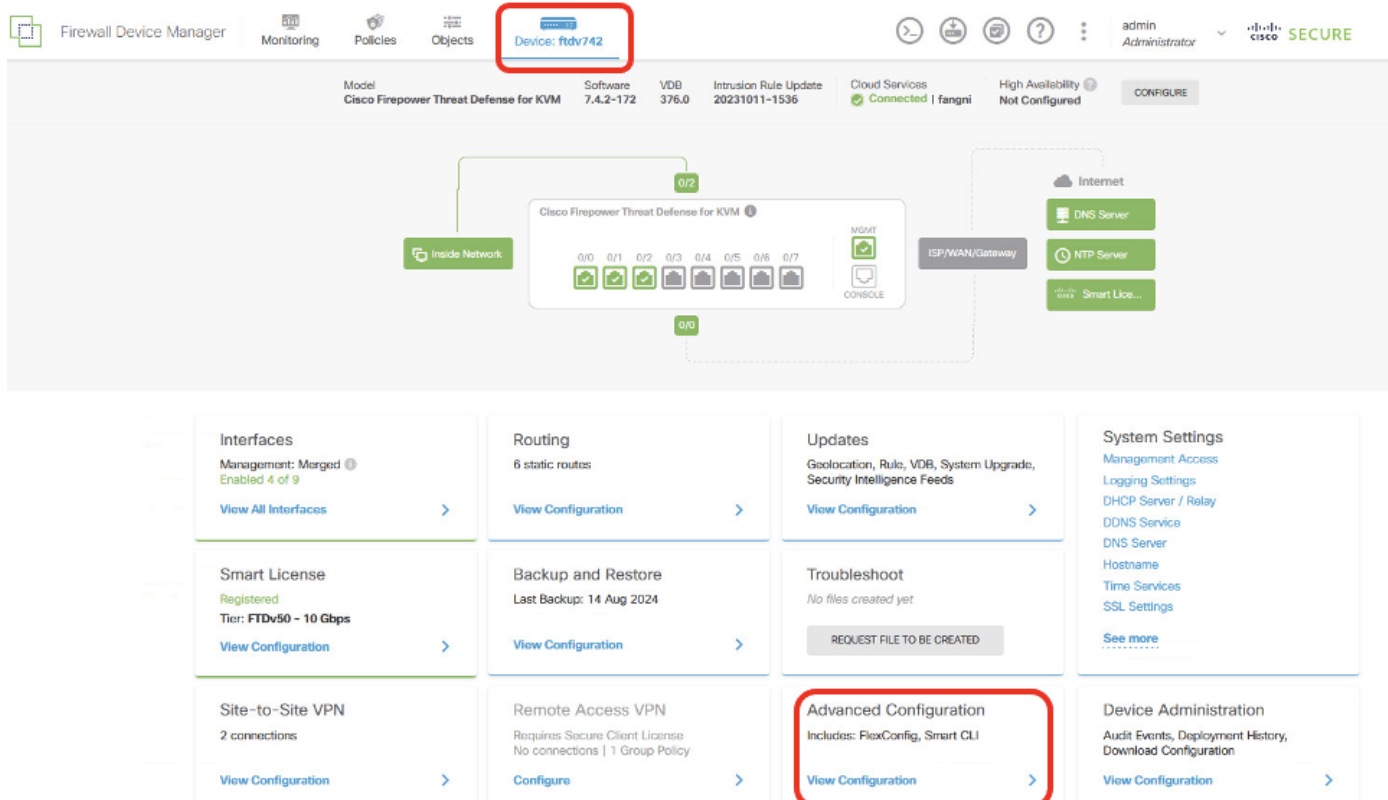
ステップ 11.2 : Site2 Client2 IPアドレスのオブジェクトを作成します。必要な情報を提供します。OKボタンをクリックします。

- 名前 : remote_192.168.50.10
- タイプ : ホスト
- ホスト : 192.168.50.10



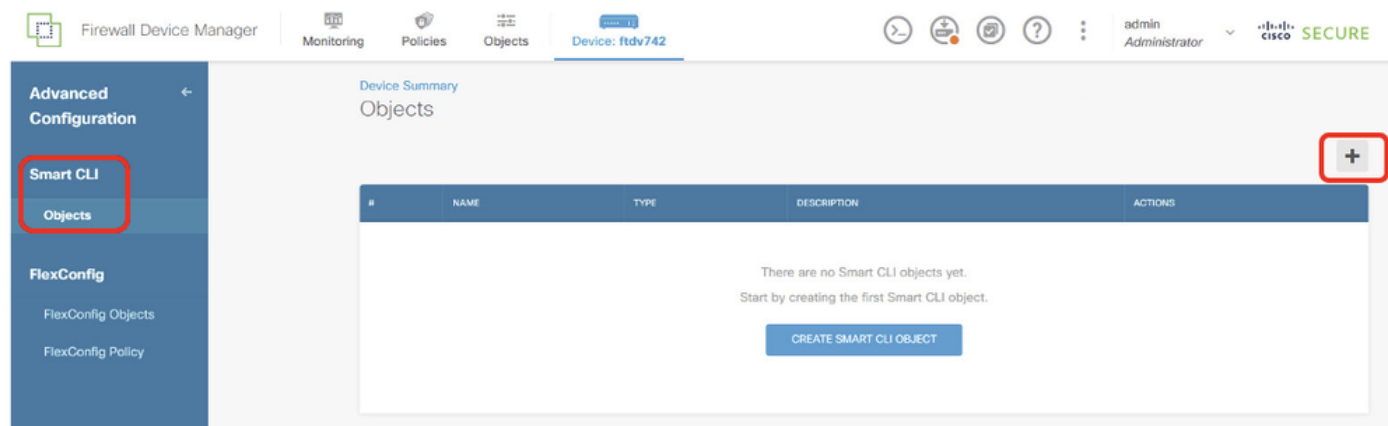
Site1FTD_PBR_RemoteObject

ステップ 12PBR用の拡張アクセスリストを作成します。Device > Advanced Configurationの順に移動します。View Configurationをクリックします。



Site1FTD_View_Advanced_設定

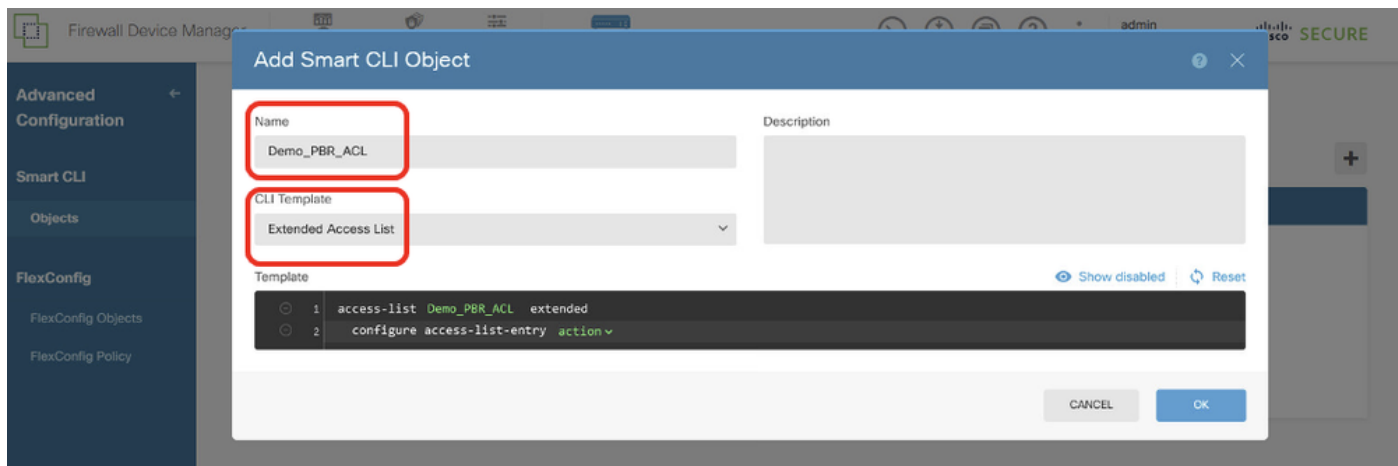
ステップ 12.1 : Smart CLI > Objectsの順に移動します。+ボタンをクリックします。



Site1FTD_Add_SmartCLI_オブジェクト

ステップ 12.2 : オブジェクトの名前を入力し、CLIテンプレートを選択します。

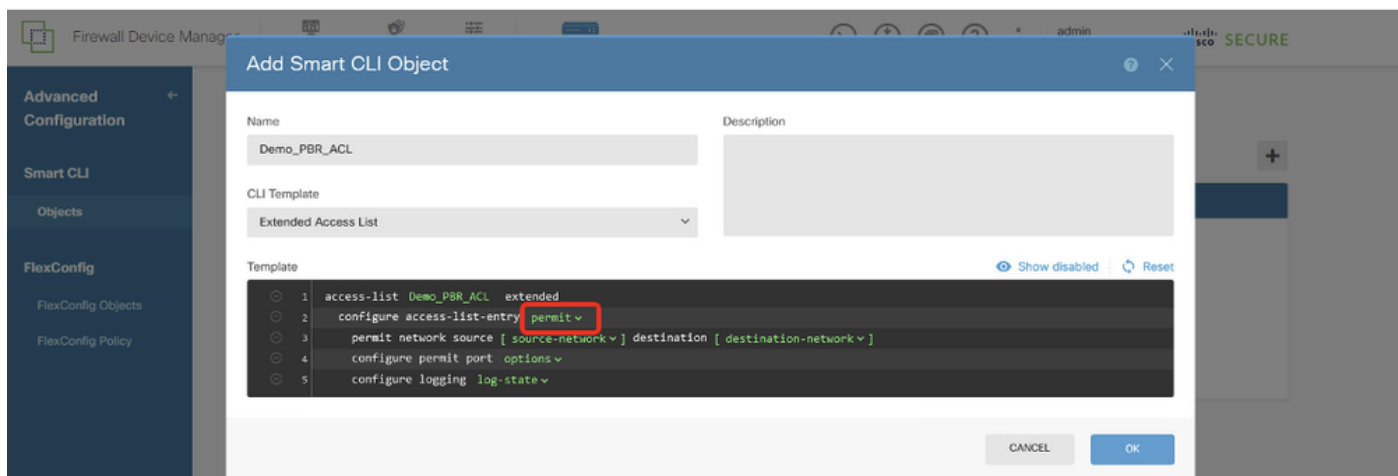
- 名前 : Demo_PBR_ACL
- CLIテンプレート : 拡張アクセスリスト



サイト1FTD_作成_PBR_ACL_1

ステップ 12.3 : Templateに移動して設定します。OKボタンをクリックして保存します。

2行目で、actionをクリックします。[Permit] を選択します。

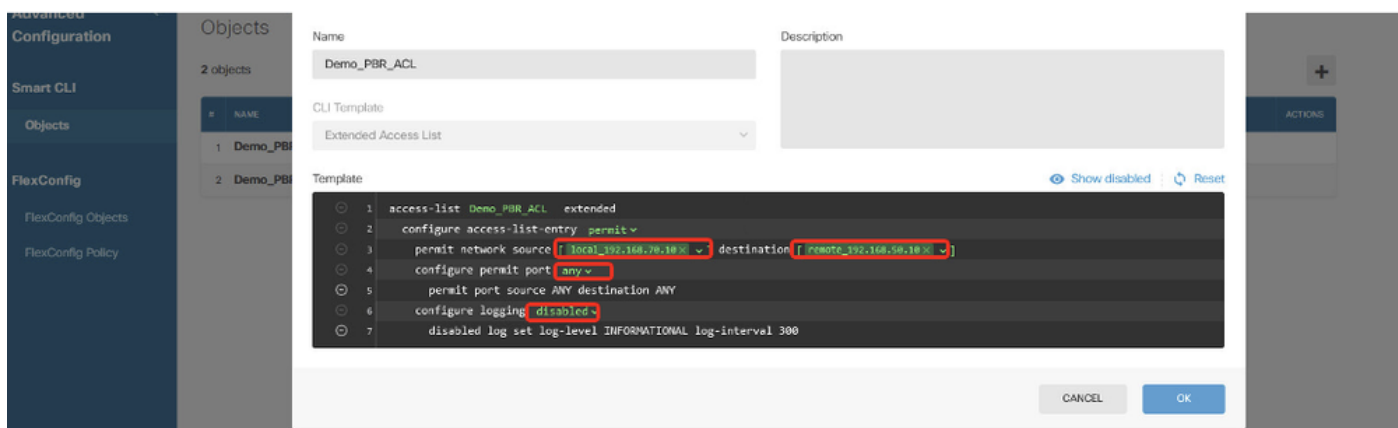


サイト1FTD_Create_PBR_ACL_2

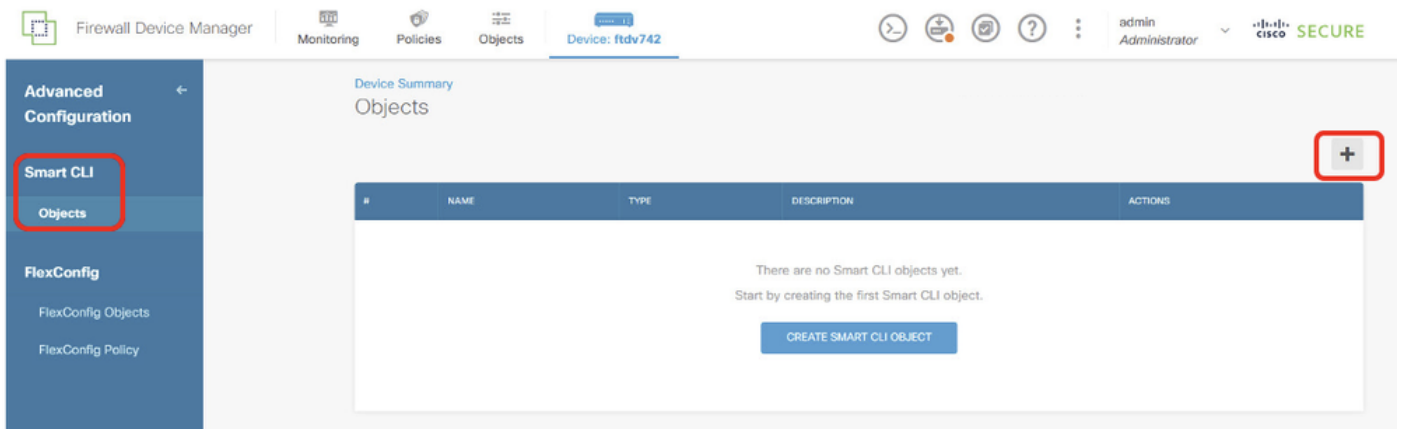
3行目で、source-networkをクリックします。local_192.168.70.10を選択します。destination-networkをクリックします。remote_192.168.50.10を選択します。

4行目で、optionsをクリックし、anyを選択します。

6行目で、log-stateをクリックし、disabledを選択します。



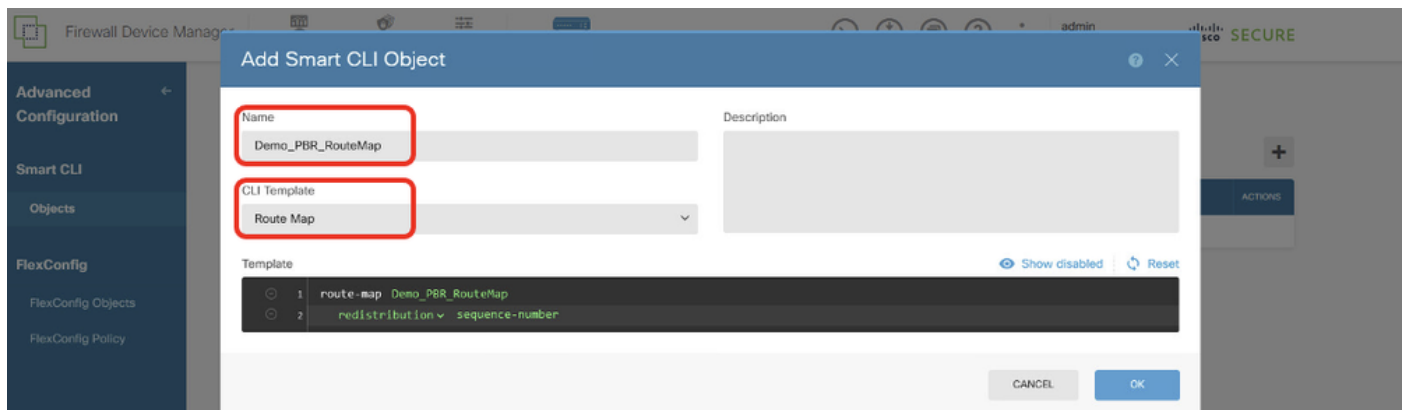
ステップ 13PBRのルートマップを作成します。 Device > Advanced Configuration > Smart CLI > Objectsの順に移動します。+ボタンをクリックします。



Site1FTD_Add_SmartCLI_オブジェクト

ステップ 13.1：オブジェクトの名前を入力し、CLIテンプレートを選択します。

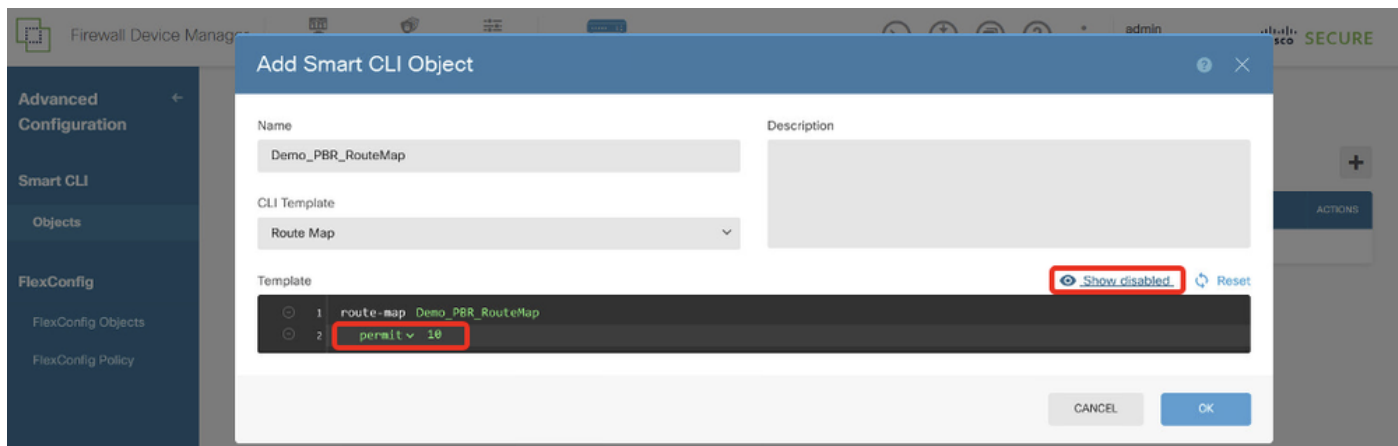
- 名前：Demo_PBR_RouteMap
- CLIテンプレート：ルートマップ



サイト1FTD_作成_PBR_ルートマップ_1

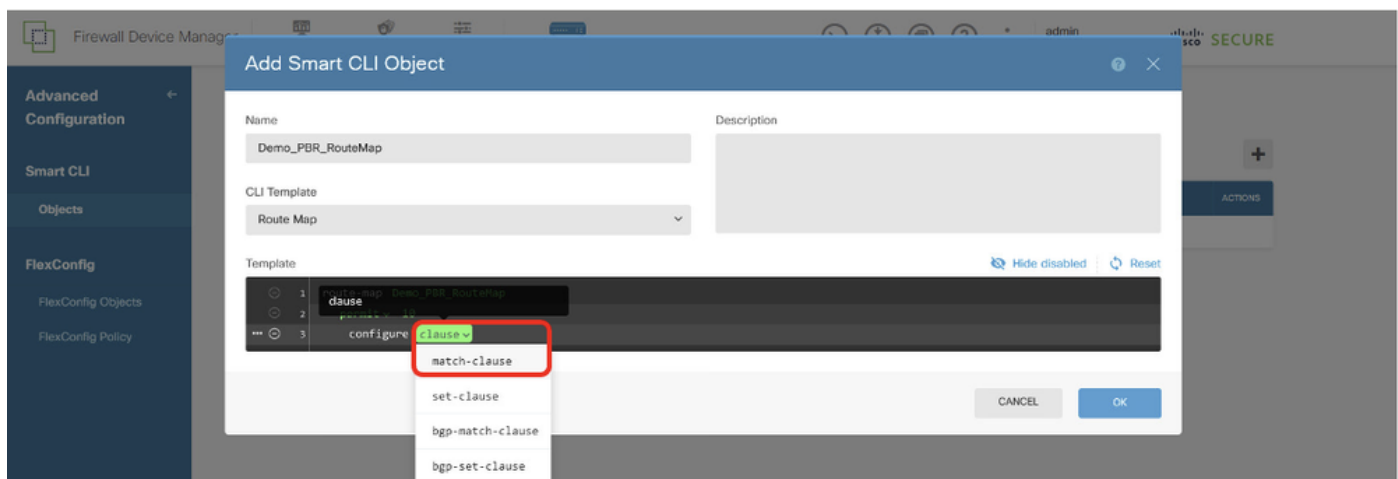
ステップ 13.2：Templateに移動して設定します。OKボタンをクリックして保存します。

Line 2で、redistributionをクリックします。[Permit] を選択します。sequence-number、手動入力10の順にクリックします。Show disabledをクリックします。



サイト1FTD_作成_PBR_ルートマップ2

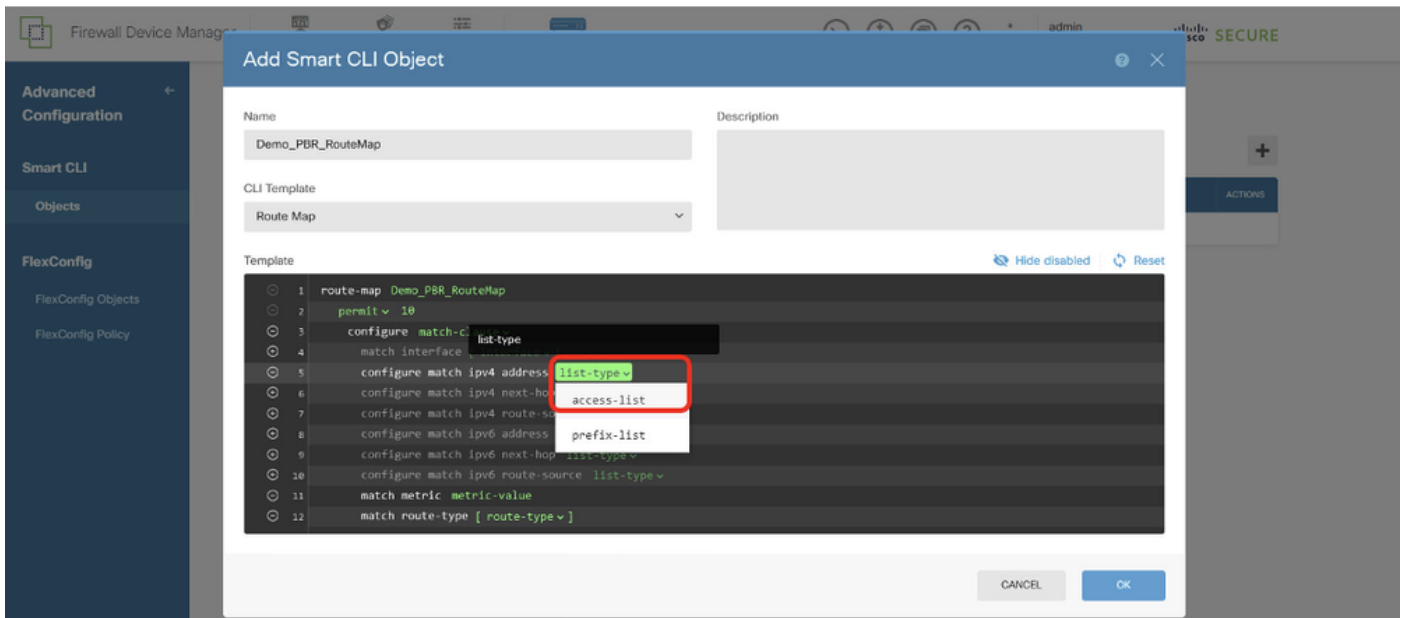
回線3で、+ をクリックして回線を有効にします。clause をクリックします。match-clause を選択します。



サイト1FTD_作成_PBR_ルートマップ_3

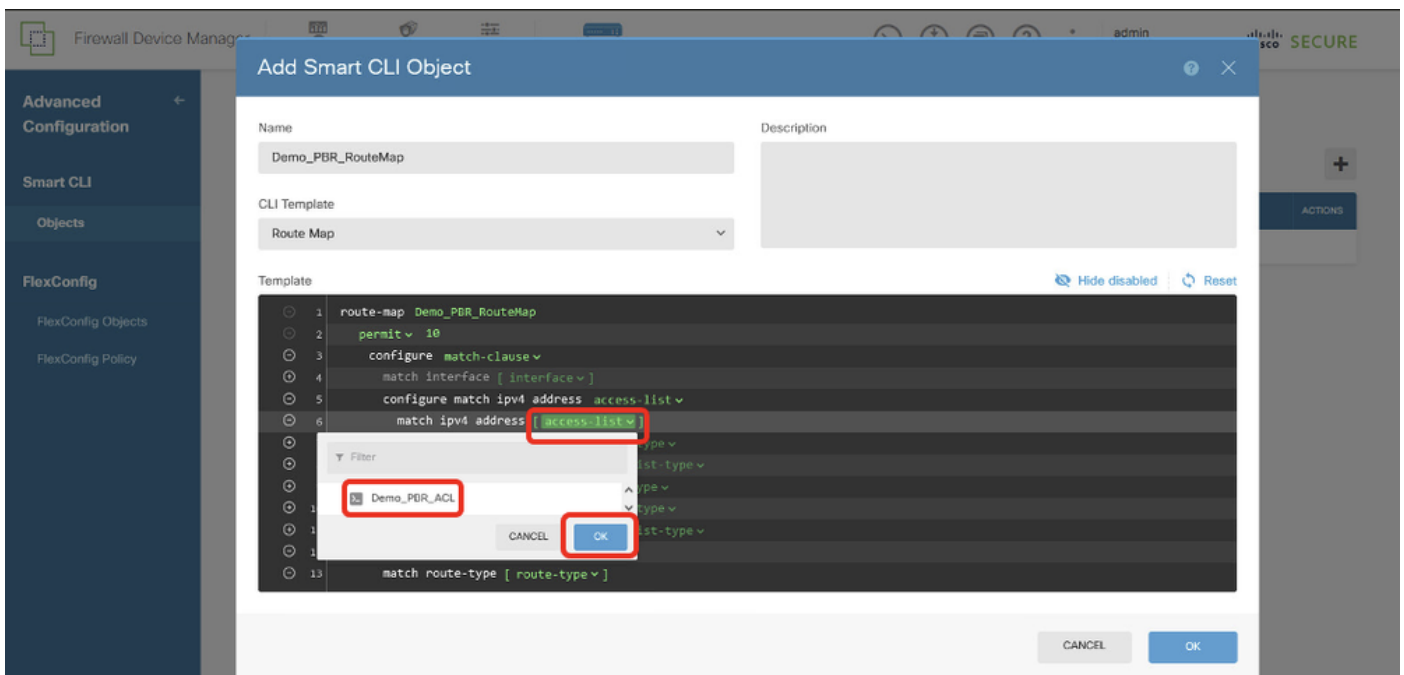
回線4で、- (マイナス) をクリックして回線を無効にします。

回線5で、+ をクリックして回線を有効にします。list-type をクリックします。access-list を選択します。



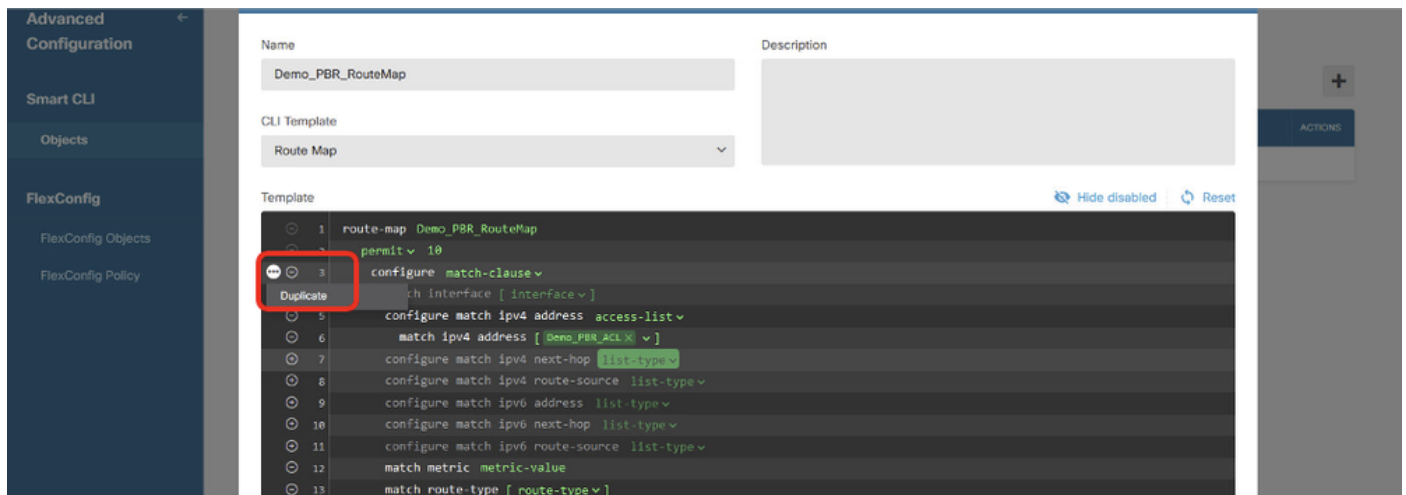
サイト1FTD_作成_PBR_ルートマップ_4

回線6で、access-listをクリックします。ステップ12で作成したACL名を選択します。この例では、Demo_PBR_ACLです。



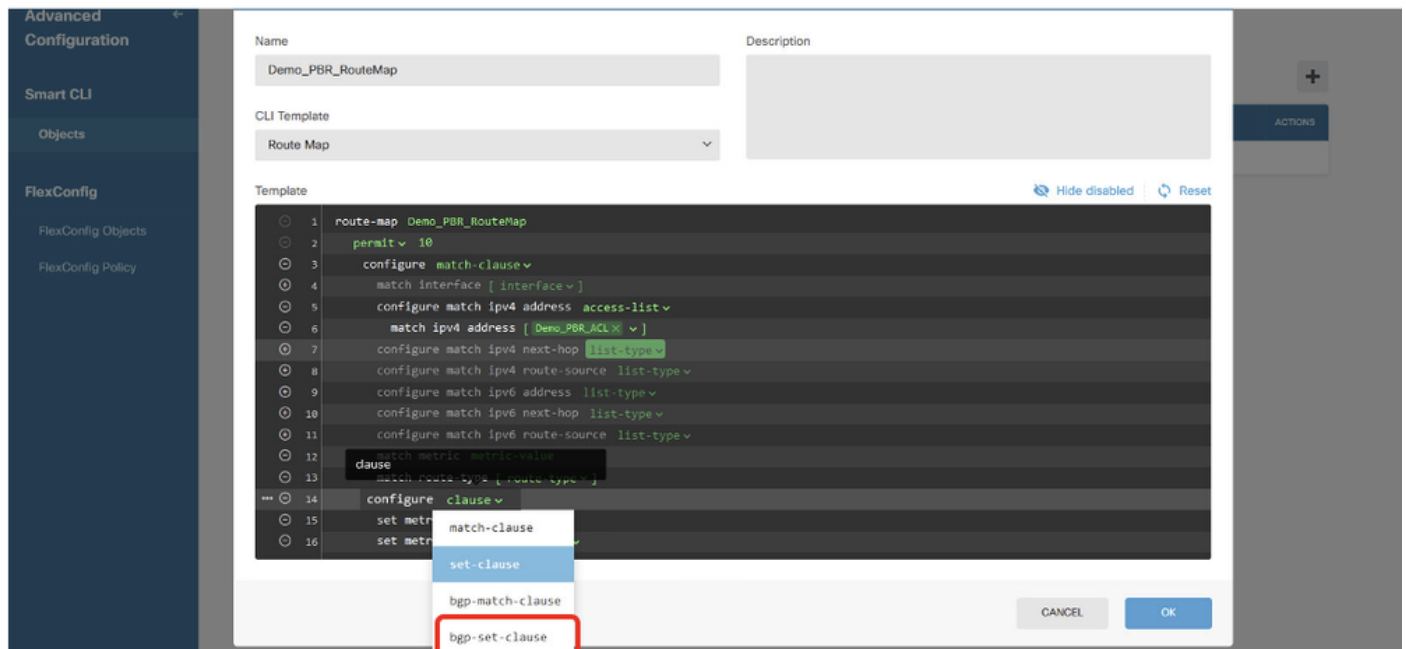
サイト1FTD_作成_PBR_ルートマップ_5

行3に戻ります。options ...ボタンをクリックして、Duplicateを選択します。



サイト1FTD_作成_PBR_ルートマップ_6

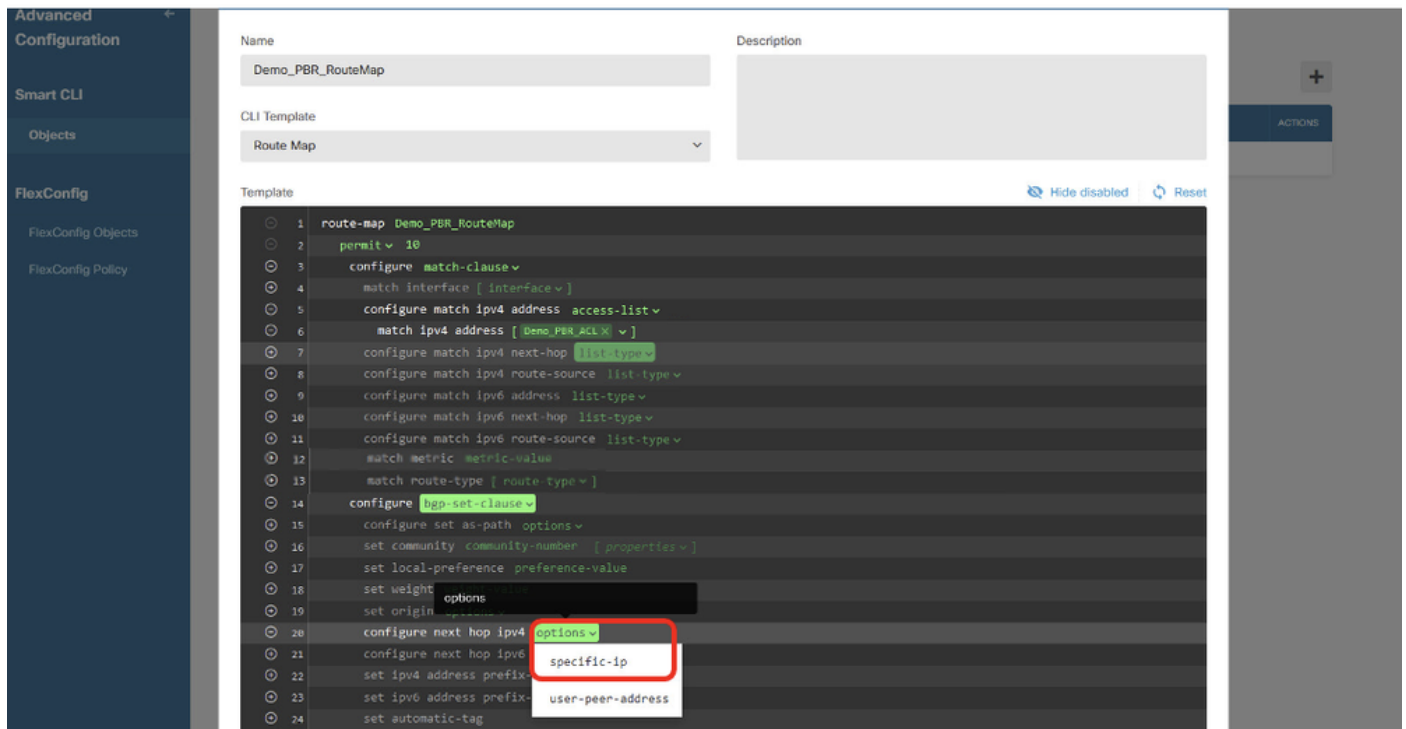
14行目で、clauseをクリックし、bgp-set-clauseを選択します。



サイト1FTD_作成_PBR_ルートマップ_7

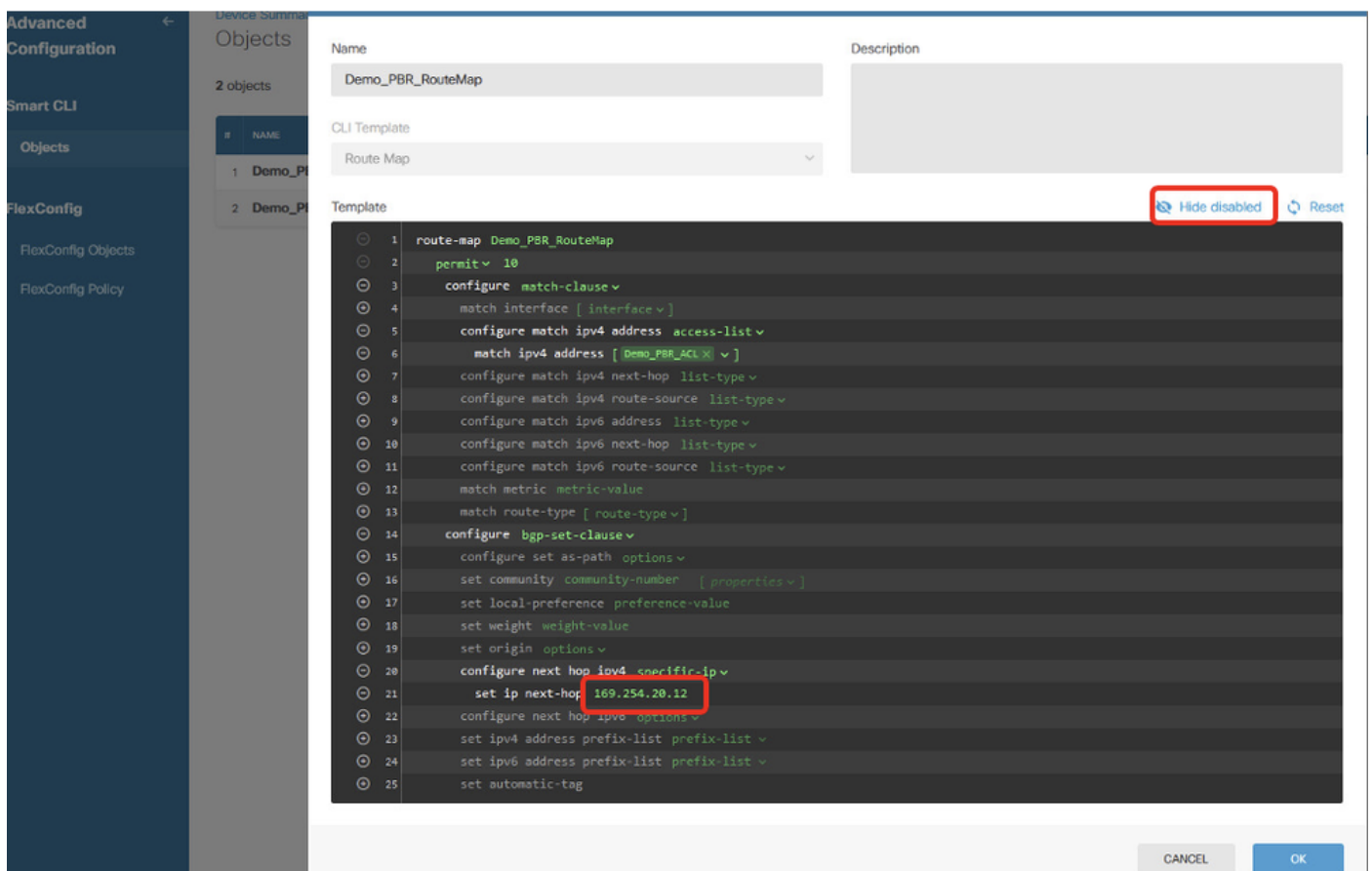
行12、13、15、16、17、18、19、21、22、23、24で-ボタンをクリックして無効にします。

行20で、optionsをクリックし、specific-ipを選択します。



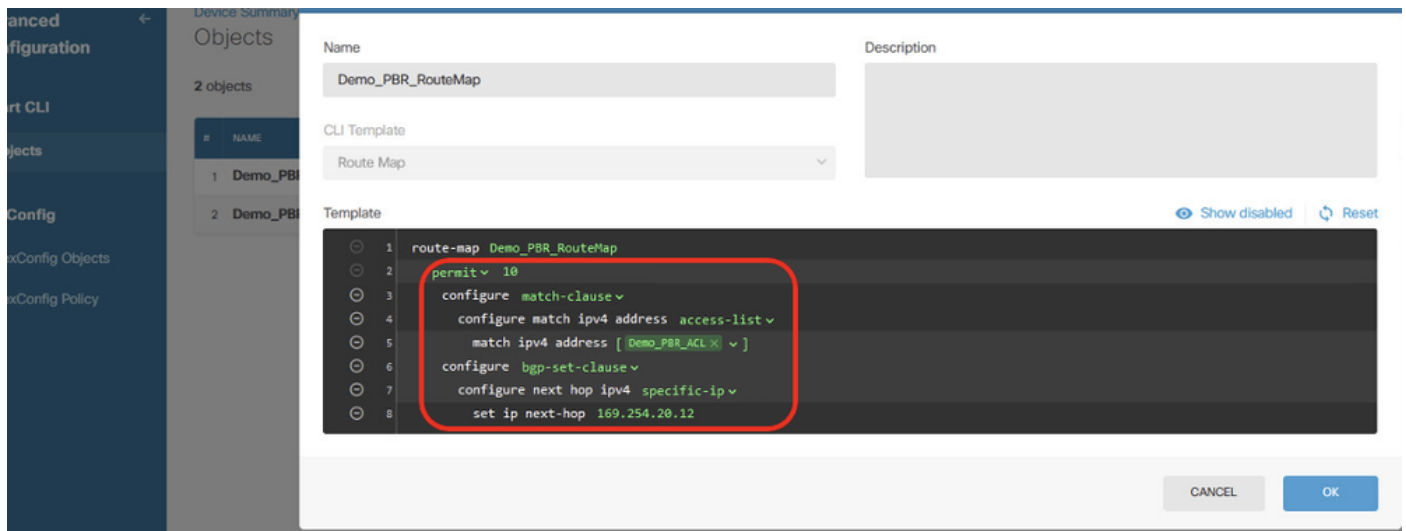
サイト1FTD_作成_PBR_ルートマップ_8

行21で、ip-addressをクリックします。手動でネクストホップIPアドレスを入力します。この例では、ピアSite2 FTD VTI tunnel2(169.254.20.12)のIPアドレスです。 Hide disabledをクリックします。



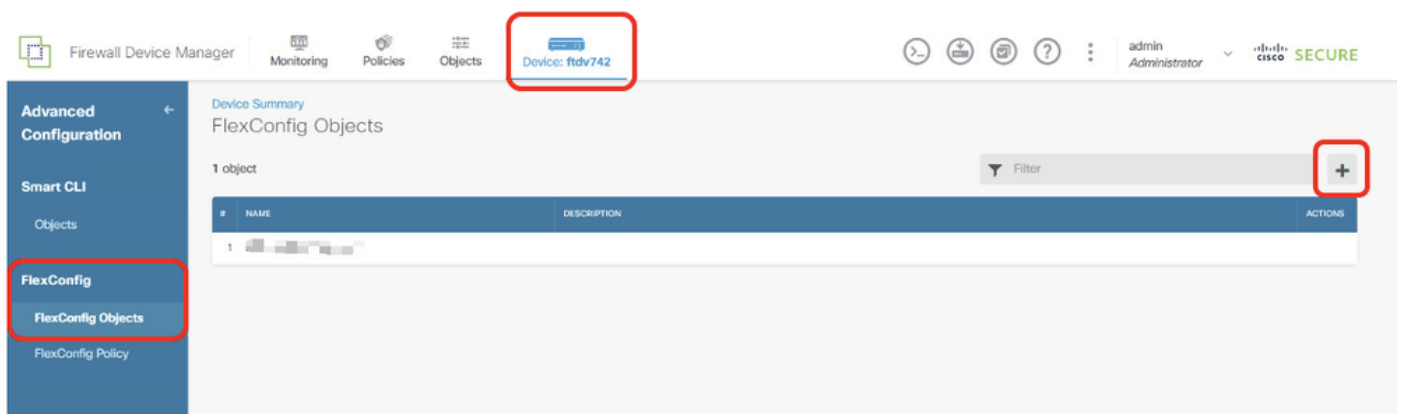
サイト1FTD_作成_PBR_ルートマップ_9

ルートマップの設定を確認します。



サイト1FTD_作成_PBR_ルートマップ_10

ステップ 14 : PBRのFlexConfigオブジェクトを作成します。Device > Advanced Configuration > FlexConfig Objectsの順に移動し、+ボタンをクリックします。



Site1FTD_Create_PBR_FlexObj_1

ステップ 14.1 : オブジェクトの名前を入力します。この例ではDemo_PBR_FlexObjです。TemplateおよびNegate Templateエディタで、コマンドラインを入力します。

- テンプレート :

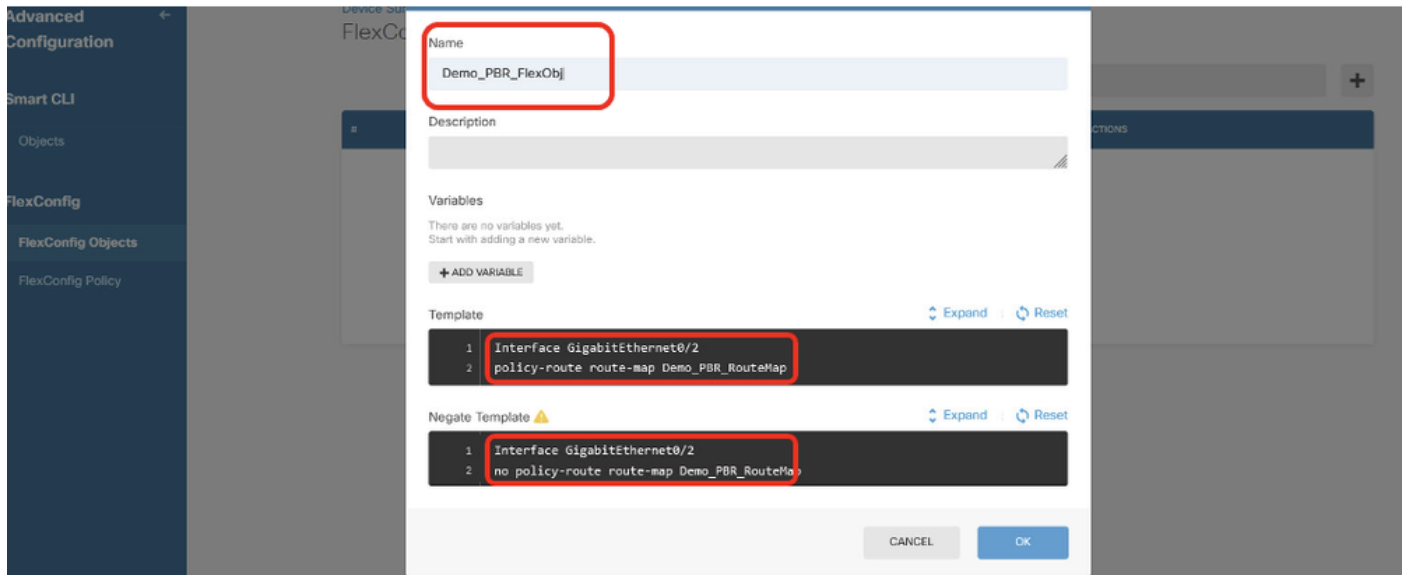
```
interface GigabitEthernet0/2
```

```
policy-route route-map Demo_PBR_ルートマップ_サイト2
```

- ネゲートテンプレート :

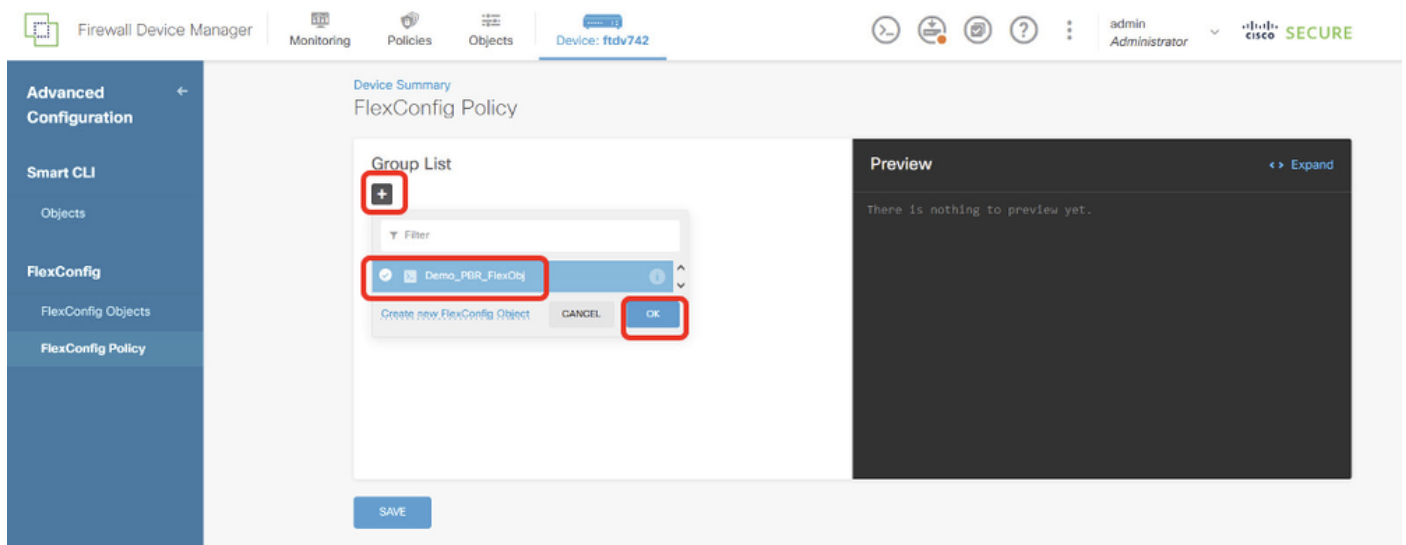
```
interface GigabitEthernet0/2
```

```
no policy-route route-map Demo_PBR_RouteMap_Site2
```



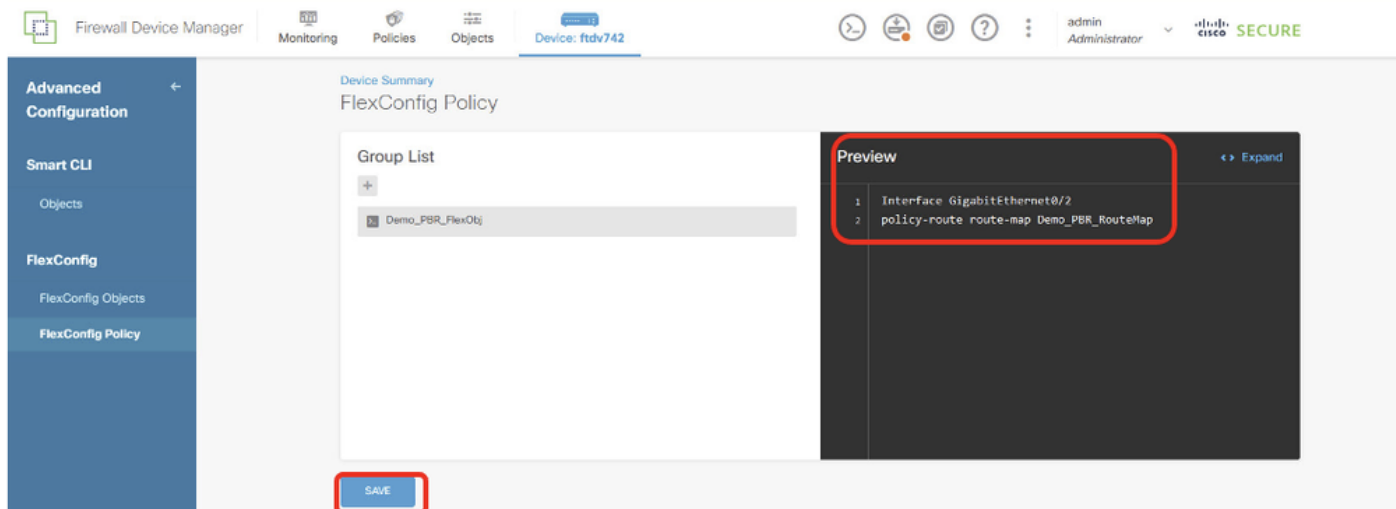
Site1FTD_Create_PBR_FlexObj_2

ステップ 15 : PBR用のFlexConfigポリシーを作成します。 Device > Advanced Configuration > FlexConfig Policyの順に移動します。+ボタンをクリックします。ステップ14で作成した FlexConfigオブジェクト名を選択します。OKボタンをクリックします。



サイト1FTD_Create_PBR_FlexPolicy_1

ステップ 15.1 : Previewウィンドウでコマンドを確認します。問題がなければ、Saveをクリックします。



サイト1FTD_Create_PBR_FlexPolicy_2

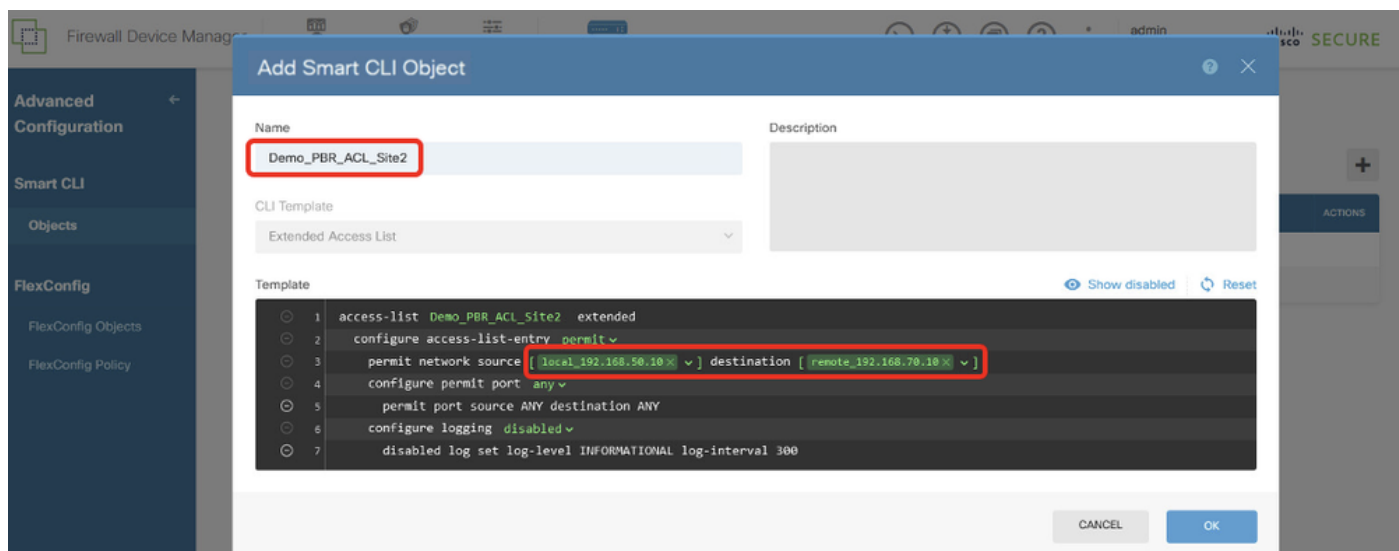
ステップ 16：設定変更を導入します。



Site1FTD_Deployment_Changes

Site2 FTD PBRの設定

ステップ 17：ステップ11 ~ 16を繰り返し、Site2 FTDの対応するパラメータでPBRを作成します。



サイト2FTD_作成_PBR_ACL

Add Smart CLI Object

Name: Demo_PBR_RouteMap_Site2

Description:

CLI Template: Route Map

Template:

```

1 route-map Demo_PBR_RouteMap_Site2
2 permit 10
3 configure match-clause
4 configure match ipv4 address access-list
5 match ipv4 address Demo_PBR_ACL_Site2
6 configure bgp-set-clause
7 configure next hop ipv4 specific-ip
8 set ip next-hop 169.254.20.11

```

CANCEL OK

Site2FTD_Create_PBR_ルートマップ

Create FlexConfig Object

Name: Demo_PBR_FlexObj_Site2

Description:

Variables:

There are no variables yet.
Start with adding a new variable.

+ ADD VARIABLE

Template:

```

1 Interface GigabitEthernet0/2
2 policy-route route-map Demo_PBR_RouteMap_Site2

```

Negate Template:

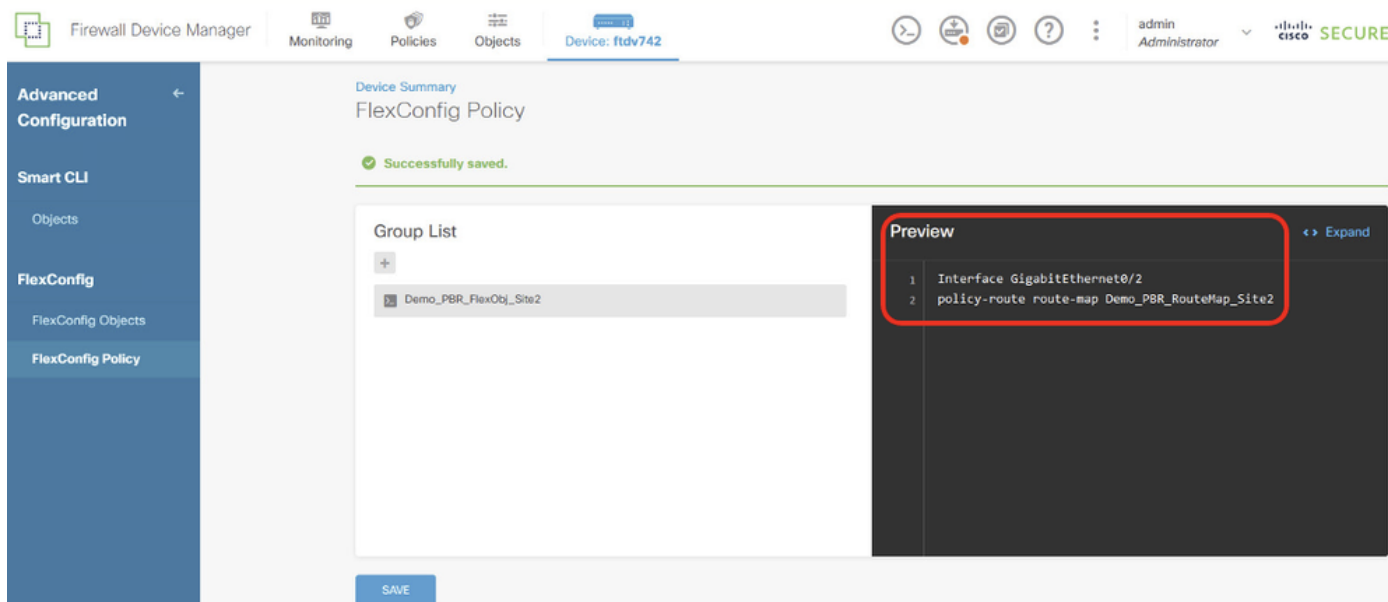
```

1 Interface GigabitEthernet0/2
2 no policy-route route-map Demo_PBR_RouteMap_Site2

```

CANCEL OK

サイト2FTD_作成_PBR_FlexObj

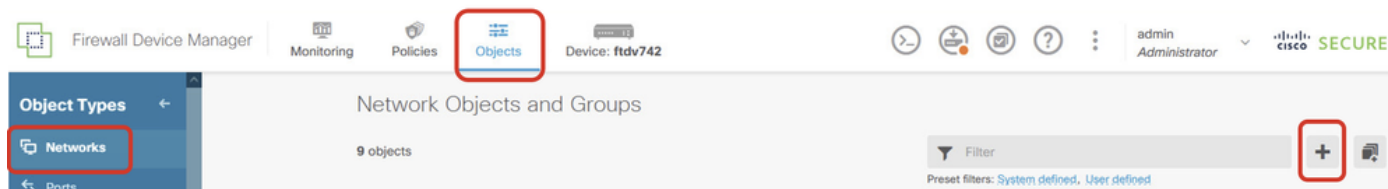


Site2FTD_Create_PBR_Flexポリシー

SLAモニタの設定

Site1 FTD SLAモニタの設定

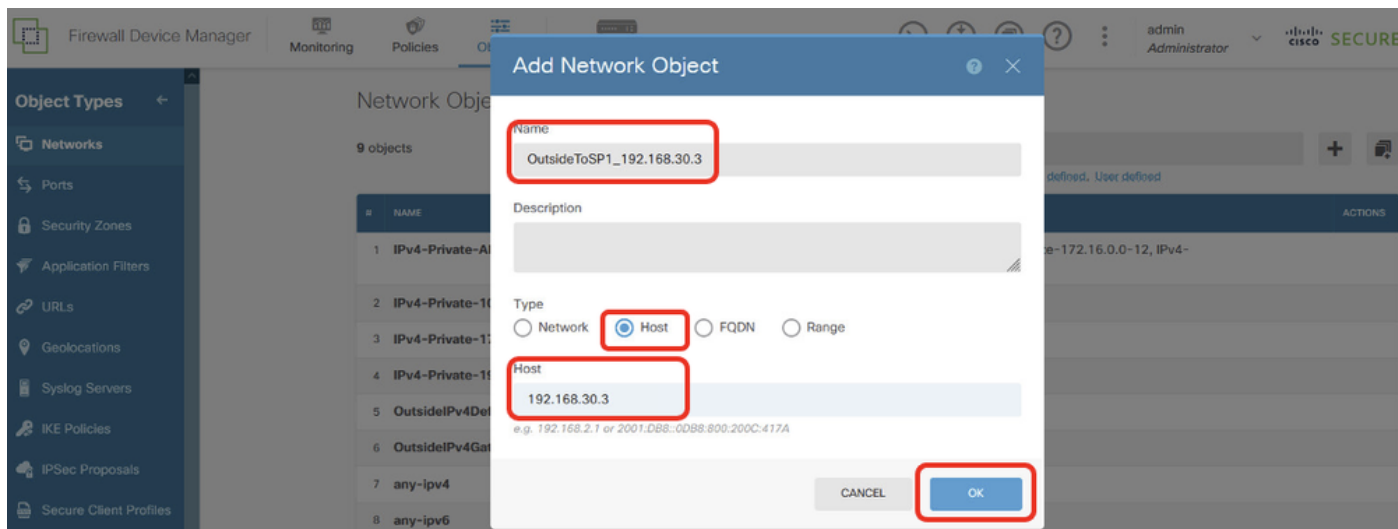
ステップ 18 : Site1 FTDのSLAモニタで使用する新しいネットワークオブジェクトを作成します。 Objects > Networksの順に移動し、+ボタンをクリックします。



Site1FTD_Create_Network_オブジェクト

ステップ 18.1 : ISP1ゲートウェイのIPアドレスのオブジェクトを作成します。 必要な情報を提供します。 OKボタンをクリックします。

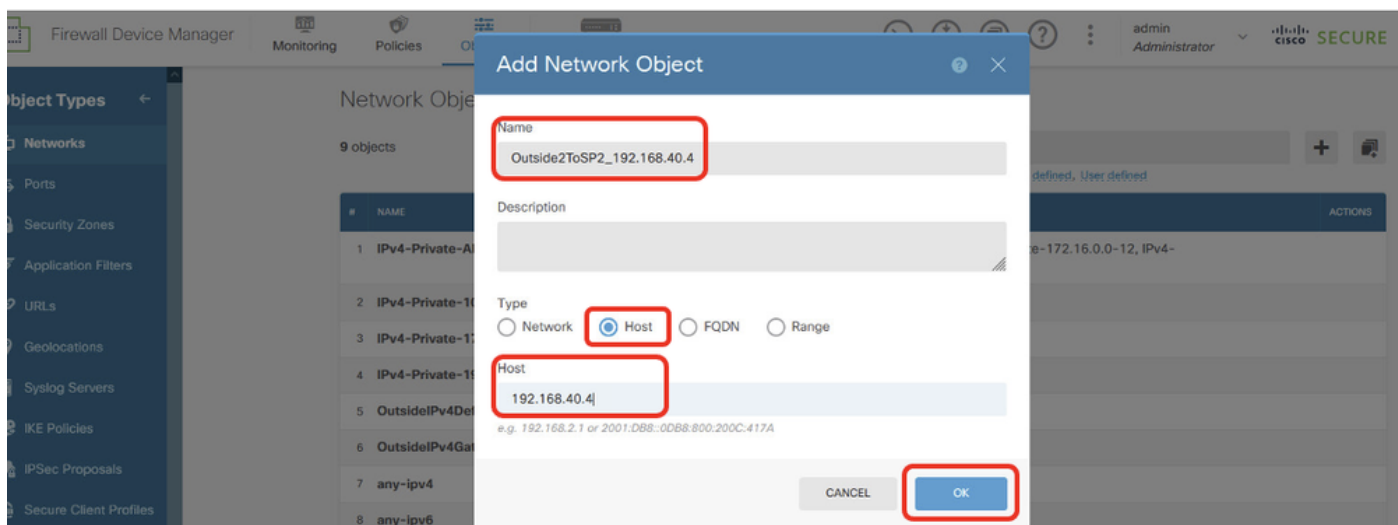
- 名前 : OutsideToSP1_192.168.30.3
- タイプ : ホスト
- ホスト : 192.168.30.3



サイト1FTD_Create_SLAMonitor_NetObj_ISP1

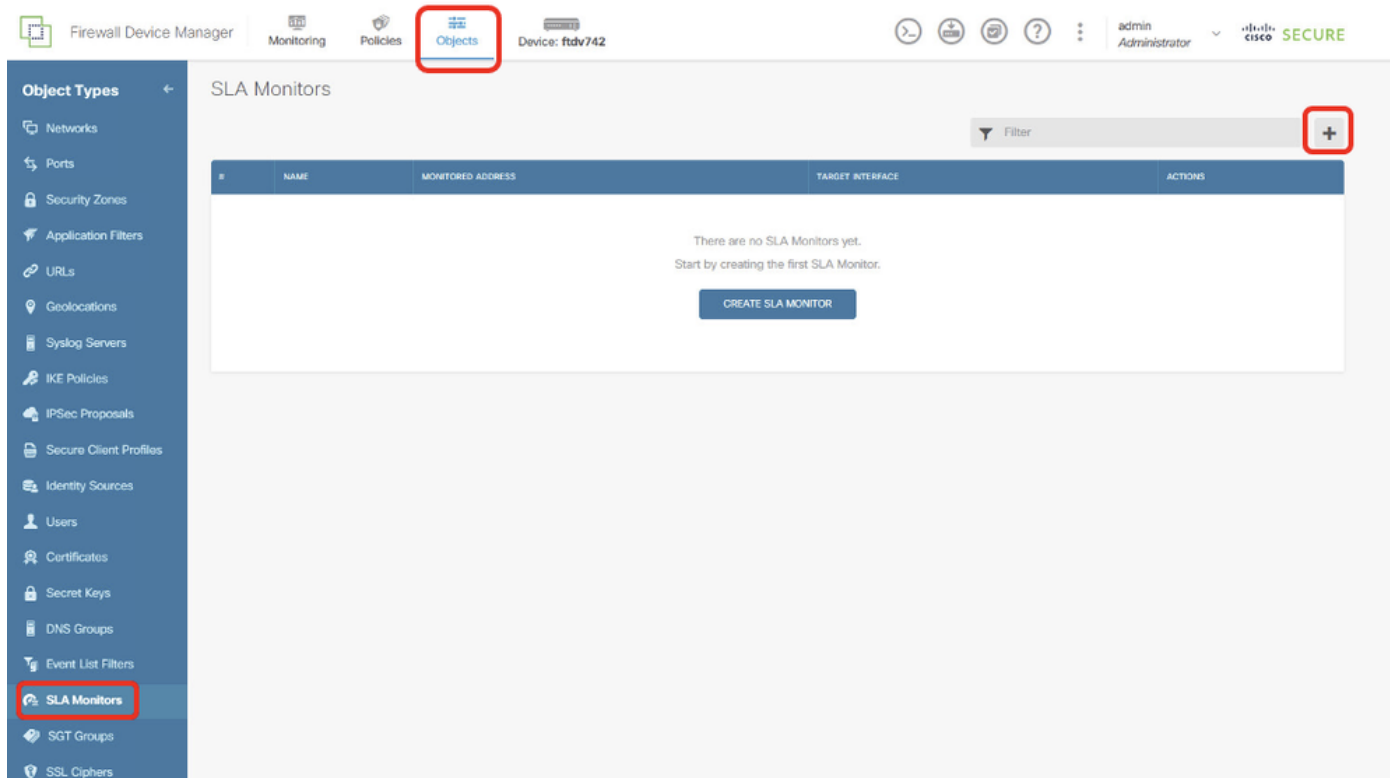
ステップ 18.2 : ISP2ゲートウェイのIPアドレスのオブジェクトを作成します。 必要な情報を提供します。 OKボタンをクリックします。

- 名前 : Outside2ToSP2_192.168.40.4
- タイプ : ホスト
- ホスト : 192.168.40.4



サイト1FTD_Create_SLAMonitor_NetObj_ISP2

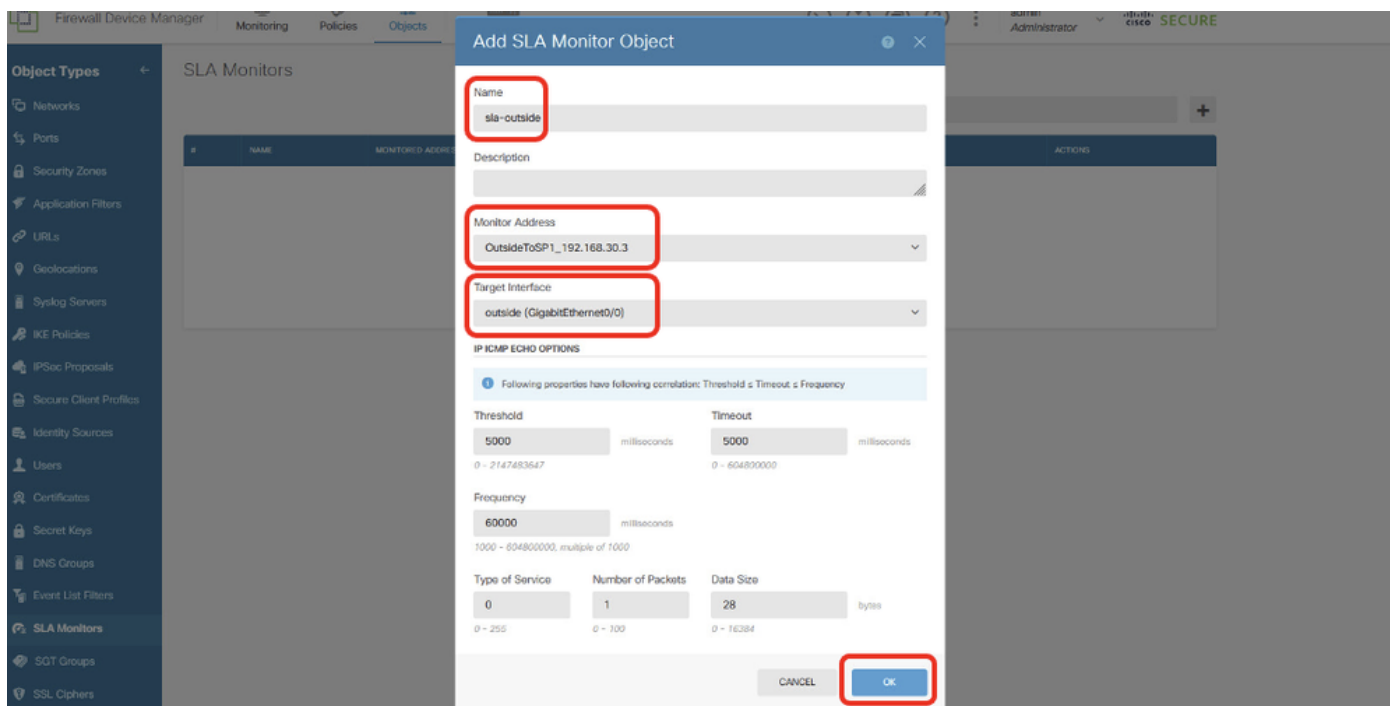
ステップ 19 : SLAモニタを作成します。 Objects > Object Types > SLA Monitorsの順に移動します。 新しいSLAモニタを作成するには、+ボタンをクリックします。



サイト1FTD_Create_SLAMonitor

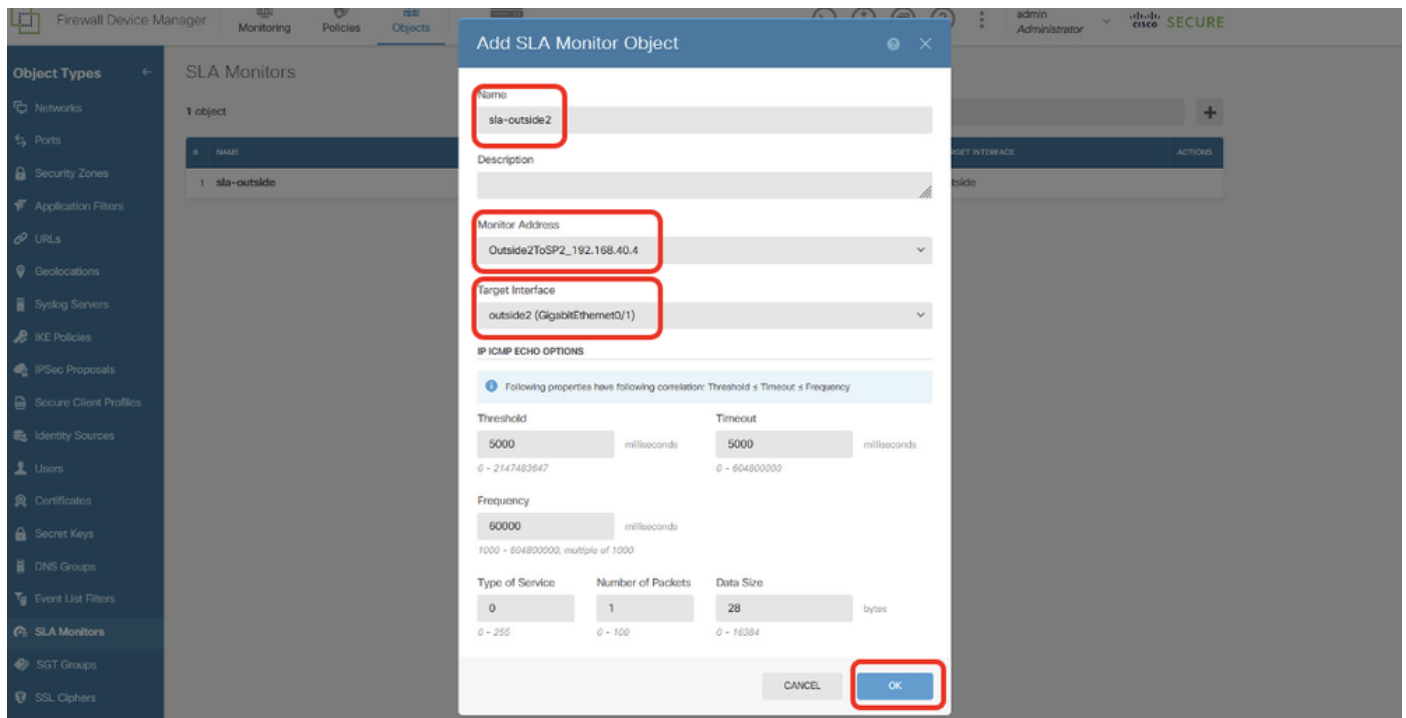
ステップ 19.1 : Add SLA Monitor Objectウィンドウで、ISP1ゲートウェイに必要な情報を入力します。OKボタンをクリックして保存します。

- 名前 : sla-outside
- モニタアドレス : OutsideToSP1_192.168.30.3
- ターゲットインターフェイス : outside(GigabitEthernet0/0)
- IP ICMPエコーオプション : デフォルト



ステップ 19.2：引き続き+ボタンをクリックして、ISP2ゲートウェイの新しいSLAモニタを作成します。Add SLA Monitor Objectウィンドウで、ISP2ゲートウェイに必要な情報を入力します。OKボタンをクリックして保存します。

- ・ 名前：sla-outside2
- ・ モニタアドレス：Outside2ToSP2_192.168.40.4
- ・ ターゲットインターフェイス：outside2(GigabitEthernet0/1)
- ・ IP ICMPエコーオプション：デフォルト



ステップ 20：設定変更を導入します。



Site2 FTD SLAモニタの設定

ステップ 21：ステップ18～20を繰り返します。Site2 FTDの対応するパラメータでSLAモニタを作成します。

Object Types

SLA Monitor

2 objects

#	NAME
1	sla-outside
2	sla-outside

Name: sla-outside

Description:

Monitor Address: OutsideToSP1_192.168.10.3

Target Interface: outside (GigabitEthernet0/0)

IP ICMP ECHO OPTIONS

Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency

Threshold: 5000 milliseconds (0 - 2147483647)

Timeout: 5000 milliseconds (0 - 604800000)

Frequency: 60000 milliseconds (1000 - 604800000, multiple of 1000)

Type of Service: 0 (0 - 255)

Number of Packets: 1 (0 - 100)

Data Size: 28 bytes (0 - 16384)

CANCEL OK

Site2FTD_Create_SLAMonitor_NetObj_ISP1_Details

Object Types

SLA Monitor

2 objects

#	NAME
1	sla-outside
2	sla-outside

Name: sla-outside2

Description:

Monitor Address: Outside2ToSP2_192.168.20.4

Target Interface: outside2 (GigabitEthernet0/1)

IP ICMP ECHO OPTIONS

Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency

Threshold: 5000 milliseconds (0 - 2147483647)

Timeout: 5000 milliseconds (0 - 604800000)

Frequency: 60000 milliseconds (1000 - 604800000, multiple of 1000)

Type of Service: 0 (0 - 255)

Number of Packets: 1 (0 - 100)

Data Size: 28 bytes (0 - 16384)

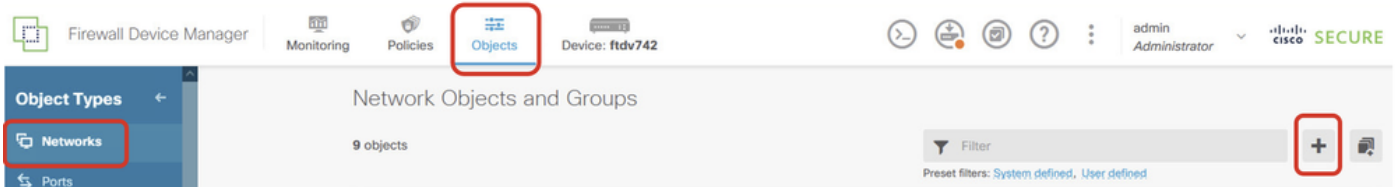
CANCEL OK

Site2FTD_Create_SLAMonitor_NetObj_ISP2_Details

スタティックルートの設定

Site1 FTDスタティックルートの設定

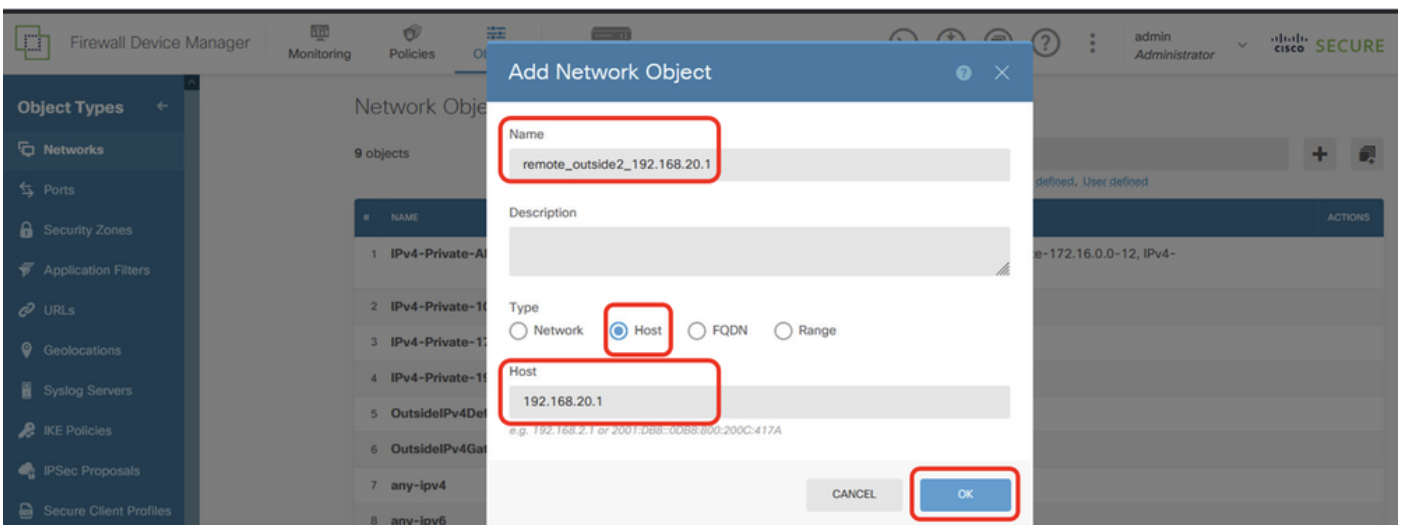
ステップ 22： Site1 FTDのスタティックルートで使用される新しいネットワークオブジェクトを作成します。 Objects > Networksの順に移動し、+ボタンをクリックします。



サイト1FTD_Create_Obj

ステップ 22.1： ピアSite2 FTDのoutside2 IPアドレスのオブジェクトを作成します。 必要な情報を提供します。 OKボタンをクリックします。

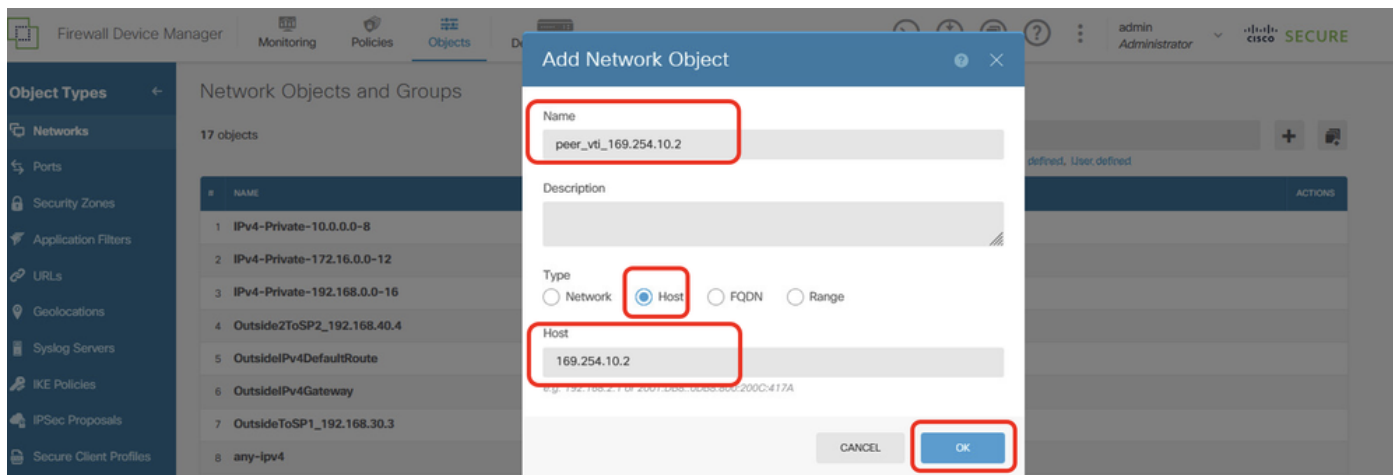
- 名前： remote_outside2_192.168.20.1
- タイプ： HOST
- ネットワーク： 192.168.20.1



Site1FTD_Create_NetObj_StaticRoute_1

ステップ 22.2： ピアSite2 FTDのVTI Tunnel1 IPアドレスのオブジェクトを作成します。 必要な情報を提供します。 OKボタンをクリックします。

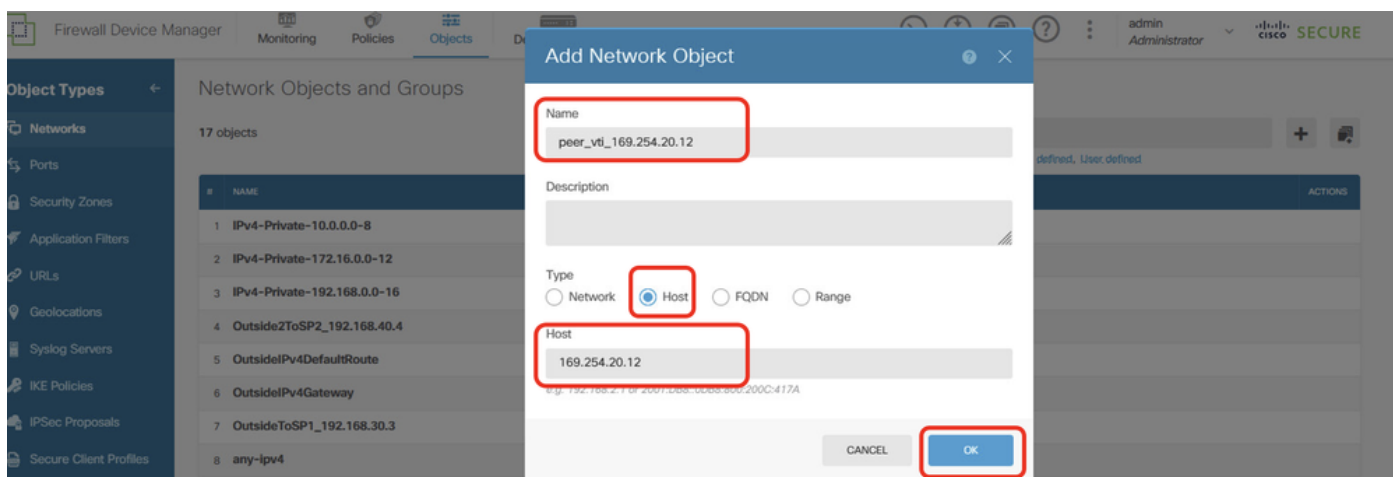
- 名前： peer_vti_169.254.10.2
- タイプ： HOST
- ネットワーク： 169.254.10.2



Site1FTD_Create_NetObj_StaticRoute_2

ステップ 22.3 : ピアSite2 FTDのVTI Tunnel2のIPアドレスのオブジェクトを作成します。必要な情報を提供します。OKボタンをクリックします。

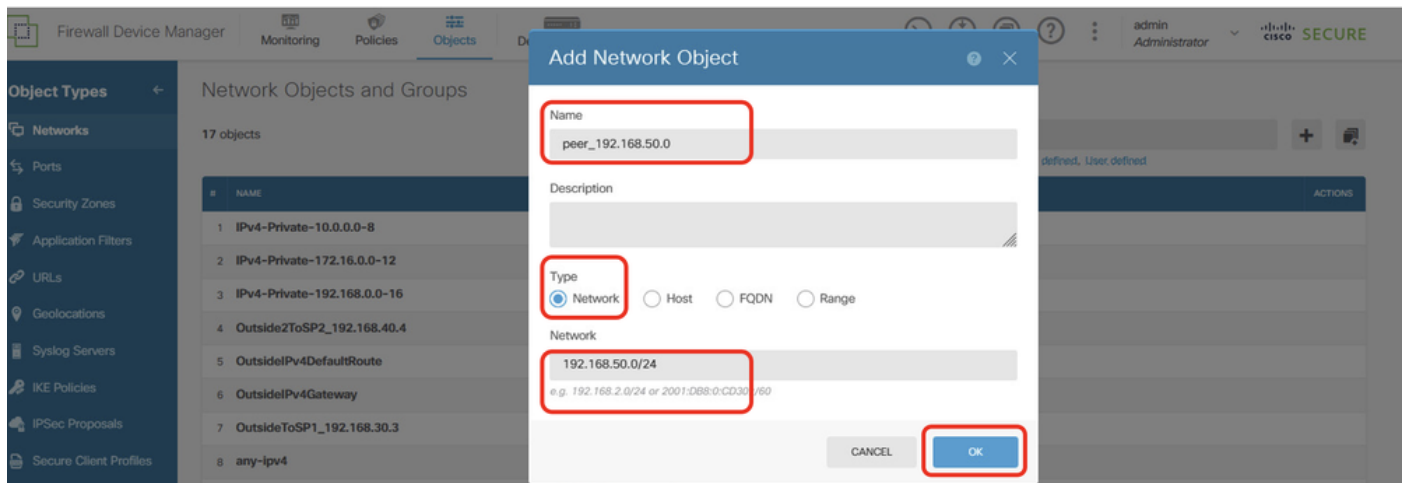
- 名前 : peer_vti_169.254.20.12
- タイプ : HOST
- ネットワーク : 169.254.20.12



Site1FTD_Create_NetObj_StaticRoute_3

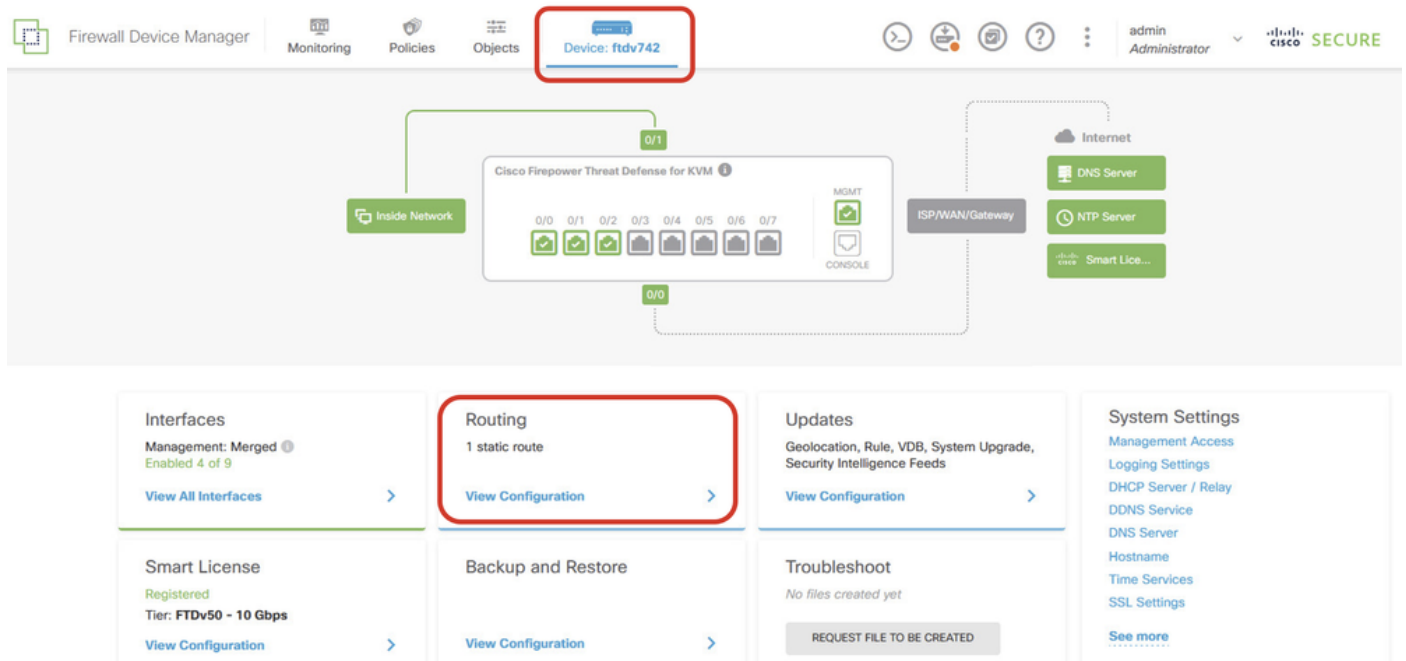
ステップ 22.4 : ピアSite2 FTDの内部ネットワークのオブジェクトを作成します。必要な情報を提供します。OKボタンをクリックします。

- 名前 : peer_192.168.50.0
- タイプ : NETWORK
- ネットワーク : 192.168.50.0/24



Site1FTD_Create_NetObj_StaticRoute_4

ステップ 23： Device > Routingの順に移動します。View Configurationをクリックします。Static Routingタブをクリックします。+ボタンをクリックして、新しいスタティックルートを追加します。



Site1FTD_View_Route_設定



サイト1FTD_Add_Static_Route

ステップ 23.1： SLAモニタリング付きのISP1ゲートウェイを使用して、デフォルトルートを作成

します。ISP1ゲートウェイで中断が発生すると、トラフィックはISP2経由でバックアップデフォルトルートに切り替わります。ISP1が回復すると、トラフィックはISP1の使用に戻ります。必要な情報を提供します。OKボタンをクリックして保存します。

- 名前 : ToSP1GW
- インターフェイス : outside(GigabitEthernet0/0)
- プロトコル : IPv4
- ネットワーク : any-ipv4
- ゲートウェイ : OutsideToSP1_192.168.30.3
- メトリック : 1
- SLAモニタ : sla-outside

Add Static Route



Name

ToSP1GW

Description

Interface

outside (GigabitEthernet0/0)

Protocol



IPv4



IPv6

Networks



any-ipv4

Gateway

OutsideToSP1_192.168.30.3

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

sla-outside

CANCEL

OK

ステップ 23.2 : ゲートウェイISP2ゲートウェイ経由でバックアップデフォルトルートを作成します。メトリックは1より大きくなければなりません。この例では、metricは2です。必要な情報を提供します。OKボタンをクリックして保存します。

- 名前 : DefaultToSP2GW
- インターフェイス : outside2(GigabitEthernet0/1)
- プロトコル : IPv4
- ネットワーク : any-ipv4
- ゲートウェイ : Outside2ToSP2_192.168.40.4
- メトリック : 2

Add Static Route



Name

DefaultToSP2GW

Description

Interface

outside2 (GigabitEthernet0/1)

Protocol



IPv4



IPv6

Networks



any-ipv4

Gateway

Outside2ToSP2_192.168.40.4

Metric

2

SLA Monitor Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

OK

ステップ 23.3 : SLAモニタリングを使用して、ピアSite2 FTDのOutside2 IPアドレスのOutside2へのスタティックルートを作成します。このスタティックルートは、Site2 FTDのOutside2とのVPNを確立するために使用されます。必要な情報を提供します。OKボタンをクリックして保存します。

- 名前 : SpecificToSP2GW
- インターフェイス : outside2(GigabitEthernet0/1)
- プロトコル : IPv4
- ネットワーク : remote_outside2_192.168.20.1
- ゲートウェイ : Outside2ToSP2_192.168.40.4
- メトリック : 1
- SLAモニタ : sla-outside2

Add Static Route



Name

SpecificToSP2GW

Description

Interface

outside2 (GigabitEthernet0/1)

Protocol



IPv4



IPv6

Networks



remote_outside2_192.168.20.1

Gateway

Outside2ToSP2_192.168.40.4

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

sla-outside2

CANCEL

OK

ステップ 23.4 : ゲートウェイとしてSite2 FTDのピアVTIトンネル1を経由してピアSite2 FTDの内部ネットワークへの宛先トラフィックのスタティックルートを作成し、トンネル1を経由したクライアントトラフィックを暗号化するためのSLAモニタリングを設定します。ISP1ゲートウェイで中断が発生すると、VPNトラフィックはISP2のVTIトンネル2に切り替わります。ISP1が回復すると、トラフィックはISP1のVTIトンネル1に戻ります。必要な情報を提供します。OKボタンをクリックして保存します。

- 名前 : ToVTISP1
- インターフェイス : demovti(Tunnel1)
- プロトコル : IPv4
- ネットワーク : peer_192.168.50.0
- ゲートウェイ : peer_vti_169.254.10.2
- メトリック : 1
- SLAモニタ : sla-outside

Add Static Route



Name

ToVTISP1

Description

Interface

demovti (Tunnel1)

Protocol



IPv4



IPv6

Networks



peer_192.168.50.0

Gateway

peer_vti_169.254.10.2

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

sla-outside

CANCEL

OK

ステップ 23.5 : Site2 FTDのピアVTIトンネル2を経由してピアSite2 FTDの内部ネットワークに宛先トラフィックのバックアップスタティックルートをゲートウェイとして作成し、トンネル2を経由したクライアントトラフィックの暗号化に使用します。メトリックを1より大きい値に設定します。この例では、metricは22です。 必要な情報を提供します。OKボタンをクリックして保存します。

- 名前 : ToVTISP2_Backup
- インタフェース : demovti_sp2(Tunnel2)
- プロトコル : IPv4
- ネットワーク : peer_192.168.50.0
- ゲートウェイ : peer_vti_169.254.20.12
- メトリック : 22

Add Static Route



Name

ToVTISP2_Backup

Description

Interface

demovti_sp2 (Tunnel2)

Protocol



IPv4



IPv6

Networks



peer_192.168.50.0

Gateway

peer_vti_169.254.20.12

Metric

22

SLA Monitor Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

OK

ステップ 23.6 : PBRトラフィックのスタティックルートを作成します。SLAモニタリングを使用し、ゲートウェイとしてSite2 FTDのピアVTIトンネル2を介してSite2 Client2に送信される宛先トラフィック 必要な情報を提供します。OKボタンをクリックして保存します。

- 名前 : ToVTISP2
- インタフェース : demovti_sp2(Tunnel2)
- プロトコル : IPv4
- ネットワーク : remote_192.168.50.10
- ゲートウェイ : peer_vti_169.254.20.12
- メトリック : 1
- SLAモニタ : sla-outside2

Add Static Route



Name

ToVTISP2

Description

Interface

demovti_sp2 (Tunnel2)

Protocol



IPv4



IPv6

Networks



remote_192.168.50.10

Gateway

peer_vti_169.254.20.12

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

sla-outside2

CANCEL

OK

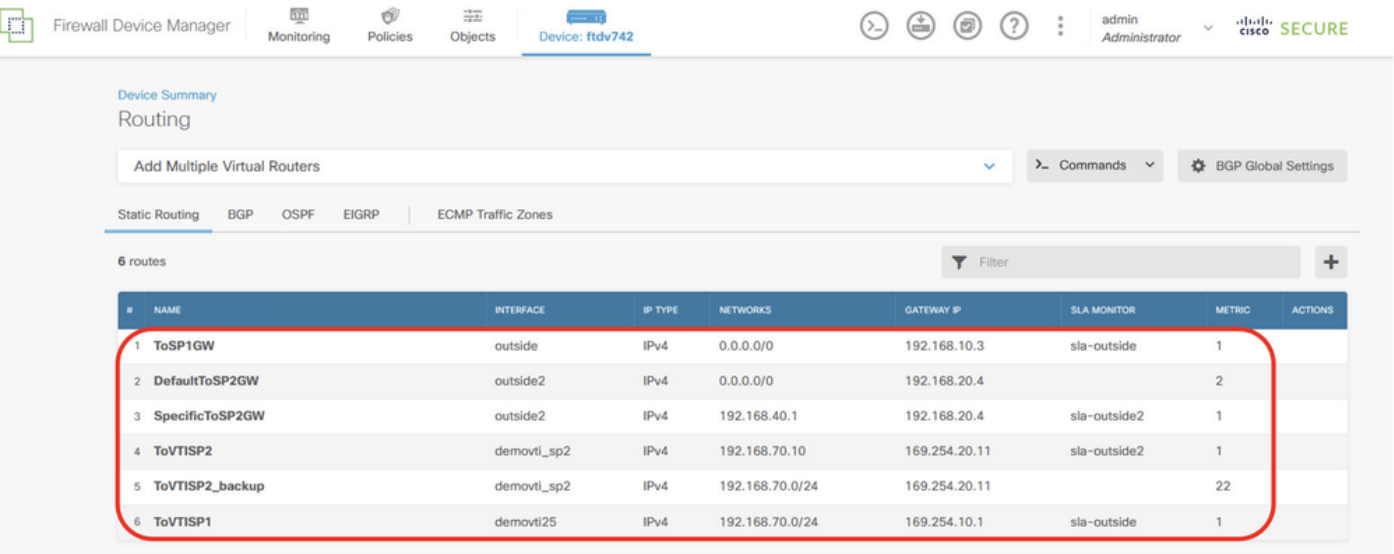
ステップ 24：設定変更を導入します。



Site1FTD_Deployment_Changes

Site2のFTDスタティックルートの設定

ステップ 25：手順22 ~ 24を繰り返し、Site2 FTDの対応するパラメータを使用してスタティックルートを作成します。



Site2FTD_Create_スタティックルート

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。コンソールまたはSSHを使用して、Site1 FTDとSite2 FTDのCLIに移動します。

ISP1とISP2の両方が正常に動作します

VPN

//Site1 FTD:

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:156, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local	Remote
1072332533 192.168.30.1/500	192.168.10.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK	
Life/Active Time: 86400/44895 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: 0xec031247/0xc2f3f549

IKEv2 SAs:

Session-id:148, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local	Remote
1045734377 192.168.40.1/500	192.168.20.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK	
Life/Active Time: 86400/77860 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: 0x47bfa607/0x82e8781d	

// Site2 FTD:

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:44, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local	Remote
499259237 192.168.10.1/500	192.168.30.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK	
Life/Active Time: 86400/44985 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: 0xc2f3f549/0xec031247	

IKEv2 SAs:

Session-id:36, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local	Remote
477599833 192.168.20.1/500	192.168.40.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK	
Life/Active Time: 86400/77950 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: 0x82e8781d/0x47bfa607	

ルート

// Site1 FTD:

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
C       169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L       169.254.20.11 255.255.255.255 is directly connected, demovti_sp2
S       192.168.20.1 255.255.255.255 [1/0] via 192.168.40.4, outside2
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
C       192.168.40.0 255.255.255.0 is directly connected, outside2
L       192.168.40.1 255.255.255.255 is directly connected, outside2
S       192.168.50.0 255.255.255.0 [1/0] via 169.254.10.2, demovti
S       192.168.50.10 255.255.255.255 [1/0] via 169.254.20.12, demovti_sp2
C       192.168.70.0 255.255.255.0 is directly connected, inside
L       192.168.70.1 255.255.255.255 is directly connected, inside
```

// Site2 FTD:

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 192.168.10.3 to network 0.0.0.0

```
S*      0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C       169.254.10.0 255.255.255.0 is directly connected, demovti25
L       169.254.10.2 255.255.255.255 is directly connected, demovti25
C       169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L       169.254.20.12 255.255.255.255 is directly connected, demovti_sp2
C       192.168.10.0 255.255.255.0 is directly connected, outside
L       192.168.10.1 255.255.255.255 is directly connected, outside
C       192.168.20.0 255.255.255.0 is directly connected, outside2
L       192.168.20.1 255.255.255.255 is directly connected, outside2
S       192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C       192.168.50.0 255.255.255.0 is directly connected, inside
L       192.168.50.1 255.255.255.255 is directly connected, inside
S       192.168.70.0 255.255.255.0 [1/0] via 169.254.10.1, demovti25
S       192.168.70.10 255.255.255.255 [1/0] via 169.254.20.11, demovti_sp2
```

SLAモ二タ

// Site1 FTD:

ftdv742# show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 188426425
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.40.4
Interface: outside2
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 855903900
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.30.3
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.132 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1748
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 30
Latest operation start time: 13:44:05.173 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 30 RTTMin: 30 RTTMax: 30
NumOfRTT: 1 RTTSum: 30 RTTSum2: 900

Entry number: 855903900
Modification time: 08:37:05.133 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1748
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 30
Latest operation start time: 13:44:05.178 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 30 RTTMin: 30 RTTMax: 30
NumOfRTT: 1 RTTSum: 30 RTTSum2: 900

// Site2 FTD:

ftdv742# show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 550063734
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.20.4
Interface: outside2
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 609724264
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.10.3
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never

Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

```
ftdv742# show sla monitor operational-state
Entry number: 550063734
Modification time: 09:05:52.864 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1718
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 190
Latest operation start time: 13:42:52.916 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 190    RTTMin: 190    RTTMax: 190
NumOfRTT: 1    RTTSum: 190    RTTSum2: 36100
```

```
Entry number: 609724264
Modification time: 09:05:52.856 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1718
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 190
Latest operation start time: 13:42:52.921 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 190    RTTMin: 190    RTTMax: 190
NumOfRTT: 1    RTTSum: 190    RTTSum2: 36100
```

ping テスト

シナリオ 1.Site1 Client1 ping Site2 Client1。

pingを発行する前に、Site1 FTDの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にカプセル化のための1497パケットとカプセル化解除のための1498パケットが表示されています。

// Site1 FTD:

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
```

```
#pkts encaps: 1497, #pkts encrypt: 1497, #pkts digest: 1497
#pkts decaps: 1498, #pkts decrypt: 1498, #pkts verify: 1498
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
#pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 16
#pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 ping Site2 Client1が正常に実行されました。

```
Site1_Client1#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 = 10/97/227 ms
```

pingが成功した後、Site1 FTDのshow crypto ipsec sa | inc interface:|encap|decapのカウンタをチェックします。

この例では、Tunnel 1にカプセル化の場合は1502パケット、カプセル化解除の場合は1503パケットと、どちらのカウンタも5パケット増加しており、5つのpingエコー要求に一致しています。これは、Site1 Client1からSite2 Client1へのpingが、ISP1のTunnel 1経由でルーティングされていることを示しています。Tunnel 2では、カプセル化カウンタまたはカプセル化解除カウンタの増加は示されていません。そのため、このトラフィックにはトンネル2が使用されていないことが確認されます。

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
#pkts encaps: 1502, #pkts encrypt: 1502, #pkts digest: 1502
#pkts decaps: 1503, #pkts decrypt: 1503, #pkts verify: 1503
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
#pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 16
#pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

シナリオ 2.Site1 Client2 ping Site2 Client2を実行します。

pingを発行する前に、Site1 FTDのshow crypto ipsec sa | inc interface:|encap|decapのカウンタを確認します。

この例では、Tunnel2にカプセル化のための21個のパケットとカプセル化解除のための20個のパケットが表示されています。

// Site1 FTD:

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 1520, #pkts encrypt: 1520, #pkts digest: 1520
    #pkts decaps: 1521, #pkts decrypt: 1521, #pkts verify: 1521
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
    #pkts encaps: 21, #pkts encrypt: 21, #pkts digest: 21
    #pkts decaps: 20, #pkts decrypt: 20, #pkts verify: 20
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client2 ping Site2 Client2が正常に実行されました。

```
Site1_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 = 4/39/87 ms
```

pingが成功した後、Site1 FTDのshow crypto ipsec sa | inc interface:|encap|decapのカウンタをチェックします。

この例では、Tunnel 2はカプセル化のための26パケットとカプセル化解除のための25パケットを示しており、両方のカウンタは5パケット増加し、5つのpingエコー要求に一致しています。これは、Site1 Client2からSite2 Client2へのpingがISP2 Tunnel 2経由でルーティングされることを示しています。Tunnel 1では、カプセル化カウンタまたはカプセル化解除カウンタの増加は示されていません。そのため、このトラフィックにはトンネル1が使用されていないことが確認されます。

// Site1 FTD:

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 1520, #pkts encrypt: 1520, #pkts digest: 1520
    #pkts decaps: 1521, #pkts decrypt: 1521, #pkts verify: 1521
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
    #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
    #pkts decaps: 25, #pkts decrypt: 25, #pkts verify: 25
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

ISP2が正常に動作している間、ISP1に割り込みが発生する

この例では、ISP1のインターフェイスE0/1を手動でシャットダウンして、中断が発生しているISP1をシミュレートします。

```
Internet_SP1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Internet_SP1(config)#
Internet_SP1(config)#interface E0/1
Internet_SP1(config-if)#shutdown
Internet_SP1(config-if)#exit
Internet_SP1(config)#
```

VPN

Tunnel1がダウンしました。IKEV2 SAではTunnel2だけがアクティブです。

// Site1 FTD:

```
ftdv742# show interface tunnel 1
Interface Tunnel1 "demovti", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
  IP address 169.254.10.1, subnet mask 255.255.255.0
Tunnel Interface Information:
  Source interface: outside    IP address: 192.168.30.1
  Destination IP address: 192.168.10.1
  IPsec MTU Overhead : 0
  Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d
```

```
ftdv742# show crypto ikev2 sa
```

IKEv2 SAs:

Session-id:148, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local                                Remote
1045734377 192.168.40.1/500                    192.168.20.1/500
  Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
  Life/Active Time: 86400/80266 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: 0x47bfa607/0x82e8781d
```

// Site2 FTD:

```
ftdv742# show interface tunnel 1
Interface Tunnel1 "demovti25", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
  IP address 169.254.10.2, subnet mask 255.255.255.0
Tunnel Interface Information:
  Source interface: outside    IP address: 192.168.10.1
  Destination IP address: 192.168.30.1
  IPsec MTU Overhead : 0
  Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d
```

```
ftdv742#
```

```
ftdv742# show crypto ikev2 sa
```

IKEv2 SAs:

Session-id:36, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote
477599833 192.168.20.1/500 192.168.40.1/500
    Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
    Life/Active Time: 86400/80382 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: 0x82e8781d/0x47bfa607
```

ルート

ルートテーブルでは、バックアップルートが有効になります。

// Site1 FTD:

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 192.168.40.4 to network 0.0.0.0

```
S* 0.0.0.0 0.0.0.0 [2/0] via 192.168.40.4, outside2
C 169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L 169.254.20.11 255.255.255.255 is directly connected, demovti_sp2
S 192.168.20.1 255.255.255.255 [1/0] via 192.168.40.4, outside2
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
C 192.168.40.0 255.255.255.0 is directly connected, outside2
L 192.168.40.1 255.255.255.255 is directly connected, outside2
S 192.168.50.0 255.255.255.0 [22/0] via 169.254.20.12, demovti_sp2
S 192.168.50.10 255.255.255.255 [1/0] via 169.254.20.12, demovti_sp2
C 192.168.70.0 255.255.255.0 is directly connected, inside
L 192.168.70.1 255.255.255.255 is directly connected, inside
```

// Site2 FTD:

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 192.168.10.3 to network 0.0.0.0

```
S*    0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C     169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L     169.254.20.12 255.255.255.255 is directly connected, demovti_sp2
C     192.168.10.0 255.255.255.0 is directly connected, outside
L     192.168.10.1 255.255.255.255 is directly connected, outside
C     192.168.20.0 255.255.255.0 is directly connected, outside2
L     192.168.20.1 255.255.255.255 is directly connected, outside2
S     192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C     192.168.50.0 255.255.255.0 is directly connected, inside
L     192.168.50.1 255.255.255.255 is directly connected, inside
S     192.168.70.0 255.255.255.0 [22/0] via 169.254.20.11, demovti_sp2
S     192.168.70.10 255.255.255.255 [1/0] via 169.254.20.11, demovti_sp2
```

SLAモニタ

Site1 FTDで、SLAモニタはISP1のエントリ番号855903900タイムアウト (ターゲットアドレスは192.168.30.3) を示します。

// Site1 FTD:

```
ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.131 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1786
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 100
Latest operation start time: 14:22:05.132 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 100    RTTMin: 100    RTTMax: 100
NumOfRTT: 1    RTTSum: 100    RTTSum2: 10000
```

```
Entry number: 855903900
Modification time: 08:37:05.132 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1786
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 14:22:05.134 UTC Thu Aug 15 2024
Latest operation return code: Timeout
```

```
RTT Values:
RTTAvg: 0    RTTMin: 0    RTTMax: 0
NumOfRTT: 0    RTTSum: 0    RTTSum2: 0
```

```
ftdv742# show track
```

```
Track 1
```

```
Response Time Reporter 855903900 reachability
Reachability is Down
7 changes, last change 00:11:03
Latest operation return code: Timeout
Tracked by:
  STATIC-IP-ROUTING 0
```

```
Track 2
```

```
Response Time Reporter 188426425 reachability
Reachability is Up
4 changes, last change 13:15:11
Latest operation return code: OK
Latest RTT (milliseconds) 140
Tracked by:
  STATIC-IP-ROUTING 0
```

ping テスト

pingを発行する前に、Site1 FTDのshow crypto ipsec sa | inc interface:|encap|decapのカウントを確認します。

この例では、Tunnel2にカプセル化のための36個のパケットとカプセル化解除のための35個のパケットが表示されています。

```
// Site1 FTD:
```

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti_sp2
  #pkts encaps: 36, #pkts encrypt: 36, #pkts digest: 36
  #pkts decaps: 35, #pkts decrypt: 35, #pkts verify: 35
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 ping Site2 Client1が正常に実行されました。

```
Site1_Client1#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 = 22/133/253 ms
```

Site1 Client2 ping Site2 Client2が正常に実行されました。

```
Site1_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 = 34/56/87 ms
```

pingが成功した後、Site1 FTDのshow crypto ipsec sa | inc interface:|encap|decapのカウントをチェックします。

この例では、Tunnel 2はカプセル化のための46パケットとカプセル化解除のための45パケットを示しており、両方のカウンタは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パケットがISP2のTunnel 2経由でルーティングされることを示しています。

```
// Site1 FTD:
```

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti_sp2
    #pkts encaps: 46, #pkts encrypt: 46, #pkts digest: 46
    #pkts decaps: 45, #pkts decrypt: 45, #pkts verify: 45
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

ISP1が正常に動作している間に、ISP2で中断が発生する

この例では、ISP2のインターフェイスE0/1を手動でシャットダウンして、中断が発生しているISP2をシミュレートします。

```
Internet_SP2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Internet_SP2(config)#
Internet_SP2(config)#int e0/1
Internet_SP2(config-if)#shutdown
Internet_SP2(config-if)#^Z
Internet_SP2#
```

VPN

Tunnel2がダウンしました。IKEV2 SAではTunnel1だけがアクティブです。

```
// Site1 FTD:
```

```
ftdv742# show interface tunnel 2
Interface Tunnel2 "demovti_sp2", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
  IP address 169.254.20.11, subnet mask 255.255.255.0
  Tunnel Interface Information:
```

```
Source interface: outside2    IP address: 192.168.40.1
Destination IP address: 192.168.20.1
IPsec MTU Overhead : 0
Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d
```

```
ftdv742# show crypto ikev2 sa
```

IKEv2 SAs:

Session-id:159, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote
1375077093 192.168.30.1/500 192.168.10.1/500
  Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
  Life/Active Time: 86400/349 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: 0x40f407b4/0x26598bcc
```

// Site2 FTD:

```
ftdv742# show int tunnel 2
Interface Tunnel2 "demovti_sp2", is down, line protocol is down
Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
IP address 169.254.20.12, subnet mask 255.255.255.0
Tunnel Interface Information:
Source interface: outside2    IP address: 192.168.20.1
Destination IP address: 192.168.40.1
IPsec MTU Overhead : 0
Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d
```

```
ftdv742# show crypto ikev2 sa
```

IKEv2 SAs:

Session-id:165, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote
1025640731 192.168.10.1/500 192.168.30.1/500
  Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
  Life/Active Time: 86400/379 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: 0x26598bcc/0x40f407b4
```

ルート

ルートテーブルで、ISP2関連のルートがPBRトラフィック用に消失しました。

// Site1 FTD:

```
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
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
C       192.168.40.0 255.255.255.0 is directly connected, outside2
L       192.168.40.1 255.255.255.255 is directly connected, outside2
S       192.168.50.0 255.255.255.0 [1/0] via 169.254.10.2, demovti
C       192.168.70.0 255.255.255.0 is directly connected, inside
L       192.168.70.1 255.255.255.255 is directly connected, inside
```

// Site2 FTD:

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 192.168.10.3 to network 0.0.0.0

```
S*      0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C       169.254.10.0 255.255.255.0 is directly connected, demovti25
L       169.254.10.2 255.255.255.255 is directly connected, demovti25
C       192.168.10.0 255.255.255.0 is directly connected, outside
L       192.168.10.1 255.255.255.255 is directly connected, outside
C       192.168.20.0 255.255.255.0 is directly connected, outside2
L       192.168.20.1 255.255.255.255 is directly connected, outside2
S       192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C       192.168.50.0 255.255.255.0 is directly connected, inside
L       192.168.50.1 255.255.255.255 is directly connected, inside
S       192.168.70.0 255.255.255.0 [1/0] via 169.254.10.1, demovti25
```

SLAモニタ

Site1 FTDで、SLAモニタはISP2のエントリ番号188426425タイムアウト (ターゲットアドレスは192.168.40.4) を示します。

// Site1 FTD:

```
ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.133 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1816
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 14:52:05.174 UTC Thu Aug 15 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0    RTTMin: 0    RTTMax: 0
NumOfRTT: 0    RTTSum: 0    RTTSum2: 0
```

```
Entry number: 855903900
Modification time: 08:37:05.135 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1816
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 10
Latest operation start time: 14:52:05.177 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 10    RTTMin: 10    RTTMax: 10
NumOfRTT: 1    RTTSum: 10    RTTSum2: 100
```

```
ftdv742# show track
```

```
Track 1
```

```
Response Time Reporter 855903900 reachability
Reachability is Up
8 changes, last change 00:14:37
Latest operation return code: OK
Latest RTT (millisecs) 60
Tracked by:
  STATIC-IP-ROUTING 0
```

```
Track 2
```

```
Response Time Reporter 188426425 reachability
Reachability is Down
5 changes, last change 00:09:30
Latest operation return code: Timeout
Tracked by:
  STATIC-IP-ROUTING 0
```

ping テスト

pingを発行する前に、Site1 FTDのshow crypto ipsec sa | inc interface:|encap|decapのカウントを

確認します。

この例では、Tunnel 1にカプセル化のための74個のパケットとカプセル化解除のための73個のパケットが示されています。

// Site1 FTD:

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 74, #pkts encrypt: 74, #pkts digest: 74
    #pkts decaps: 73, #pkts decrypt: 73, #pkts verify: 73
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 ping Site2 Client1が正常に実行されました。

```
Site1_Client1#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 = 30/158/255 ms
```

Site1 Client2 ping Site2 Client2が正常に実行されました。

```
Site1_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 = 6/58/143 ms
```

pingが成功した後、Site1 FTDのshow crypto ipsec sa | inc interface:|encap|decapのカウンタをチェックします。

この例では、Tunnel 1にカプセル化のための84個のパケットとカプセル化解除のための83個のパケットがあり、両方のカウンタが10パケット増加して、10個のpingエコー要求に一致しています。これは、pingパケットがISP1のTunnel 1経由でルーティングされることを示しています。

// Site1 FTD:

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 84, #pkts encrypt: 84, #pkts digest: 84
    #pkts decaps: 83, #pkts decrypt: 83, #pkts verify: 83
    #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。

次の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
```

PBRセクションのトラブルシューティングを行うには、次のdebugコマンドを使用できます。

```
debug policy-route
```

次のdebugコマンドを使用して、SLAモニタ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。

```
ftdv742# debug sla monitor ?
  error  Output IP SLA Monitor Error Messages
  trace  Output IP SLA Monitor Trace Messages
```

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。