単一のFMCによって管理されるFTD間のVPN移行の設定

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

設定

- 手順

確認

トラブルシュート

- 初期接続の問題
- トラフィック固有の問題

はじめに

このドキュメントでは、ルータへのVPN接続を維持しながら、同じFMCによって管理される1つのFTDから別のFTDにサイト間VPNを移行する方法について説明します。

前提条件

要件

移行プロセスを効果的に実行するために、次の項目に精通しておくことをお勧めします。
・ FMCへのFTD登録： Firepower Threat Defense(FTD)デバイスをFirepower Management Center(FMC)に登録する方法について
・ サイト間VPN設定： FMCの管理対象FTDデバイスでサイト間VPNを設定した経験。

使用するコンポーネント

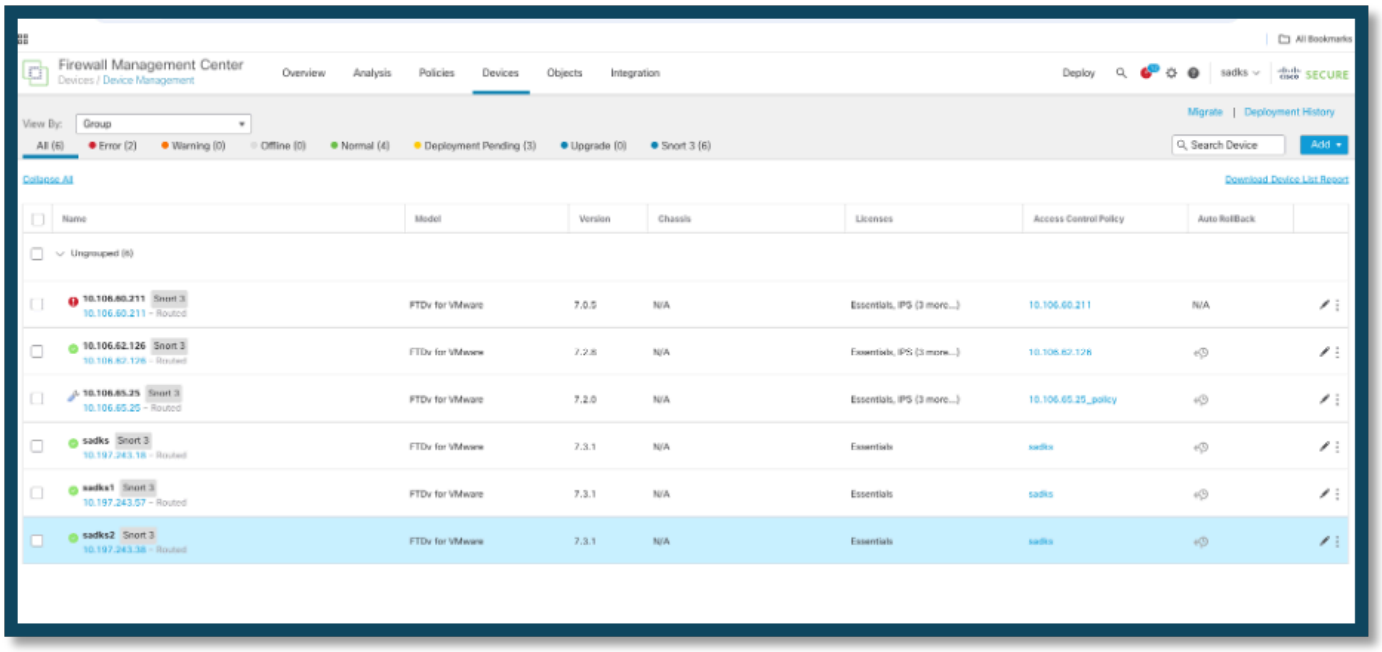
このドキュメントは、次のソフトウェアとハードウェアのバージョンに基づいています。
・ Firepower Threat Defense(FTDv)仮想：バージョン7.3.1を実行する2つのインスタンス。
・ Firepower Management Center(FMC):バージョン7.4.0

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。

設定

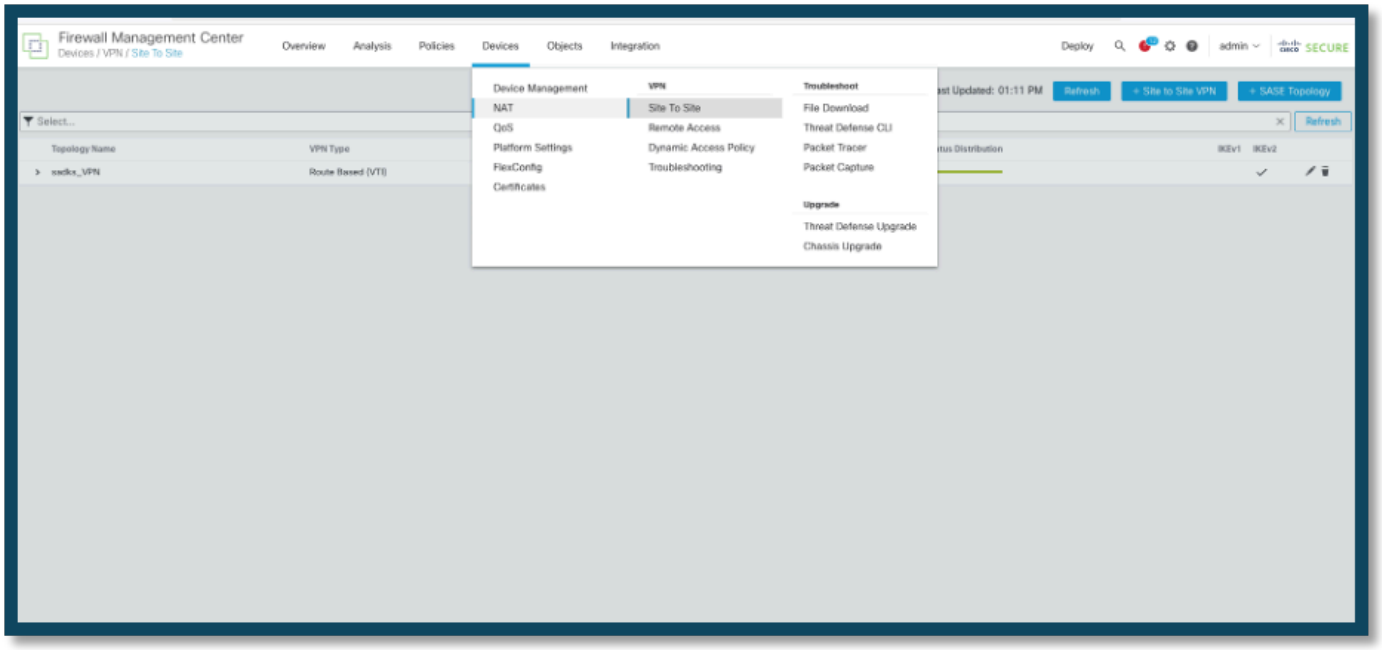
手順

1. FMCに新しいFTDを登録します。
　・ Firepower Management Center(FMC)のDevices > Device Managementで、新しいFirepower Threat Defense(FTD)デバイスを登録することから始めます。
　・ この例では、登録された新しいデバイスの名前は「sadks2」です。



新しいFTDの登録

2. サイト間トンネル設定へのアクセス：
　・ FMCインターフェイスでDevices > Site to Siteの順に選択し、サイト間トンネルの設定に移動します。

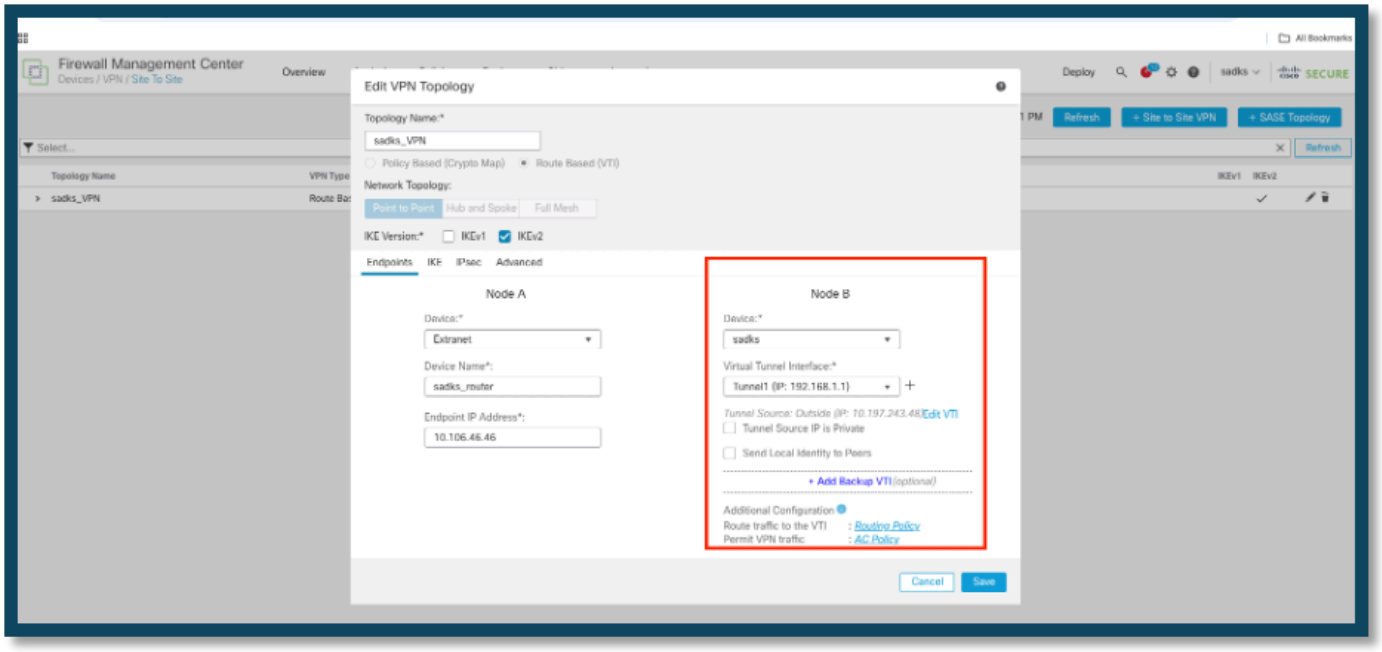


VPN Configに移動します。

3. VPN設定を変更します。

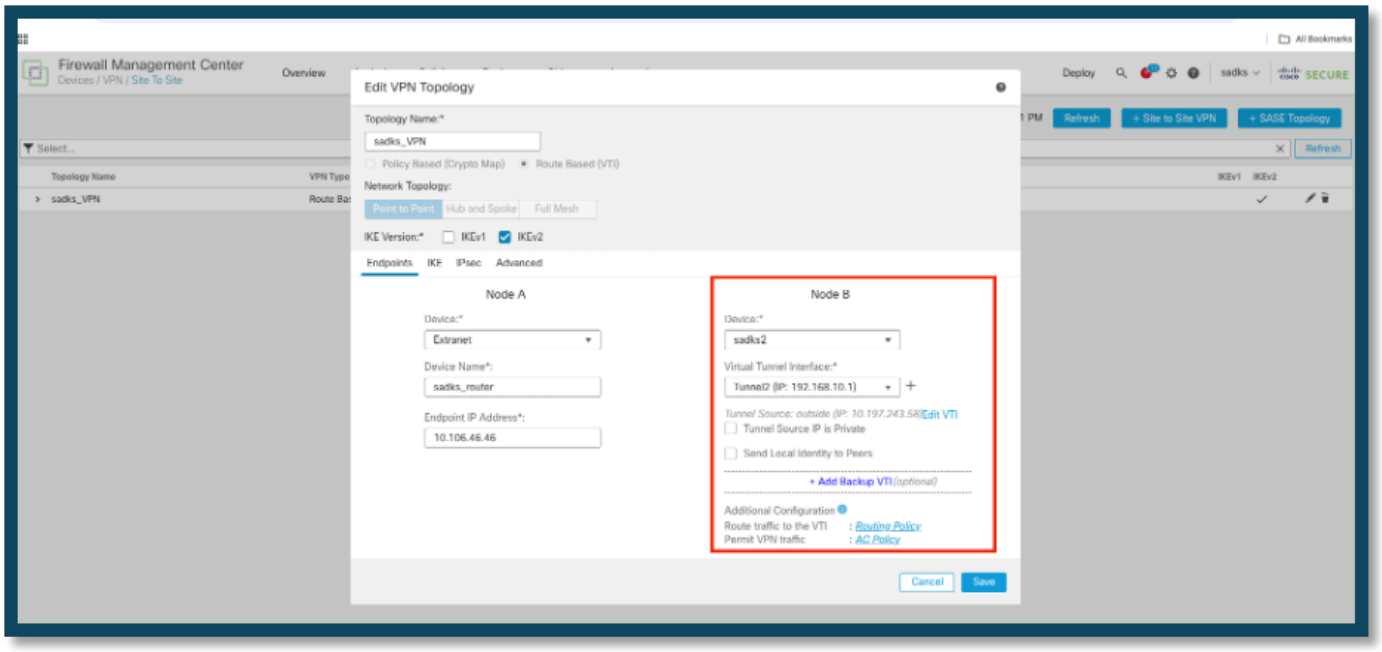
・ 更新するVPN構成を選択します。

・ 例：このシナリオでは、VPN設定にFTDデバイスとルータが含まれます。ここで、ノードBはFTDデバイスを表し、設定が更新されて、デバイスの関連付けが「sadks」から「sadks2」に変更されました。



古いFTDデバイス

TO



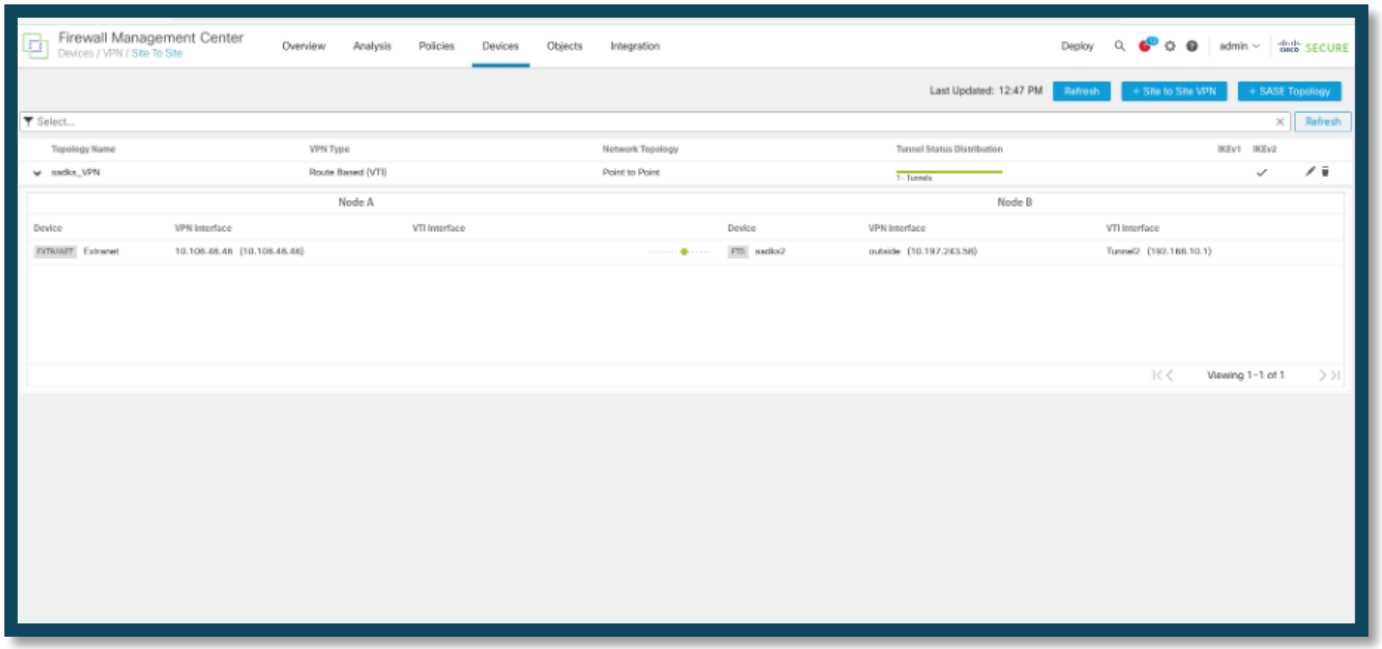
新しいFTDデバイス

4. 設定を保存して展開します。

- 必要な変更を行った後、構成を保存して展開し、更新プログラムをアクティブ化します。

確認

トンネルは、導入後にアップ状態になります。



トンネルステータス

トラブルシュート

初期接続の問題

VPNを構築する際には、トンネルをネゴシエートしている2つの側があります。したがって、あらゆるタイプのトンネル障害をトラブルシューティングする場合は、会話の両側を調べるのが最善です。 IKEv2トンネルのデバッグ方法の詳細については、「IKEv2 VPNのデバッグ方法」を参照してください。

トンネル障害の最も一般的な原因は、接続の問題です。これを判断する最善の方法は、デバイスでパケットキャプチャを取得することです。 デバイスでパケットキャプチャを取得するには、次のコマンドを使用します。

<#root>

```
capture capout interface outside match ip host 10.106.46.46 host 10.197.243.58
```

キャプチャが設定されたら、VPN経由でトラフィックを送信し、パケットキャプチャに双方向トラフィックが含まれていないかを確認します。

次のコマンドを使用して、パケットキャプチャを確認します。

<#root>

```
show cap capout
```

トラフィック固有の問題

発生する一般的なトラフィックの問題は次のとおりです。

- FTDの背後のルーティング問題：内部ネットワークが、割り当てられたIPアドレスとVPNクライアントにパケットをルーティングして戻すことができません。
- トラフィックをブロックするアクセスコントロールリスト。
- Network Address Translation（NAT；ネットワークアドレス変換）がVPNトラフィックにバイパスされていない。

FMCによって管理されるFTDでのVPNに関する詳細については、次のリンクで設定ガイドを参照できます。FMCによって管理されるFTD設定ガイド

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。