シームレスな移行：Palo AltoファイアウォールからCisco FTDへの移行

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

Firepower移行ツール(FMT)

移行ガイドライン

- 1. 移行前チェックリスト
- 2. 移行ツールの使用
- 3. 移行後の検証

既知の問題

- 1. FTDにインターフェイスがない
- 2. ルーティングテーブル
- 3. 最適化

結論

はじめに

このドキュメントでは、FMTバージョン6.0を採用して、Palo AltoファイアウォールからCisco FTDシステムに移行するプロセス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。

- Palo Altoファイアウォールから現在の実行コンフィギュレーションをXML形式(*.xml)でエクスポートします。
- Palo AltoファイアウォールCLIにアクセスし、show routing routeコマンドを実行してから、出力をテキストファイル(*.txt)として保存します。
- コンフィギュレーションファイル(*.xml)とルーティング出力ファイル(*.txt)の両方を1つのZIPアーカイブ(*.zip)に圧縮します。

使用するコンポーネント

このドキュメントの情報は、Palo Alto Firewallバージョン8.4.x以降に基づくものです。

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。

Firepower移行ツール(FMT)

FMTは、エンジニアリングチームが既存のベンダーファイアウォールをシスコの次世代ファイアウォール(NGFW)/Firepower Threat Defense(FTD)に移行する際に役立ちます。 シスコのWebサイトからダウンロードした最新バージョンのFMTを使用していることを確認します。

移行ガイドライン

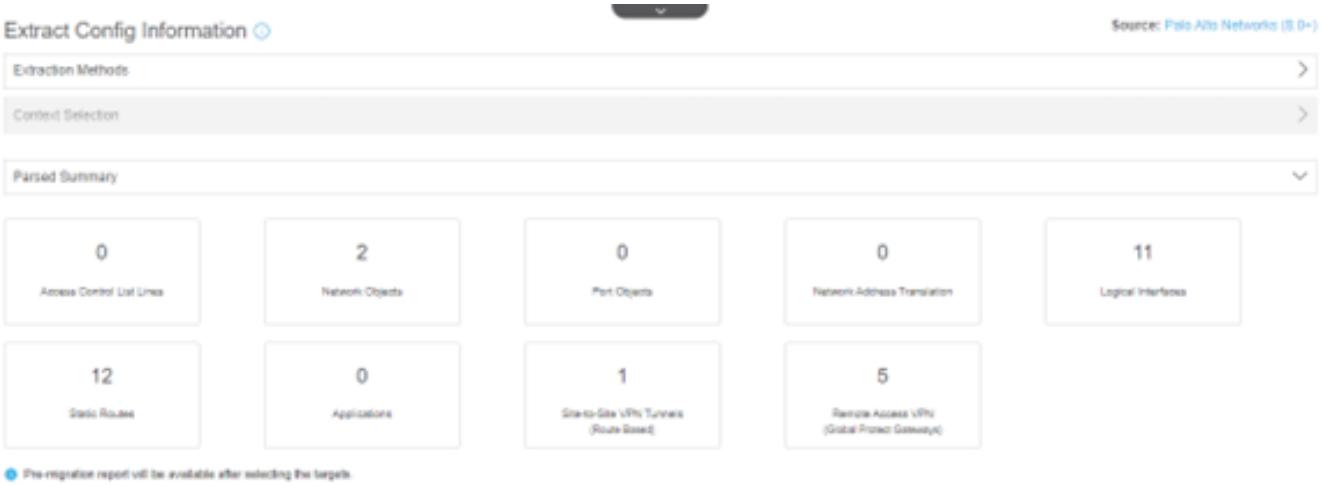
1. 移行前チェックリスト

- 移行プロセスを開始する前に、FTDがFMCに追加されていることを確認します。
- 管理者権限を持つ新しいユーザアカウントがFMCに作成されました。
- エクスポートされたPalo Alto実行コンフィギュレーションfile.xmlは、拡張子.zipでzip圧縮する必要があります。
- NGFW/FTDは、物理インターフェイスまたはサブインターフェイスの数が同じであるか、ポートチャネルがPalo Alto Firewallインターフェイスと同じである必要があります。

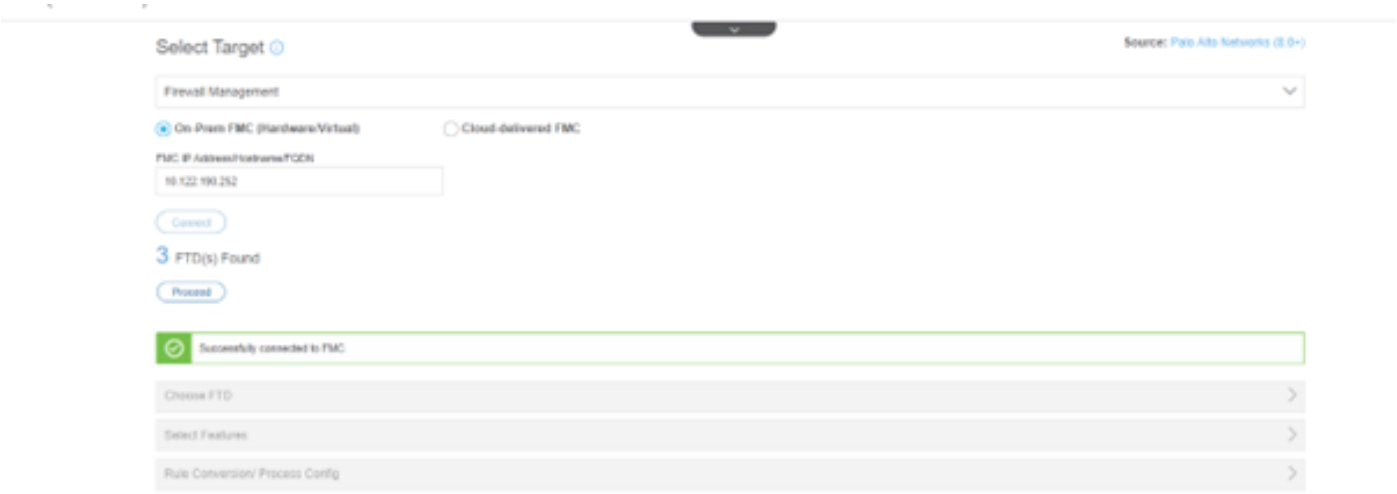
2. 移行ツールの使用

- FMTツール.exeをダウンロードし、管理者として実行します。
- FMTにログインするには、CEC IDまたはシスコユーザアカウントが必要です。
- ログインに成功すると、ツールがダッシュボードを表示します。ここでファイアウォールベンダーを選択し、対応する*.zipファイルをアップロードできます。次の図を参照してください。

- 移行を進める前に、右側に表示される指示をよく確認してください。
- 準備ができたら、Start Migrationをクリックします。
- Palo Altoファイアウォールの設定を含む保存済みの*.zipファイルをアップロードします。
- コンフィギュレーションファイルをアップロードすると、内容の「Parsed Summary」を確認し、nextをクリックできます。次の図を参照してください。

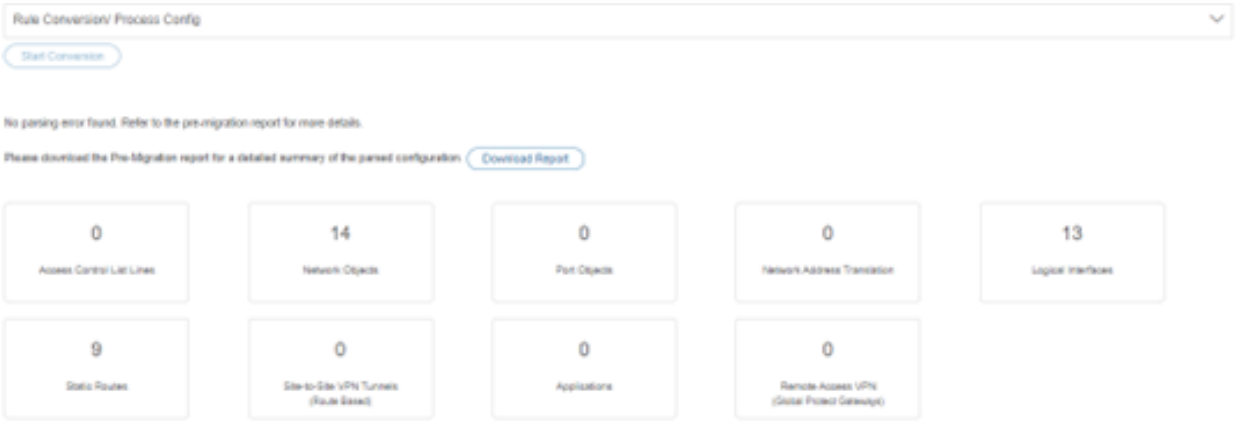


- FMCのIPアドレスを入力してログインします。
- このツールは、FMCに登録されているアクティブなFTDを検索します。
- 移行するFTDを選択し、次の図に示すようにProceedをクリックします。

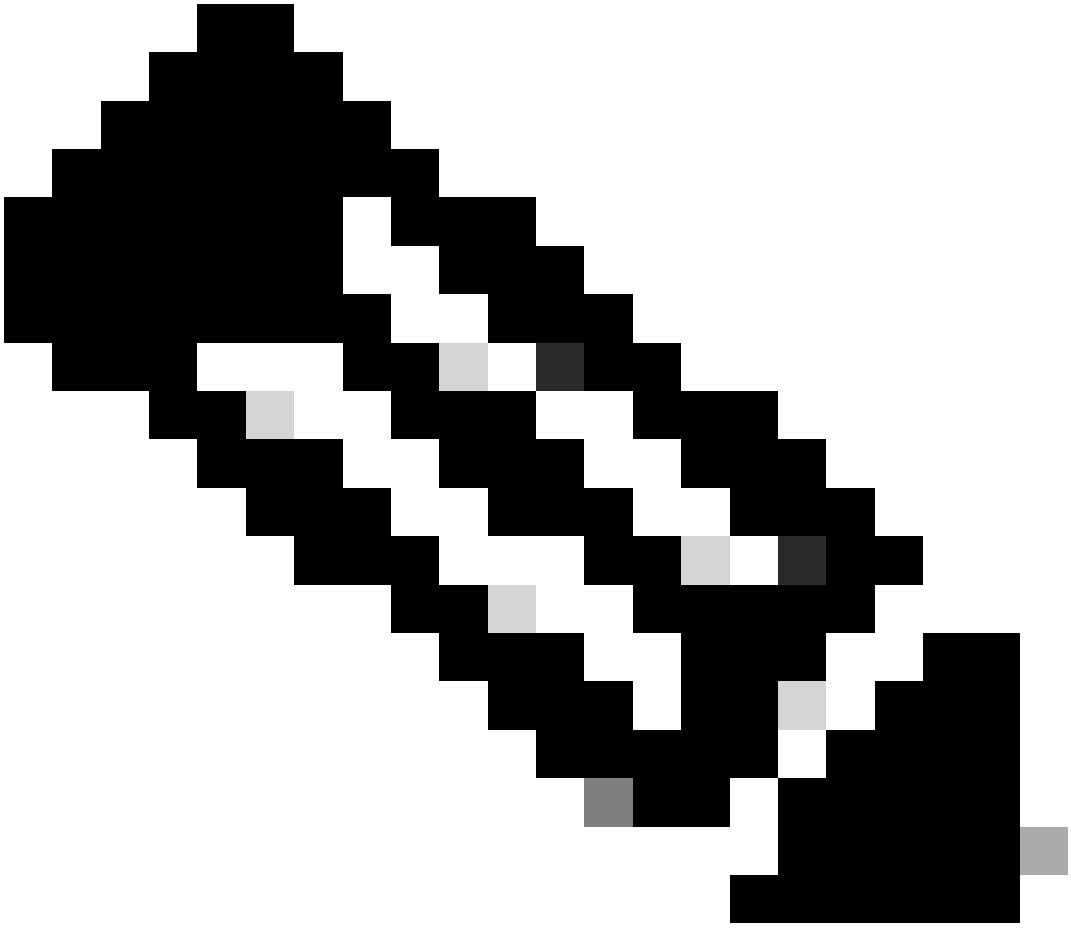


- お客様の要件に基づいて、移行する具体的な機能を選択します。Palo Altoのファイアウォールには、FTDとは異なる機能セットがあることに注意してください。
- Proceedをクリックし、次の図を参照して確認してください。

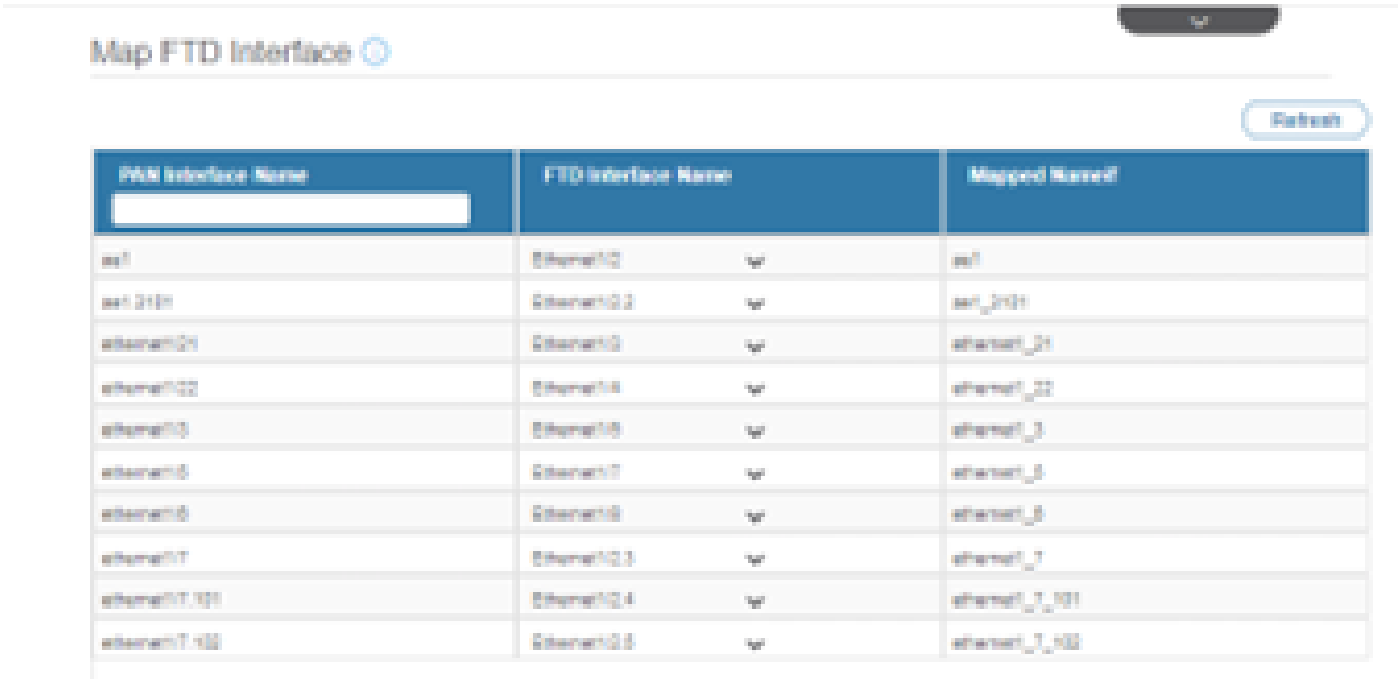
- FMTは、選択に従って変換を実行します。移行前レポートの変更を確認し、Proceedをクリックします。次の図を参照してください。



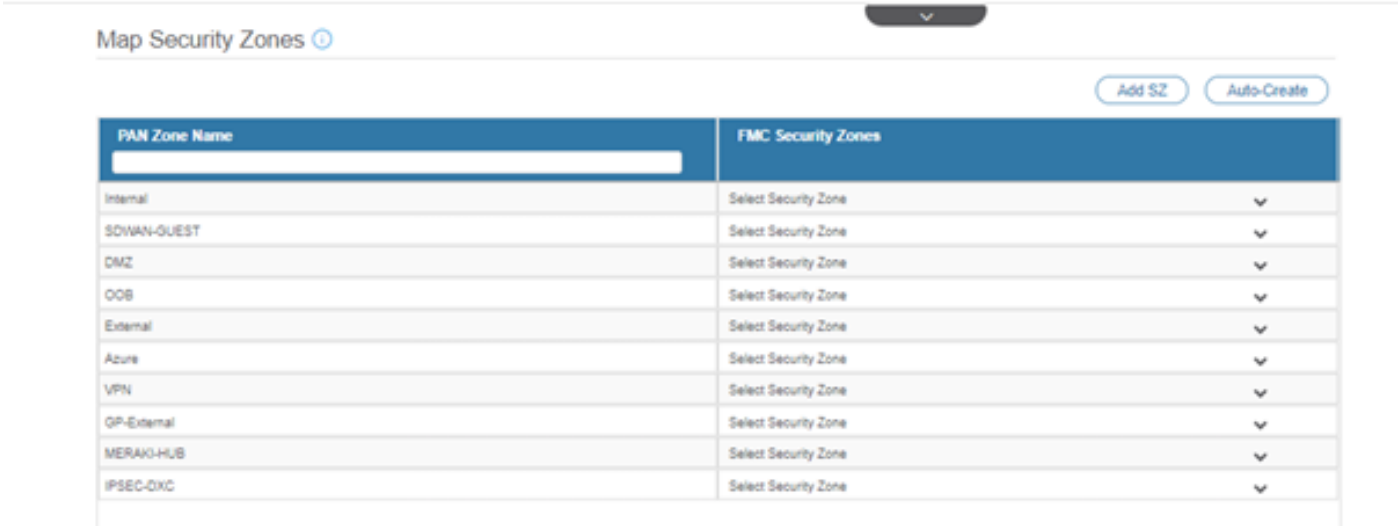
- Palo Altoファイアウォールのインターフェイスを FTDのインターフェイスにマッピングします。詳細については、次の図を参照してください。



注:NGFW/FTDは、物理インターフェイスまたはサブインターフェイスの数が同じであるか、ポートチャネルがサブインターフェイスを含むPalo Alto Firewallインターフェイスと同じである必要があります。



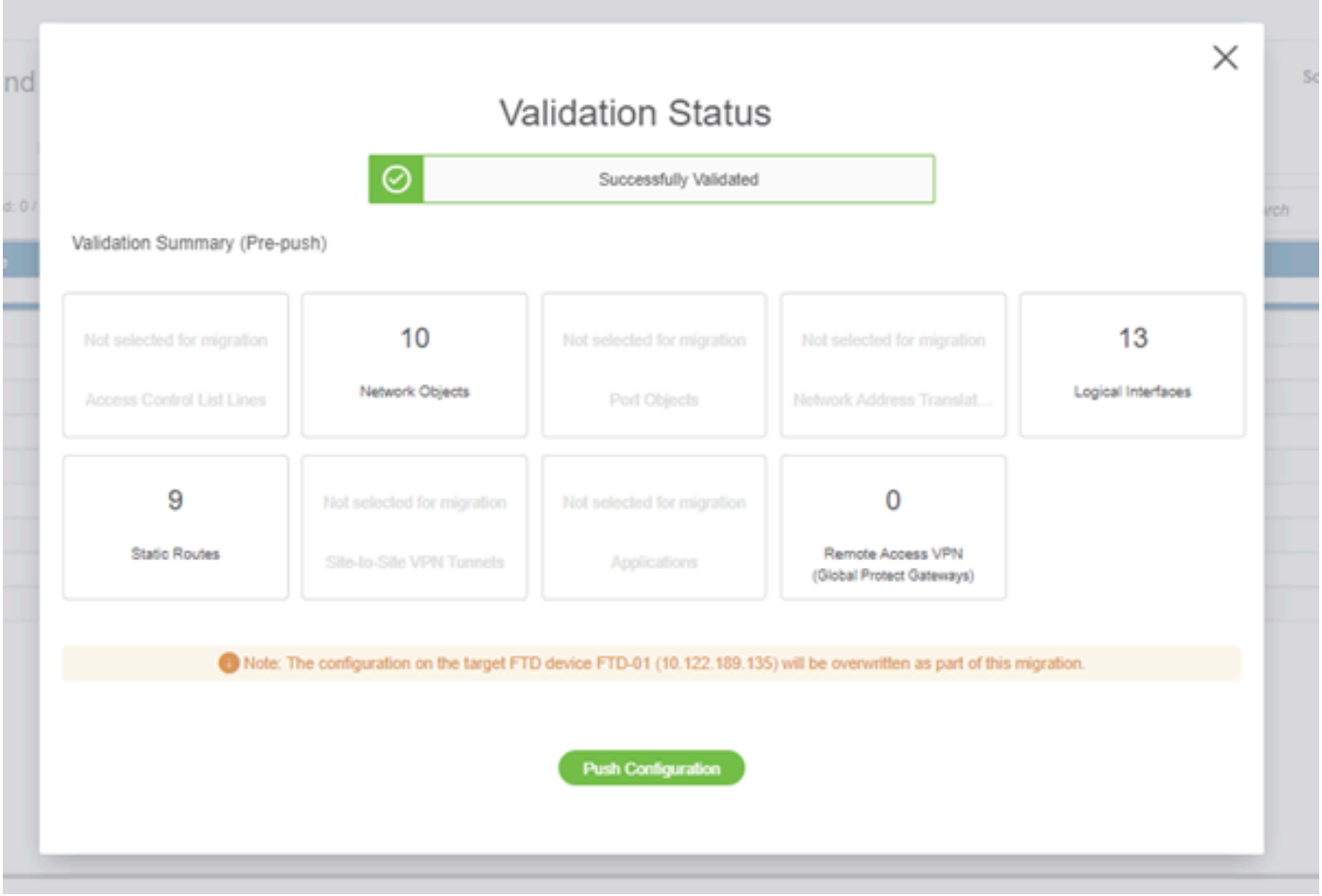
- 手動または自動作成機能を使用して、ゾーンのマッピングを決定します。視覚化については、次の図を参照してください。



- アプリケーションブロッキングプロファイルを割り当てます。これはアプリケーションマッピングを使用しないラボデバイスであるため、デフォルト設定を続行できます。Nextをクリックして、表示された画像を参照します。

- 必要に応じて、ACL、オブジェクト、インターフェイス、およびルートを最適化します。これは最小限の設定のラボ設定であるため、デフォルトのオプションを使用して続行できます。次に、Validateをクリックして次のイメージを参照します。

- 検証が成功すると、設定は対象のFTDに展開される準備が整います。詳細な手順については、次の図を参照してください。



- プッシュ設定では、移行された設定がFMCに保存され、FTDに自動的に展開されます。
- 移行中に問題が発生した場合は、TACケースをオープンしてサポートを受けてください。

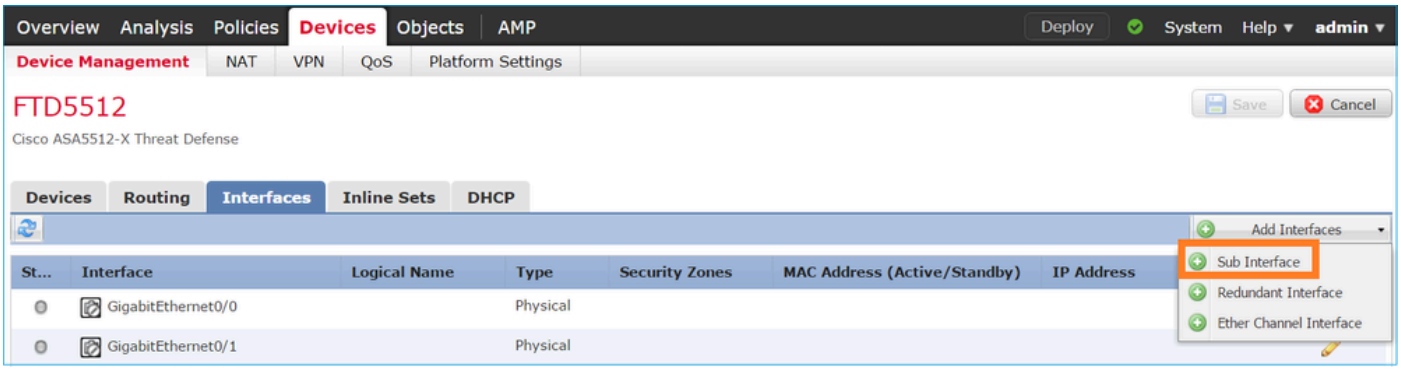
3. 移行後の検証

- FTDおよびFMCの設定を検証します。
- デバイスのACL、ポリシー、接続、およびその他の高度な機能をテストする。
- 変更を実行する前に、ロールバック· ポイントを作成します。
- 実稼働環境に移行する前に、ラボ環境で移行をテストします。

既知の問題

1. FTDにインターフェイスがない

- Palo Alto CLIにログインし、show interface allを実行します。FTDのインターフェイスの数以上が必要です。
- サブインターフェイス、ポートチャネル、またはFMC GUIを介した物理インターフェイスの数と同数以上のインターフェイスを作成します。
- FMC GUI Device > Device Managementの順に移動し、必要なインターフェイスを作成するFTDをクリックします。Interfaceセクションの下で、右隅のドロップダウンメニューからCreate Sub-interface/BVIを選択し、それに応じてインターフェイスを作成し、対応するインターフェイスを関連付けます。設定を保存し、デバイスに同期します。



- show interface ip briefを実行してインターフェイスがFTD上に作成されたことを確認し、インターフェイスマッピングの移行に進みます。

2. ルーティングテーブル

- Show routing routeまたはShow routing route summaryを実行して、Palo Altoファイアウォールのルーティングテーブルを確認します。
- FTDにルートを移行する前に、テーブルを確認し、プロジェクトのニーズに応じて必要なルートを選択します。
- show route allとshow route summaryを使用して、FTD内の同じルーティングテーブルを確認します。

3. 最適化

- [オブジェクトを最適化]パネルがグレー表示され、FMCで手動オブジェクトを作成してマッピングする必要がある場合があります。FTDでオブジェクトを表示するには、オブジェクトでShow Running |を使用し、Palo AltoではShow address <object name>を使用します。
- アプリケーションの移行には、移行前にPalo Altoファイアウォールの監査が必要です。FTDには専用のIPSデバイスが用意されていますが、FTDでこの機能を有効にすることもできるため、お客様の要件に従ってアプリケーション移行タスクを計画する必要があります。
- Palo AltoファイアウォールのNAT設定は、show running nat-policyにより確認する必要があり、カスタムNATポリシーをFTDで設定する必要があります。このポリシーは、Show Running natによりFTDで表示できます。

結論

Palo Altoファイアウォールは、FMTの支援により、Cisco FTDへの移行に成功しました。FTDでの移行後に問題が発生した場合は、さらにトラブルシューティングを行うために、TACケースを開きます。

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。