FMTを使用したPaloaltoのFirepower Threat Defense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
- 概要

背景説明

- Paloaltoファイアウォール設定zipファイルの取得
- 移行前のチェックリスト

設定

- 移行の手順

トラブルシュート

- Secure Firewall Migration Toolのトラブルシューティング
  - 一般的な移行エラー：
  - トラブルシューティングのためのサポートバンドルの使用：

はじめに

このドキュメントでは、PaloaltoファイアウォールをCisco Firepower Threat Device(FTD)に移行する手順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。

- Firepower移行ツール
- Paloaltoファイアウォール
- セキュアファイアウォール脅威対策(FTD)
- Cisco Secure Firewall Management Center(FMC)

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。

- Mac OSとFirepower Migration Tool(FMT)v7.7
- PAN NGFWバージョン8.0+
- Secure Firewall Management Center(FMCv)v7.6
- Secure Firewall Threat Defenseバージョン7.4.2

免責事項：このドキュメントで参照されているネットワークおよびIPアドレスは、個々のユーザ、グループ、または組織に関連付けられていません。この設定は、ラボ環境での使用のみを目的として作成されています。

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。

概要

このドキュメントの要件は次のとおりです。

- PAN NGFWバージョン8.4+以降
- Secure Firewall Management Center(FMCv)バージョン6.2.3以降

ファイアウォール移行ツールは、次のデバイスリストをサポートしています。

- Cisco ASA（8.4以降）
- Cisco ASA(9.2.2+)（FPSあり）
- Cisco Secure Firewall Device Manager（7.2以降）
- チェックポイント(r75-r77)
- チェックポイント(r80-r81)
- Fortinet（5.0以上）
- Palo Alto Networks（8.0以上）

背景説明

Paloalto Firewallの設定を移行する前に、次の作業を実行してください。

Paloaltoファイアウォール設定zipファイルの取得

- Paloalto Firewallはバージョン8.4以降である必要があります。
- 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エクスポートします（*.xmlはxml形式である必要があります）。
- Paloalto Firewall Cliにログインしてshow routing routeを実行し、出力をtxt形式(*.txt)で保存します。
- 実行コンフィギュレーションファイル(*.xml)とルーティングファイル(*.txt)を拡張子*.zipで圧縮します。

移行前のチェックリスト

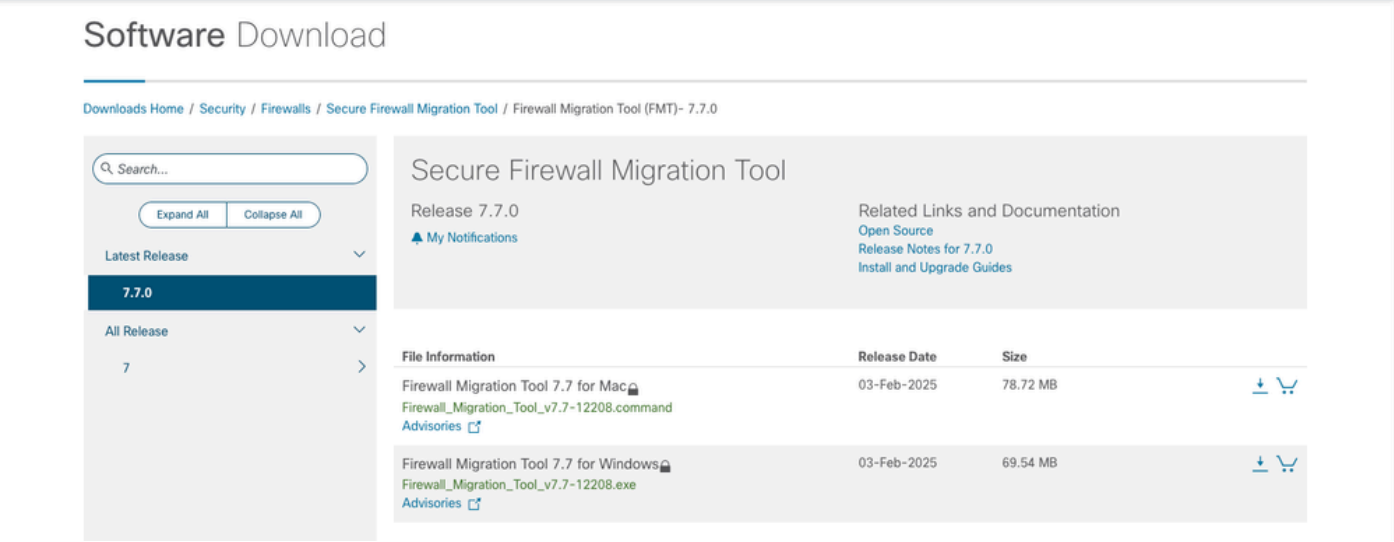
- 移行プロセスを開始する前に、FTDがFMCに登録されていることを確認します。
- 管理者権限を持つ新しいユーザアカウントがFMCに作成されました。または、既存の管理者クレデンシャルを使用することもできます。

- エクスポートされたPalo Altoの実行コンフィギュレーションfile.xmlは、拡張子.zipで圧縮する必要があります（前のセクションで説明した手順に従ってください）。
- Firepowerデバイスは、Paloalto Firewallインターフェイスと同数以上の物理インターフェイス、サブインターフェイス、またはポートチャネルを備えている必要があります。

設定

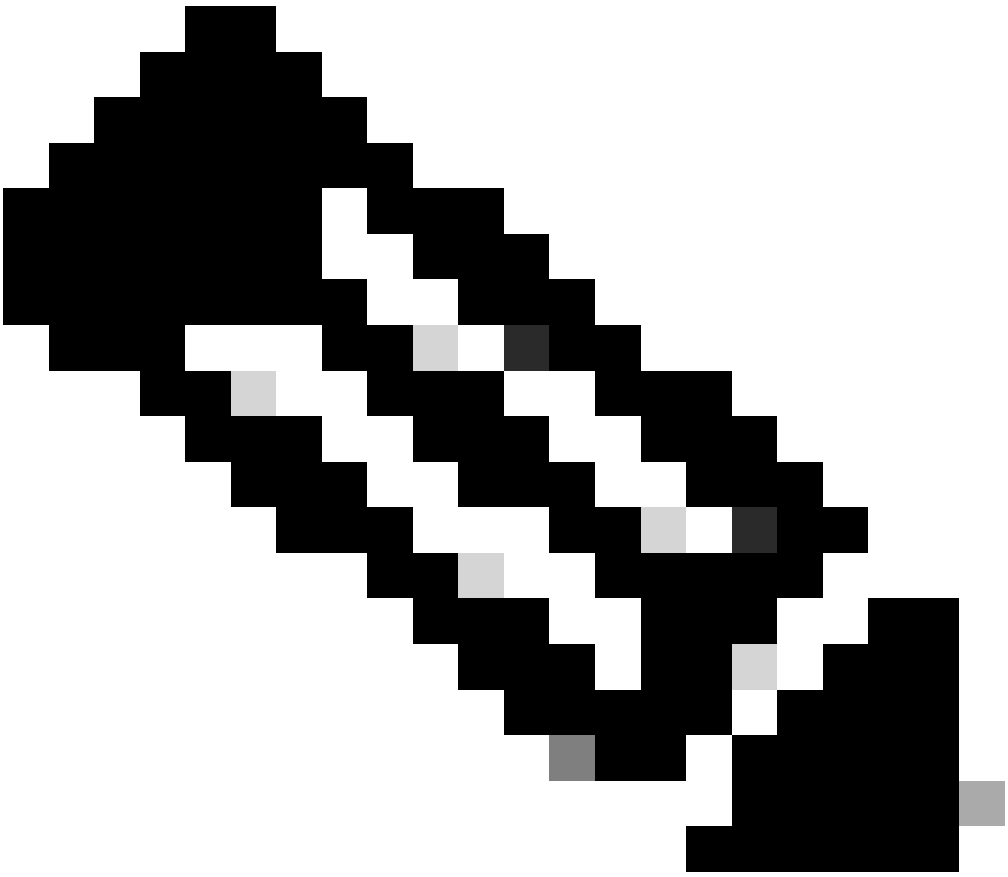
移行の手順

1. ご使用のコンピュータと互換性のあるCisco Software Centralから最新のFirepower移行ツールをダウンロードします。



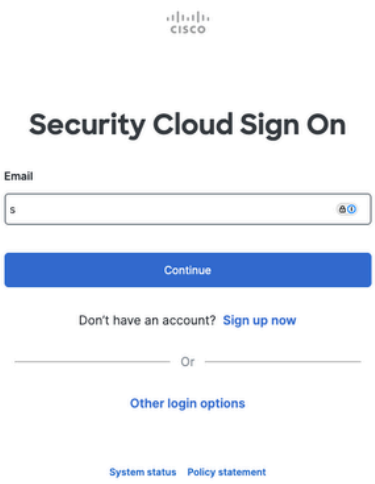
FMTダウンロード

3. コンピュータに以前にダウンロードしたファイルを開きます。



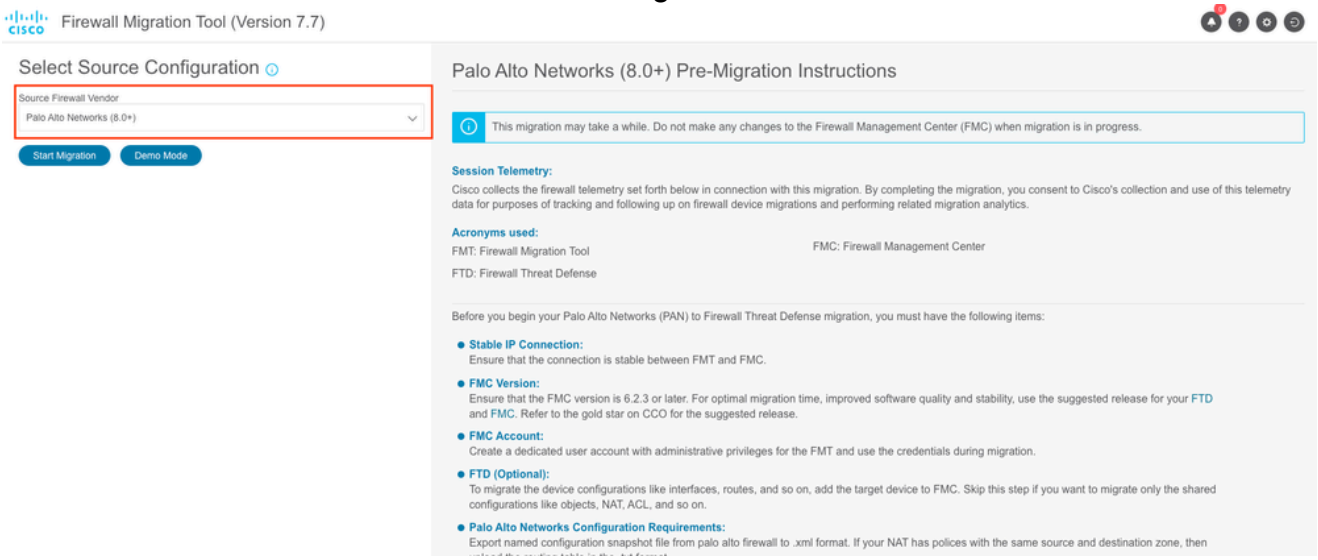
注：プログラムが自動的に開き、ファイルを実行したディレクトリのコンテンツがコンソールによって自動的に生成されます。

4. プログラムを実行すると、Webブラウザが開き、使用許諾契約書が表示されます。
    1. 契約条件に同意する場合は、このチェックボックスを選択します。
    2. [続行]をクリックします。
5. 有効なCCOクレデンシャルを使用してログインし、FMT GUIにアクセスします。



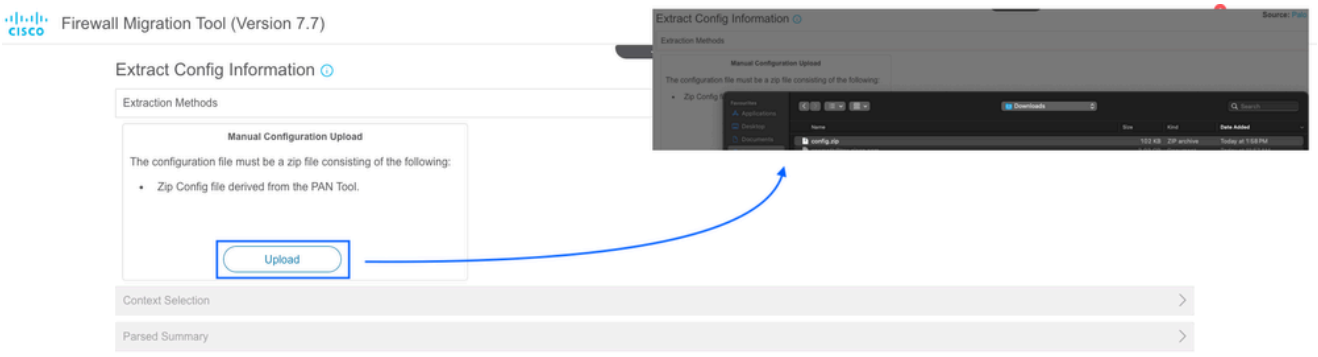
FMTログインプロンプト

6. 移行するSource Firewallを選択して、Start Migrationをクリックします。



FMTのGUI

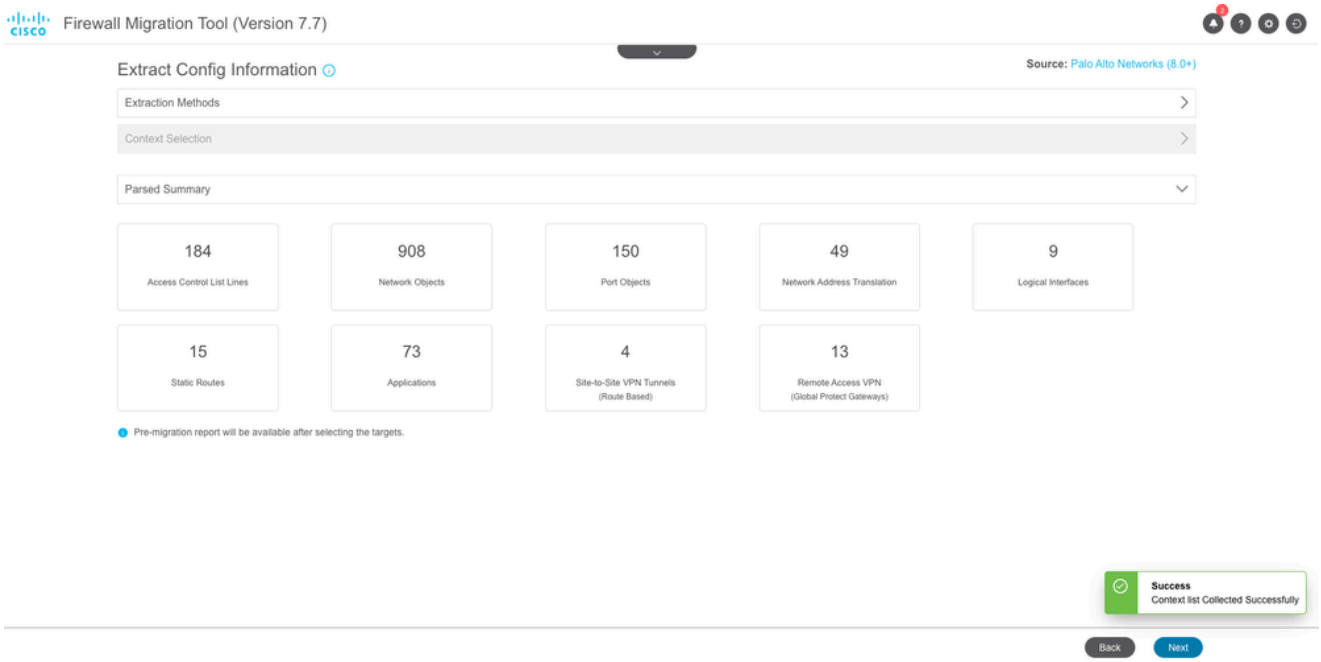
7. 抽出方法セクションが表示されるようになりました。このセクションで、Paloalto FirewallからFMTにZIP設定ファイルをアップロードする必要があります。



構成アップロードウィザード

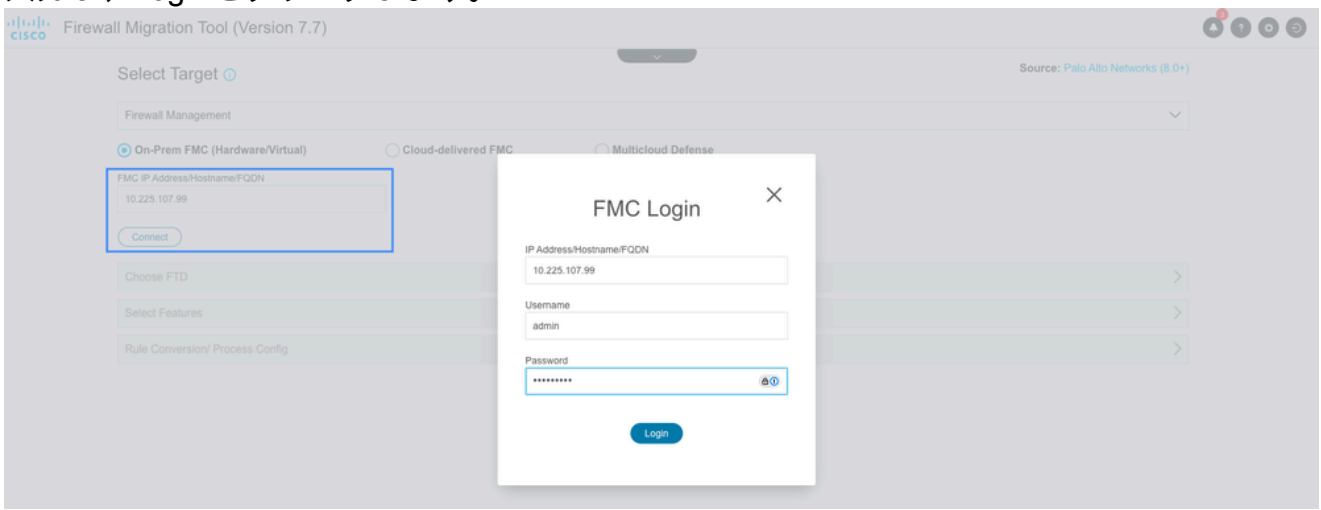
8. 構成ファイルのアップロード後に、解析された構成の概要が表示されるようになりました。VSYSの場合は、個別のVSYSを選択できます。各データを解析し、次々に移行する必要が

あります。
解析された要約を検証し、Nextアイコンをクリックします。



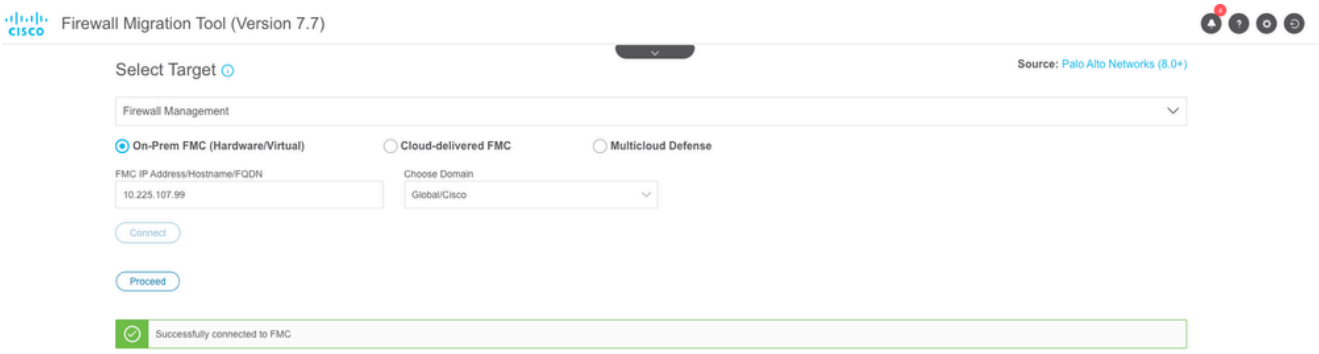
構成検証の概要

9. このセクションでは、FMCのタイプを選択できます。管理IPアドレスを入力して、Connectをクリックします。
ポップアップが表示され、FMCクレデンシャルの入力を求められます。クレデンシャルを入力し、Loginをクリックします。



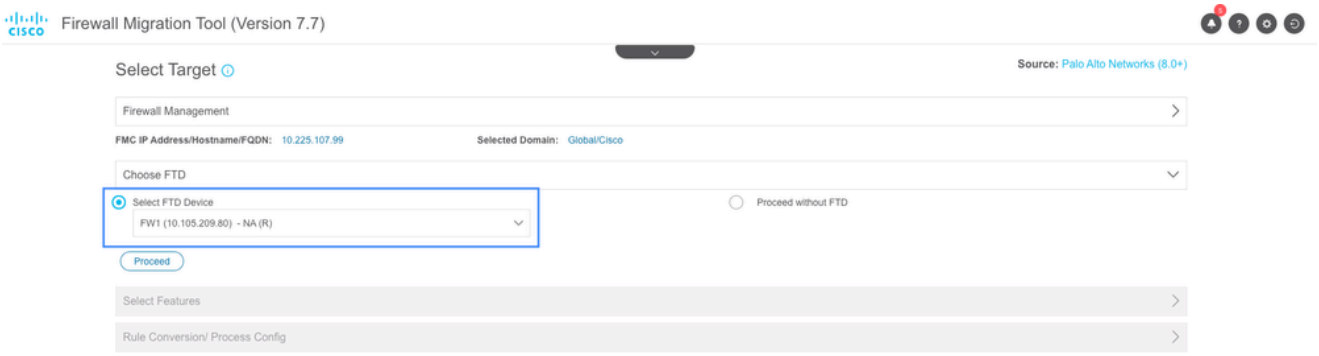
FMCログイン

10. FMCへの接続が成功したら、Domain（存在する場合）を選択し、Proceedをクリックします。



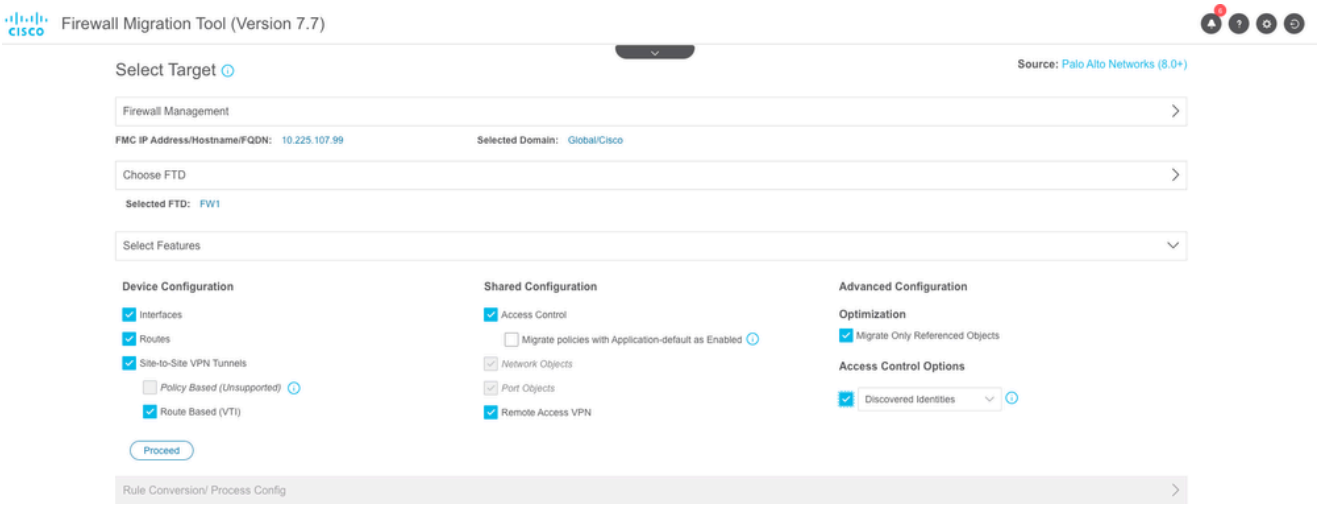
ドメインの選択

11. 移行先のFTDを選択し、Proceedをクリックします。

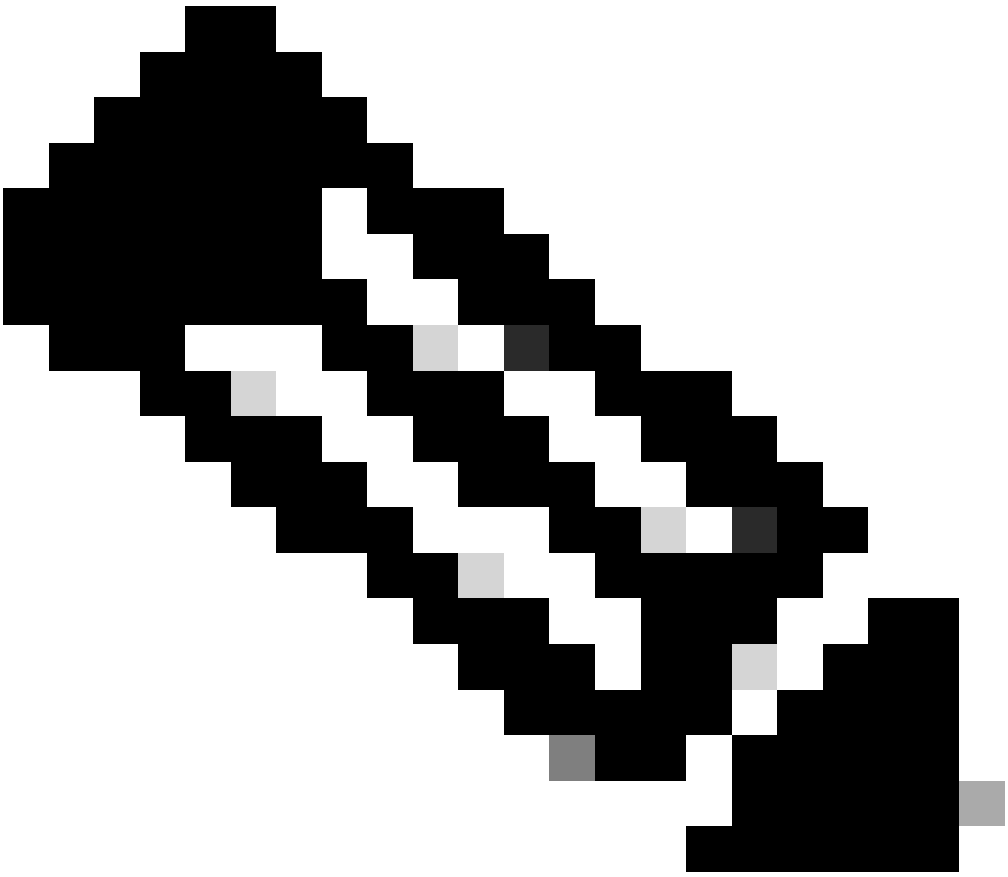


ターゲットFTDの選択

12. ツールに、移行される機能のリストが表示されます。[続行（Proceed）] をクリックします。

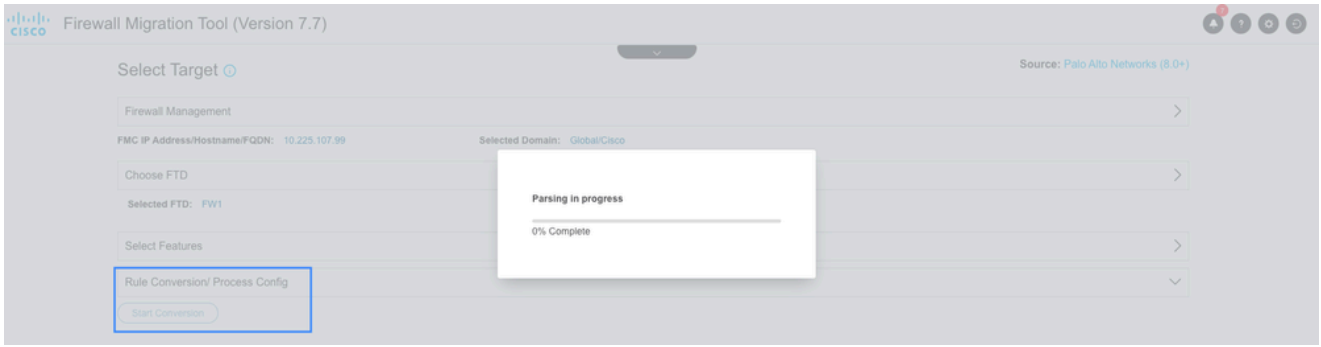


機能の選択



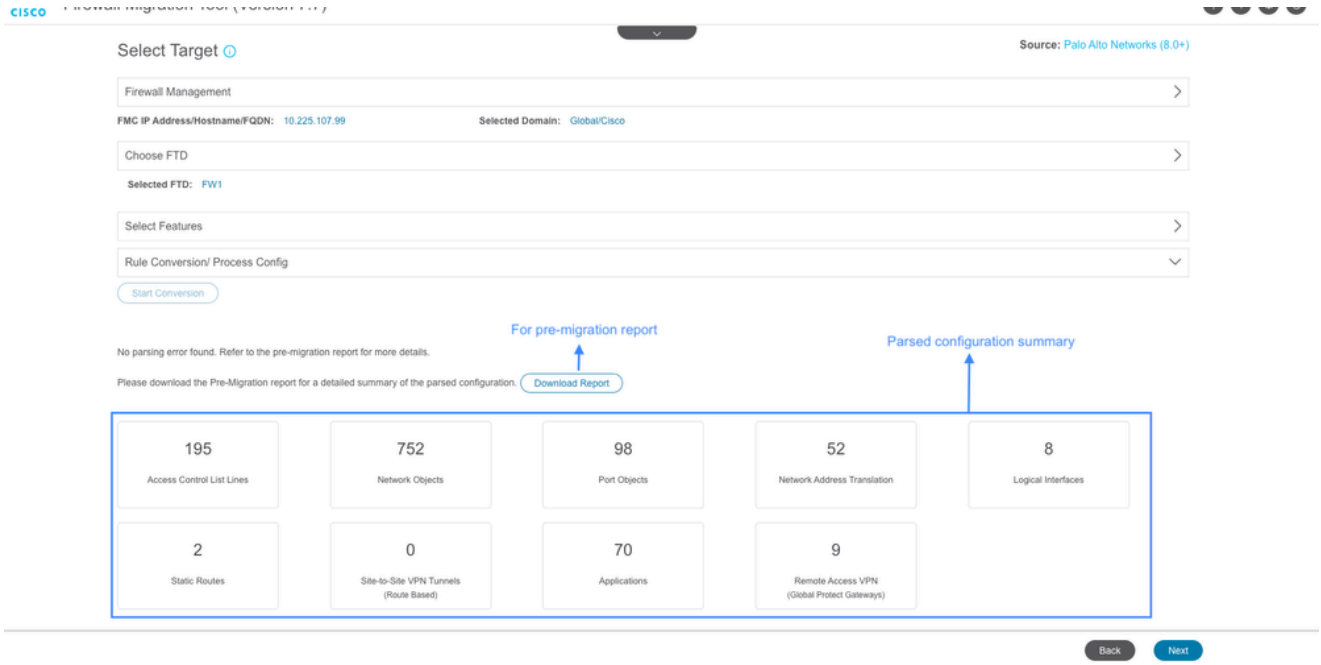
注：デフォルトでは、すべての機能が選択されています。移行しない構成は、すべて選択解除できます。

13. Start Conversionをクリックして、設定を変換します。



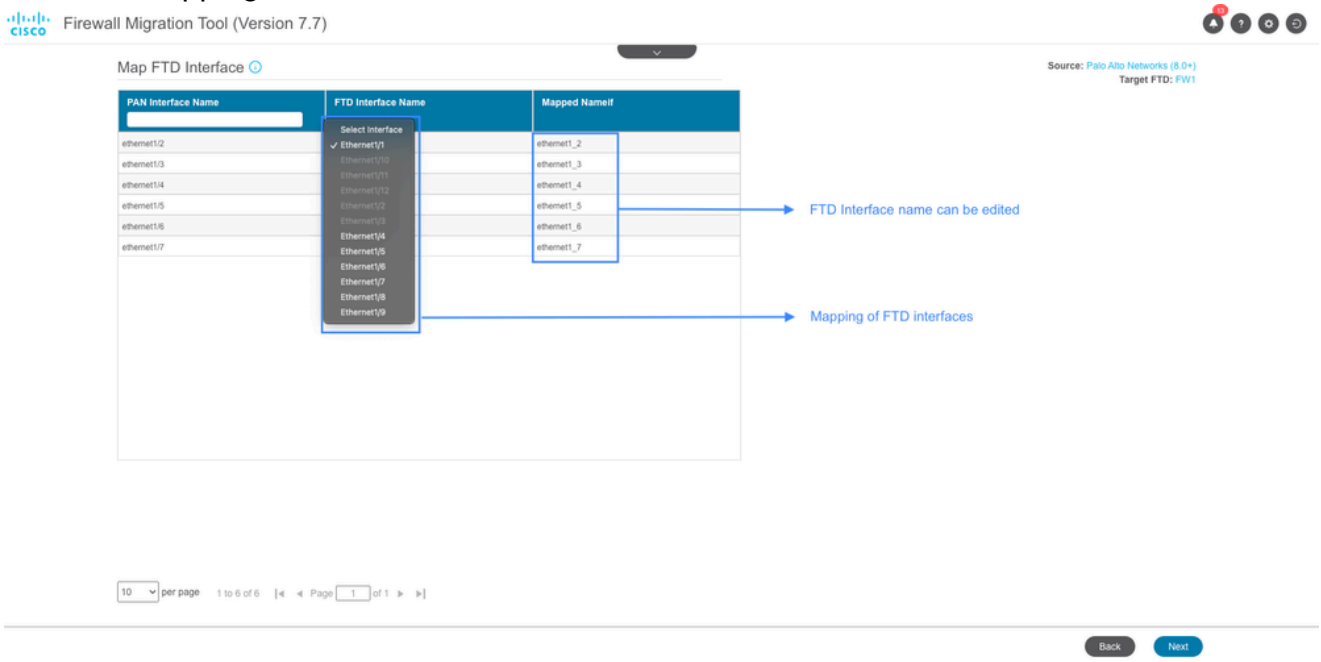
設定の解析

ツールは設定を解析し、図に示すように変換の概要を表示します。また、エラーまたは警告（存在する場合）に関して移行された設定を検証するための移行前レポートをダウンロードすることもできます。 Nextをクリックして、次のページに移動します。



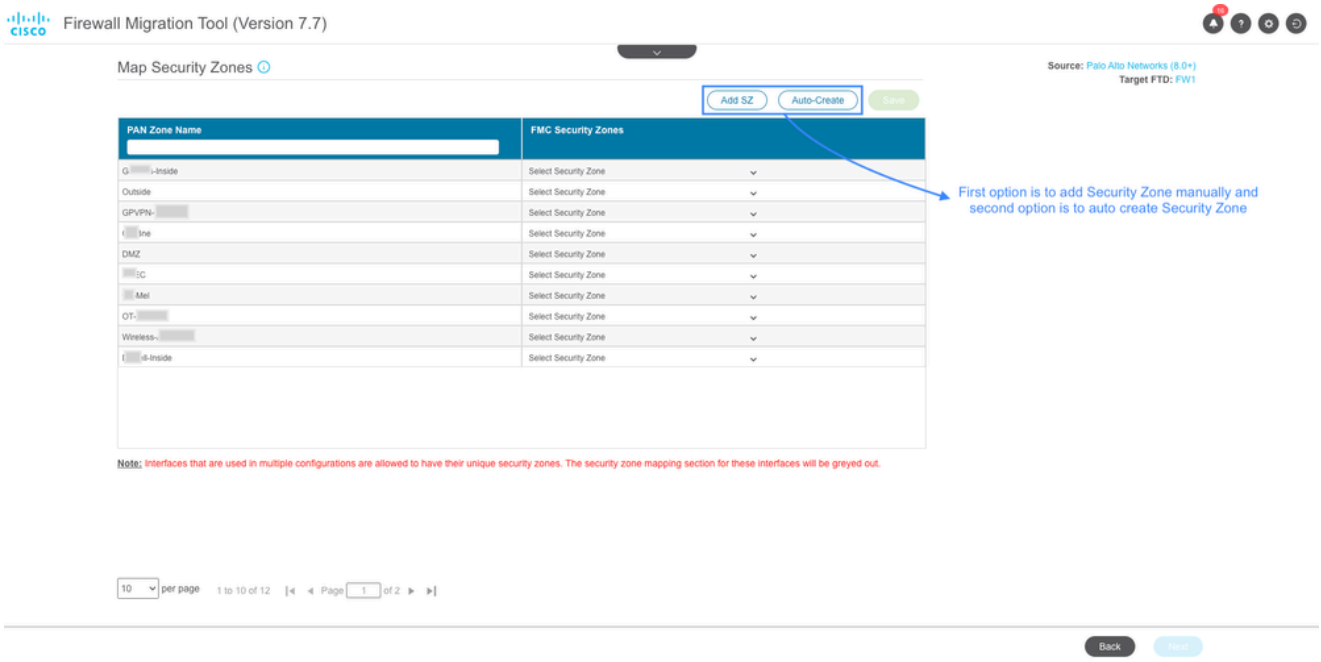
解析された設定の概要

14. PaloaltoからFTDへのインターフェイスマッピングを定義したり、「インターフェイスマッピング」セクションで各インターフェイスのインターフェイス名を編集したりできます。Interface Mappingが完了したら、Nextをクリックします。



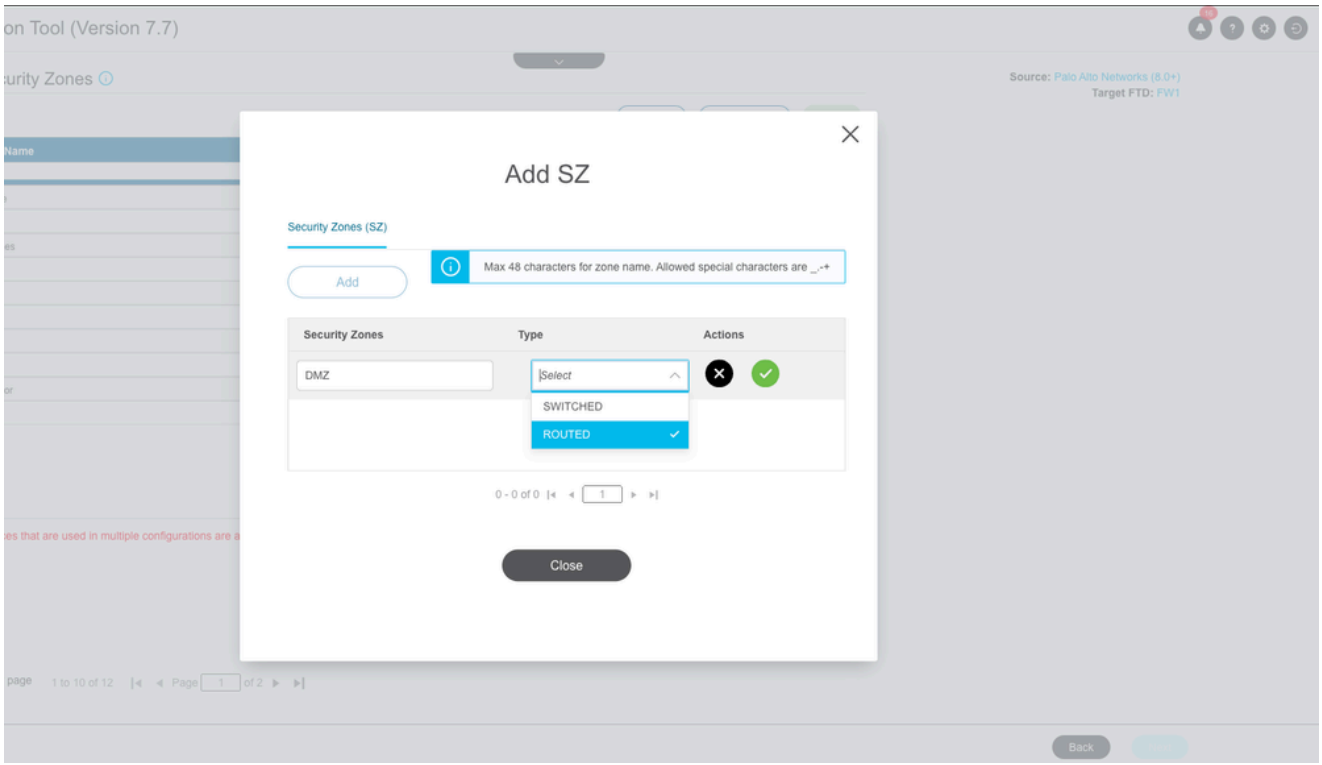
インターフェイス マッピング

15. 各インターフェイスに対してセキュリティゾーンを手動で追加するか、「セキュリティゾーンのマッピング」セクションで自動作成することができます。セキュリティゾーンを作成してマッピングした後で、Nextをクリックします。



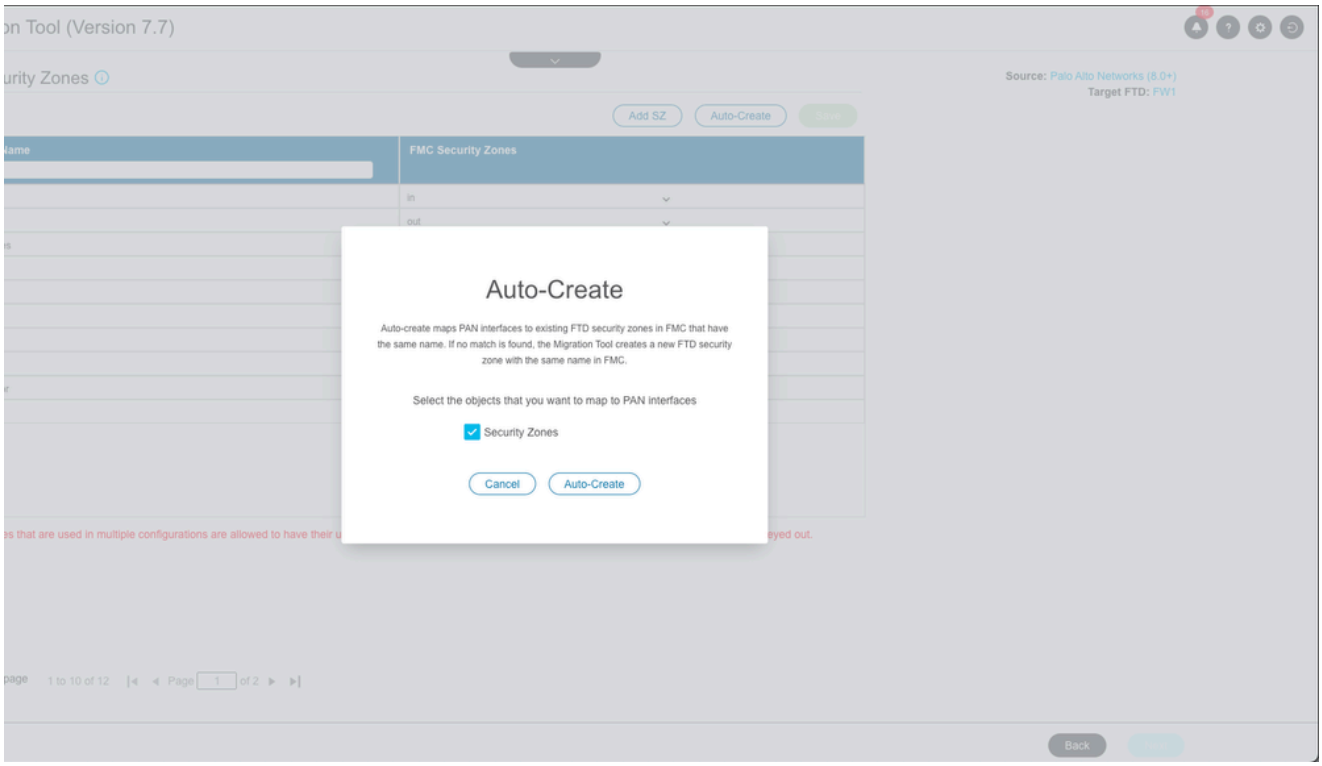
セキュリティゾーンの作成

セキュリティゾーンの手動作成：



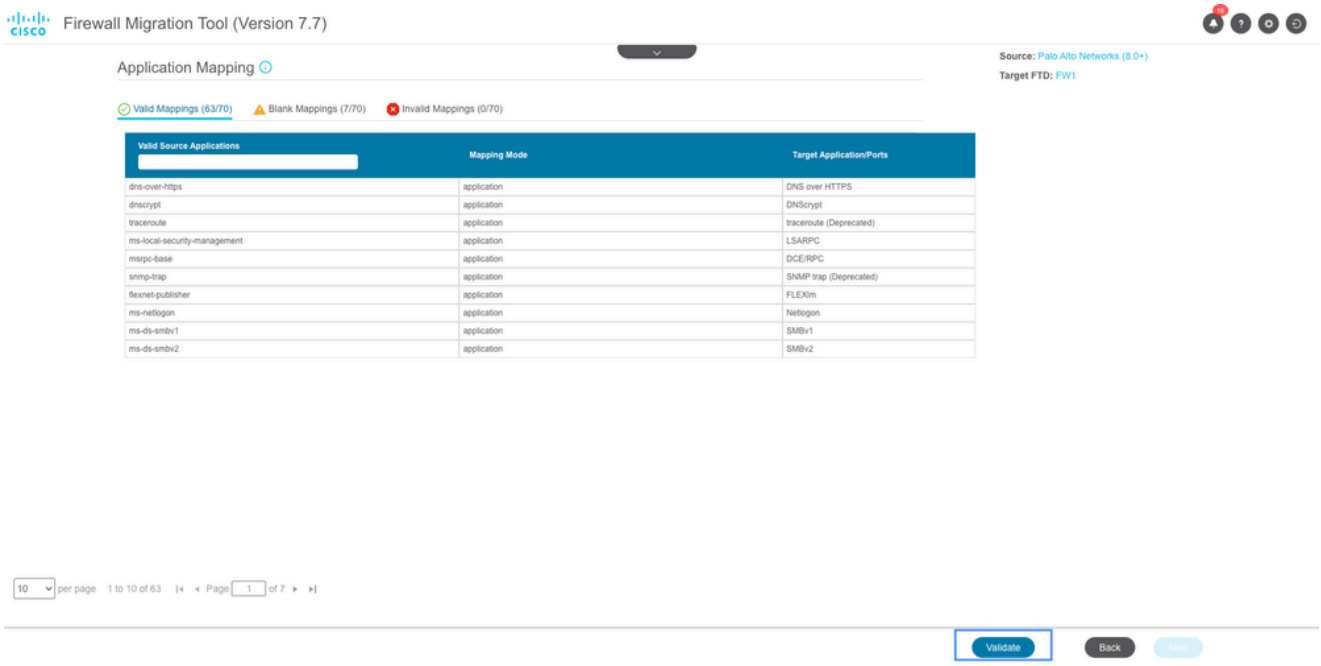
セキュリティゾーンの手動作成

セキュリティゾーンの自動作成：

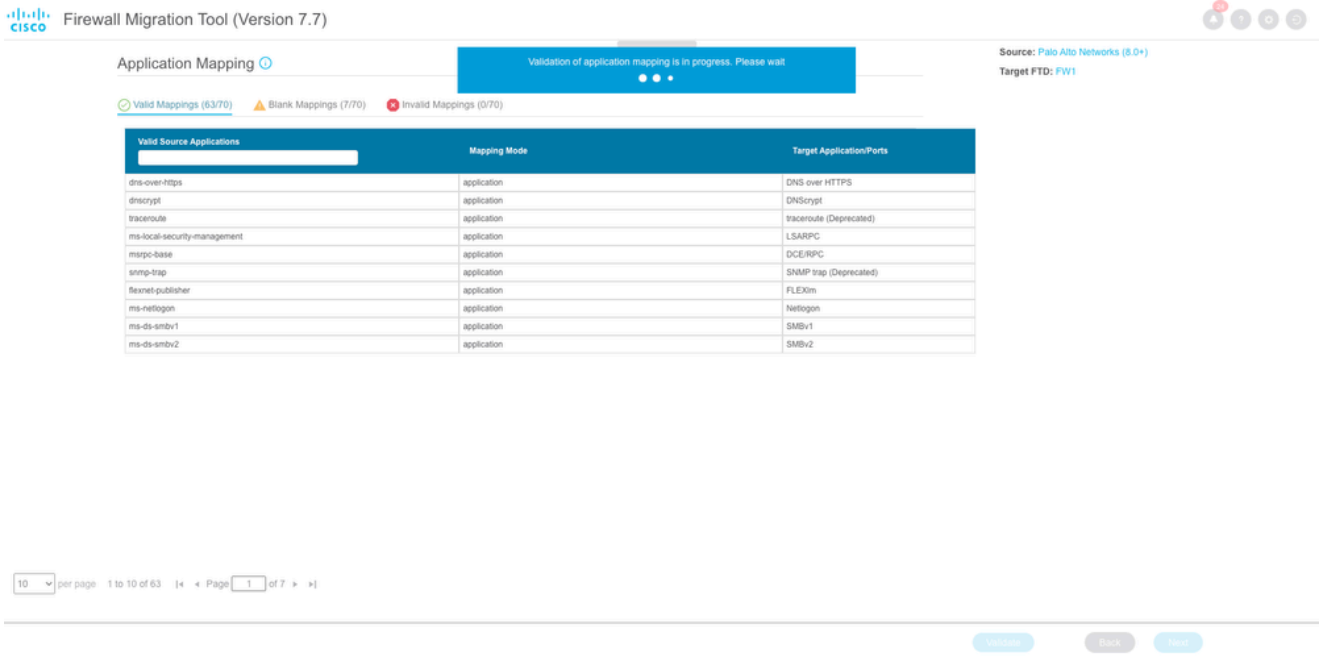


自動セキュリティゾーン作成

16. 次に、「アプリケーションマッピング」セクションに進みます。Validateボタンをクリックして、アプリケーションマッピングを検証します。



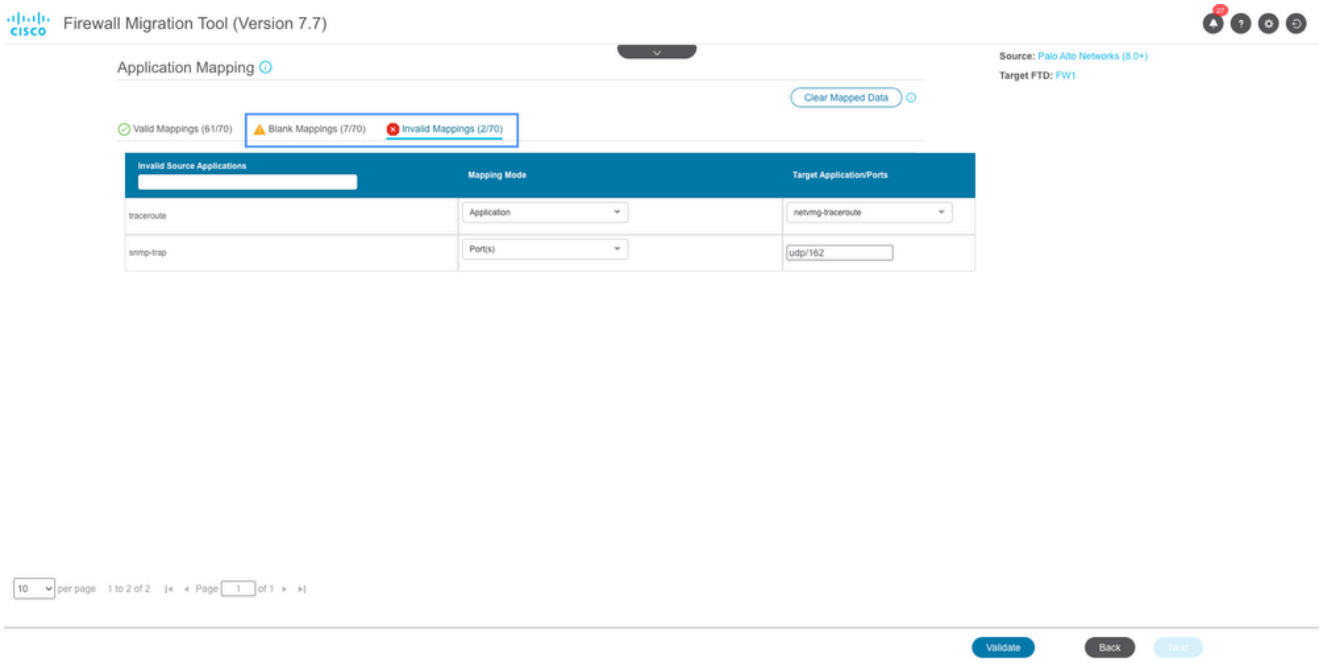
アプリケーションのマッピング



アプリケーションマッピングの検証

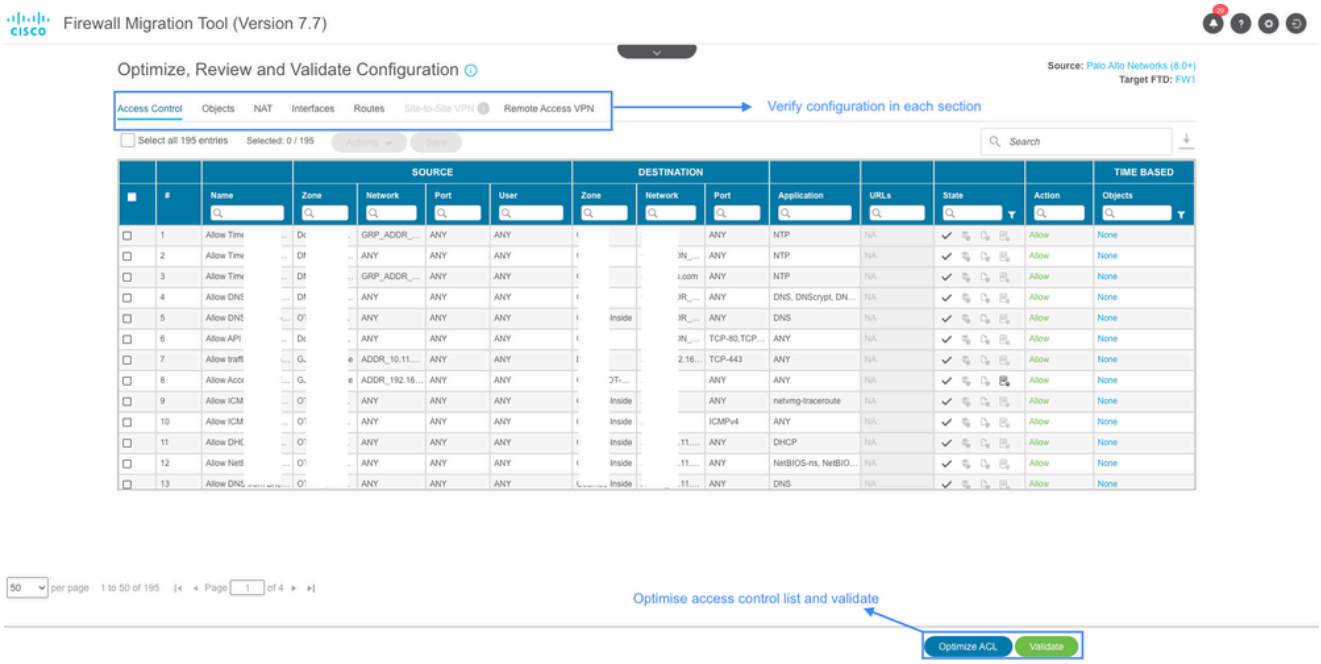
検証の際、FMTはブランクおよび無効なマッピングをリストします。無効なマッピングは先に進む前に修正する必要があり、ブランクマッピングの修正はオプションです。

再度Validateをクリックして、修正されたマッピングを検証します。検証が成功したら、Nextをクリックします。



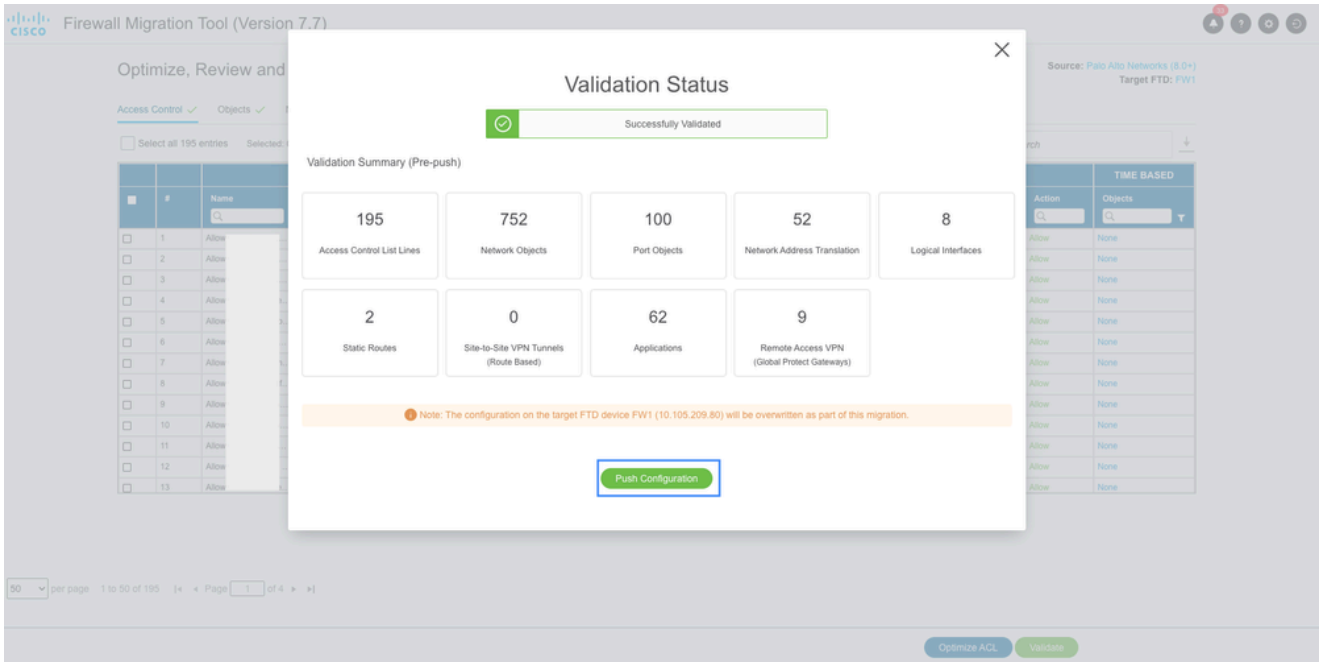
空白および無効なアプリケーションマッピング

17. ACLは、必要に応じて次のセクションで最適化できます。アクセスコントロール、オブジェクト、NAT、インターフェイス、ルート、リモートアクセスVPNなど、各セクションの設定を確認します。設定を確認したら、Validateをクリックします。



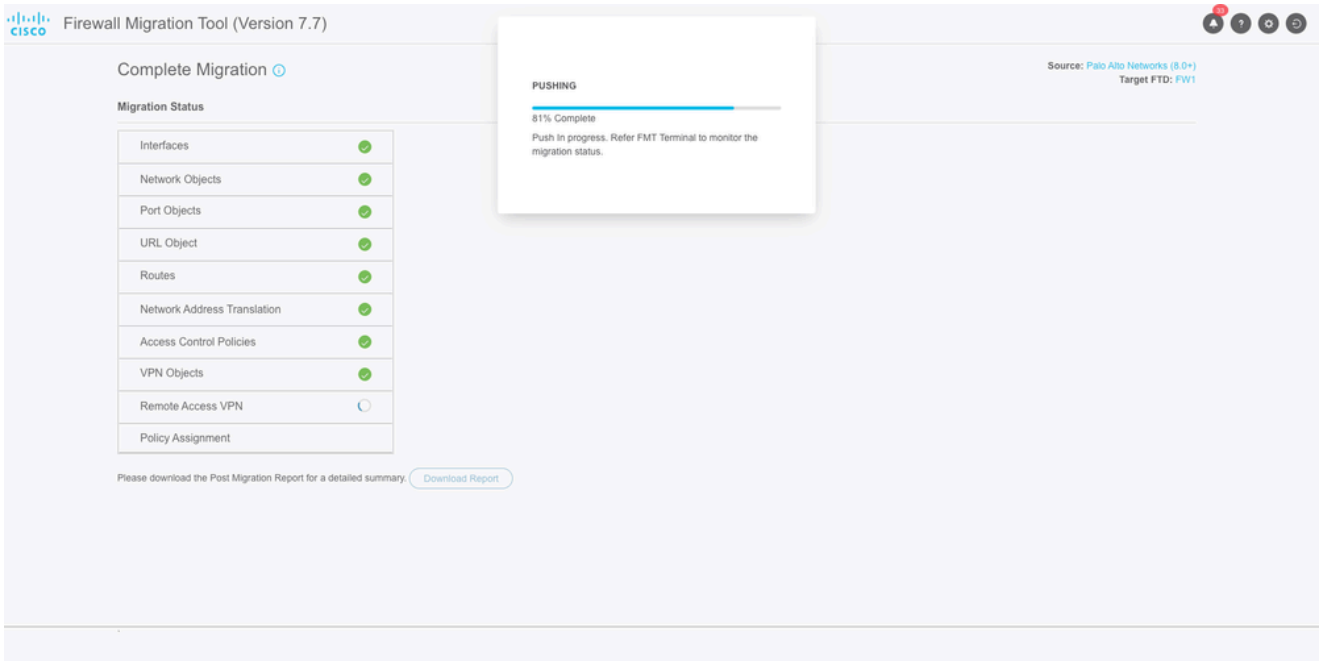
設定の検証

18. 検証が正常に完了すると、検証の概要が表示されます。Push Configurationをクリックして、ターゲットのFMCに設定をプッシュします。



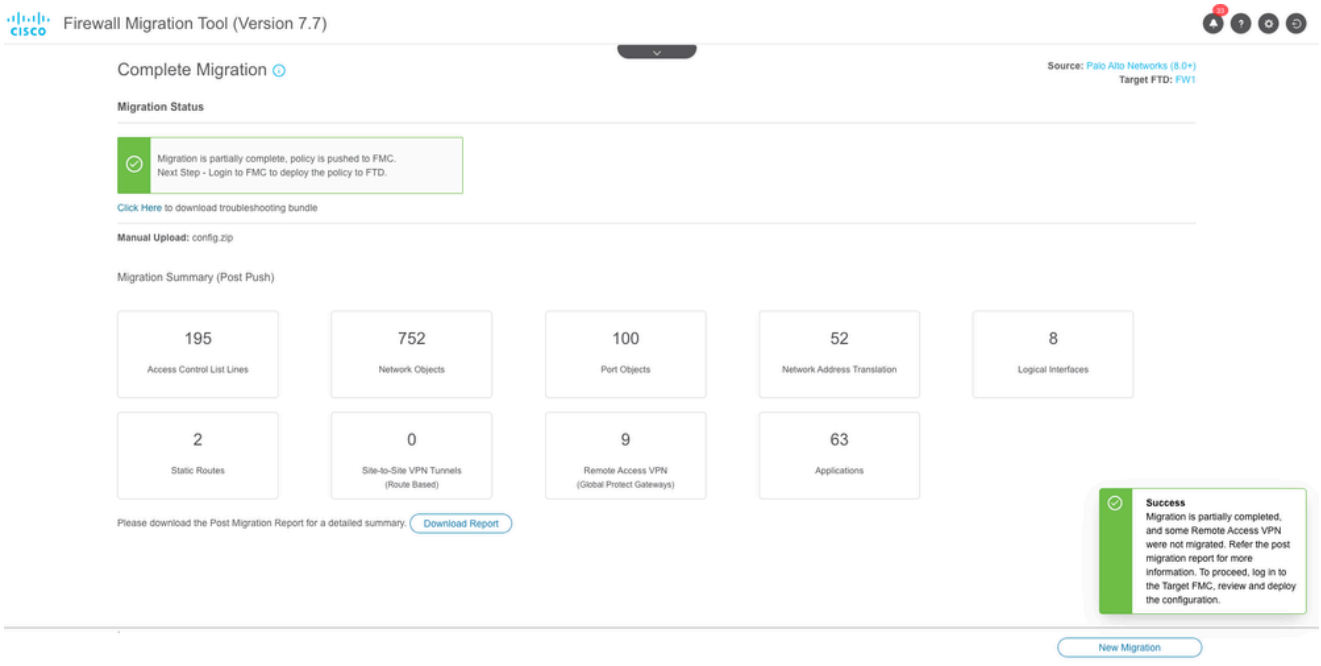
構成検証の概要

19. FMCへの設定のプッシュの進行状況がMigration Statusセクションに表示されるようになりました。FMTターミナルウィンドウを使用して、移行ステータスを監視することもできます。



移行ステータス

20. 移行が成功すると、ツールアップによって移行の概要が表示されます。また、部分的に移行された構成がある場合は、その構成も一覧表示されます。たとえば、このシナリオでは、Secure Client Packageがないため、リモートアクセスVPNを設定します。
また、移行後のレポートをダウンロードして、移行後の設定を確認したり、エラーや修正を加える必要があるかどうかを確認することもできます。



正常な移行の概要

21. 最後のステップでは、FMCから移行された設定を確認し、その設定をFTDに展開します。
設定を展開するには、次の手順を実行します。
    1. FMCのGUIにログインします。
    2. Deployタブに移動します。
    3. 設定をファイアウォールにプッシュする展開を選択します。
    4. [Deploy] をクリックします。

トラブルシュート

Secure Firewall Migration Toolのトラブルシューティング

一般的な移行エラー：

- PaloAlto設定ファイルの不明または無効な文字。
- 構成要素が見つからないか、不完全です。
- ネットワーク接続の問題または遅延
- PaloAlto設定ファイルのアップロード中、または設定をFMCにプッシュ中の問題。

トラブルシューティングのためのサポートバンドルの使用：

- 「Complete Migration」画面でSupportボタンをクリックします。
- Support Bundleを選択し、ダウンロードする設定ファイルを選択します。
- ログおよびDBファイルはデフォルトで選択されています。
- Downloadをクリックして、.zipファイルを取得します。
- ログ、DB、およびコンフィギュレーションファイルを表示するには、.zipを抽出します。
- Email usをクリックして、障害の詳細をテクニカルチームに送信します。
- 電子メールにサポートバンドルを添付してください。
- Visit TAC pageをクリックして、Cisco TACケースを作成し、サポートを依頼してください。

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。