FMTを使用したASAからFirepower Threat Defense(FTD)への移行

内容

はじめに

このドキュメントでは、Cisco適応型セキュリティアプライアンス(ASA)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

Cisco Firewall Threat Defense(FTD)および適応型セキュリティアプライアンス(ASA)に関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、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)v7.0.1
- 適応型セキュリティアプライアンス(ASA)v9.16(1)
- セキュアファイアウォール管理センター(FMCv)v7.4.2
- セキュアファイアウォール脅威防御仮想(FTDv)v7.4.1

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。

- Cisco 適応型セキュリティ アプライアンス（ASA）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)
- Fortinet（5.0以上）

・ Palo Alto Networks（6.1以降）

背景説明

ASA設定を移行する前に、次の作業を実行します。

ASAコンフィギュレーションファイルの取得

ASAデバイスを移行するには、シングルコンテキストの場合はshow running-configを、マルチコンテキストモードの場合はshow tech-supportを使用して設定を取得し、.cfgまたは.txtファイルとして保存し、Secure Firewall移行ツールを使用してコンピュータに転送します。

ASAからのPKI証明書のエクスポートとManagement Centerへのインポート

次のコマンドを使用して、CLIを介してソースASAコンフィギュレーションからPKCS12ファイルにキーを使用してPKI証明書をエクスポートします。
ASA(config)#crypto ca export <trust-point-name> pkcs12 <パスフレーズ>
次に、PKI証明書を管理センター（オブジェクト管理PKIオブジェクト）にインポートします。 詳細については、『Firepower Management Centerコンフィギュレーションガイド』の「PKIオブジェクト」を参照してください。

AnyConnectのパッケージとプロファイルの取得

AnyConnectプロファイルはオプションであり、Management Centerまたはセキュアファイアウォール移行ツールを使用してアップロードできます。

次のコマンドを使用して、必要なパッケージをソースASAからFTPまたはTFTPサーバにコピーします。

Copy <ソースファイルの場所：/ソースファイル名> <コピー先>

ASA# copy disk0:/anyconnect-win-4.10.02086-webdeploy-k9.pkg tftp://1.1.1.1 <----- Anyconnectパッケージのコピー例。

ASA# copy disk0:/ external-sso- 4.10.04071-webdeploy-k9.zip tftp://1.1.1.1 <-----外部ブラウザパッケージのコピー例。

ASA# copy disk0:/ hostscan_4.10.04071-k9.pkg tftp://1.1.1.1 <----- Hostscanパッケージのコピー例。

ASA# copy disk0:/ dap.xml tftp://1.1.1.1. <----- Dap.xmlのコピー例

ASA# copy disk0:/ sdesktop/data.xml tftp://1.1.1.1 <----- Data.xmlのコピー例

ASA# copy disk0:/ VPN_Profile.xml tftp://1.1.1.1 <----- Anyconnectプロファイルのコピー例。

ダウンロードしたパッケージをManagement Centerにインポートします(Object Management > VPN > AnyConnect File)。

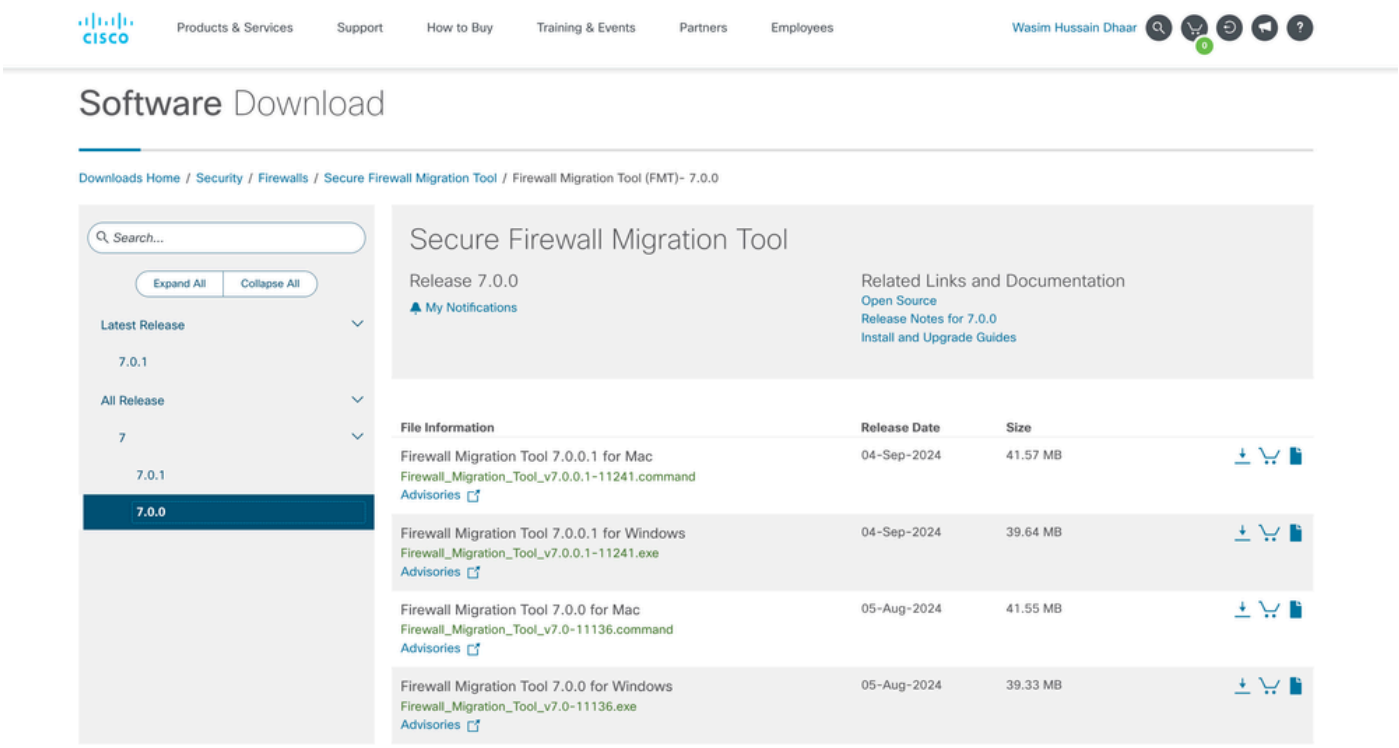
a-Dap.xmlとData.xmlは、Review and Validate > Remote Access VPN > AnyConnect Fileセクションのsecure Firewall migration toolからManagement Centerにアップロードする必要があります。

b-AnyConnectプロファイルは、Management Centerに直接アップロードするか、Review and Validate > Remote Access VPN > AnyConnect Fileセクションのsecure Firewall移行ツールを使用してアップロードできます。

設定

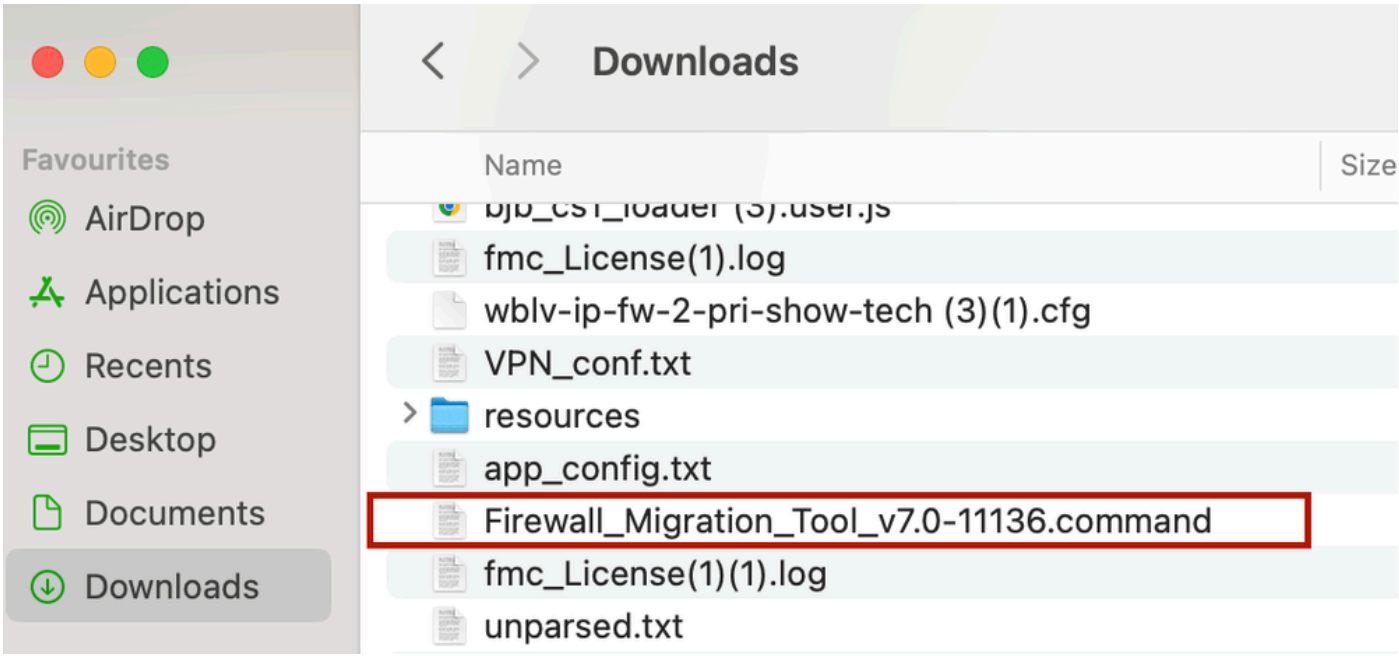
設定手順：

1. ダウンロード cisco Software Centralの最新のFirepower移行ツール：

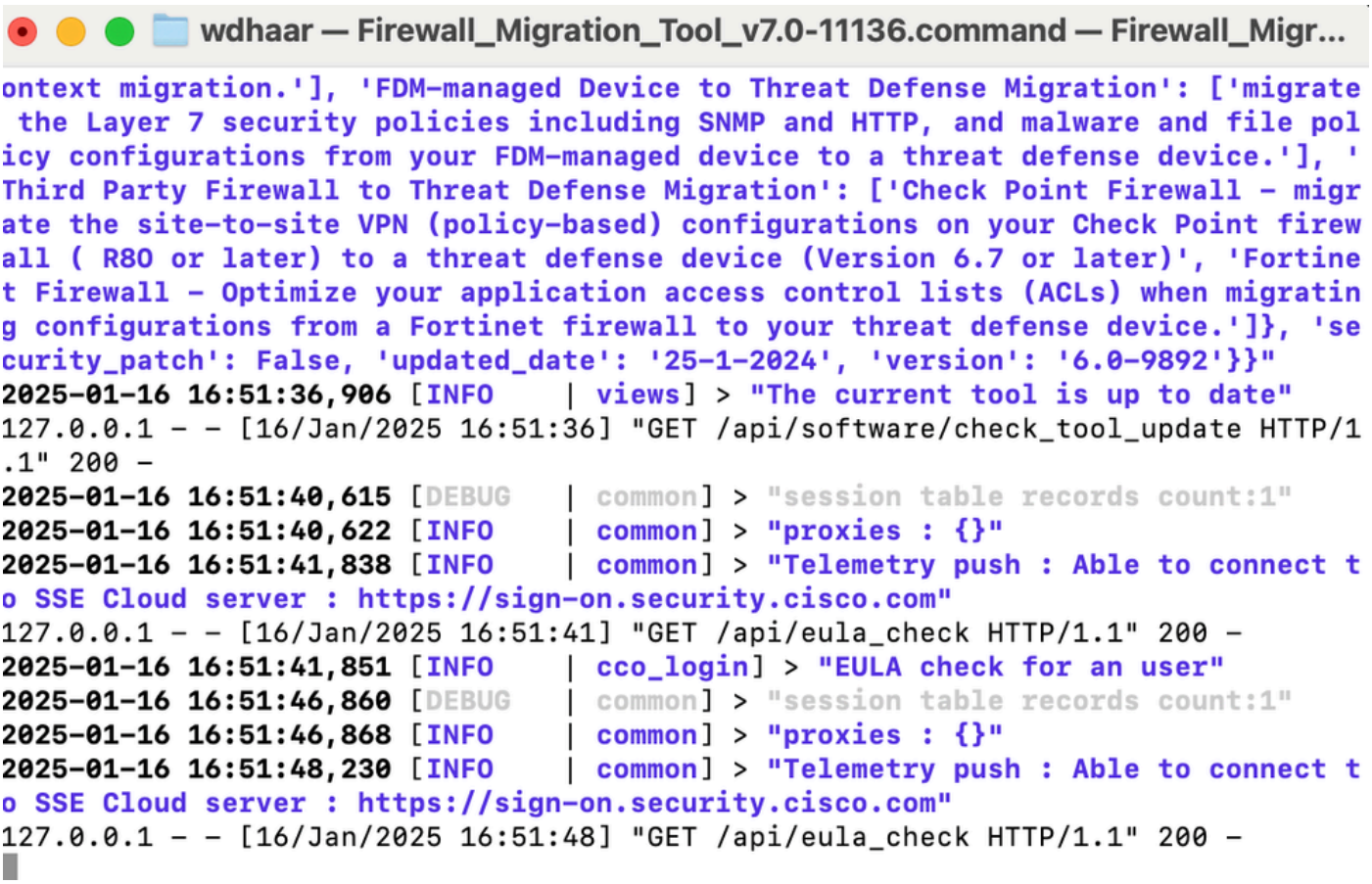


ソフトウェアのダウンロード

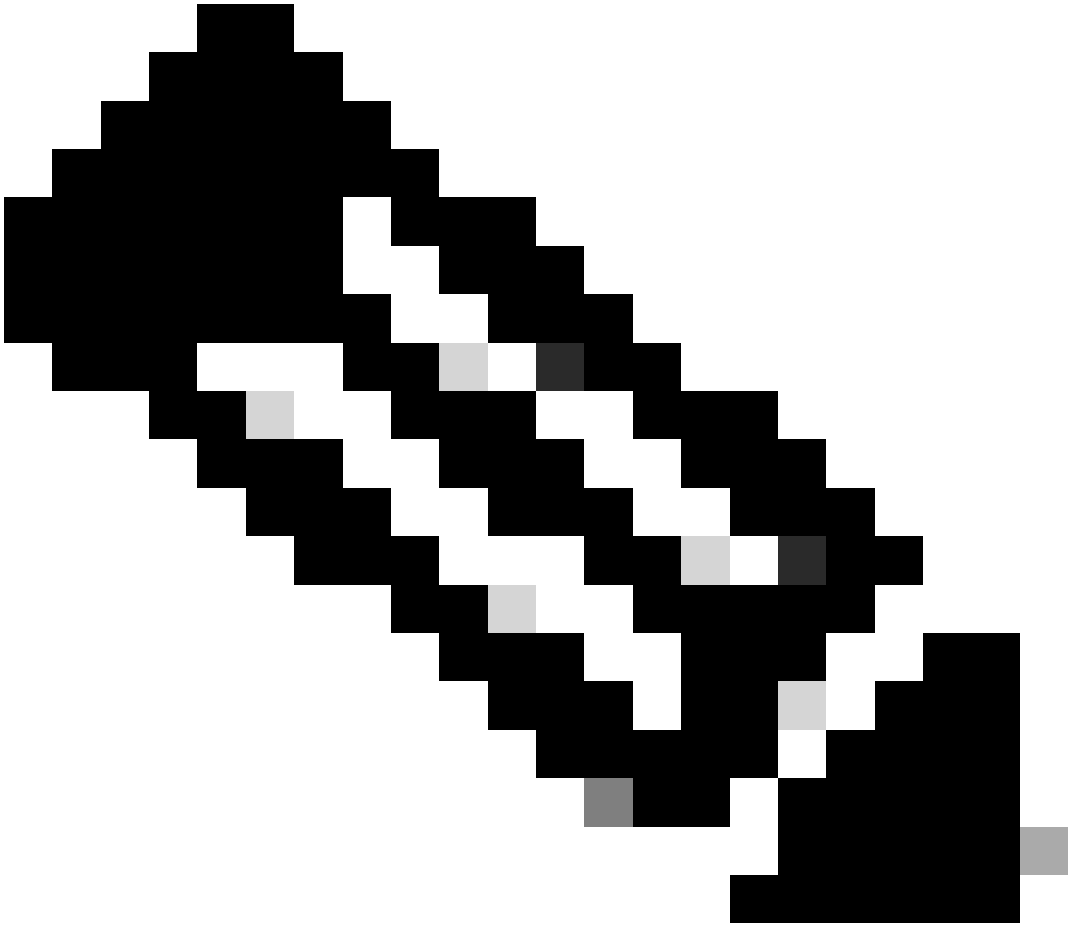
2. コンピュータにダウンロードしたファイルをクリックします。



ファイル

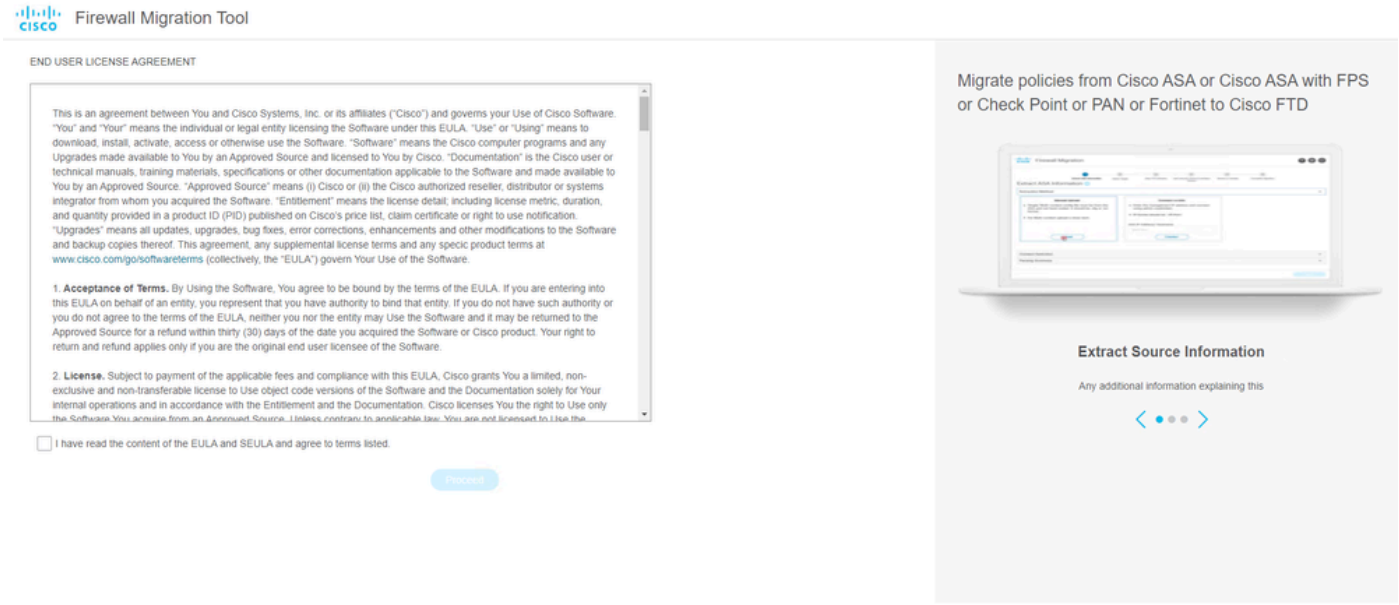

wdhaar — Firewall_Migration_Tool_v7.0-11136.command — Firewall_Migr...
ontext migration.'], 'FDM-managed Device to Threat Defense Migration': ['migrate the Layer 7 security policies including SNMP and HTTP, and malware and file policy configurations from your FDM-managed device to a threat defense device.'], 'Third Party Firewall to Threat Defense Migration': ['Check Point Firewall - migrate the site-to-site VPN (policy-based) configurations on your Check Point firewall (R80 or later) to a threat defense device (Version 6.7 or later)', 'Fortinet Firewall - Optimize your application access control lists (ACLs) when migrating configurations from a Fortinet firewall to your threat defense device.']}, 'security_patch': False, 'updated_date': '25-1-2024', 'version': '6.0-9892'}}"
2025-01-16 16:51:36,906 [INFO | views] > "The current tool is up to date"
127.0.0.1 - - [16/Jan/2025 16:51:36] "GET /api/software/check_tool_update HTTP/1.1" 200 -
2025-01-16 16:51:40,615 [DEBUG | common] > "session table records count:1"
2025-01-16 16:51:40,622 [INFO | common] > "proxies : {}"
2025-01-16 16:51:41,838 [INFO | common] > "Telemetry push : Able to connect to SSE Cloud server : https://sign-on.security.cisco.com"
127.0.0.1 - - [16/Jan/2025 16:51:41] "GET /api/eula_check HTTP/1.1" 200 -
2025-01-16 16:51:41,851 [INFO | cco_login] > "EULA check for an user"
2025-01-16 16:51:46,860 [DEBUG | common] > "session table records count:1"
2025-01-16 16:51:46,868 [INFO | common] > "proxies : {}"
2025-01-16 16:51:48,230 [INFO | common] > "Telemetry push : Able to connect to SSE Cloud server : https://sign-on.security.cisco.com"
127.0.0.1 - - [16/Jan/2025 16:51:48] "GET /api/eula_check HTTP/1.1" 200 -

コンソール ログ



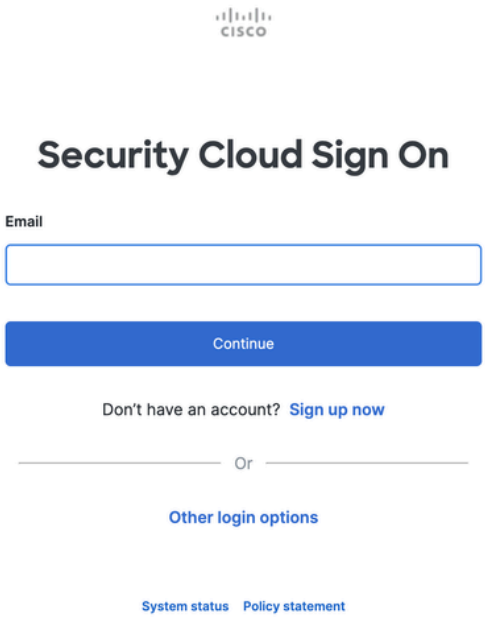
注：プログラムが自動的に開き、ファイルを実行したディレクトリのコンテンツがコンソールによって自動的に生成されます。

3. 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（Proceed）] をクリックします。



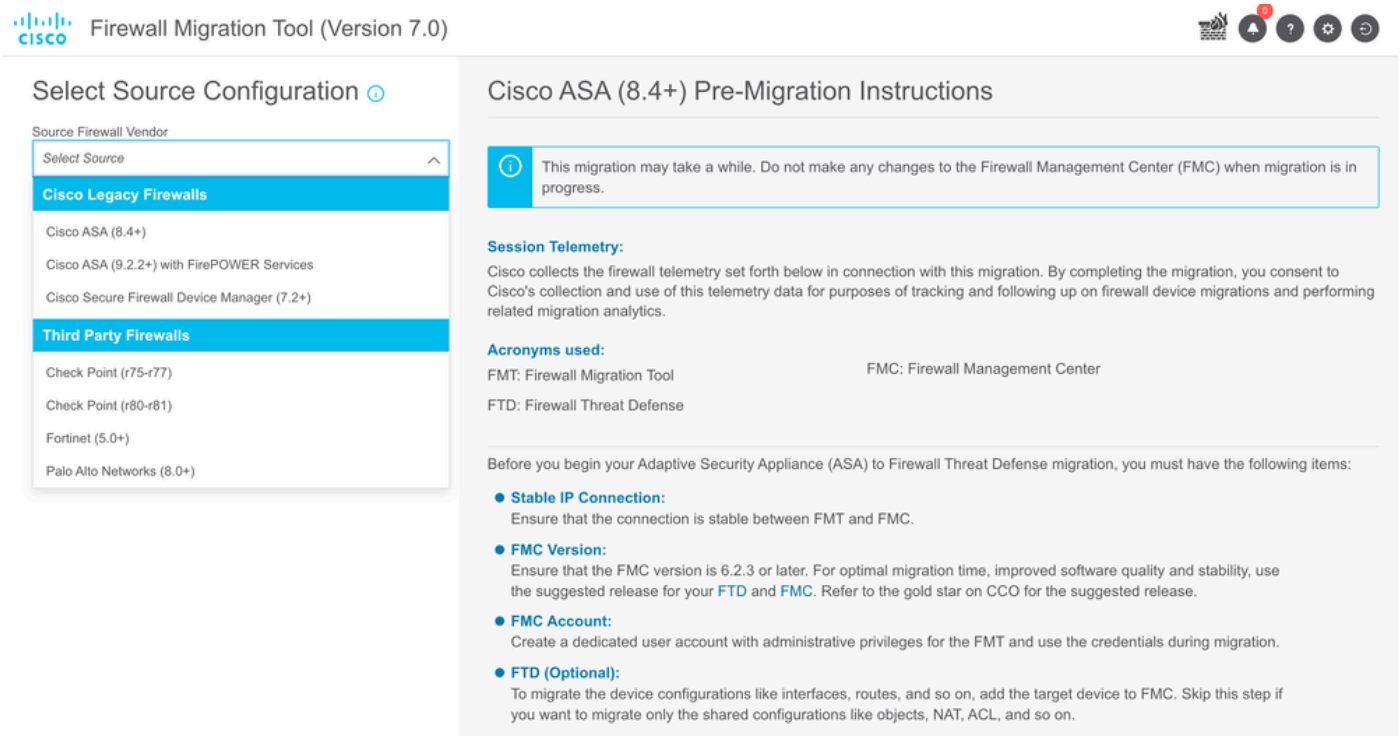
使用許諾契約書

4. 有効なCCOアカウントを使用してログインすると、WebブラウザにFMT GUIインターフェイスが表示されます。



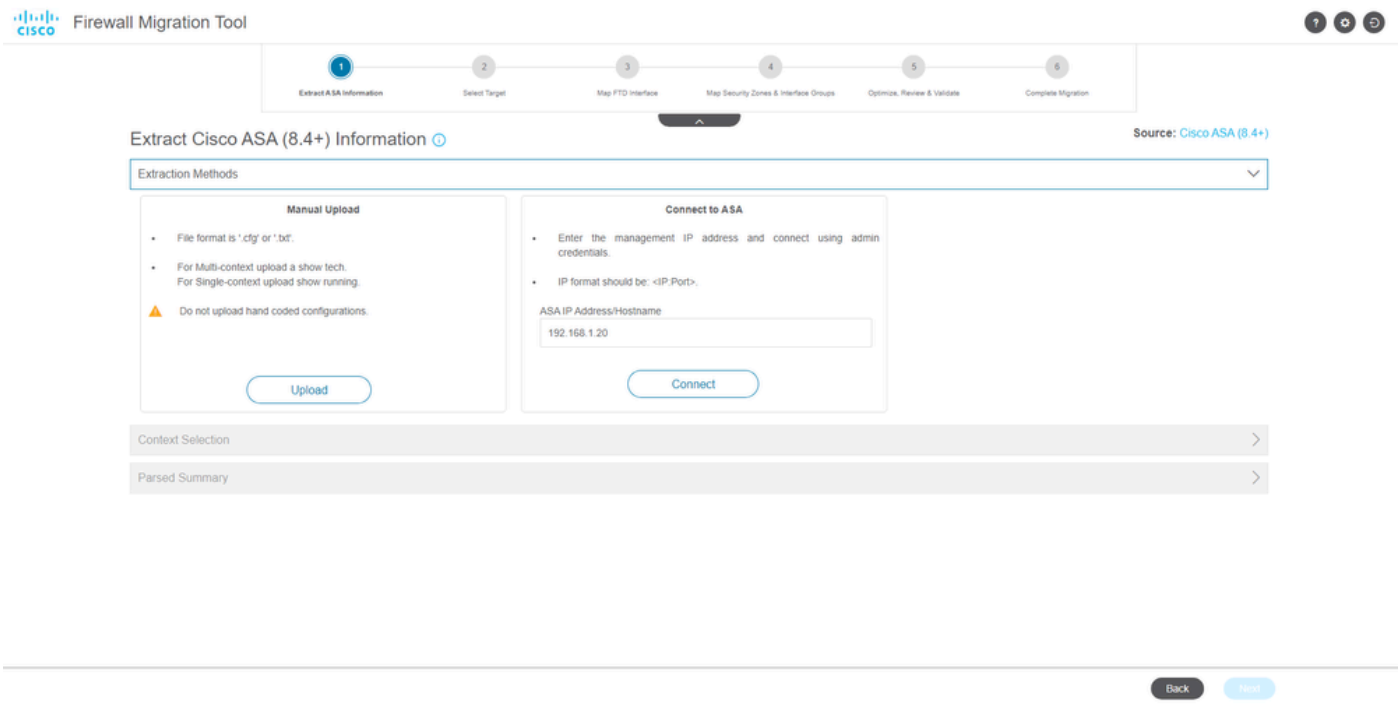
FMTログイン

5. 移行するソースファイアウォールを選択します。

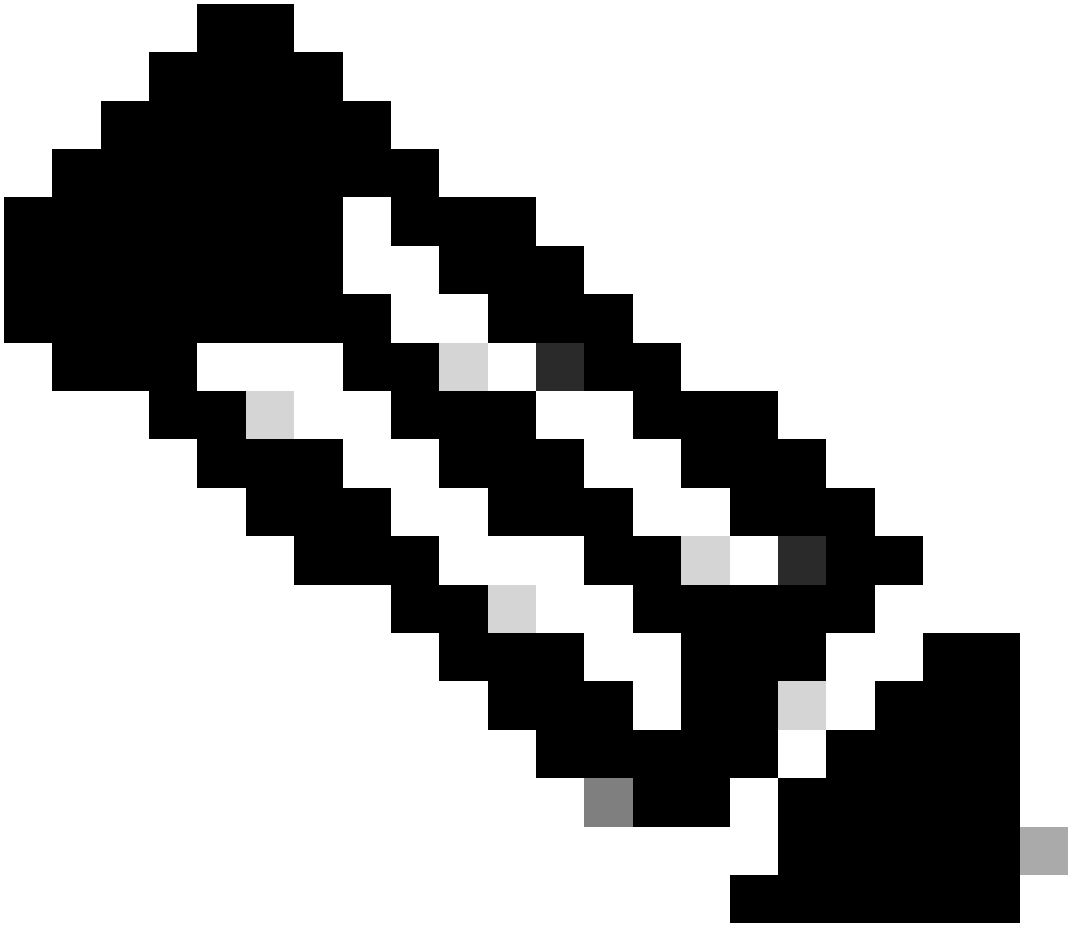


送信元ファイアウォール

6. 構成の取得に使用する抽出方法を選択します。
    1. 手動アップロードでは、ASAの「**Running Config**」ファイルを「.cfg」または「.txt」形式でアップロードする必要があります。
    2. ASAに接続して、ファイアウォールからコンフィギュレーションを直接抽出します。

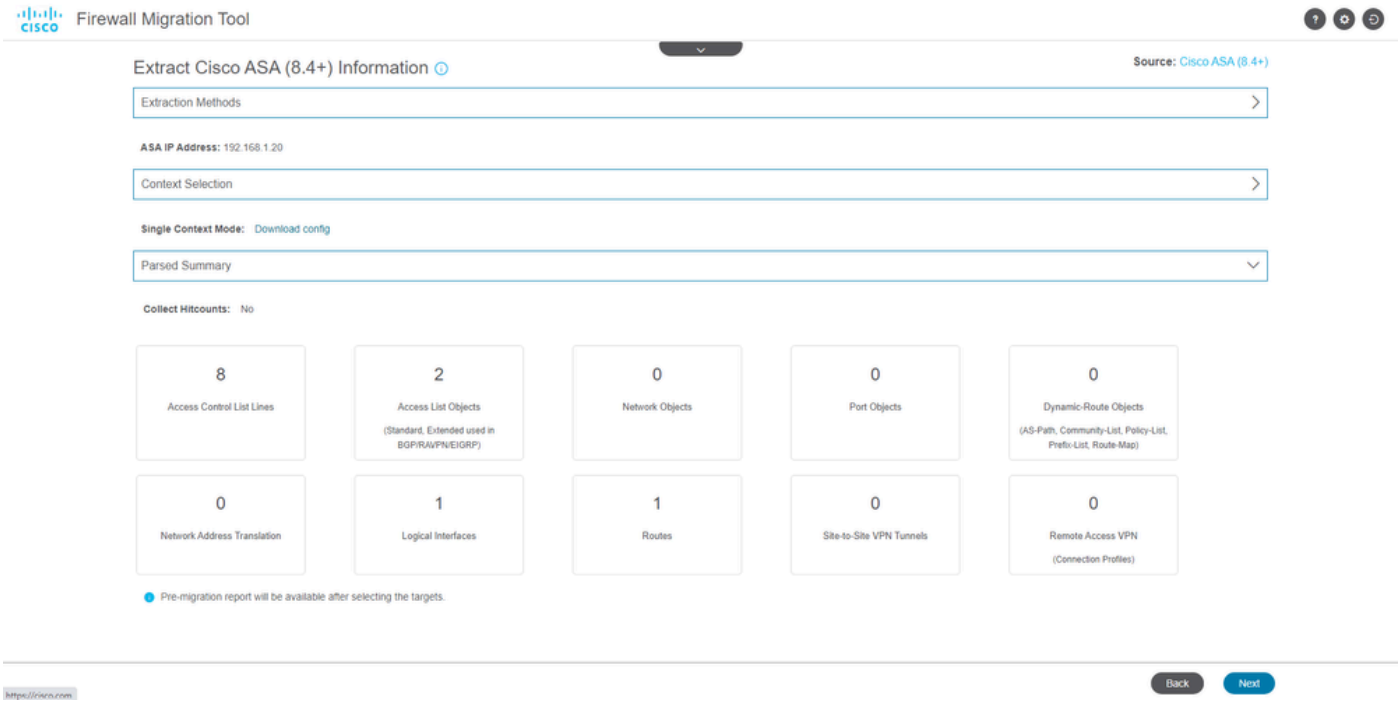


抽出



注：この例では、ASAに直接接続します。

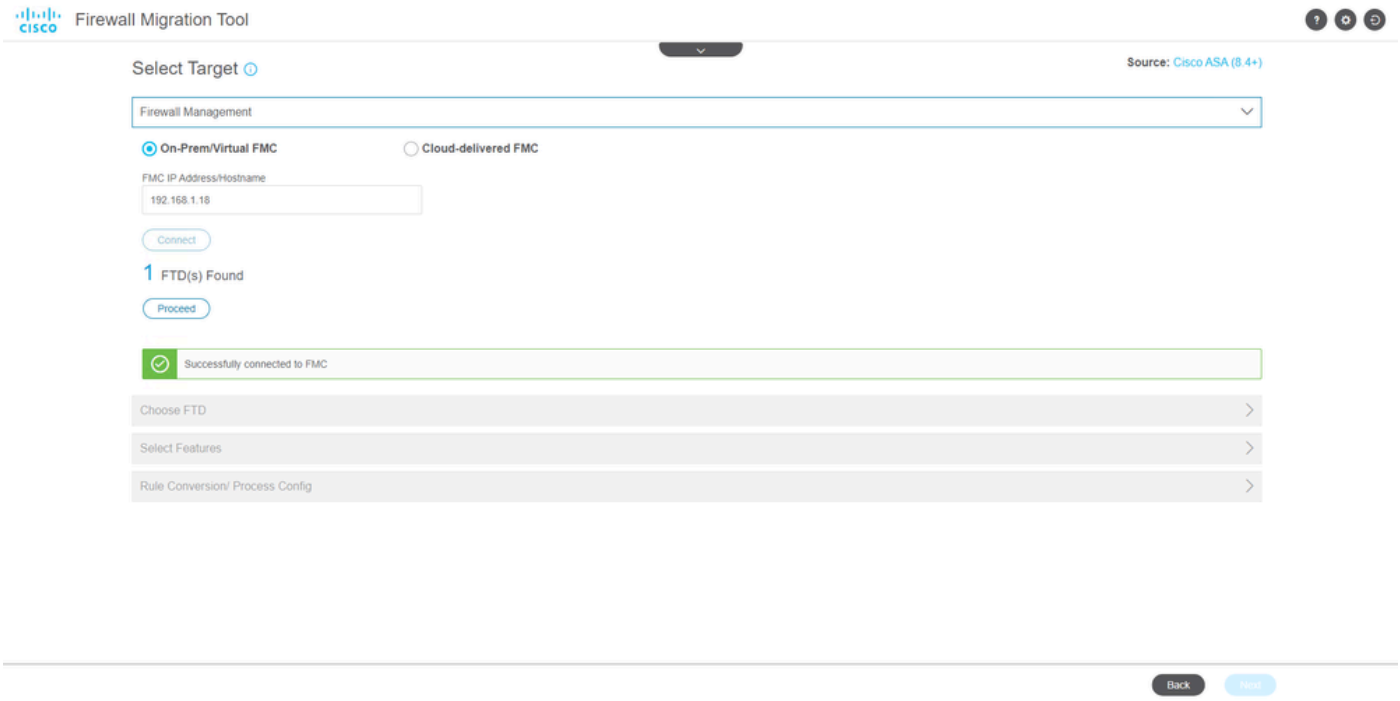
7. ファイアウォールで検出された設定の要約がダッシュボードとして表示されます。Nextをクリックします。



要約

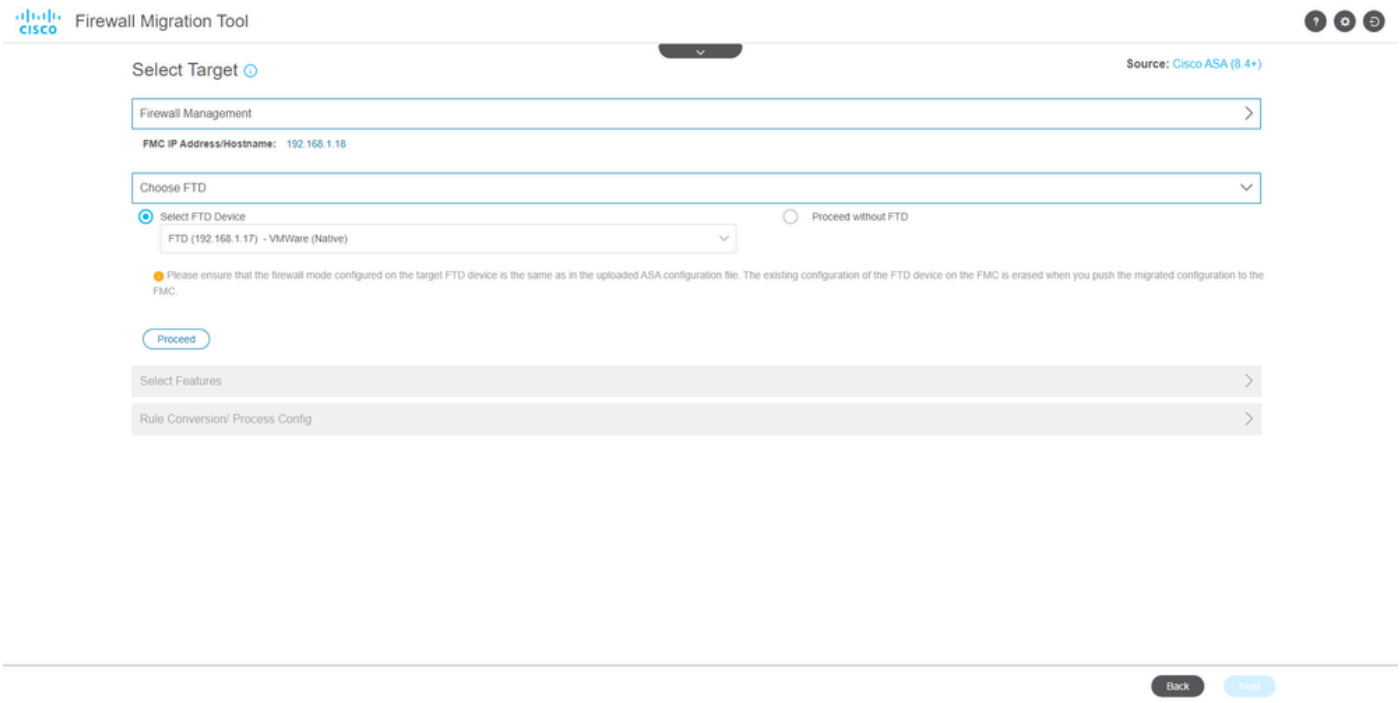
8. 移行で使用するターゲットFMCを選択します。

FMCのIPを入力します。ポップアップウィンドウが開き、FMCのログインクレデンシャルの入力を求められます。



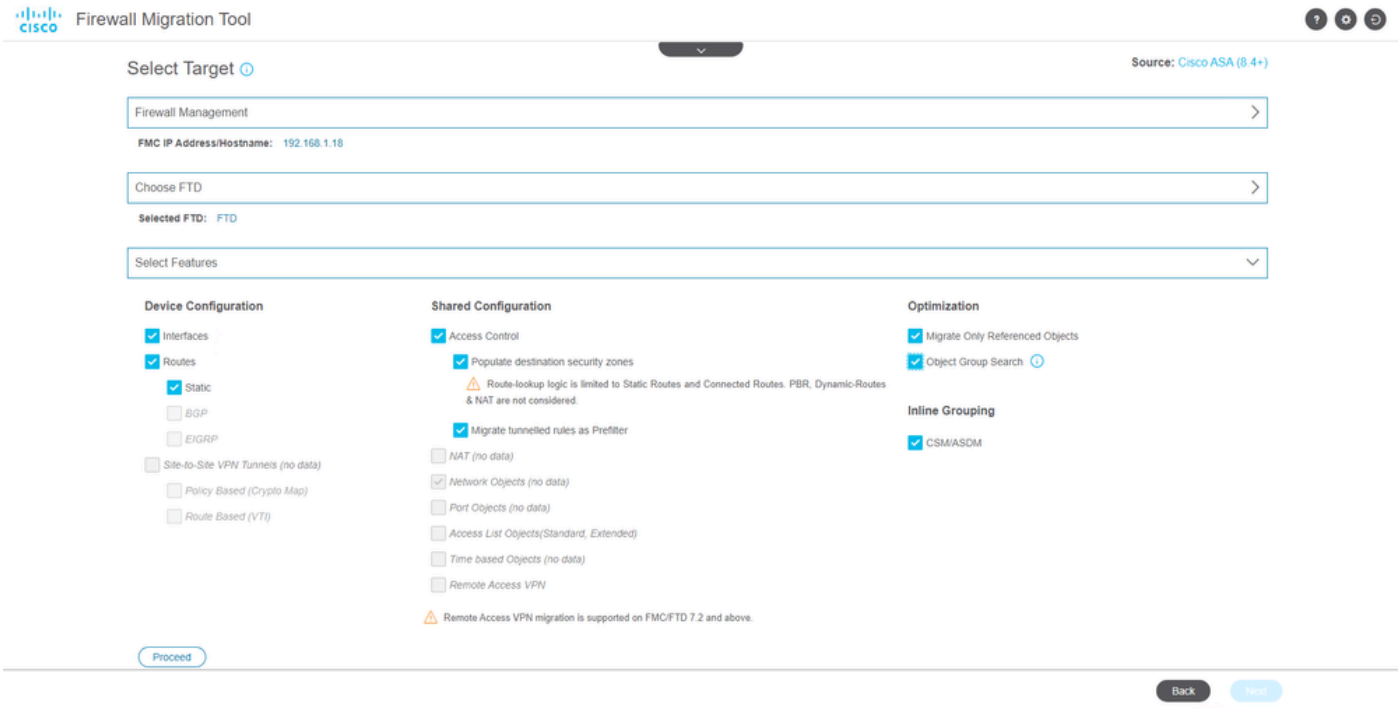
FMCのIP

9. （オプション）使用するターゲットFTDを選択します。
    1. FTDへの移行を選択する場合は、使用するFTDを選択します。
    2. FTDを使用しない場合は、このチェックボックスをオンにします Proceed without FTD



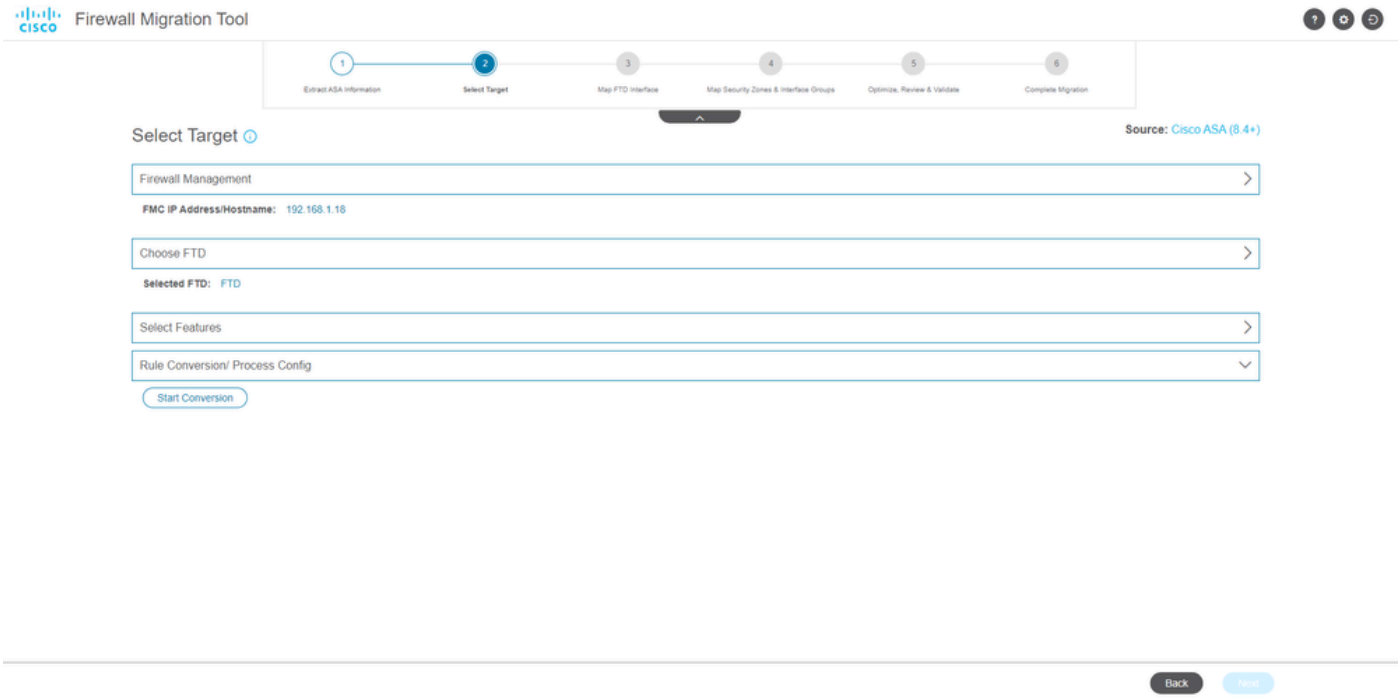
ターゲットFTD

10. 移行する構成を選択すると、スクリーンショットにオプションが表示されます。



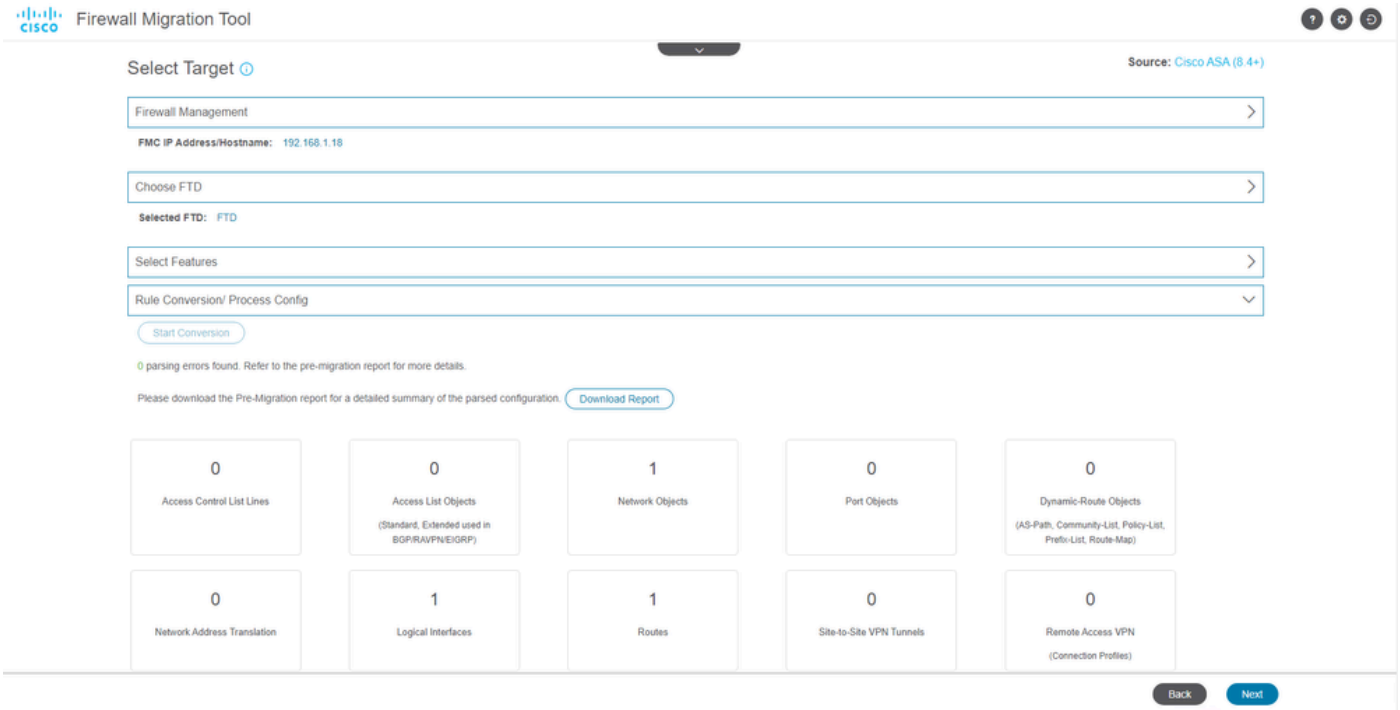
コンフィギュレーション

11. ASAからFTDへの設定の変換を開始します。



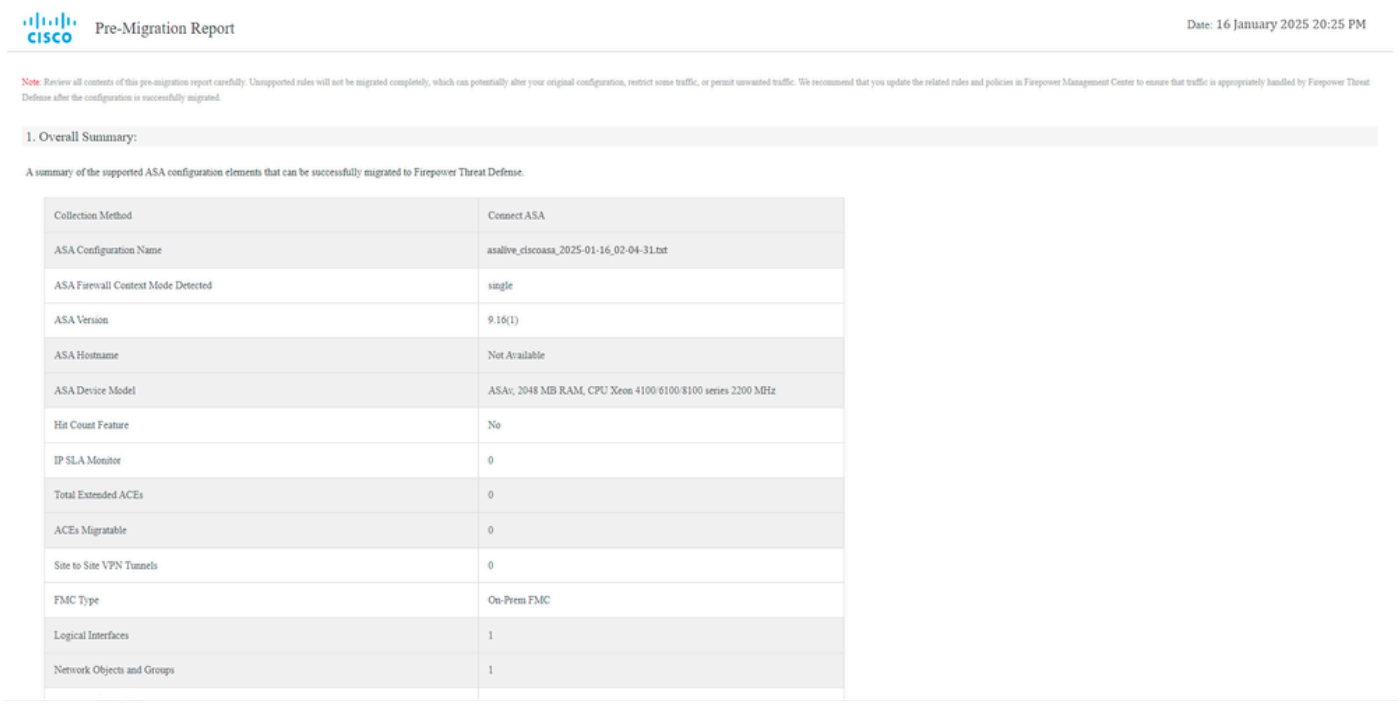
変換の開始

12. 変換が完了すると、移行するオブジェクトの概要を示すダッシュボードが表示されます（互換性に制限されています）。
    1. オプションで、「**Download Report**」をクリックして、移行する設定のサマリーを受信できます。



レポートのダウンロード

図に示す移行前レポートの例：



Pre-Migration Report

Date: 16 January 2025 20:25 PM

Note: Review all contents of this pre-migration report carefully. Unsupported rules will not be migrated completely, which can potentially alter your original configuration, restrict some traffic, or permit unwanted traffic. We recommend that you update the related rules and policies in Firepower Management Center to ensure that traffic is appropriately handled by Firepower Threat Defense after the configuration is successfully migrated.

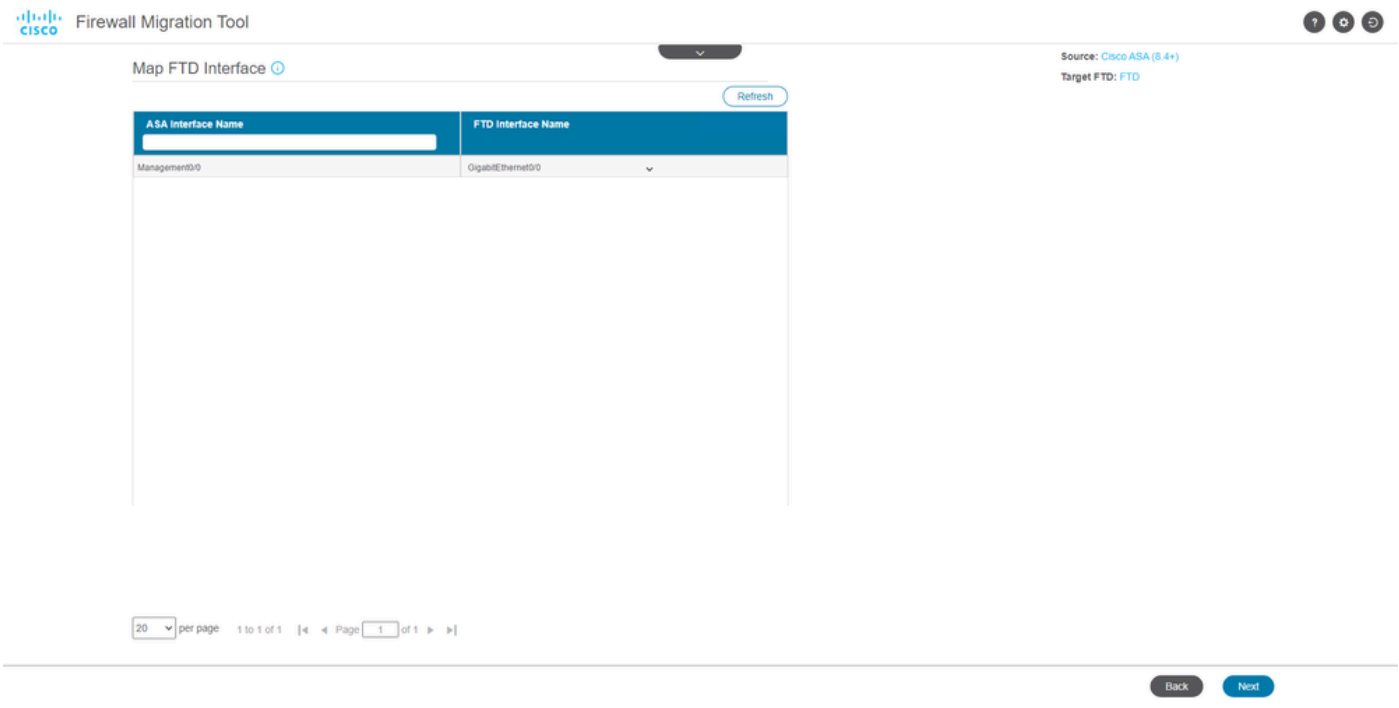
1. Overall Summary:

A summary of the supported ASA configuration elements that can be successfully migrated to Firepower Threat Defense.

Collection Method	Connect ASA
ASA Configuration Name	asalive_ciscoasa_2025-01-16_02-04-31.txt
ASA Firewall Context Mode Detected	single
ASA Version	9.16(1)
ASA Hostname	Not Available
ASA Device Model	ASAv, 2048 MB RAM, CPU Xeon 4100/6100/8100 series 2200 MHz
Hit Count Feature	No
IP SLA Monitor	0
Total Extended ACEs	0
ACEs Migratable	0
Site to Site VPN Tunnels	0
FMC Type	On-Prem FMC
Logical Interfaces	1
Network Objects and Groups	1

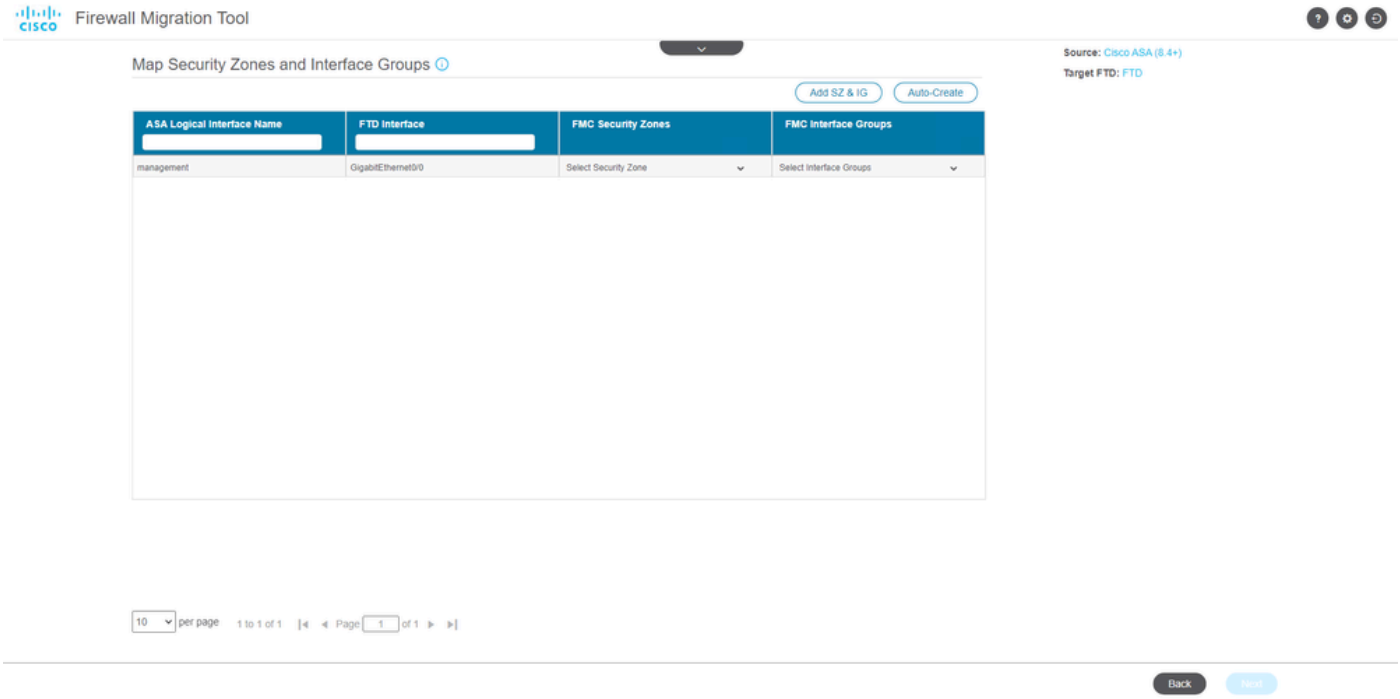
移行前のレポート

13. Migration Toolで、ASAインターフェイスをFTDインターフェイスにマッピングします。



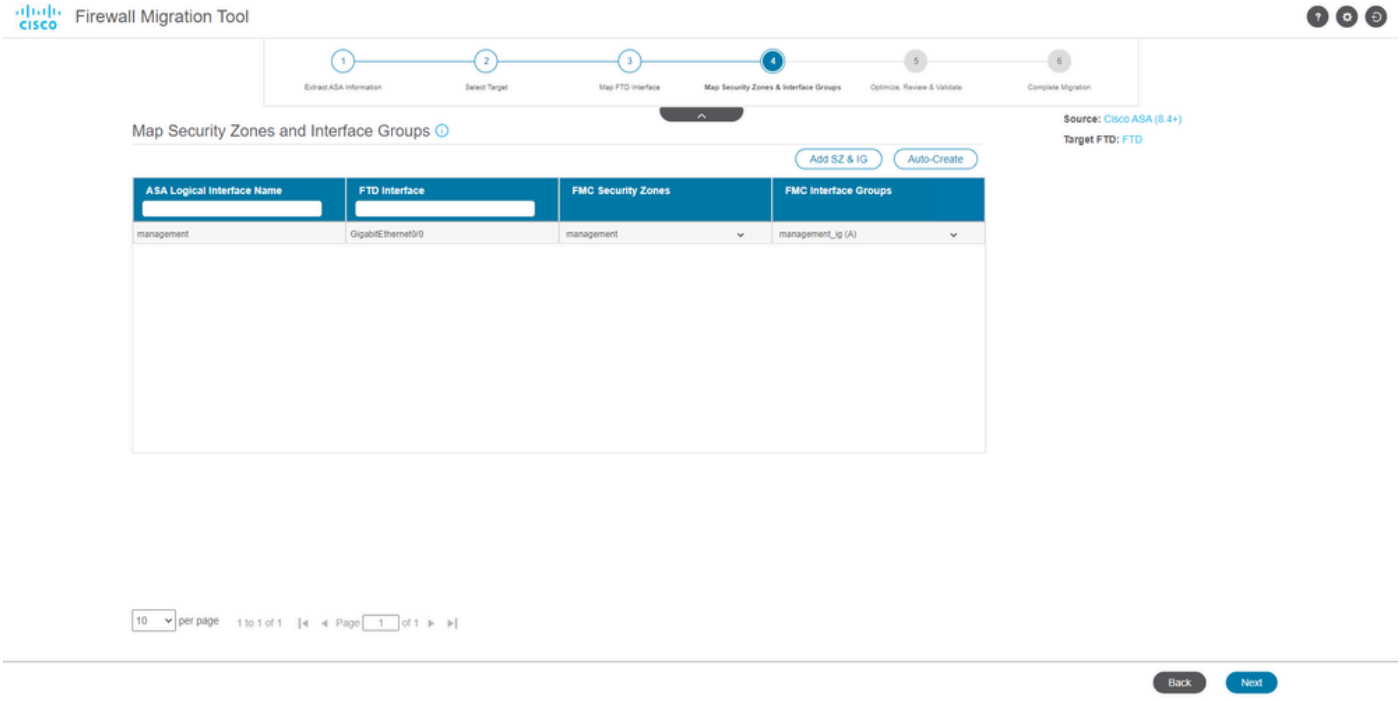
インターフェイスのマッピング

14. FTDのインターフェイスのセキュリティゾーンとインターフェイスグループを作成します



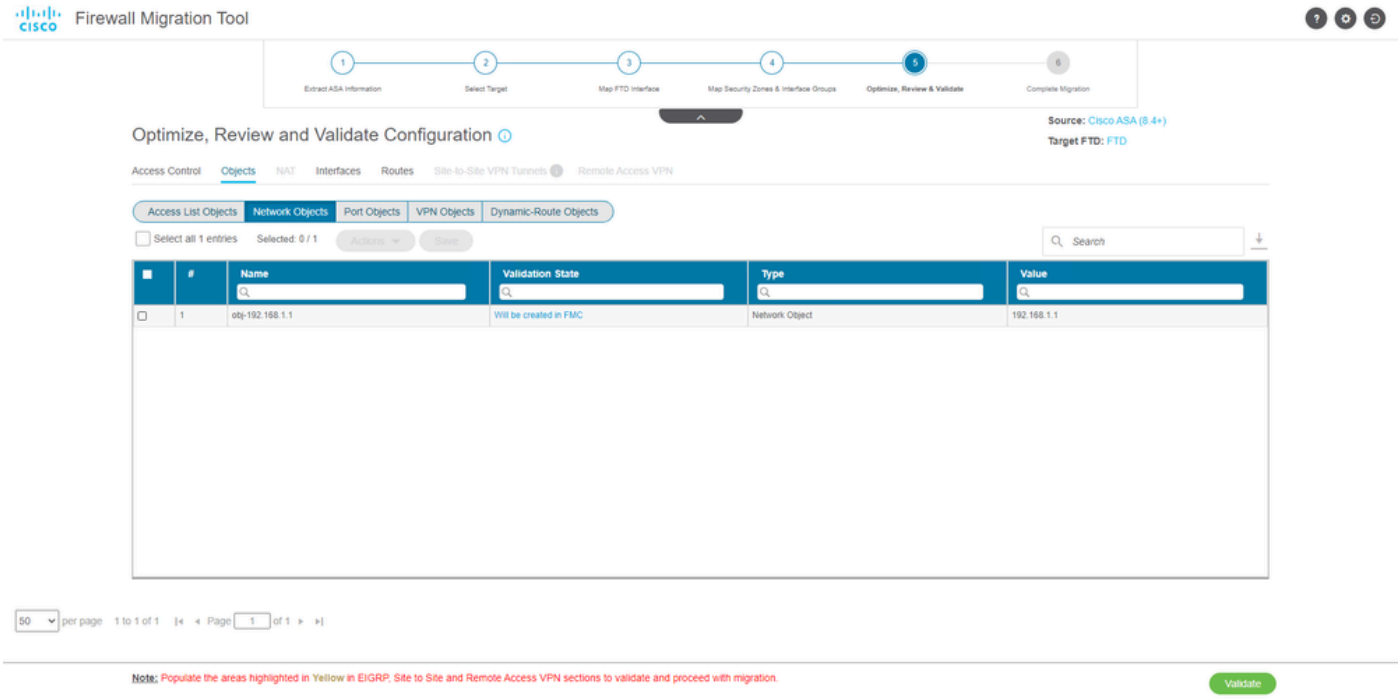
セキュリティゾーンとインターフェイスグループ

図に示すように、セキュリティゾーン(SZ)とインターフェイスグループ(IG)はツールによって自動的に作成されます。



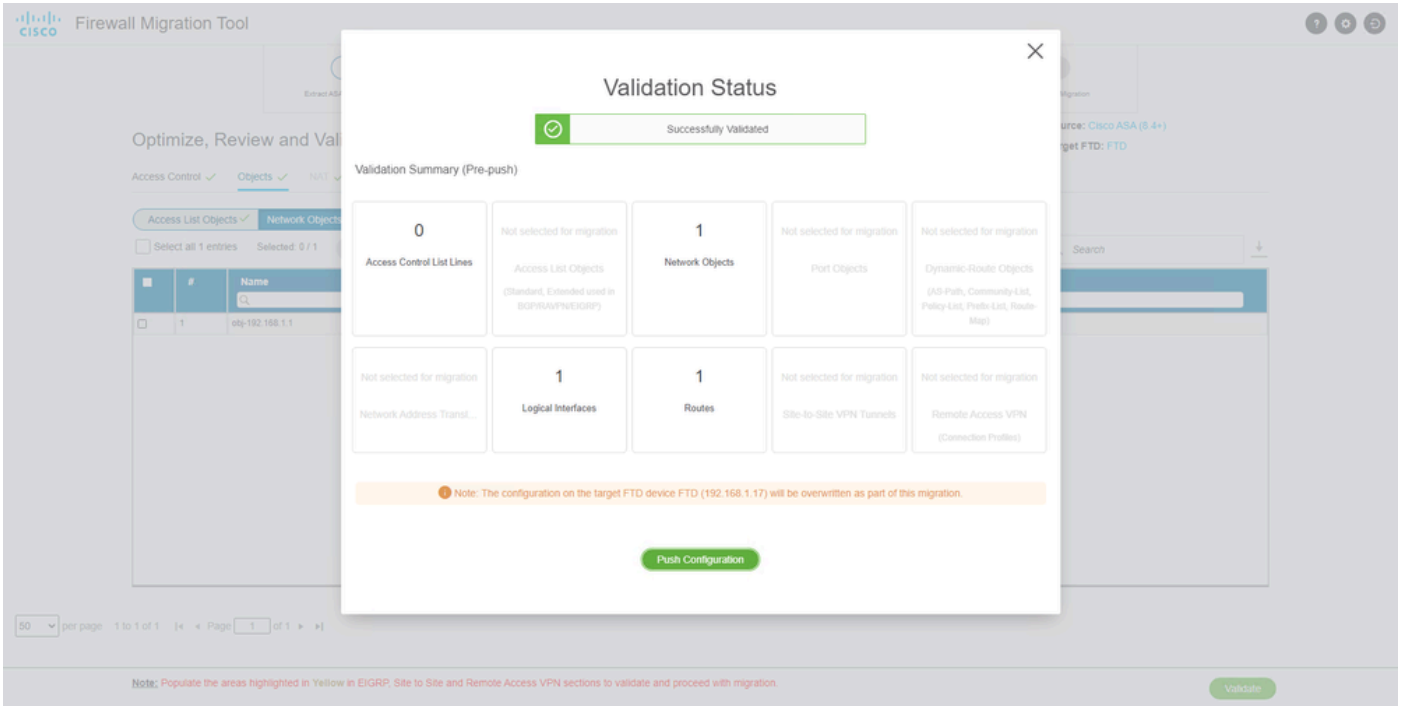
自動作成ツール

15. 移行ツールで、移行する構成をレビューして検証します。
    1. 設定のレビューと最適化をすでに終了している場合は、Validateをクリックします。



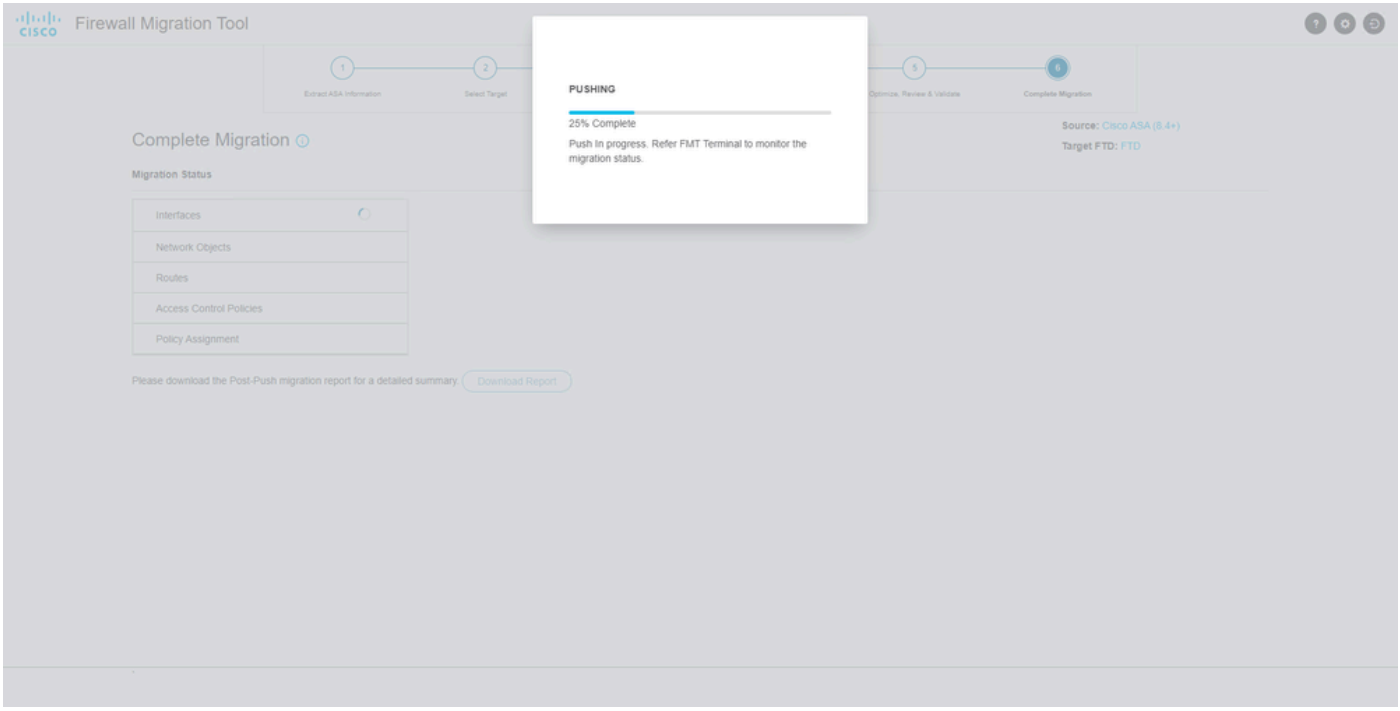
確認と検証

16. 検証ステータスが正常であれば、ターゲットデバイスに設定をプッシュします。



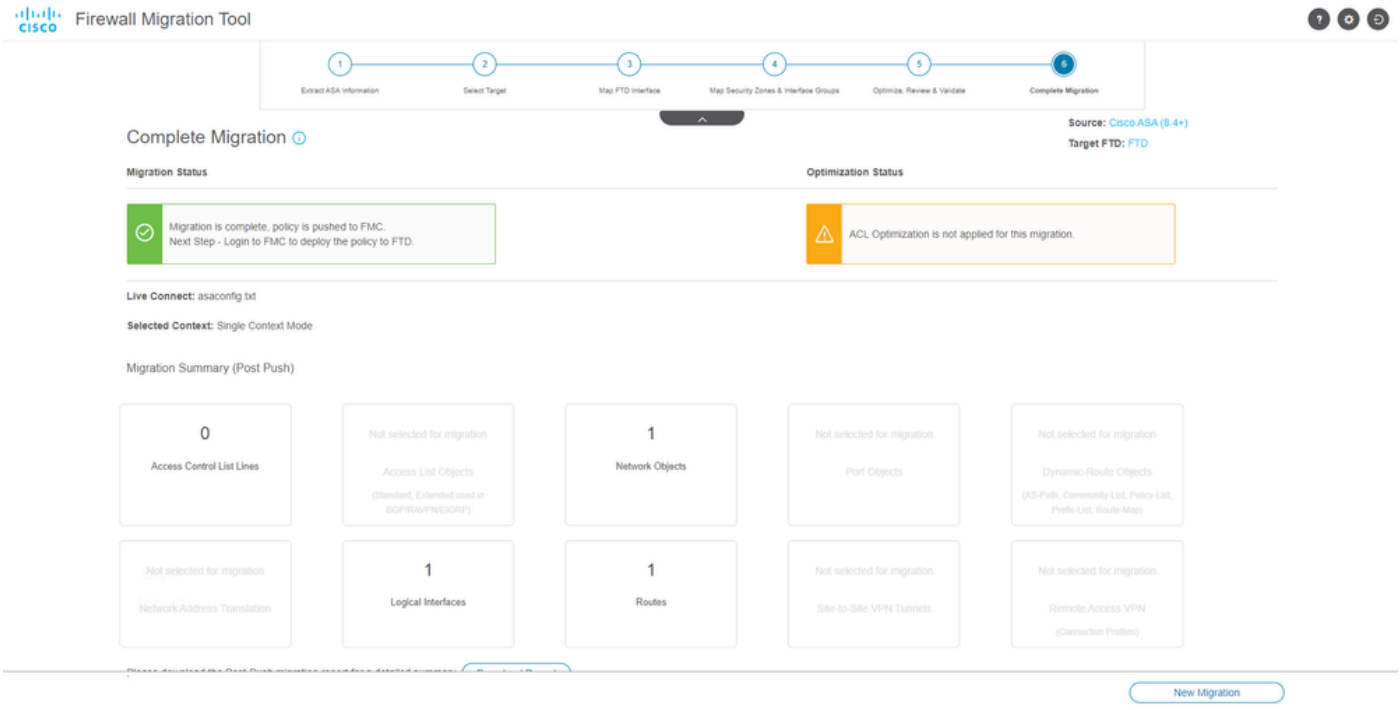
検証

図に示すように、移行ツールを介してプッシュされた設定の例：



プッシュ

図に示すように、正常な移行の例：



正常な移行

(オプション) 設定をFTDに移行することを選択した場合は、展開によって使用可能な設定をFMCからファイアウォールにプッシュする必要があります。

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. をクリックします。 Deploy

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:
  - ASA設定ファイルに不明または無効な文字があります。
  - 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
  - ASA設定ファイルのアップロード中または管理センターへの設定のプッシュ中の問題。
  - 一般的な問題として、次のようなものがあります。
- 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。
  - このツールを使用すると、ログファイル、データベース、および設定ファイルのサポートバンドルをダウンロードできます。
  - ダウンロード手順：
  - サポートの詳細：

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。