

FMTを使用したASAからFirepower Threat Defense(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](#)

[概要](#)

[背景説明](#)

[ASAコンフィギュレーションファイルの取得](#)

[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](#)

[AnyConnectのパッケージとプロファイルの取得](#)

[設定](#)

[設定手順:](#)

[トラブルシューティング](#)

[Secure Firewall Migration Toolの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、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 :

Software Download

Downloads Home / Security / Firewalls / Secure Firewall Migration Tool / Firewall Migration Tool (FMT)- 7.0.0

Expand All Collapse All

Latest Release

7.0.1

All Release

7

7.0.1

7.0.0

Secure Firewall Migration Tool

Release 7.0.0

[My Notifications](#)

Related Links and Documentation

[Open Source](#)

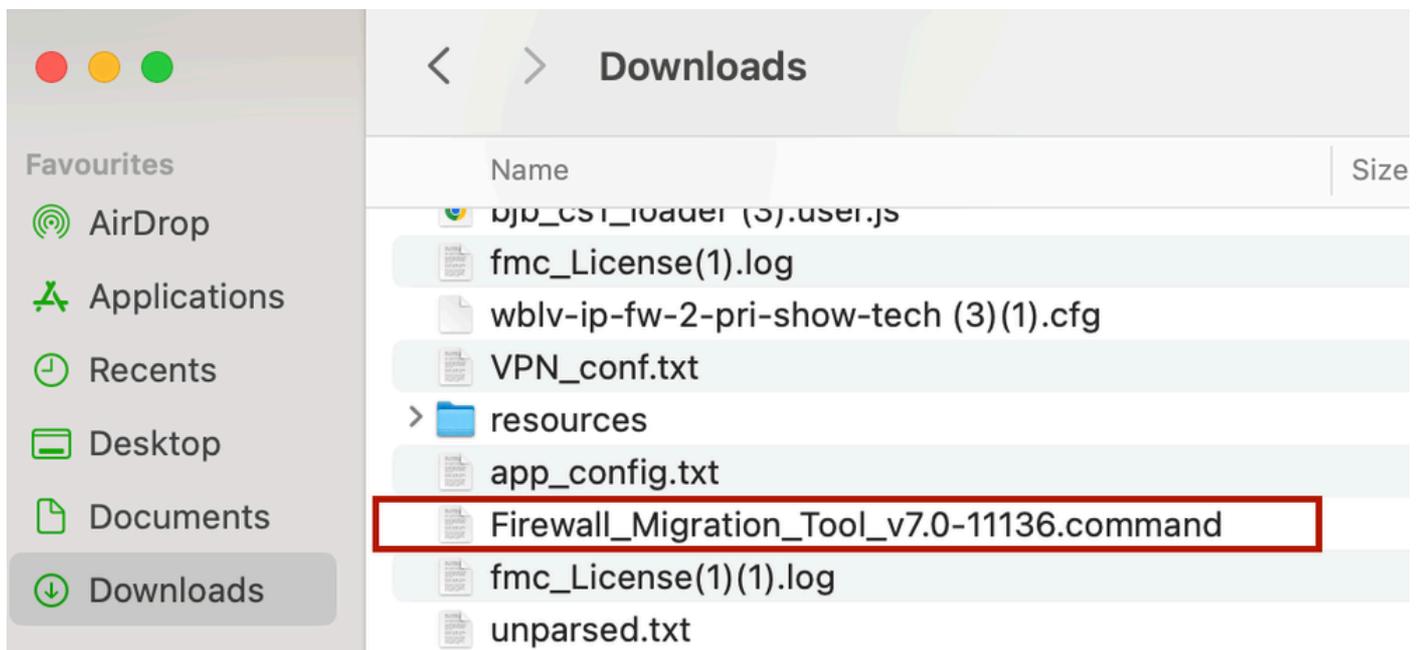
[Release Notes for 7.0.0](#)

[Install and Upgrade Guides](#)

File Information	Release Date	Size	
Firewall Migration Tool 7.0.0.1 for Mac Firewall_Migration_Tool_v7.0.0.1-11241.command Advisories	04-Sep-2024	41.57 MB	↓ 🛒 📄
Firewall Migration Tool 7.0.0.1 for Windows Firewall_Migration_Tool_v7.0.0.1-11241.exe Advisories	04-Sep-2024	39.64 MB	↓ 🛒 📄
Firewall Migration Tool 7.0.0 for Mac Firewall_Migration_Tool_v7.0-11136.command Advisories	05-Aug-2024	41.55 MB	↓ 🛒 📄
Firewall Migration Tool 7.0.0 for Windows Firewall_Migration_Tool_v7.0-11136.exe Advisories	05-Aug-2024	39.33 MB	↓ 🛒 📄

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

```
ontext migration.'], 'FDM-managed Device to Threat Defense Migration': ['migrate
the Layer 7 security policies including SNMP and HTTP, and malware and file pol
icy configurations from your FDM-managed device to a threat defense device.'], '
Third Party Firewall to Threat Defense Migration': ['Check Point Firewall - migr
ate the site-to-site VPN (policy-based) configurations on your Check Point firew
all ( R80 or later) to a threat defense device (Version 6.7 or later)', 'Fortine
t Firewall - Optimize your application access control lists (ACLs) when migratin
g configurations from a Fortinet firewall to your threat defense device.']], 'se
curity_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 t
o 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 t
o 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。

END USER LICENSE AGREEMENT

This is an agreement between You and Cisco Systems, Inc. or its affiliates ("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the individual or legal entity licensing the Software under this EULA. "Use" or "Using" means to download, install, activate, access or otherwise use the Software. "Software" means the Cisco computer programs and any Upgrades made available to You by an Approved Source and licensed to You by Cisco. "Documentation" is the Cisco user or technical manuals, training materials, specifications or other documentation applicable to the Software and made available to You by an Approved Source. "Approved Source" means (i) Cisco or (ii) the Cisco authorized reseller, distributor or systems integrator from whom you acquired the Software. "Entitlement" means the license detail, including license metric, duration, and quantity provided in a product ID (PID) published on Cisco's price list, claim certificate or right to use notification. "Upgrades" means all updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software and backup copies thereof. This agreement, any supplemental license terms and any specific product terms at www.cisco.com/go/software/terms (collectively, the "EULA") govern Your Use of the Software.

1. **Acceptance of Terms.** By Using the Software, You agree to be bound by the terms of the EULA. If you are entering into this EULA on behalf of an entity, you represent that you have authority to bind that entity. If you do not have such authority or you do not agree to the terms of the EULA, neither you nor the entity may Use the Software and it may be returned to the Approved Source for a refund within thirty (30) days of the date you acquired the Software or Cisco product. Your right to return and refund applies only if you are the original end user licensee of the Software.

2. **License.** Subject to payment of the applicable fees and compliance with this EULA, Cisco grants You a limited, non-exclusive and non-transferable license to Use object code versions of the Software and the Documentation solely for Your internal operations and in accordance with the Entitlement and the Documentation. Cisco licenses You the right to Use only the Software You acquire from an Approved Source. It makes no warranty, applicable law. You are not licensed to Use the

I have read the content of the EULA and SEULA and agree to terms listed.

Proceed

Migrate policies from Cisco ASA or Cisco ASA with FPS or Check Point or PAN or Fortinet to Cisco FTD



Extract Source Information

Any additional information explaining this



使用許諾契約書

- 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。



Security Cloud Sign On

Email

Continue

Don't have an account? [Sign up now](#)

Or

[Other login options](#)

[System status](#) [Policy statement](#)

FMTログイン

- 移行するソースファイアウォールを選択します。



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。

Extract Cisco ASA (8.4+) Information

Source: Cisco ASA (8.4+)

Extraction Methods >

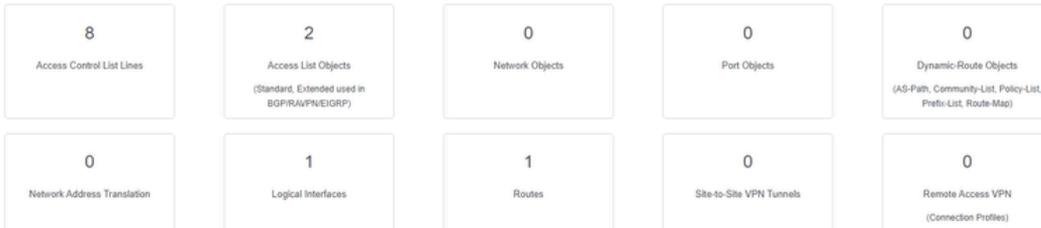
ASA IP Address: 192.168.1.20

Context Selection >

Single Context Mode: Download config

Parsed Summary v

Collect Hitcounts: No



● Pre-migration report will be available after selecting the targets.

https://cisco.com

Back

Next

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。

Select Target

Source: Cisco ASA (8.4+)

Firewall Management v

 On-Prem/Virtual FMC Cloud-delivered FMC

FMC IP Address/Hostname

192.168.1.18

Connect

1 FTD(s) Found

Proceed

 Successfully connected to FMC

Choose FTD >

Select Features >

Rule Conversion/ Process Config >

Back

Next

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

Select Target

Source: Cisco ASA (8.4+)

Firewall Management >

FMC IP Address/Hostname: 192.168.1.18

Choose FTD >

Select FTD Device Proceed without FTD

FTD (192.168.1.17) - VMWare (Native) v

Please ensure that the firewall mode configured on the target FTD device is the same as in the uploaded ASA configuration file. The existing configuration of the FTD device on the FMC is erased when you push the migrated configuration to the FMC.

Proceed

Select Features >

Rule Conversion/ Process Config >

Back

Next

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。

Select Target

Source: Cisco ASA (8.4+)

Firewall Management >

FMC IP Address/Hostname: 192.168.1.18

Choose FTD >

Selected FTD: FTD

Select Features >

Device Configuration	Shared Configuration	Optimization
<input checked="" type="checkbox"/> Interfaces	<input checked="" type="checkbox"/> Access Control	<input checked="" type="checkbox"/> Migrate Only Referenced Objects
<input checked="" type="checkbox"/> Routes	<input checked="" type="checkbox"/> Populate destination security zones	<input checked="" type="checkbox"/> Object Group Search
<input checked="" type="checkbox"/> Static	<input type="checkbox"/> NAT (no data)	Inline Grouping
<input type="checkbox"/> BGP	<input type="checkbox"/> Network Objects (no data)	<input checked="" type="checkbox"/> CSM/ASDM
<input type="checkbox"/> EIGRP	<input type="checkbox"/> Port Objects (no data)	
<input type="checkbox"/> Site-to-Site VPN Tunnels (no data)	<input type="checkbox"/> Access List Objects(Standard, Extended)	
<input type="checkbox"/> Policy Based (Crypto Map)	<input type="checkbox"/> Time based Objects (no data)	
<input type="checkbox"/> Route Based (VTI)	<input type="checkbox"/> Remote Access VPN	
	<input type="checkbox"/> Remote Access VPN migration is supported on FMC/FTD 7.2 and above.	

Proceed

Back

Next

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。



Select Target

Source: Cisco ASA (8.4+)

Firewall Management >

FMC IP Address/Hostname: 192.168.1.18

Choose FTD >

Selected FTD: FTD

Select Features >

Rule Conversion/ Process Config >

Start Conversion

Back

Next

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。

Select Target

Source: Cisco ASA (8.4+)

Firewall Management >

FMC IP Address/Hostname: 192.168.1.18

Choose FTD >

Selected FTD: FTD

Select Features >

Rule Conversion/ Process Config >

Start Conversion

0 parsing errors found. Refer to the pre-migration report for more details.

Please download the Pre-Migration report for a detailed summary of the parsed configuration.

Download Report

0 Access Control List Lines	0 Access List Objects (Standard, Extended used in BGP/RAVP/NEIGRP)	1 Network Objects	0 Port Objects	0 Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)
0 Network Address Translation	1 Logical Interfaces	1 Routes	0 Site-to-Site VPN Tunnels	0 Remote Access VPN (Connection Profiles)

Back

Next

レポートのダウンロード

図に示す移行前レポートの例：

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	ASA; 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

Map Security Zones and Interface Groups

Source: Cisco ASA (8.4+)
Target FTD: FTD

ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
management	GigabitEthernet0/0	Select Security Zone	Select Interface Groups

10 per page 1 to 1 of 1 |< < Page 1 of 1 > >|

Back Next

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。



Map Security Zones and Interface Groups

Source: Cisco ASA (8.4+)
Target FTD: FTD

ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
management	GigabitEthernet0/0	management	management_lg (A)

10 per page 1 to 1 of 1 |< < Page 1 of 1 > >|

Back Next

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。



Optimize, Review and Validate Configuration

Source: Cisco ASA (8.4+)
Target FTD: FTD

Access Control Objects NAT Interfaces Routes Site-to-Site VPN Tunnels Remote Access VPN

Access List Objects Network Objects Port Objects VPN Objects Dynamic-Route Objects

Select all 1 entries Selected: 0/1

#	Name	Validation State	Type	Value
1	obj-192.168.1.1	Will be created in FMC	Network Object	192.168.1.1

50 per page 1 to 1 of 1 Page 1 of 1

Note: Populate the areas highlighted in Yellow in EIGRP, Site to Site and Remote Access VPN sections to validate and proceed with migration.

Validate

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。

Validation Status

Successfully Validated

Validation Summary (Pre-push)

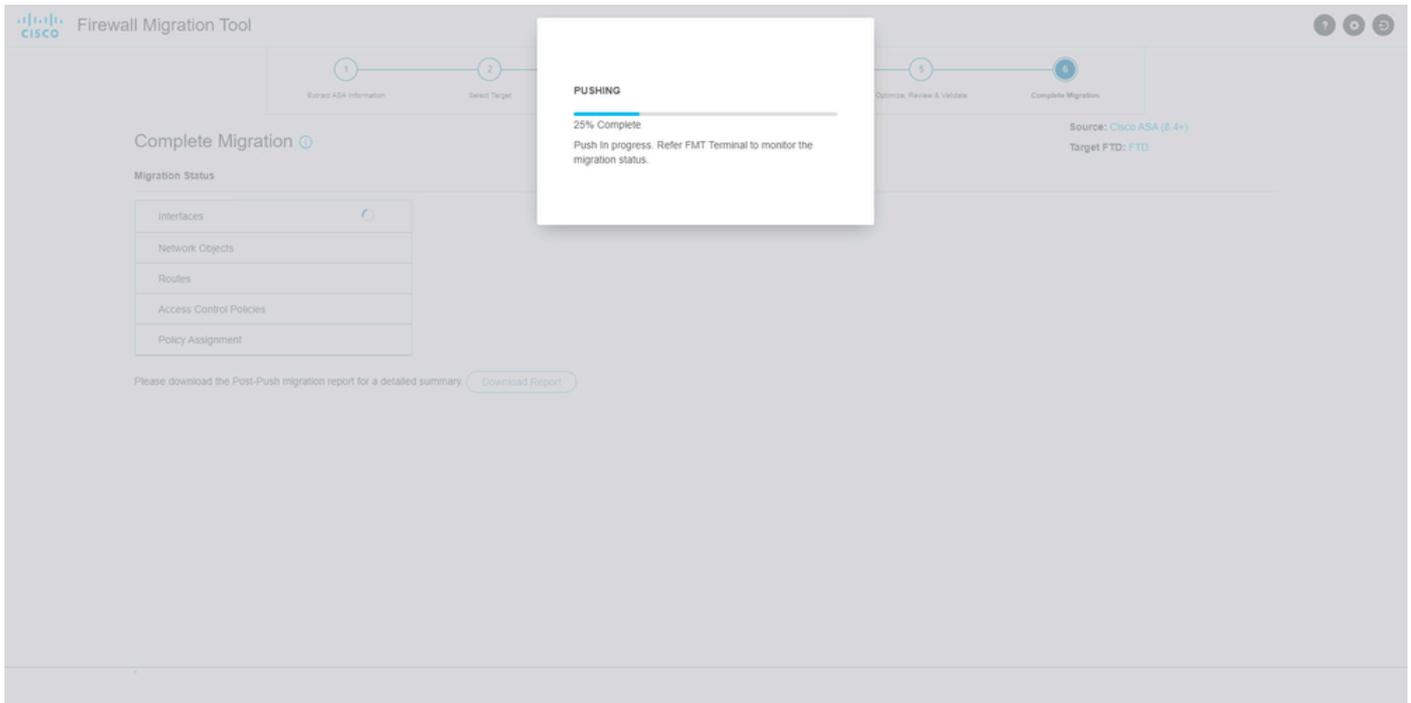
0 Access Control List Lines	Not selected for migration Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)	1 Network Objects	Not selected for migration Port Objects	Not selected for migration Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)
Not selected for migration Network Address Transl...	1 Logical Interfaces	1 Routes	Not selected for migration Site-to-Site VPN Tunnels	Not selected for migration Remote Access VPN (Connection Profiles)

Note: The configuration on the target FTD device FTD (192.168.1.17) will be overwritten as part of this migration.

Push Configuration

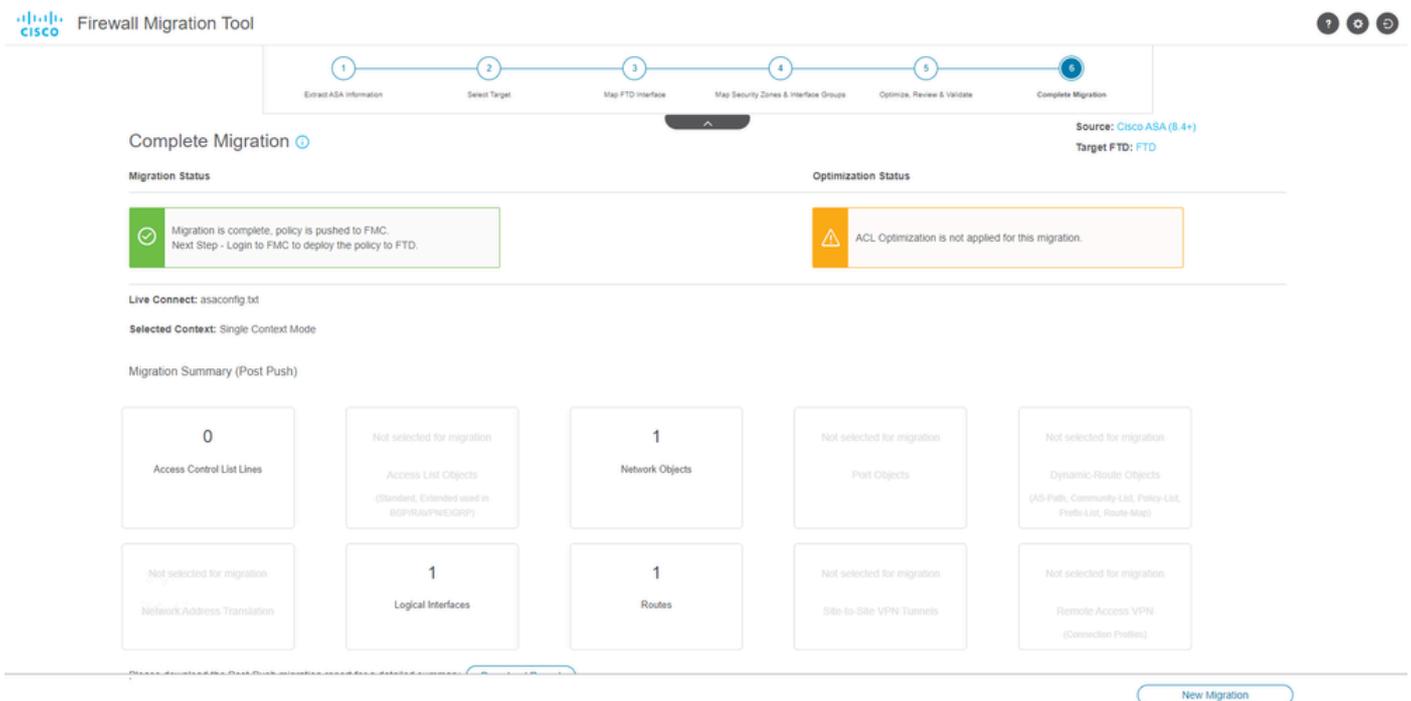
検証

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

トラブルシューティング

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。