

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:](#)

[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

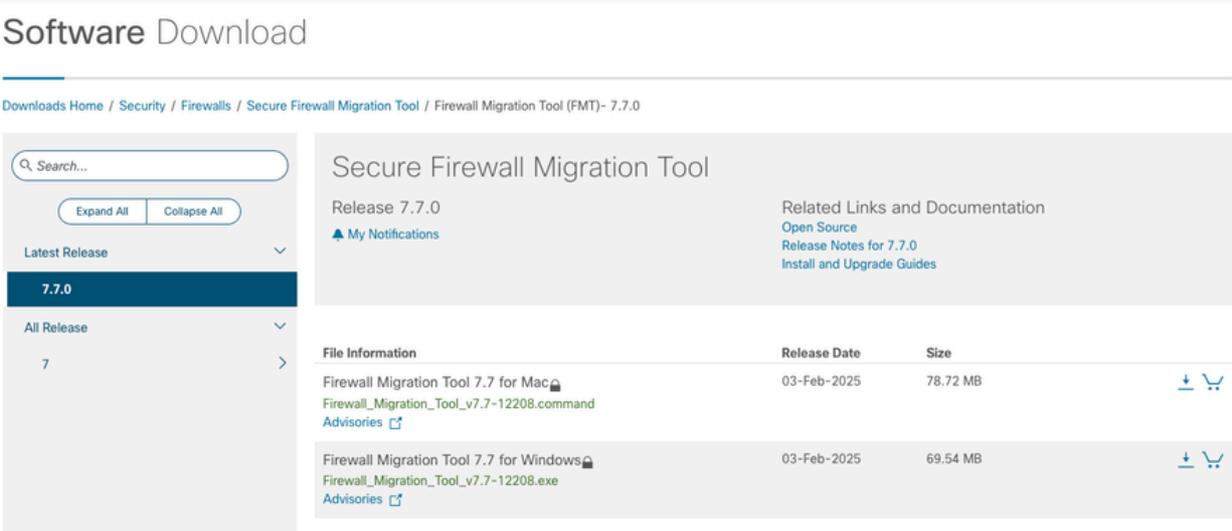
- 移行プロセスを開始する前に、FTDがFMCに登録されていることを確認します。
- 管理者権限を持つ新しいユーザアカウントがFMCに作成されました。または、既存の管理者クレデンシャルを使用することもできます。

- 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。



Software Download

Downloads Home / Security / Firewalls / Secure Firewall Migration Tool / Firewall Migration Tool (FMT)- 7.7.0

Search...

Expand All Collapse All

Latest Release

7.7.0

All Release

7

Secure Firewall Migration Tool

Release 7.7.0

My Notifications

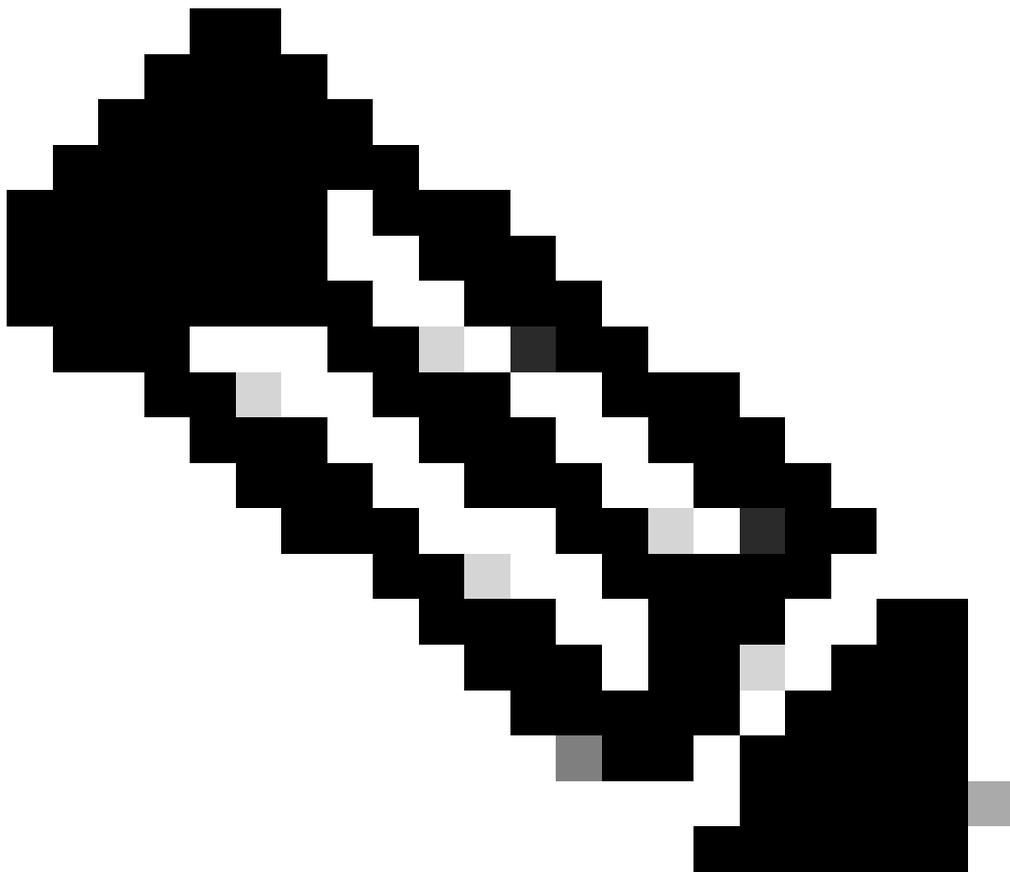
Related Links and Documentation

- Open Source
- Release Notes for 7.7.0
- Install and Upgrade Guides

File Information	Release Date	Size	
Firewall Migration Tool 7.7 for Mac Firewall_Migration_Tool_v7.7-12208.command Advisories	03-Feb-2025	78.72 MB	Download
Firewall Migration Tool 7.7 for Windows Firewall_Migration_Tool_v7.7-12208.exe Advisories	03-Feb-2025	69.54 MB	Download

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。

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。

Firewall Migration Tool (Version 7.7)

Select Source Configuration

Source Firewall Vendor
Palo Alto Networks (8.0+)

Start Migration Demo Mode

Palo Alto Networks (8.0+) Pre-Migration Instructions

This migration may take a while. Do not make any changes to the Firewall Management Center (FMC) when migration is in progress.

Session Telemetry:
Cisco collects the firewall telemetry set forth below in connection with this migration. By completing the migration, you consent to Cisco's collection and use of this telemetry data for purposes of tracking and following up on firewall device migrations and performing related migration analytics.

Acronyms used:
FMT: Firewall Migration Tool FMC: Firewall Management Center
FTD: Firewall Threat Defense

Before you begin your Palo Alto Networks (PAN) to Firewall Threat Defense migration, you must have the following items:

- Stable IP Connection:**
Ensure that the connection is stable between FMT and FMC.
- FMC Version:**
Ensure that the FMC version is 6.2.3 or later. For optimal migration time, improved software quality and stability, use the suggested release for your FTD and FMC. Refer to the gold star on CCO for the suggested release.
- FMC Account:**
Create a dedicated user account with administrative privileges for the FMT and use the credentials during migration.
- FTD (Optional):**
To migrate the device configurations like interfaces, routes, and so on, add the target device to FMC. Skip this step if you want to migrate only the shared configurations like objects, NAT, ACL, and so on.
- Palo Alto Networks Configuration Requirements:**
Export named configuration snapshot file from palo alto firewall to .xml format. If your NAT has polices with the same source and destination zone, then

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。

Firewall Migration Tool (Version 7.7)

Extract Config Information

Extraction Methods

Manual Configuration Upload
The configuration file must be a zip file consisting of the following:

- Zip Config file derived from the PAN Tool.

Upload

Context Selection

Parsed Summary

Extract Config Information

Extraction Methods

Manual Configuration Upload

The configuration file must be a zip file consisting of the following:

- Zip Config

Downloads

config.zip

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。

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。

Firewall Migration Tool (Version 7.7) Source: Palo Alto Networks (8.0+)

Extract Config Information

Extraction Methods

Context Selection

Parsed Summary

184 Access Control List Lines	908 Network Objects	150 Port Objects	49 Network Address Translation	9 Logical Interfaces
15 Static Routes	73 Applications	4 Site-to-Site VPN Tunnels (Route Based)	13 Remote Access VPN (Global Protect Gateways)	

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

Success
Context list Collected Successfully

Back Next

構成検証の概要

- 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。

Firewall Migration Tool (Version 7.7) Source: Palo Alto Networks (8.0+)

Select Target

Firewall Management

On-Prem FMC (Hardware/Virtual) Cloud-delivered FMC Multicloud Defense

FMC IP Address/Hostname/FQDN
10.225.107.99
Connect

Choose FTD

Select Features

Rule Conversion/ Process Config

FMC Login

IP Address/Hostname/FQDN
10.225.107.99

Username
admin

Password

Login

FMCログイン

- 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。

Select Target

Firewall Management

On-Prem FMC (Hardware/Virtual) Cloud-delivered FMC Multicloud Defense

FMC IP Address/Hostname/FQDN: 10.225.107.99

Choose Domain: Global/Cisco

Connect

Proceed

Successfully connected to FMC

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。

Select Target

Firewall Management

FMC IP Address/Hostname/FQDN: 10.225.107.99 Selected Domain: Global/Cisco

Choose FTD

Select FTD Device Proceed without FTD

FW1 (10.105.209.80) - NA (R)

Proceed

Select Features

Rule Conversion/ Process Config

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

Select Target

Firewall Management

FMC IP Address/Hostname/FQDN: 10.225.107.99 Selected Domain: Global/Cisco

Choose FTD

Selected FTD: FW1

Select Features

Device Configuration

- Interfaces
- Routes
- Site-to-Site VPN Tunnels
- Policy Based (Unsupported)
- Route Based (VTI)

Shared Configuration

- Access Control
- Migrate policies with Application-default as Enabled
- Network Objects
- Port Objects
- Remote Access VPN

Advanced Configuration

Optimization

- Migrate Only Referenced Objects

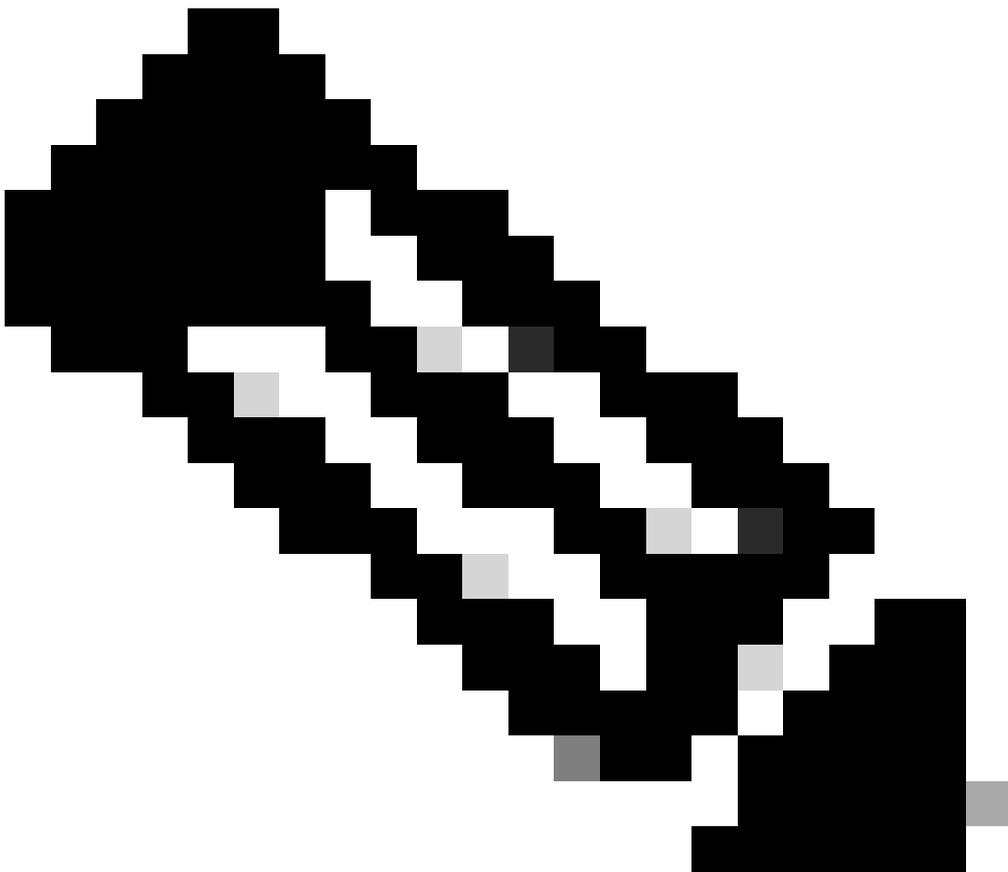
Access Control Options

- Discovered Identities

Proceed

Rule Conversion/ Process Config

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。

Source: Palo Alto Networks (8.0+)

Select Target ○

Firewall Management >

FMC IP Address/Hostname/FQDN: 10.225.107.99 Selected Domain: Global/Cisco

Choose FTD >

Selected FTD: FW1

Select Features >

Rule Conversion/ Process Config >

Start Conversion

No parsing error 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](#)

For pre-migration report

Parsed configuration summary

195 Access Control List Lines	752 Network Objects	98 Port Objects	52 Network Address Translation	8 Logical Interfaces
2 Static Routes	0 Site-to-Site VPN Tunnels (Route Based)	70 Applications	9 Remote Access VPN (Global Protect Gateways)	

Back Next

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。

Source: Palo Alto Networks (8.0+)
Target FTD: FW1

Map FTD Interface ○

PAN Interface Name	FTD Interface Name	Mapped Name#
ethernet1/2	Select interface ✓ Ethernet1/1	ethernet1_2
ethernet1/3	Ethernet1/10	ethernet1_3
ethernet1/4	Ethernet1/11	ethernet1_4
ethernet1/5	Ethernet1/12	ethernet1_5
ethernet1/6	Ethernet1/13	ethernet1_6
ethernet1/7	Ethernet1/14	ethernet1_7
	Ethernet1/15	
	Ethernet1/16	
	Ethernet1/17	
	Ethernet1/18	
	Ethernet1/19	

FTD Interface name can be edited

Mapping of FTD interfaces

10 per page 1 to 6 of 6 [4] Page 1 of 1 >

Back Next

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。

Map Security Zones

PAN Zone Name	FMC Security Zones
G...-Inside	Select Security Zone
Outside	Select Security Zone
GP/PA-	Select Security Zone
I...Ine	Select Security Zone
DMZ	Select Security Zone
I...C	Select Security Zone
Mel	Select Security Zone
OT-	Select Security Zone
Wireless-	Select Security Zone
I...-Inside	Select Security Zone

Add SZ Auto-Create Save

First option is to add Security Zone manually and second option is to auto create Security Zone

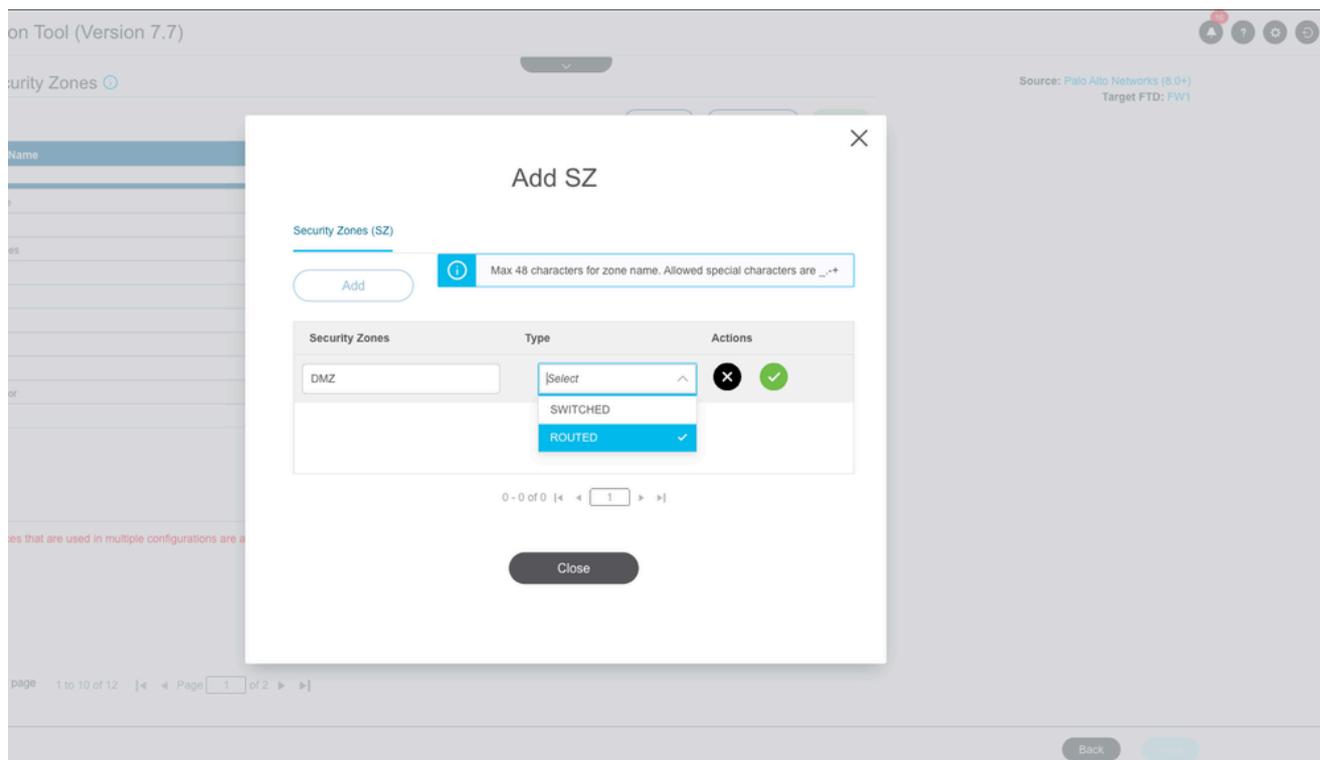
Note: Interfaces that are used in multiple configurations are allowed to have their unique security zones. The security zone mapping section for these interfaces will be grayed out.

10 per page 1 to 10 of 12 Page 1 of 2

Back Next

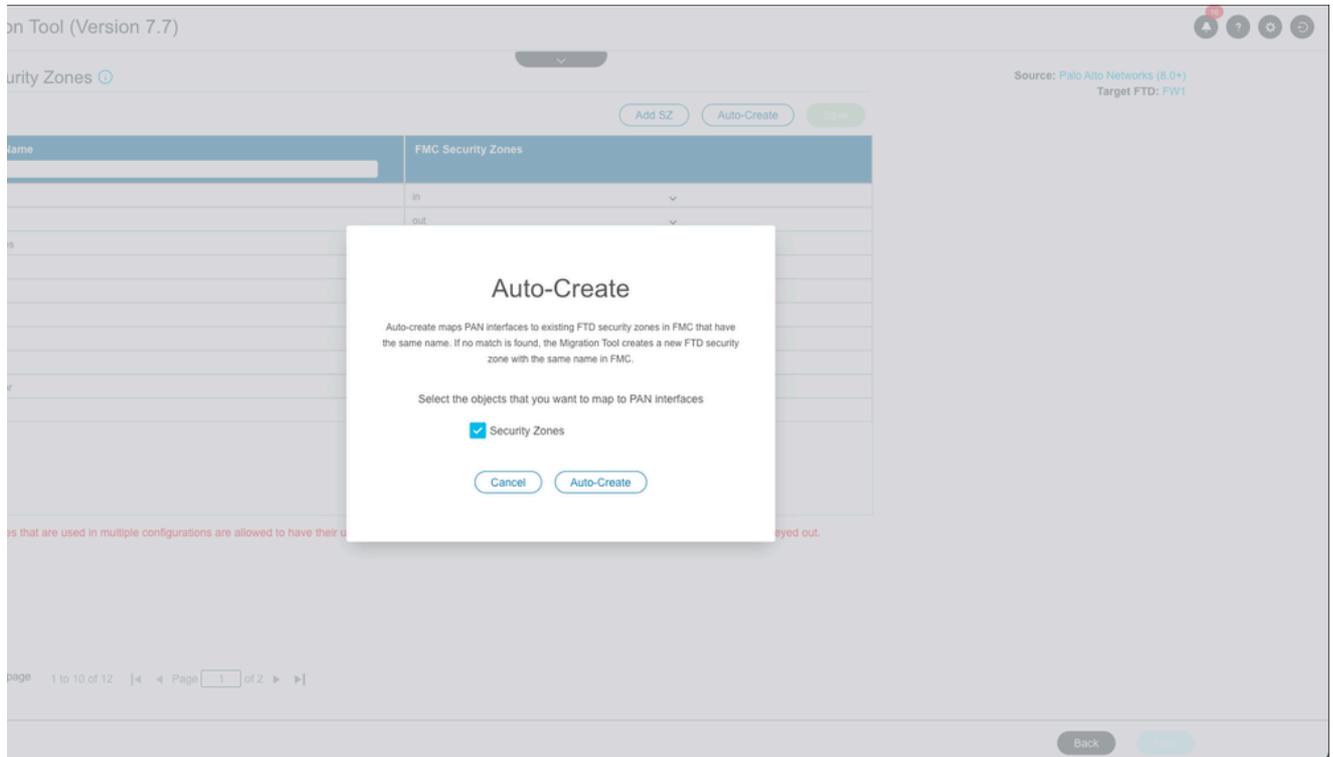
セキュリティゾーンの作成

セキュリティゾーンの手動作成 :



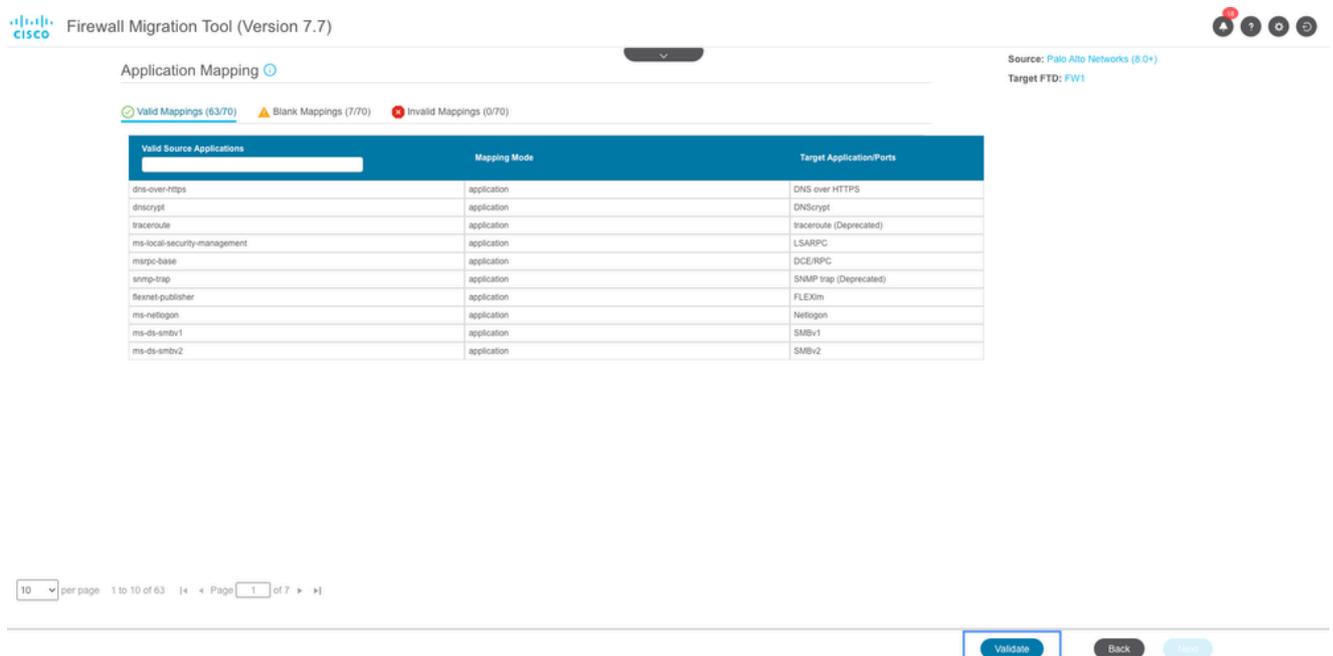
セキュリティゾーンの手動作成

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

- 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

Application Mapping

Validation of application mapping is in progress. Please wait

Source: Palo Alto Networks (8.0+)

Target FTD: FW1

Valid Mappings (63/70) Blank Mappings (7/70) Invalid Mappings (0/70)

Valid Source Applications	Mapping Mode	Target Application/Ports
dns-over-https	application	DNS over HTTPS
dnscrypt	application	DNScrypt
traceroute	application	traceroute (Deprecated)
ms-local-securitymanagement	application	LSARPC
snmp-base	application	DCE/RPC
snmp-trap	application	SNMP trap (Deprecated)
flexnet-publisher	application	FLEXlm
ms-netlogon	application	Netlogon
ms-ds-smbv1	application	SMBv1
ms-ds-smbv2	application	SMBv2

10 per page 1 to 10 of 63 | Page 1 of 7

[Validate](#) [Back](#) [Next](#)

アプリケーションマッピングの検証

検証の際、FMTは空白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、空白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。

Application Mapping

Clear Mapped Data

Valid Mappings (61/70) Blank Mappings (7/70) Invalid Mappings (2/70)

Invalid Source Applications	Mapping Mode	Target Application/Ports
traceroute	Application	netmg-traceroute
snmp-trap	Port(s)	udp/162

10 per page 1 to 2 of 2 | Page 1 of 1

[Validate](#) [Back](#) [Next](#)

空白および無効なアプリケーションマッピング

- 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。

Optimize, Review and Validate Configuration

Source: Palo Alto Networks (8.0+)
Target FTD: FW1

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

Select all 195 entries Selected: 0 / 195

#	Name	SOURCE				DESTINATION				Application	URLs	State	Action	TIME BASED	
		Zone	Network	Port	User	Zone	Network	Port	Application						
1	Allow Tm...	Dc	GRP_ADDR...	ANY	ANY			ANY	NTP	NA	✓	Allow	None		
2	Allow Tm...	Df	ANY	ANY	ANY			IN...	ANY	NA	✓	Allow	None		
3	Allow Tm...	Df	GRP_ADDR...	ANY	ANY			com	ANY	NA	✓	Allow	None		
4	Allow DNS	Df	ANY	ANY	ANY			3R...	ANY	DNS, DNSCrypt, DN...	NA	✓	Allow	None	
5	Allow DNS	O	ANY	ANY	ANY			3R...	ANY	DNS	NA	✓	Allow	None	
6	Allow API	Dc	ANY	ANY	ANY			3M...	TCP-80,TCP...	ANY	NA	✓	Allow	None	
7	Allow traffi	G...	ADDR_10.11...	ANY	ANY			2.16...	TCP-443	ANY	NA	✓	Allow	None	
8	Allow Acco	G...	ADDR_192.16...	ANY	ANY			DT...	ANY	ANY	NA	✓	Allow	None	
9	Allow ICM	O	ANY	ANY	ANY			Inside	ANY	netmg-traceroute	NA	✓	Allow	None	
10	Allow ICM	O	ANY	ANY	ANY			Inside	ICMPv4	ANY	NA	✓	Allow	None	
11	Allow DHC	O	ANY	ANY	ANY			Inside	.11...	DHCP	NA	✓	Allow	None	
12	Allow NetE	O	ANY	ANY	ANY			Inside	.11...	ANY	NetBIOS-ns, NetBIO...	NA	✓	Allow	None
13	Allow DNS	O	ANY	ANY	ANY			Inside	.11...	ANY	DNS	NA	✓	Allow	None

50 per page 1 to 50 of 195 Page 1 of 4

Optimize access control list and validate

Optimize ACL Validate

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。

Validation Status

Successfully Validated

Validation Summary (Pre-push)

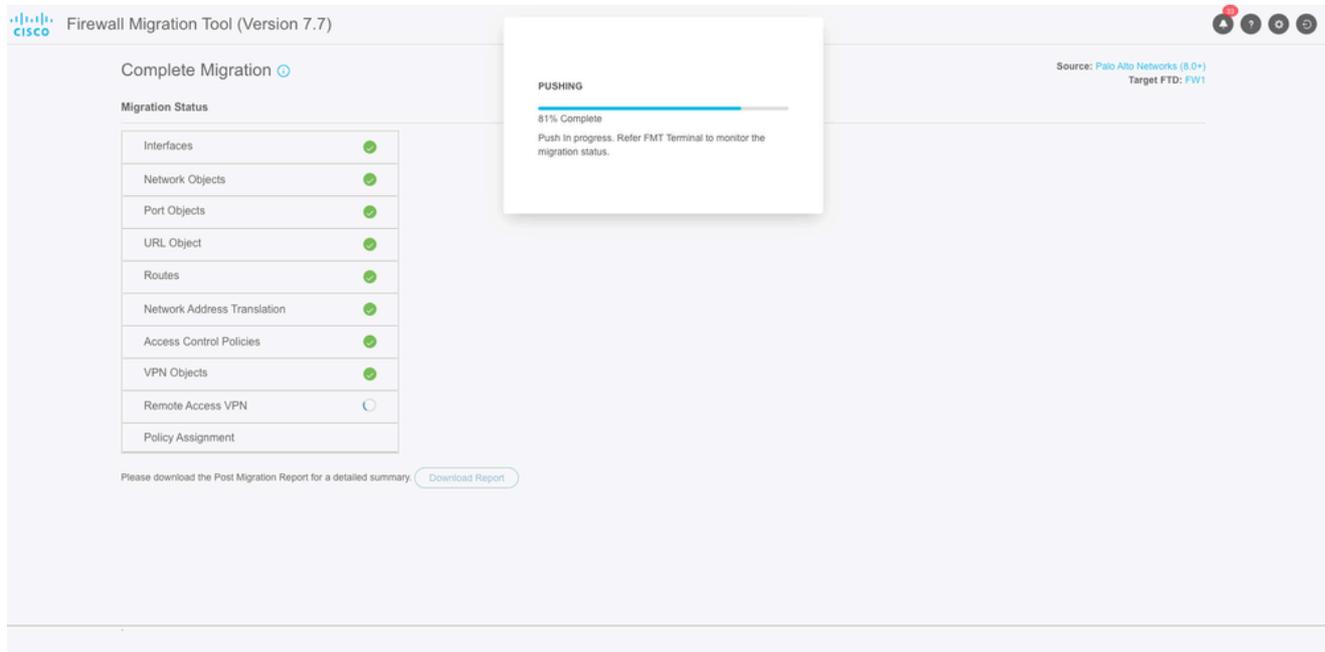
195 Access Control List Lines	752 Network Objects	100 Port Objects	52 Network Address Translation	8 Logical Interfaces
2 Static Routes	0 Site-to-Site VPN Tunnels (Route Based)	62 Applications	9 Remote Access VPN (Global Protect Gateways)	

Note: The configuration on the target FTD device FW1 (10.105.209.80) will be overwritten as part of this migration.

Push Configuration

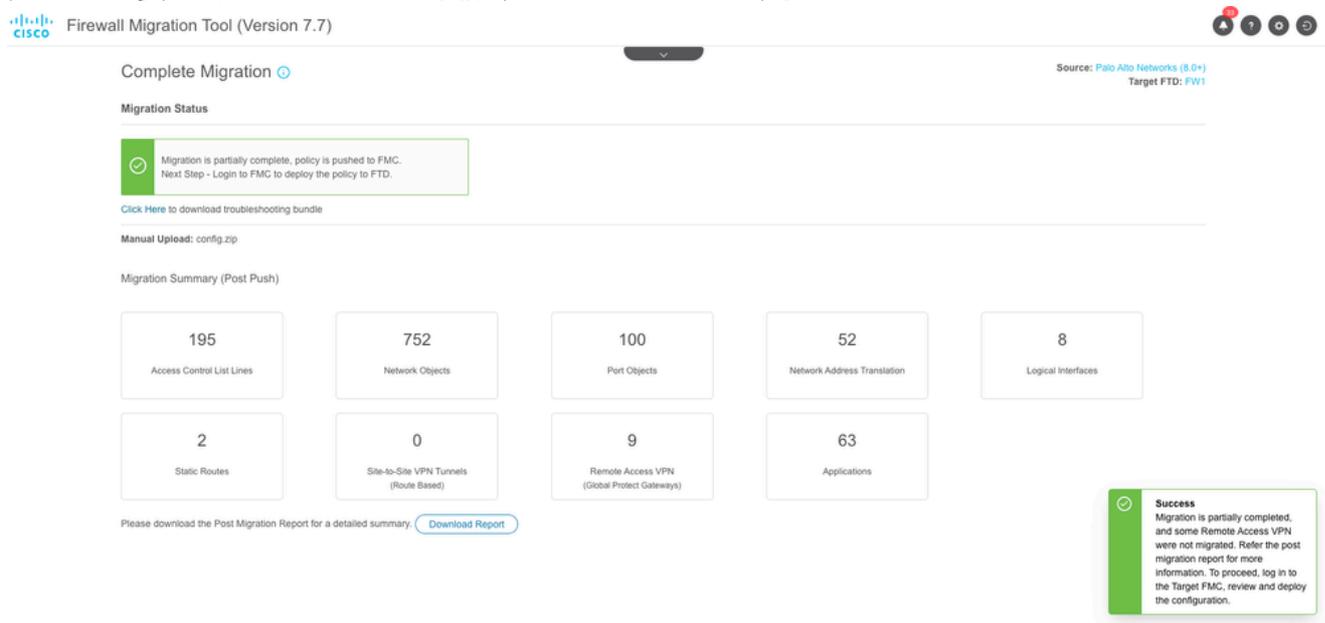
構成検証の概要

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。