

ASA移行用のSecure Firewall Migration Toolの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[設定手順](#)

[トラブルシューティング](#)

概要

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に移行する手順について説明します。

著者 : Cisco TACエンジニア、Ricardo Vera

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。

- Firepower Migration Tool(FMT)v3.0.1を搭載したWindows PC
- 適応型セキュリティアプライアンス(ASA)v9.16.1
- Secure Firewall Management Center(FMCv)v7.0.1
- Secure Firewall Threat Defense Virtual(FTDv)v7.0.1

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、初期（デフォルト）設定の状態から起動しています。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。

このドキュメントの具体的な要件は次のとおりです。

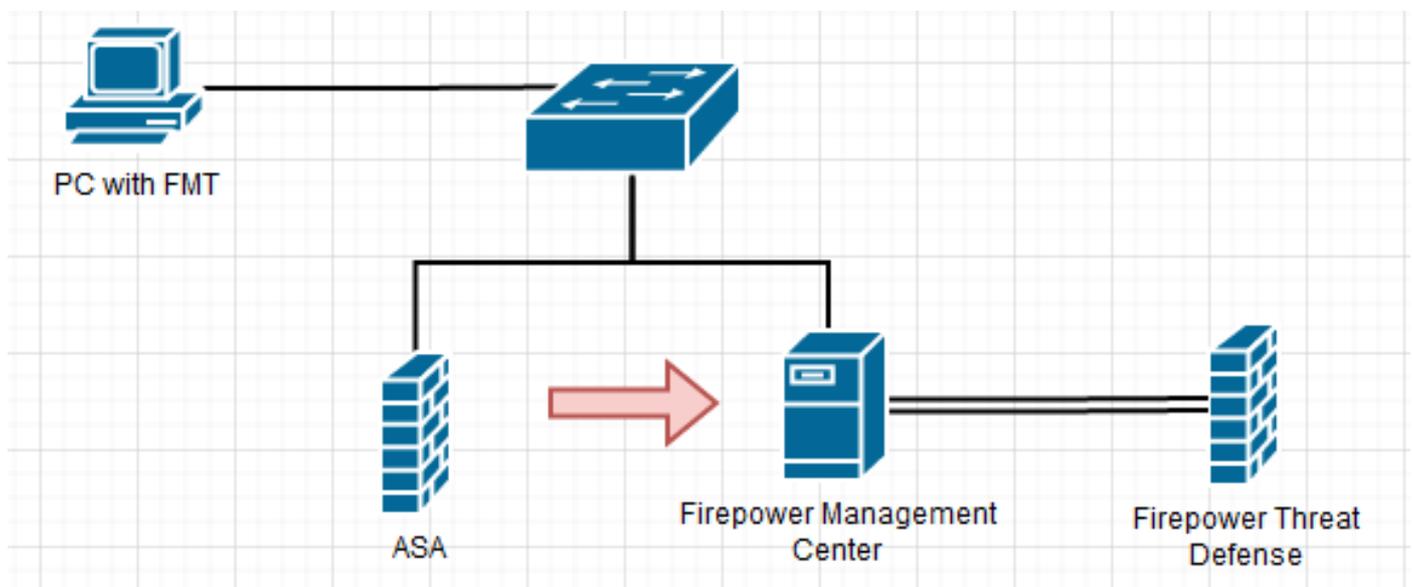
- Cisco 適応型セキュリティ アプライアンス (ASA) バージョン 8.4 以降
- Secure Firewall Management Center(FMCv)バージョン6.2.3以降

Firewall Migration Tool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以降) (FPS)
- 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)

移行を進める前に、「ファイアウォール移行ツールの[ガイドラインと制限事項](#)」を考慮してください。

設定



1. 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 / Next-Generation Firewalls (NGFW) / Secure Firewall Threat Defense Virtual / Firepower Migration Tool (FMT) - 3.0.1

Expand All | Collapse All

Latest Release

3.0.1

2.5.3

All Release

3 >

2 >

Secure Firewall Threat Defense Virtual

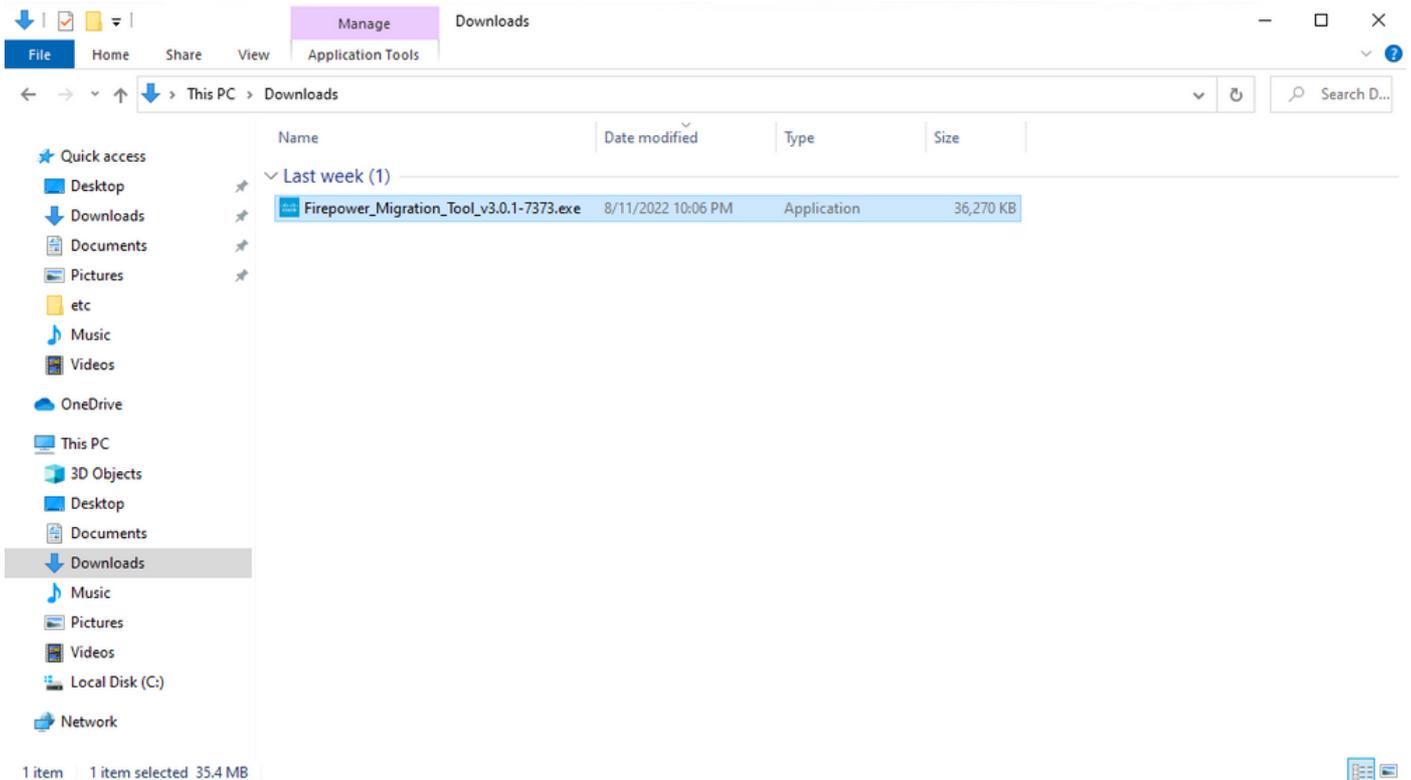
Release 3.0.1

[My Notifications](#)

[Related Links and Documentation](#)
[Open Source](#)
[Release Notes for 3.0.1](#)
[Install and Upgrade Guides](#)

File Information	Release Date	Size	
The extractor will be used to extract checkpoint device-specific configurations which will be used as an input to Firepower Migration Tool. FMT-CP-Config-Extractor_v3.0.1-7373.exe Advisories	10-Aug-2022	9.83 MB	↓ 🛒 📄
Firepower Migration Tool 3.0.1 for Mac Firepower_Migration_Tool_v3.0.1-7373.command Advisories	10-Aug-2022	34.75 MB	↓ 🛒 📄
Firepower Migration Tool 3.0.1 for Windows Firepower_Migration_Tool_v3.0.1-7373.exe Advisories	10-Aug-2022	35.42 MB	↓ 🛒 📄

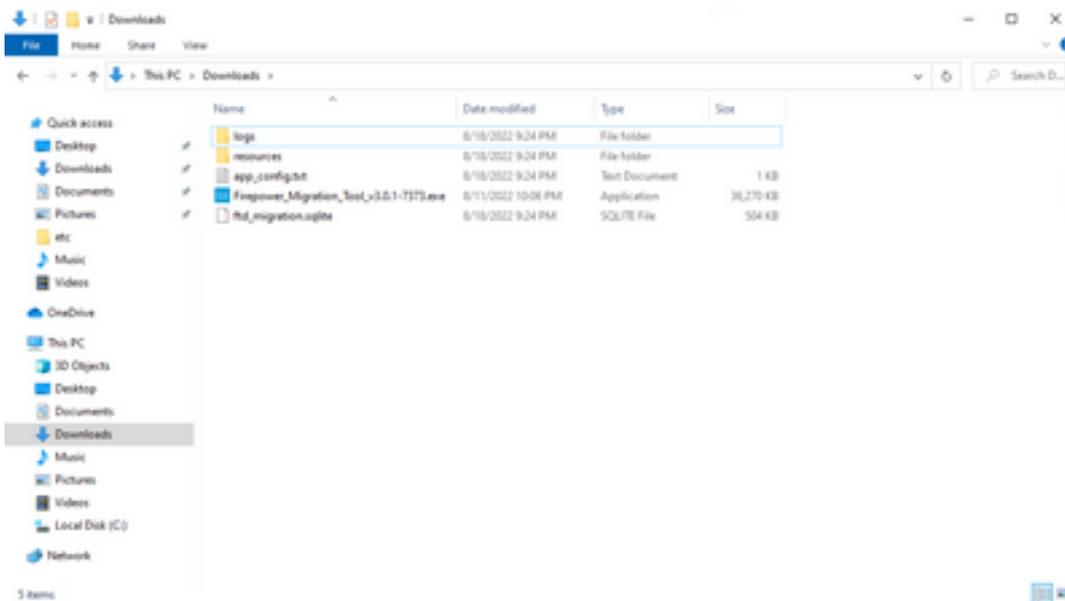
2. コンピュータにダウンロードしたファイルをクリックします。



注：プログラムが自動的に開き、コンソールがファイルを実行したディレクトリのコンテンツを自動生成します。

```
C:\Users\cali\Downloads\Firepower_Migration_Tool_v1.0.1-7171.exe
2022-08-18 21:24:49,752 [INFO] _init_ > "Initializing..."
2022-08-18 21:24:49,767 [INFO] settings > "Settings:[global_suffix]"
2022-08-18 21:24:50,189 [INFO] tool_version > "ToolVersion:[0817373]"
2022-08-18 21:24:50,252 [INFO] _init_ > "Initializing..."
2022-08-18 21:24:51,252 [INFO] config > "loading settings"
2022-08-18 21:24:51,268 [INFO] client > "Getting ssl context for auth server"
2022-08-18 21:24:51,299 [INFO] tools > "Not verifying ssl certificates"
2022-08-18 21:24:51,299 [INFO] client > "No discovery url configured, all endpoints needs to be configured manually"

2022-08-18 21:24:51,314 [INFO] settings > "Disabled console quick edit mode"
2022-08-18 21:24:51,314 [DEBUG] common > "session table records count:1"
2022-08-18 21:24:51,314 [INFO] common > "Using port: 8888"
2022-08-18 21:24:51,799 [INFO] run > "***** Starting server at http://localhost:8888 *****"
 * Running on http://localhost:8888/ (Press CTRL+C to quit)
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /styles.a0d79d0031ca150b236f.bundle.css HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /inline.318b50c57b4eba3d437b.bundle.js HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /cui-font.800241c8aa87aa899c6a.woff2 HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /polyfills.76c2f21d4e2a1188f46c.bundle.js HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /main.777e77bd49fe82694a1a.bundle.js HTTP/1.1" 200 -
2022-08-18 21:24:57,075127.0.0.1 - - [18/Aug/2022 21:24:57] "GET /assets/cisco.svg HTTP/1.1" 200 -
[INFO] cco_login > "USA check for an user"
2022-08-18 21:24:57,704 [DEBUG] common > "session table records count:1"
127.0.0.1 - - [18/Aug/2022 21:24:57] "GET /api/eula_check HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:57] "GET /assets/icons/login.png HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:58] "GET /assets/images/1.png HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:58] "GET /assets/images/3.png HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:58] "GET /assets/images/2.png HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:58] "GET /favicon.ico HTTP/1.1" 200 -
```



3. プログラムを実行すると、Webブラウザが開き、「エンドユーザライセンス契約書」が表示されます。チェックボックスをオンにして利用条件に同意します。[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 is not intended to be a license to Use the Software. You are not licensed to Use the Software.

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

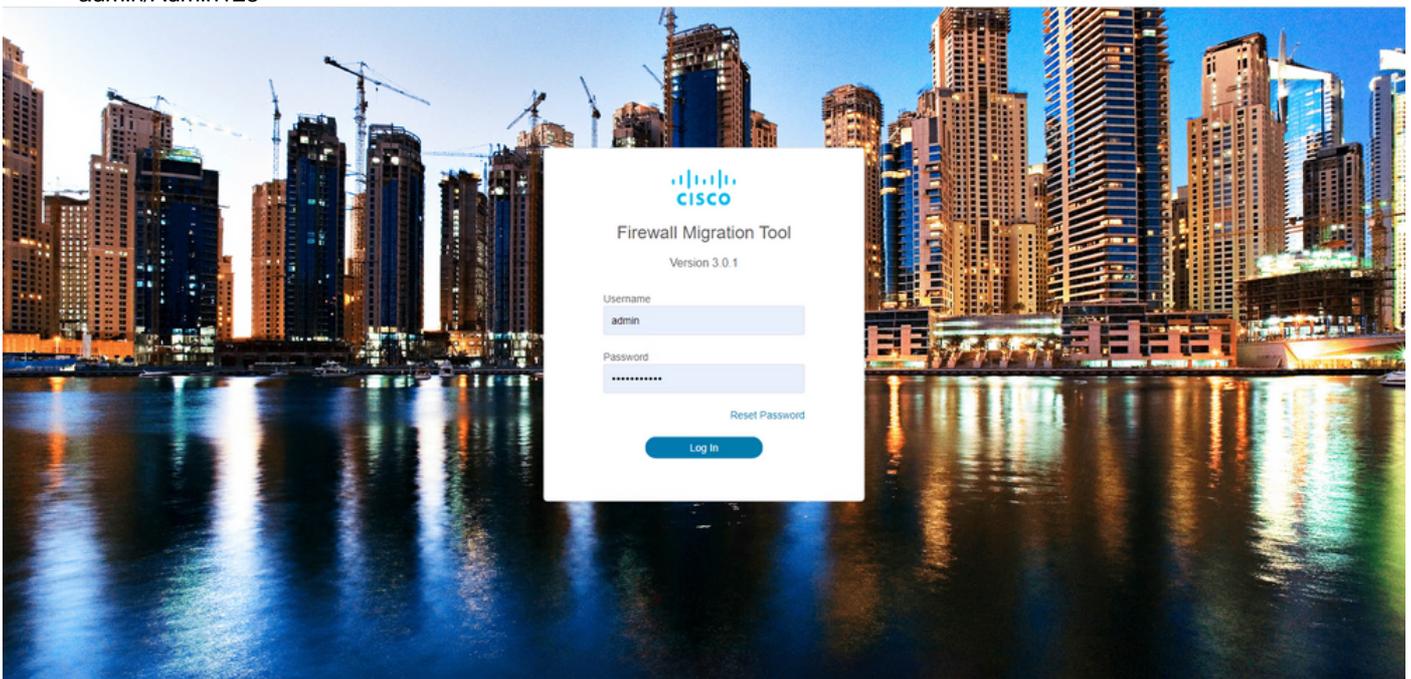


Extract Source Information

Any additional information explaining this



4. 移行ツールにログインします。CCOアカウントまたはローカルのデフォルトアカウントでログインできます。ローカルのデフォルトのアカウント資格情報は次のとおりです。
admin/Admin123



5. 移行するソースファイアウォールを選択します。この例では、Cisco ASA(8.4+)が送信元として使用されています。

Select Source Configuration

Source Firewall Vendor

[Select Source]

- Cisco ASA (8.4+)
- Cisco ASA (9.2.2+) with FPS
- Check Point (775-777)
- Check Point (880)
- Fortinet (5.0+)
- Palo Alto Networks (6.1+)

Cisco ASA (8.4+) Pre-Migration Instructions

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

Acronyms used:

FMT: Firewall Migration Tool

FMC: Firepower Management Center

FTD: Firepower Threat Defense

Before you begin your Adaptive Security Appliance (ASA) to Firepower 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.
- ASA Configuration Requirements:**
 Export configuration file from ASA to .cfg or .txt format. Connect to live ASA to extract the configuration file for one or more contexts. To migrate following features in ASA:
 1. **Time Based ACLs:** FMC and FTD must be on 6.6 or later versions.
 2. **IP SLA Monitor:** FMC must be on 6.6 or later and FTD must be on 6.2.3 or later.
 3. **Object Group Search:** FMC and FTD must be on 6.6 or later versions.
 4. **ASA5505 Support:** FMC and FTD must be on 6.6 or later versions.
 5. **Remote Deployment:** FMC and FTD must be on 6.7 or later versions. If remote deployment is enabled, Firewall Migration Tool will only migrate ACLs, Network Object and Port Objects. Interface and Route configuration have to be migrated manually on to FMC.
 6. **Site-to-Site VPN Tunnels:** Policy Based (Crypto Map) VPN needs FMC and FTD to be on 6.6 or later. Route Based (VTI) Support, FMC and FTD to be on 6.7 or later. Ensure FTD must be added to FMC before migration. Firewall Migration Tool will migrate VPN tunnels as Point-to-Point network.

6. 構成の取得に使用する抽出方法を選択します。手動アップロードでは、**Running Config** ASAのファイルを「.cfg」または「.txt」形式で保存します。ASAに接続して、ファイアウォールから設定を直接抽出します。

1 Extract ASA Information
 2 Select Target
 3 Map FTD Interface
 4 Map Security Zones & Interface Groups
 5 Optimize, Review & Validate
 6 Complete Migration

Extract Cisco ASA (8.4+) Information Source: Cisco ASA (8.4+)

Extraction Methods ▼

Manual Upload

- File format is '.cfg' or '.txt'.
- For Multi-context upload a show tech.
For Single-context upload show running.
- ⚠ Do not upload hand coded configurations.

Connect to ASA

- Enter the management IP address and connect using admin credentials.
- IP format should be: <IP:Port>

ASA IP Address/Hostname

Context Selection >

Parsed Summary >

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をクリックしてください。

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 >

Collect Hitcounts: No

8 Access Control List Lines	2 Access List Objects (Standard, Extended used in BGP/RAV/PNE/IGRP)	0 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)

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

8. 移行で使用するターゲットFMCを選択します。FMCのIPを指定します。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 >

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 >

9. (オプション)使用するターゲットFTDを選択します。FTDへの移行を選択した場合は、使用するFTDを選択します。FTDを使用しない場合は、このチェックボックスに入力できます
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

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 >

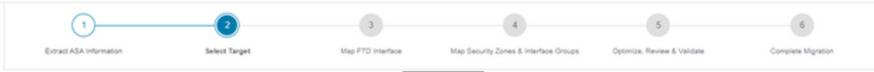
Device Configuration	Shared Configuration	Optimization
<input checked="" type="checkbox"/> Interfaces	<input checked="" type="checkbox"/> Access Control	<input checked="" type="checkbox"/> Migrate Only Referenced Objects
<input checked="" type="checkbox"/> Routes	<input checked="" type="checkbox"/> Populate destination security zones	<input checked="" type="checkbox"/> Object Group Search
<input checked="" type="checkbox"/> Static	<input type="checkbox"/> Route-lookup logic is limited to Static Routes and Connected Routes. PBR, Dynamic Routes & NAT are not considered.	Inline Grouping
<input type="checkbox"/> BGP	<input checked="" type="checkbox"/> Migrate tunnelled rules as Prefilter	<input checked="" type="checkbox"/> CSM/ASDM
<input type="checkbox"/> EIGRP	<input type="checkbox"/> NAT (no data)	
<input type="checkbox"/> Site-to-Site VPN Tunnels (no data)	<input checked="" type="checkbox"/> Network Objects (no data)	
<input type="checkbox"/> Policy Based (Crypto Map)	<input type="checkbox"/> Port Objects (no data)	
<input type="checkbox"/> Route Based (VTI)	<input type="checkbox"/> Access List Objects(Standard, Extended)	
	<input type="checkbox"/> Time based Objects (no data)	
	<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

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

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 (互換性に制限されます)。必要に応じて、Download Report 移行する構成の概要を受信します。

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

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 BGPRAVPNEIGRP)	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

次の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.

I. 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	aaalive_ciscoasa_2022-08-19_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
Hic 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

13. ASAインターフェイスを移行ツールのFTDインターフェイスにマッピングします。

Firewall Migration Tool

Map FTD Interface

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

Refresh

ASA Interface Name	FTD Interface Name
Management0/0	GigabitEthernet0/0

20 per page 1 to 1 of 1 |< 4 Page 1 of 1 >|

Back Next

14. FTDのインターフェイスに対して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

Add SZ & IG Auto-Create

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

次の図に示すように、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作成されます。



Map Security Zones and Interface Groups

Add SZ & IG Auto-Create

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_ig (A)

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

Back Next

15. 移行ツールで、移行する構成を確認および検証します。
設定の確認と最適化が完了している場合は、Validate.



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

16. 検証ステータスが正常に終了した場合は、構成をターゲット・デバイスにプッシュします

Validation Status

Successfully Validated

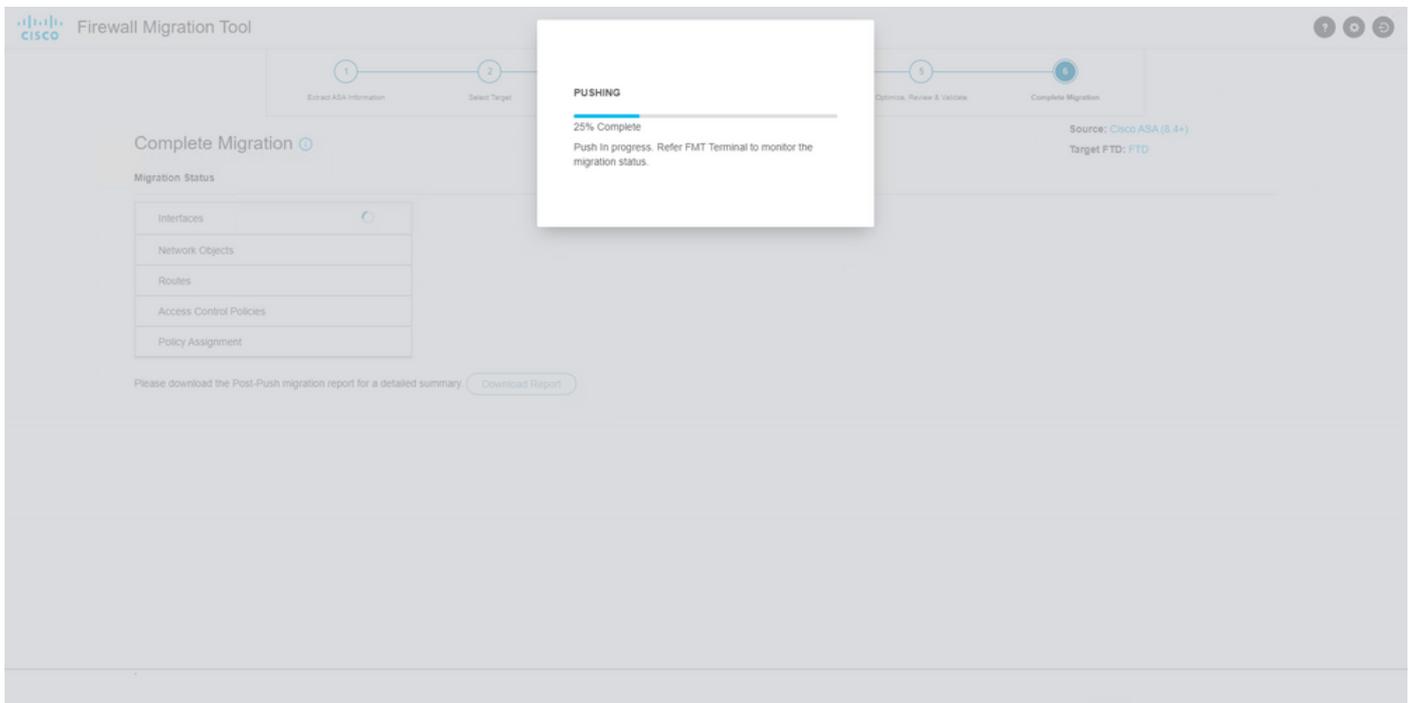
Validation Summary (Pre-push)

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

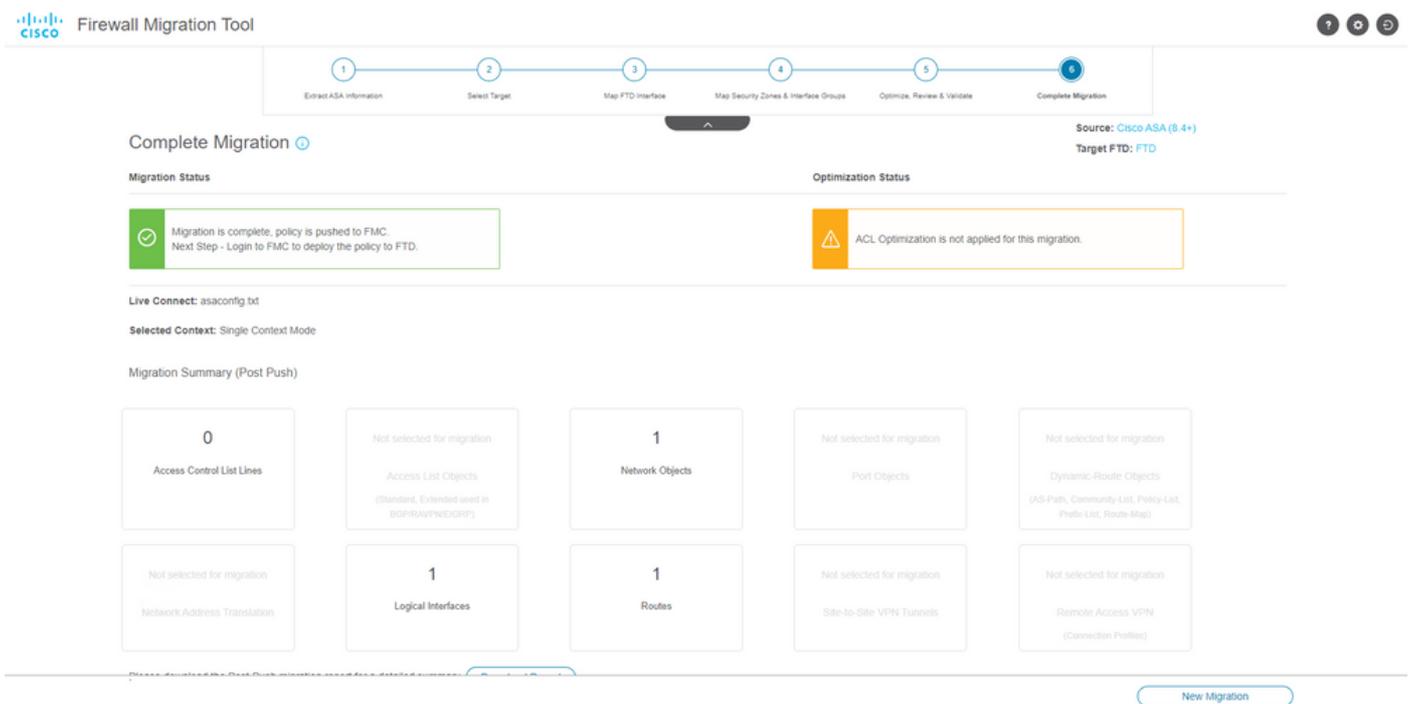
Note: The configuration on the target FTD device FTD (192.168.1.17) will be overwritten as part of this migration.

Push Configuration

図に示すように、移行ツールを通じてプッシュされた設定の例：



図に示すように、正常な移行の例：



17. (オプション)設定をFTDに移行することを選択した場合、設定を展開するには、展開が必要で、使用可能な設定をFMCからファイアウォールにプッシュします。FMC GUIにログインします。次に移動します。Deploy tab.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。クリック Deploy.

Firepower Management Center
Deploy / Deployment

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy admin

Search using device name, type, domain, group or status

Device	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
FTD		FTD		8/13/2022, 6:01:52 PM		Pending

Device Configurations

- Interface Policy
- Advanced Settings
- Routing Group
 - IPv4 Static Route Policy

How To

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

Firepower移行ツールファイルが配置されたディレクトリのログを確認します。次に例を示します。

Firepower_Migration_Tool_v3.0.1-7373.exe/logs/log_2022-08-18-21-24-46.log

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。