

Cisco NGFW 移行ラボ

最終更新日 : 2019 年 1 月 19 日

このラボについて

Cisco NGFW 移行ラボでは、ASA 設定ファイルを FMC に移行する方法を解説します。

要件

次の表に、このデモンストレーションの要件の概要を示します。

表 1. 要件

必須	オプション
● ラップトップ	● Cisco AnyConnect

最新情報

- これは新しいラボの手順です。ラボのインフラストラクチャは NGFW 攻撃ラボ 6.3 で使用されているものと同じです。

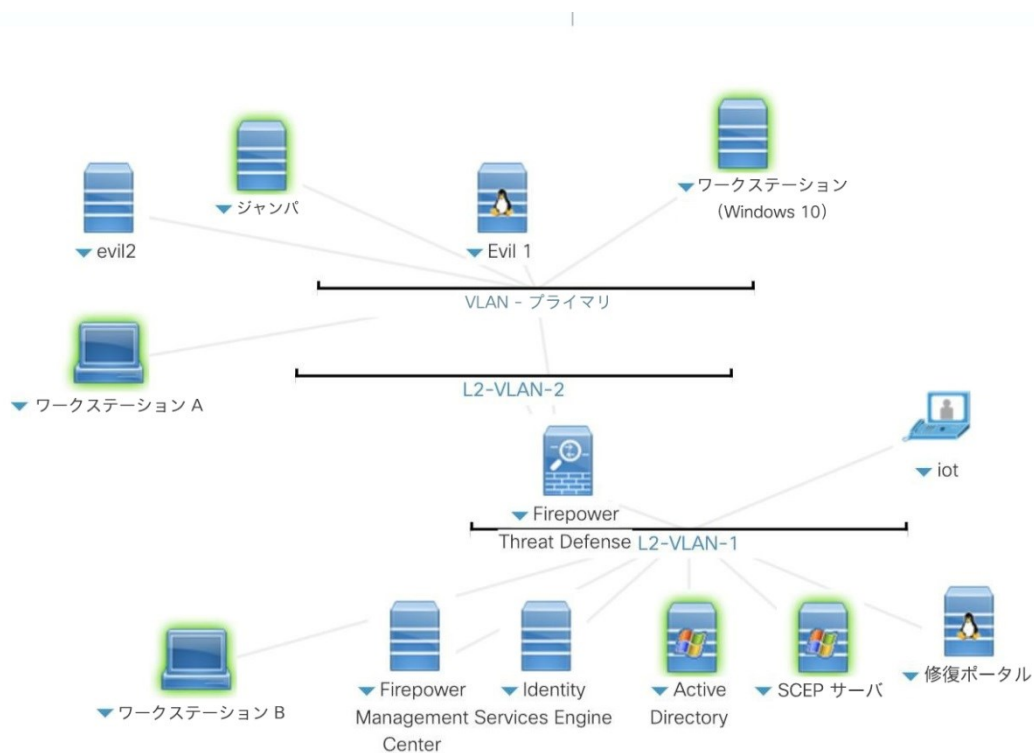
このソリューションについて

このラボは、Cisco NGFW 移行ツールの試用を希望する技術関連の意思決定者を対象にしています。

トポロジ

このコンテンツには、スクリプト形式のシナリオと、ソリューションの機能を実例で示すために事前設定された管理ユーザとコンポーネントが含まれています。コンポーネントのほとんどは、管理ユーザアカウントを使用して任意の設定が可能です。コンポーネントへのアクセスに使用する IP アドレスとユーザアカウント資格情報は、アクティブセッションの [トポロジ (Topology)] メニューのコンポーネント アイコンをクリックして確認するか、それらを必要とするシナリオ内の手順で確認できます。

図 1. dCloud のトポロジ



このラボのシステム

次の情報は、このラボの事前設定済みユーザに適用されます。

- ワークステーション - Windows 10。これは移行ツールを実行するワークステーションです。
- FMC - Firepower Management Center。これは移行された設定が作成されるシステムです。

表 2. 事前設定済みのユーザ情報

デバイス	ユーザ ID	パスワード
移行ワークステーション 198.18.133.36	admin	C1sco12345
fmc 198.18.133.10	admin	C1sco12345

はじめに

プレゼンテーションの前に

Cisco dCloud では、実際の対象者の前でプレゼンテーションを行う前に、アクティブなセッションを使用して、このドキュメントのタスクを実施しておくことを強く推奨します。そうすることで、ドキュメントとコンテンツの構成に慣れることができます。

場合によっては、環境を元の構成にリセットするため、このガイドに従った後に新しいセッションをスケジュールする必要があります。

プレゼンテーションを成功させるには入念な準備が不可欠です。

次の手順に従ってコンテンツのセッションをスケジュールし、プレゼンテーション環境を設定します。

1. dCloud セッションを開始します。[\[手順を見る\]](#)

注：セッションがアクティブになるまで最長で 10 分かかることがあります。

2. 最適なパフォーマンスを得るために、**Cisco AnyConnect VPN** [\[手順を見る\]](#) およびラップトップのローカル RDPクライアント [\[手順を見る\]](#) を使用してラボに接続します。

移行ワークステーション：198.18.133.36、ユーザ名：admin、パスワード：C1sco12345

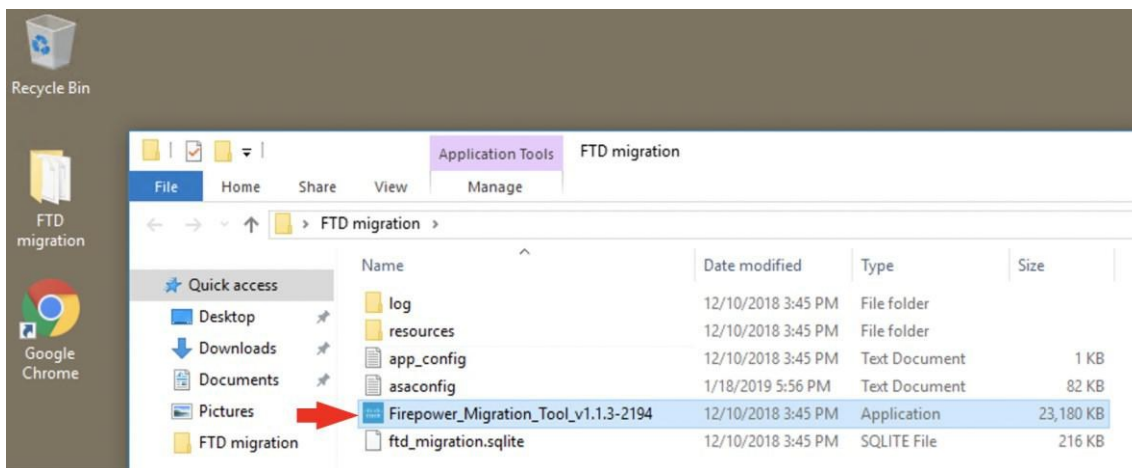
注：Cisco dCloud リモート デスクトップ クライアントを使用してワークステーションに接続することもできます [\[手順を見る\]](#)。dCloud リモート デスクトップ クライアントは、最小限の操作でアクティブ セッションにアクセスする場合に最適です。ただし、この方法では、接続ができない場合や、パフォーマンスが悪い場合があります。

シナリオ 1： 移行

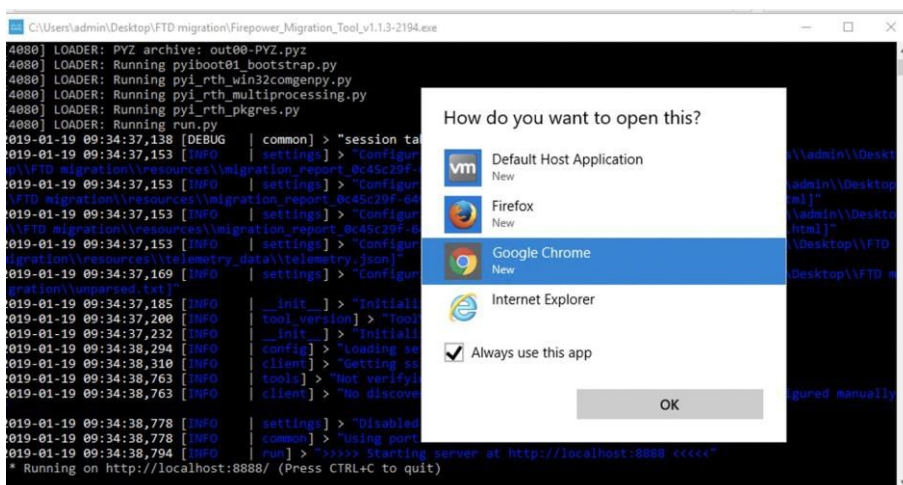
このシナリオでは、既存の ASA 設定を移行します。移行ツールは、移行されたオブジェクトとポリシーを FMC に自動的に作成します。

手順

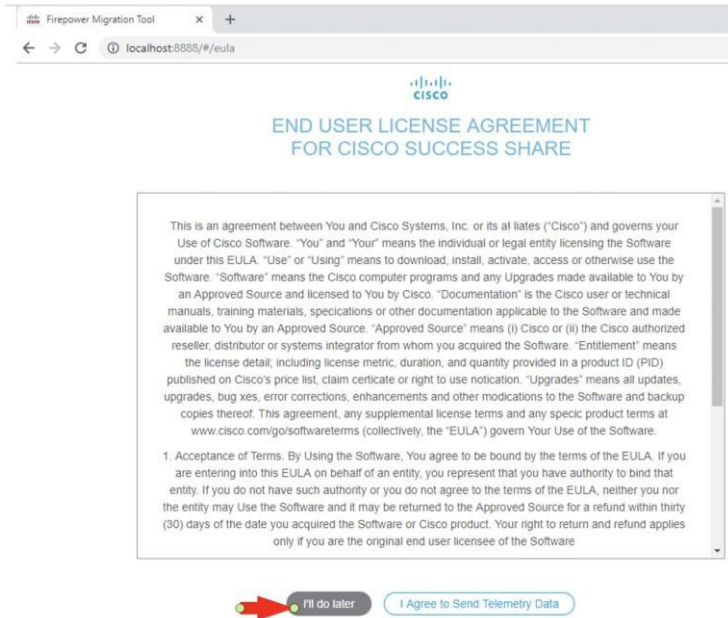
1. 移行ワークステーションで、FTD migration という名前のフォルダを開き、Firepower 移行ツールを実行します。



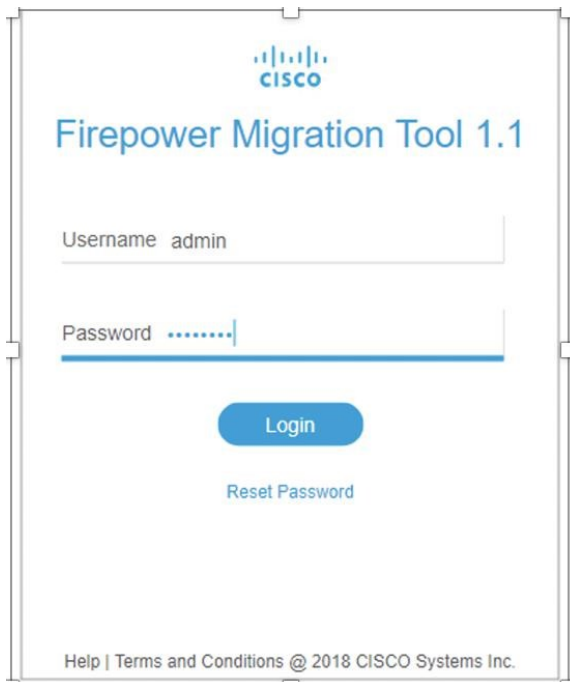
2. 移行ツールが起動します。数秒後に、アプリケーションを開く方法を選択するように求められます。Chrome を選択します（移行ツールは、ローカルホスト、ポート 8888 で実行されているローカル Web アプリケーションです）。



3. テレメトリ データを送信するよう要求されます。[後で行う (I'll do later)] を選択します。

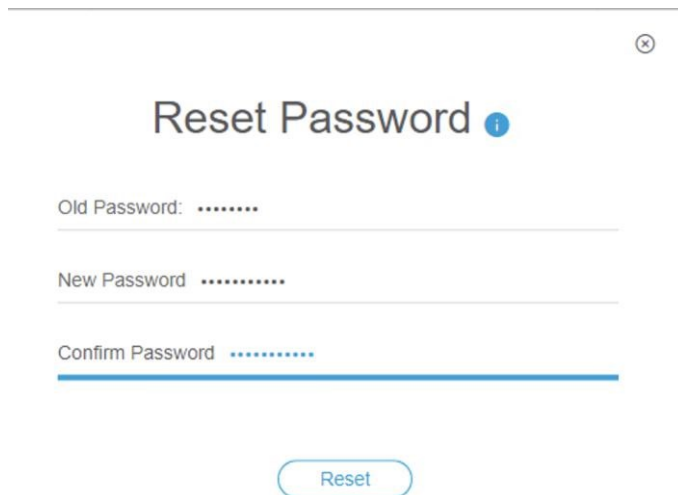


4. 次に、ログインするよう求められます。デフォルトのクレデンシャルは admin/Admin123 です。



5. 次に、パスワードの変更が要求されます。古いパスワード (Admin123) と新しいパスワード (C1sco12345! など) を入力します。

パスワードの複雑さの要件を満たすために、感嘆符のような特殊文字を含める必要があります。新しいパスワードは後で必要になりますので、忘れないようにしてください。



✕

Reset Password i

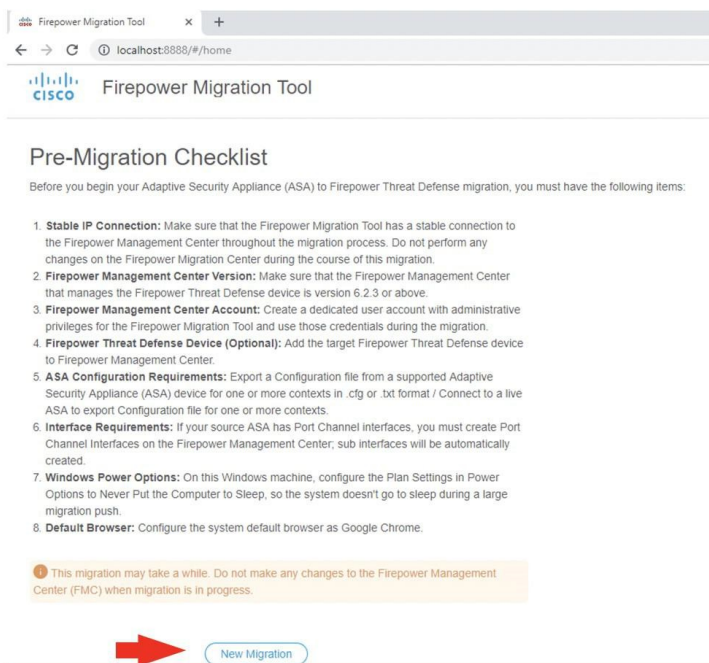
Old Password:

New Password

Confirm Password

[Reset](#)

6. 新しいクレデンシャルを使用してログオンすると、[移行前チェックリスト (Pre-migration Checklist)] が表示されます。チェックリストを読み、[新しい移行 (New Migration)] をクリックします。



Firepower Migration Tool

localhost:8888/#/home

Pre-Migration Checklist

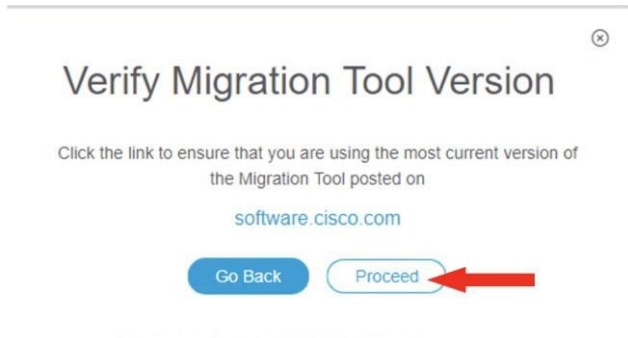
Before you begin your Adaptive Security Appliance (ASA) to Firepower Threat Defense migration, you must have the following items:

- Stable IP Connection:** Make sure that the Firepower Migration Tool has a stable connection to the Firepower Management Center throughout the migration process. Do not perform any changes on the Firepower Migration Center during the course of this migration.
- Firepower Management Center Version:** Make sure that the Firepower Management Center that manages the Firepower Threat Defense device is version 6.2.3 or above.
- Firepower Management Center Account:** Create a dedicated user account with administrative privileges for the Firepower Migration Tool and use those credentials during the migration.
- Firepower Threat Defense Device (Optional):** Add the target Firepower Threat Defense device to Firepower Management Center.
- ASA Configuration Requirements:** Export a Configuration file from a supported Adaptive Security Appliance (ASA) device for one or more contexts in .cfg or .txt format / Connect to a live ASA to export Configuration file for one or more contexts.
- Interface Requirements:** If your source ASA has Port Channel interfaces, you must create Port Channel Interfaces on the Firepower Management Center; sub interfaces will be automatically created.
- Windows Power Options:** On this Windows machine, configure the Plan Settings in Power Options to Never Put the Computer to Sleep, so the system doesn't go to sleep during a large migration push.
- Default Browser:** Configure the system default browser as Google Chrome.

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

[New Migration](#)

7. 次に、アップグレードするよう要求されます。実稼働環境では、常に最新バージョンで実行していることを確認する必要があります。このラボ環境では、このまま操作を続行します。



8. これで移行を開始できます。ASA 設定テキスト ファイルをアップロードするか、ライブの ASA に接続して設定を取得するかを選択できます。ここでは、Desktop\FTD Migration\asaconfig.txt にある ASA 設定をアップロードすることを選択します。

Firepower Migration Tool

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

Extract ASA Information ⓘ

Extraction Methods

Manual Upload

- Single/ Multi-context config file must be from the ASA and not hand coded. Please ensure that the file is in .cfg or .txt format.

Connect to ASA

Single-context : Enter the management IP address and connect using admin credentials.

9. ツールによって設定が解析され、結果が表示されます。移行レポートをダウンロードするかどうかを選択できます。移行レポートには、移行に関する詳細が表示されます（これを実行してください）。移行レポートに目を通したら、[次へ (Next)] をクリックします。

Firepower Migration Tool

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

Extract ASA Information

Extraction Methods

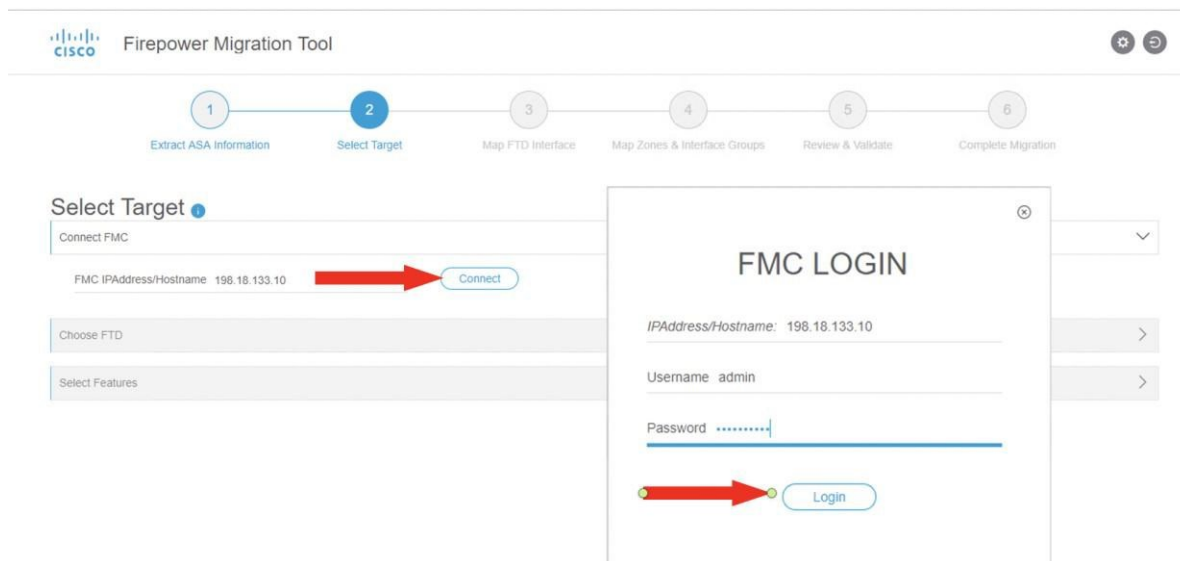
0 parsing errors found. Refer to the pre-migration report for more details

74	169	106
Access Control List Lines	Network Objects	Port Objects
8	12	7
Logical Interfaces	Static Routes	Network Address Translation

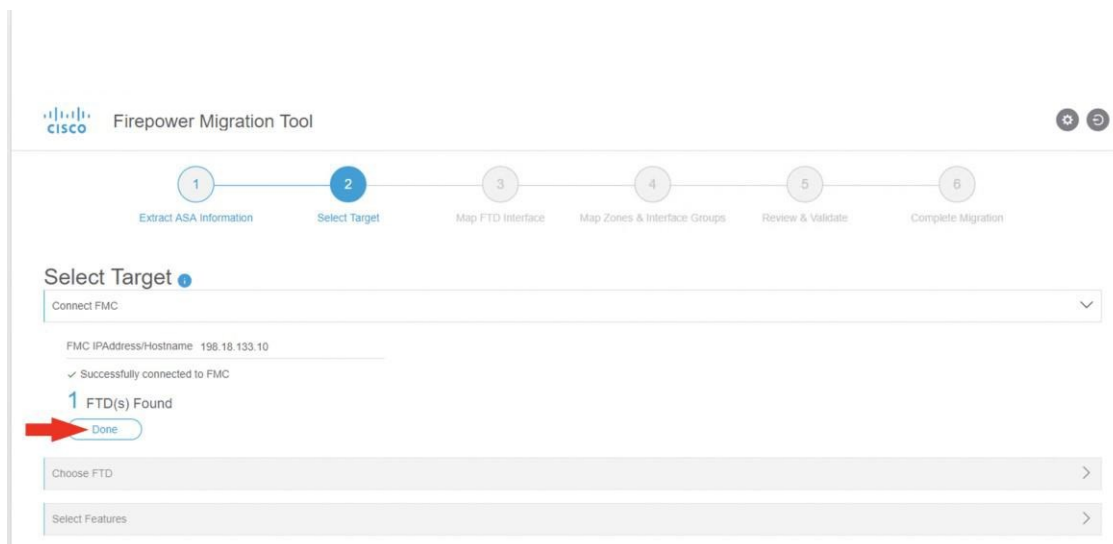
Please download the Pre-Migration report for a detailed summary of the parsed configuration. [Download Report](#)

[Next](#)

10. 次に、移行先を指定する必要があります。これはシスコの FMC (198.18.133.10) です。[接続 (Connect)] をクリックしてから、FMC にログインするためのクレデンシャル (admin/C1sco123435) を指定します。



11. 数秒後に、FMC に正常に接続されたことが示され、1 つの FTD デバイスが検出されています。[完了 (Done)] をクリックして次の画面に進みます。



12. この設定を既存の FTD に移行するか、FTD を使用せずに続行するかを選択できます。この場合、ポリシーとオブジェクトは FMC グローバル設定に追加されますが、特定のデバイスのインターフェイス コンフィギュレーションなどは変更されません。ここでは、**FTD を使用せずに続行**することを選択し、[完了 (Done)]をクリックします。

Firepower Migration Tool

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

Select Target 1

Connect FMC >

Selected FMC IPAddress/Hostname: 198.18.133.10

Choose FTD ▾

Select FTD Device ▾

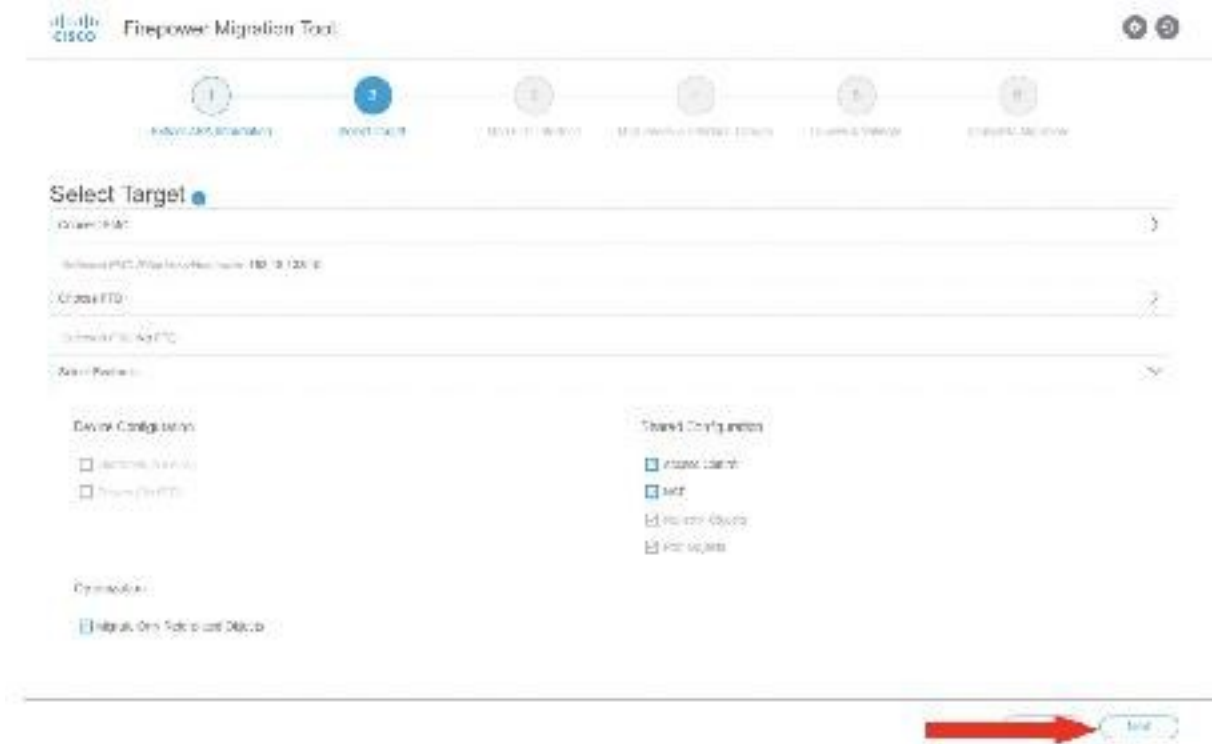
Proceed without FTD ←

Interface and Routes wont be migrated

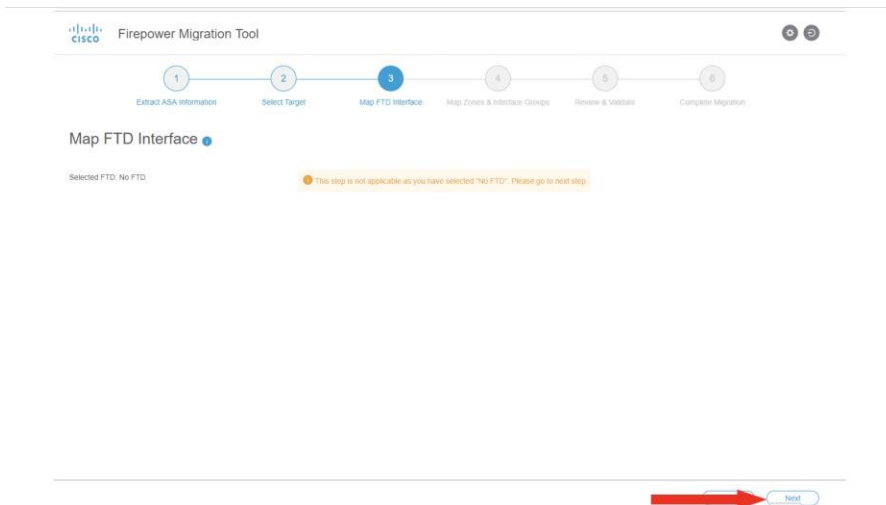
Done ←

Select Features >

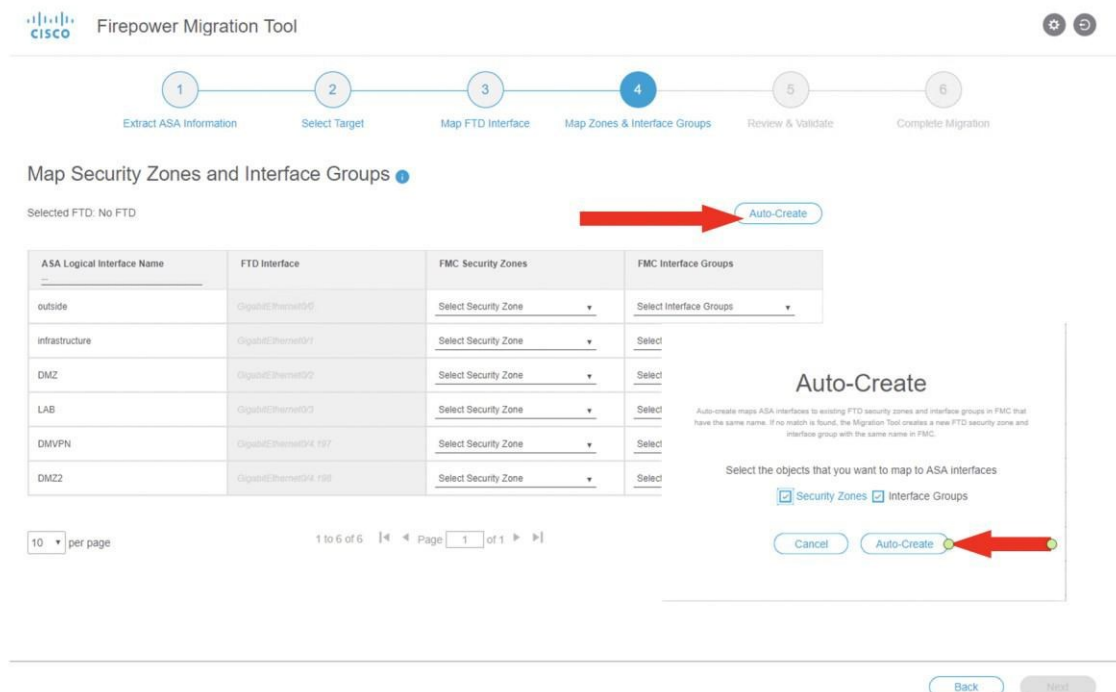
13. 移行するオブジェクトを選択できるようになります。デフォルトを選択します。デフォルトでは、アクセス ポリシー、NAT、およびネットワーク オブジェクトとポート オブジェクトを移行します。



14. 次の手順では、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。今回は実際の FTD デバイス設定ではなく FMC グローバル設定に移行しているに過ぎないため、次の手順は必須ではありません。[次へ (Next)] をクリックします。



15. 次に、ASA 設定のインターフェイスを FMC ゾーンとインターフェイス グループにマッピングするよう求められます。これはインターフェイス単位で手動で実行できます。または、ツールを使用して、FMC に新しいゾーンとインターフェイス グループを自動的に作成することもできます。[自動作成 (Auto-Create)] をクリックして、新しい FMC ゾーンとインターフェイス グループを作成します。



16. ツールで新しいゾーンとインターフェイスグループが自動的に作成されたら、[次へ (Next)] をクリックします。

Firepower Migration Tool

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

Map Security Zones and Interface Groups

Selected FTD: No FTD

ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
outside	outside	outside (A)	outside_g (A)
infrastructure	infrastructure	infrastructure (A)	infrastructure_g (A)
DMZ	DMZ	DMZ (A)	DMZ_g (A)
LAB	LAB	LAB (A)	LAB_g (A)
DMVPN	DMVPN	DMVPN (A)	DMVPN_g (A)
DMZ2	DMZ2	DMZ2 (A)	DMZ2_g (A)

10 items per page 1 of 6 Page 1 of 1

Back Next

17. もうすぐ完了です。FMCに変更をプッシュする前に設定を検証できるようになりました。アクセス制御、NAT、およびネットワークオブジェクトのポリシーを調べることができます。続行する前に、[検証 (Validate)] をクリックして実行します。

Firepower Migration Tool

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

Review and Validate Configuration

Selected FTD: No FTD

Access Control NAT Network Objects Port Objects

Actions Save

	#	Name	Zone	Network	Port	Zone	Network	Port	State	Action
<input type="checkbox"/>	1	DMZ_access_in_#1	DMZ	any	ANY	ANY	any	ANY	✓	Allow
<input type="checkbox"/>	2	DMZ_access_in_#2	DMZ	vcs-express	ANY	ANY	ntp-external-servers	udp:123	✓	Allow
<input type="checkbox"/>	3	DMZ_access_in_#3	DMZ	vcs-express	ANY	ANY	external-dns-servers	udp:53	✓	Allow
<input type="checkbox"/>	4	DMZ_access_in_#4	DMZ	vcs-express	ANY	ANY	vcs-control	VC-service	✓	Allow
<input type="checkbox"/>	5	DMZ_access_in_#5	DMZ	any	ANY	ANY	DM_INLINE_NETWORK_2	ANY	✓	Block
<input type="checkbox"/>	6	DMZ_access_in_#6	DMZ	vcs-express	ANY	ANY	any	ANY	✓	Allow
<input type="checkbox"/>	7	DMZ_access_in_#7	DMZ	any	ANY	ANY	any	ANY	✓	Block
<input type="checkbox"/>	8	LAB1_access_in_#1	LAB	expwy-c	ANY	ANY	any	ANY	✓	Allow
<input type="checkbox"/>	9	LAB1_access_in_#2	LAB	OpenDNS-VAs	ANY	ANY	any	ANY	✓	Allow

Validate

18. ここでは、競合が検出されています。ASA 設定で検出されたネットワーク オブジェクト「clients」は、FMC にもあります（ただし異なる IP サブネット値を使用）。このツールは、設定可能なサフィックスを ASA オブジェクトに追加してからインポートすることで、この競合を解決します。[競合の解決 (Resolve Conflict)] をクリックします。

Validation Status

⚠ Conflicts Detected

The following object conflicts need to be resolved

1

Network Object Conflicts

[Resolve Conflicts](#)

19. [競合の解決 (Resolve Conflict)] をもう一度クリックすると、インポートされたオブジェクト名に追加されるサフィックスを編集して変更できます。[解決 (Resolve)] をクリックします。

Firepower Migration Tool
⚙ ⏪

1 Extract ASA Information
2 Select Target
3 Map FTD Interface
4 Map Zones & Interface Groups
5
6 Complete Migration

Review and Validate Configuration

Selected FTD: No FTD

Access Control ✓ NAT ✓ **Network Objects** ⚠ Port Objects ✓ Interfaces ✓ Routes ✓

Selected: 1 Object(s) Actions Search

#	Name	Action State	Type	Value
1	clients	Conflict	Network Object	192.168.0.0/16

10 per page 1 to 1 of 1 | Page 1

Resolve Conflicts

Suffix: FTD_MIG

Enter a suffix to resolve the issue.

Resolve

Validate

20. 設定を再度検証した後、エラーは発生しません。[プッシュ設定 (Push Configuration)] をクリックして、FMC にプッシュできます。

The screenshot shows the 'Review and Validate Configuration' step in the Firepower Migration Tool. A 'Validation Status' dialog box is open, indicating that the configuration has been 'Successfully Validated'. The dialog provides a 'Validation Summary (Pre-push)' with the following counts:

Category	Count
Access Control List Lines	74
Network Objects	94
Port Objects	57
Logical Interfaces	Not selected for migration
Static Routers	Not selected for migration
Network Address Translation	7

A red arrow points to the 'Push Configuration' button in the dialog. Below the dialog, another red arrow points to the 'Validate' button in the main interface.

21. 設定のプッシュには数分かかる場合があります。

The screenshot shows the 'Migration Status' step in the Firepower Migration Tool. A progress bar indicates 'Push in progress for Network Objects'. The migration progress is shown for the following categories:

- Network Objects
- Port Objects
- Network Address Translation
- Access Control Policies

Please download the Post-Push migration report for a detailed summary. [Download Report](#)

22. しばらくすると、成功したことが示されます。オプションでレポートをダウンロードできます。



Post-Migration Report 19 January 2019 11:25 AM

Note: Review all contents of this post-migration report carefully. Confirm that the configurations, rules, interfaces, and other mappings were migrated as expected. Review any rules that were disabled by the Migration Tool and were not migrated. Make a note of any unsupported or partially supported rules or other configuration items that were not migrated. Since the unsupported rules were not migrated completely and are in disabled state, these 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.

1. Migration Summary:

A summary of the configuration that was successfully migrated from ASA to Firepower Threat Defense, including information about the source ASA device, target Firepower Threat Defense device, and the successfully migrated configuration elements.

ASA Device Hostname	loke
ASA Device Model	ASA5525, 8192 MB RAM, CPU Lynnfield 2400 MHz, 1 CPU (4 cores)
FMC Hostname	198.18.133.10
FMC Domain Selected	Global
Firepower Threat Defense Model	None
Firepower Device Name	None
Access Control Policy - Name	FTD-Mig-1547897119
Access Control Policy - Number of Rules Migrated	74
Network Address Translation Policy - Name	FTD-Mig-1547897094
Network Address Translation Policy - Number of Rules Migrated	7
Logical Interfaces Migrated	0
Network objects migrated	94
Port objects migrated	57

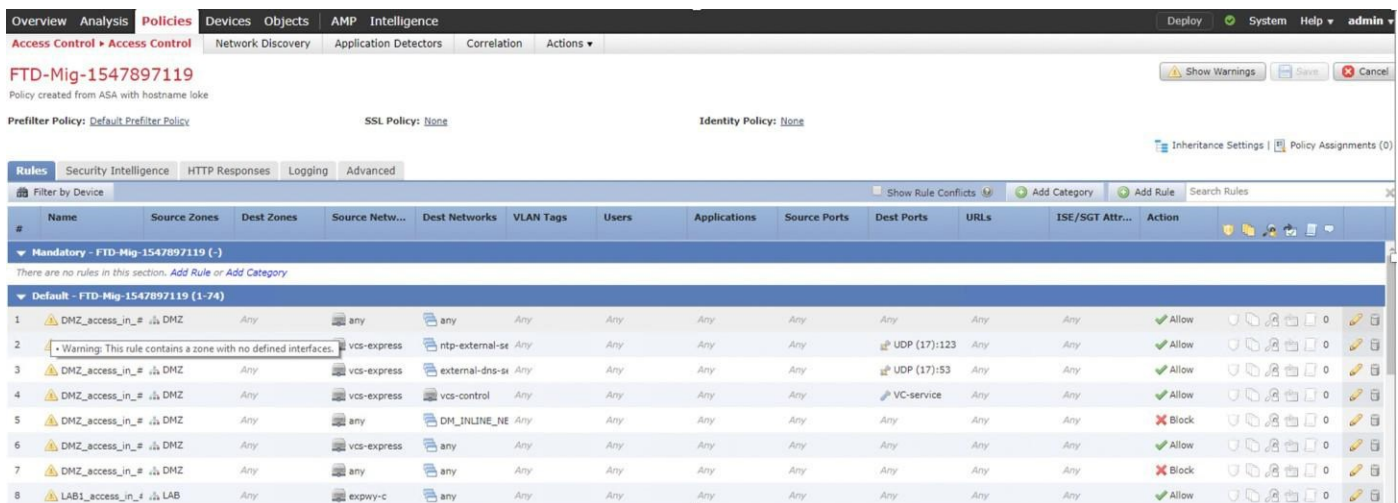
23. Chrome を使用して FMC (<https://198.18.133.10>) にユーザ名 admin とパスワード C1sco12345 でログインします。証明書に関する警告を受け入れる必要があります。

24. FMC GUI で、[ポリシー (Policy)] -> [アクセス制御 (Access Control)] の順に選択します。このツールで作成した新しいアクセス ポリシーが表示されます。ポリシー名は FTD_Mig で始まります。鉛筆アイコンをクリックして、アクセス ポリシーを編集します。



25. アクセス ポリシーを調べます。74 個のルールが ASA 設定から取得され、移行ツールによって作成されました。これらのポリシーは、まだデバイスに割り当てられていないことに注意してください ([ポリシーの割り当て (Policy Assignment)] は 0)。ゾーンにマッピングされるインターフェイスを持つ FTD デバイスがまだないため、警告が発生していることにも注意してください。また、どのルールにも IPS またはファイル ポリシーが付加されていないことにも注意が必要です。これは、移行された設定がレイヤ 3/レイヤ 4 ステートフル インспекション ファイアウォール (ASA) からのものであるためです。ルールを編集して、NGFW の機能と保護を適用します。

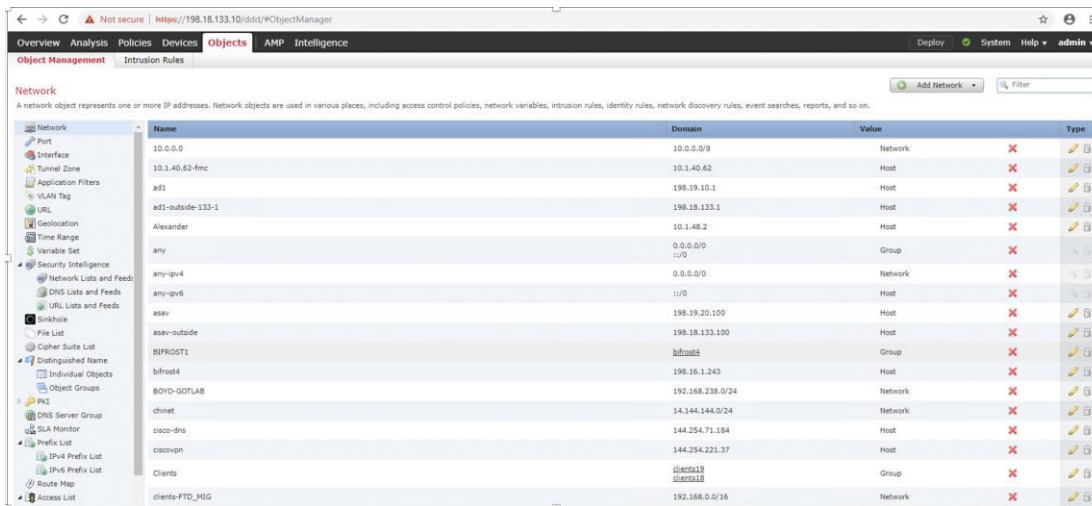
この場合も、Cisco NGFW 移行ツールでは、アクセス ポリシー内のすべてのルールと必要なネットワーク オブジェクトを自動的に作成して多くの作業を省くことができます。



26. [デバイス (Devices)] -> [NAT] の順に選択します。ツールで、新しい NAT ポリシーが作成されています (デバイスにはまだ割り当てられていません)。鉛筆アイコンを自由にクリックして、ルールを確認できます。



27. [オブジェクト (Objects)] -> [ネットワークネットワーク (Network Objects)] の順に選択します。ASA 設定から FMC 設定に追加されたいくつかの新しいオブジェクトが表示されます。



まとめ

これで、Cisco NGFW 移行ラボは終了です。まとめると次のとおりです。

- Cisco NGFW 移行ツールを使用すると、ASA 設定から FMC にネットワーク オブジェクト、ACL、および NAT を簡単に移行できます。
- このツールで、コンテンツが異なる同じオブジェクト名などの競合を検出し、競合を解決できます。
- このツールによって多くの作業が自動で実行され、何千ものネットワーク オブジェクト、アクセス ポリシー ルール、NAT ルールを手動で定義する手間を省くことができます。