

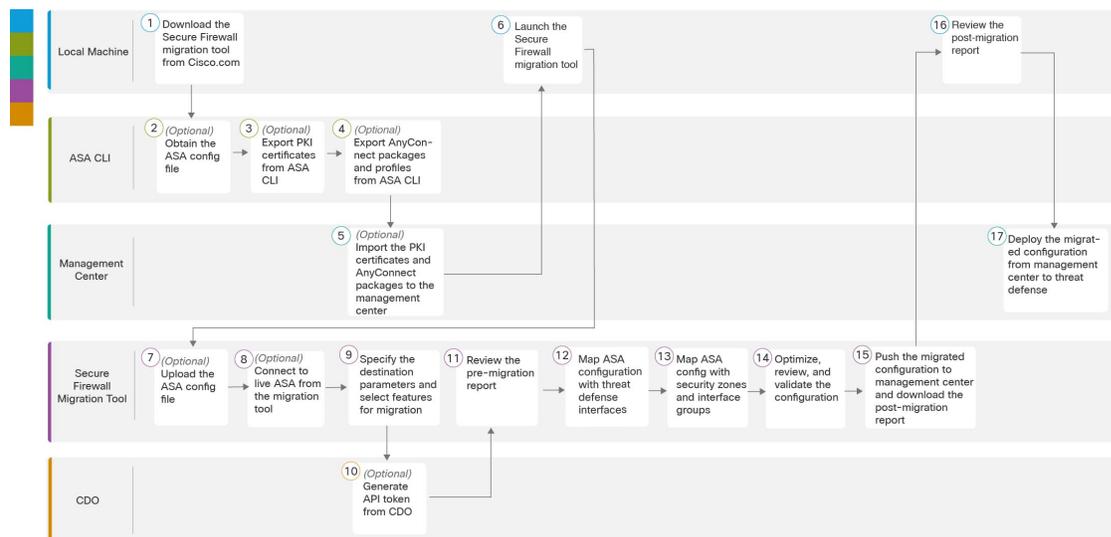


ASA から Threat Defense への移行ワークフロー

- エンドツーエンドの手順 (1 ページ)
- 移行の前提条件 (4 ページ)
- 移行の実行 (7 ページ)
- Cisco Secure Firewall 移行ツールのアンインストール (47 ページ)
- 移行例 : ASA から Threat Defense 2100 へ (48 ページ)

エンドツーエンドの手順

次のフローチャートは、Cisco Secure Firewall 移行ツールを使用して、ASA を Threat Defense に移行するワークフローを示しています。



	ワークスペース	手順
①	Local Machine	Cisco.com から Cisco Secure Firewall 移行ツールをダウンロードします。詳細な手順については、「 Cisco.com からの Cisco Secure Firewall 移行ツールのダウンロード 」を参照してください。
②	ASA CLI	(オプション) ASA 構成ファイルを取得します。ASA CLI から ASA 構成ファイルを取得するには、「 ASA 構成ファイルの取得 」を参照してください。Cisco Secure Firewall 移行ツールから ASA に接続する場合は、ステップ 3 にスキップします。
③	ASA CLI	(オプション) ASA CLI から PKI 証明書をエクスポートします。この手順は、サイト間 VPN、RA VPN、または WebVPN の設定を ASA から Threat Defense に移行する予定がある場合にのみ必要です。ASA CLI から PKI 証明書をエクスポートするには、「 ASA からの PKI 証明書のエクスポートと管理センターへのインポート 」を参照してください。サイト間 VPN、RA VPN、または WebVPN の設定を移行する予定がない場合は、ステップ 7 にスキップします。
④	ASA CLI	(オプション) ASA CLI から AnyConnect パッケージおよびプロファイルのエクスポートします。この手順は、RA VPN 機能を ASA から Threat Defense に移行することを計画している場合にのみ必要です。AnyConnect パッケージとプロファイル ASA CLI からエクスポートするには、「 AnyConnect パッケージとプロファイルの取得 」を参照してください。サイト間 VPN および RA VPN を移行する予定がない場合は、手順 7 にスキップします。
⑤	Management Center	(オプション) PKI 証明書と AnyConnect パッケージを管理センターにインポートする：PKI 証明書を管理センターにインポートするには、「 ASA からの PKI 証明書のエクスポートと管理センターへのインポート 」および「 AnyConnect パッケージとプロファイルの取得 」を参照してください。
⑥	Local Machine	ローカルマシンで Cisco Secure Firewall 移行ツールを起動します。「 Cisco Secure Firewall 移行ツールの起動 」を参照してください。
⑦	Cisco Secure Firewall 移行ツール	(オプション) ASA CLI から取得した ASA 構成ファイルをアップロードします。「 ASA 構成ファイルのアップロード 」を参照してください。ライブ ASA に接続することを計画している場合は、ステップ 8 にスキップします。
⑧	Cisco Secure Firewall 移行ツール	Cisco Secure Firewall 移行ツールから直接、ライブ ASA に接続できます。詳細については、「 Cisco Secure Firewall 移行ツールから ASA への接続 」を参照してください。

	ワークスペース	手順
9	Cisco Secure Firewall 移行ツール	このステップでは、移行の接続先パラメータを指定できます。詳細な手順については、「 Cisco Secure Firewall 移行ツールの接続先パラメータの指定 」を参照してください。
10	CDO	(オプション) この手順はオプションであり、クラウドで提供される Firewall Management Center を移行先管理センターとして選択した場合にのみ必要です。詳細な手順については、「 Cisco Secure Firewall 移行ツールの接続先パラメータの指定 」を参照してください。
11	Cisco Secure Firewall 移行ツール	移行前レポートをダウンロードした場所に移動し、レポートを確認します。詳細な手順については、「 移行前レポートの確認 」を参照してください。
12	Cisco Secure Firewall 移行ツール	Cisco Secure Firewall 移行ツールを使用すると、ASA 構成を Threat Defense インターフェイスにマッピングできます。詳細な手順については、「 ASA 構成と Threat Defense インターフェイスのマッピング 」を参照してください。
13	Cisco Secure Firewall 移行ツール	ASA 構成が正しく移行されるように、ASA インターフェイスを適切な Threat Defense インターフェイスオブジェクト、セキュリティゾーン、およびインターフェイスグループにマッピングします。詳細な手順については、「 セキュリティゾーン、インターフェイスグループ、および VRF への ASA インターフェイスのマッピング 」を参照してください。
14	Cisco Secure Firewall 移行ツール	構成を慎重に確認し、それが適切で Threat Defense デバイスの構成内容と一致することを確認します。詳細な手順については、「 最適化、構成の確認と検証 」を参照してください。
15	Cisco Secure Firewall 移行ツール	移行プロセスのこのステップでは、移行された構成を管理センターに送信し、移行後レポートをダウンロードできるようにします。詳細な手順については、「 移行された構成の以下へのプッシュ：Management Center 」を参照してください。
16	Local Machine	移行後レポートをダウンロードした場所に移動し、レポートを確認します。詳細な手順については、「 移行された構成の以下へのプッシュ：Management Center 」を参照してください。
17	Management Center	移行した構成を管理センターから Threat Defense に展開します。詳細な手順については、「 移行後レポートの確認と移行の完了 」を参照してください。

移行の前提条件

ASA 構成を移行する前に、次のアクティビティを実行します。

Cisco.com からの Cisco Secure Firewall 移行ツールのダウンロード

始める前に

Cisco.com へのインターネット接続が可能な Windows 10 64 ビットまたは macOS バージョン 10.13 以降のマシンが必要です。

手順

ステップ 1 コンピュータで、Cisco Secure Firewall 移行ツール用のフォルダを作成します。

このフォルダには、他のファイルを保存しないことをお勧めします。Cisco Secure Firewall 移行ツールを起動すると、ログ、リソース、およびその他すべてのファイルがこのフォルダに配置されます。

(注) Cisco Secure Firewall 移行ツールの最新バージョンをダウンロードする場合は、必ず新しいフォルダを作成し、既存のフォルダは使用しないでください。

ステップ 2 <https://software.cisco.com/download/home/286306503/type> を参照し、[Firewall移行ツール (Firewall Migration Tool)] をクリックします。

上記のリンクをクリックすると、[Firewall NGFWバーチャル (Firewall NGFW Virtual)] の [Cisco Secure Firewall移行ツール (Firewall Migration Tool)] に移動します。脅威に対する防御 デバイスのダウンロード領域から Cisco Secure Firewall 移行ツールをダウンロードすることもできます。

ステップ 3 Cisco Secure Firewall 移行ツールの最新バージョンを、作成したフォルダにダウンロードします。

Windows 用または macOS マシン用の適切な Cisco Secure Firewall 移行ツール実行可能ファイルをダウンロードします。

次のタスク

[ASA構成ファイルの取得](#)

ASA構成ファイルの取得

ASA 構成ファイルを取得するには、次のいずれかの方法を使用できます。

- [ASA 構成ファイルのエクスポート \(5 ページ\)](#)
- [Cisco Secure Firewall 移行ツールから ASA への接続 \(11 ページ\)](#)

ASA 構成ファイルのエクスポート

このタスクは、ASA 構成ファイルを手動でアップロードする場合にのみ必要です。Cisco Secure Firewall 移行ツールから ASA に接続する場合は、[Cisco Secure Firewall 移行ツールから ASA への接続 \(11 ページ\)](#) に進みます。



(注) ファイルをエクスポートした後、ASA 構成を手動でコーディングしたり、変更を加えたりしないでください。これらの変更は Threat Defense に移行されず、移行でエラーが発生するか、移行が失敗します。たとえば、端末で構成ファイルを開いて保存すると、Cisco Secure Firewall 移行ツールで解析できない空白または空白行が追加されることがあります。

エクスポートされた ASA 構成ファイルに "--More--" キーワードがテキストとして含まれていないことを確認します。含まれていると、移行が失敗する可能性があります。

手順

- ステップ 1** 移行する ASA デバイスまたはコンテキストに対して **show running-config** コマンドを使用し、そこから構成をコピーします。「[View the Running Configuration](#)」を参照してください。
または、移行する ASA デバイスまたはコンテキストに対して Adaptive Security Device Manager (ASDM) を使用し、[ファイル (File)] > [新しいウィンドウに実行コンフィギュレーションを表示 (Show Running Configuration in New Window)] を選択して、構成ファイルを取得します。
(注) マルチコンテキスト ASA の場合は、**show tech-support** コマンドを使用して、単一ファイル内のすべてのコンテキストの構成を取得できます。
- ステップ 2** 構成を .cfg または .txt として保存します。
異なる拡張子の ASA 構成を Cisco Secure Firewall 移行ツールにアップロードすることはできません。
- ステップ 3** Cisco Secure Firewall 移行ツールをダウンロードしたコンピュータに ASA 構成ファイルを転送します。

ASA からの PKI 証明書のエクスポートと管理センターへのインポート

始める前に

Cisco Secure Firewall 移行ツールは、証明書ベースの VPN の管理センターへの移行をサポートしています。

ASA では、トラストポイントモデルを使用して、証明書を構成に保存します。トラストポイントは、証明書が保存されるコンテナです。ASA トラストポイントは最大2つの証明書を保存できます。

ASA 構成ファイルの ASA トラストポイントまたは証明書にはハッシュ値が含まれています。したがって、それらを管理センターに直接インポートすることはできません。

インポート先の管理センターで、移行前アクティビティの一環として、ASA トラストポイントまたは VPN 証明書を PKI オブジェクトとして手動で移行します。

手順

- ステップ 1** 次のコマンドを使用し、CLI を介してインポート元の ASA 構成から PKI 証明書をキーとともに PKCS12 ファイルにエクスポートします。

```
ASA(config)#crypto ca export <trust-point-name> pkcs12 <passphrase>
```

- ステップ 2** PKI 証明書を管理センターにインポートします ([オブジェクト管理 (Object Management)] [PKI オブジェクト (PKI Objects)])。

詳細については、『[Firepower Management Center Configuration Guide](#)』の「PKI Objects」を参照してください。

手動で作成した PKI オブジェクトは、Cisco Secure Firewall 移行ツールの、[最適化、確認および検証 (Optimize, Review and Validate)] ページの [リモートアクセスVPN (Remote Access VPN)] タブの [トラストポイント (Trustpoint)] セクションで使用できるようになりました。

AnyConnect 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、管理センターまたは Cisco Secure Firewall 移行ツールを介してアップロードできます。

始める前に

- 管理センターのリモートアクセス VPN には、1 つ以上の AnyConnect パッケージが必要です。
- 構成が Hostscan と外部ブラウザパッケージで構成されている場合は、これらのパッケージをアップロードする必要があります。

- 移行前のアクティビティの一環として、すべてのパッケージを管理センターに追加する必要があります。
- Dap.xml と Data.xml は、Cisco Secure Firewall 移行ツールを介して追加する必要があります。

手順

ステップ 1 次のコマンドを使用して、必要なパッケージを送信元 ASA から FTP または TFTP サーバーにコピーします。

```
Copy <source file location:/source file name> <destination>
ASA# copy disk0:/anyconnect-win-4.10.02086-webdeploy-k9.pkg tftp://1.1.1.1 <----- Example
of copying Anyconnect Package.
ASA# copy disk0:/ external-sso- 4.10.04071-webdeploy-k9.zip tftp://1.1.1.1 <----- Example
of copying External Browser Package.
ASA# copy disk0:/ hostscan_4.10.04071-k9.pkg tftp://1.1.1.1 <----- Example of copying
Hostscan Package.
ASA# copy disk0:/ dap.xml tftp://1.1.1.1. <----- Example of copying Dap.xml
ASA# copy disk0:/ sdesktop/data.xml tftp://1.1.1.1 <----- Example of copying Data.xml
ASA# copy disk0:/ VPN_Profile.xml tftp://1.1.1.1 <----- Example of copying Anyconnect
Profile.
```

ステップ 2 ダウンロードしたパッケージを管理センターにインポートします ([オブジェクト管理 (Object Management)] > [VPN] > [AnyConnect ファイル (AnyConnect File)])。

1. Dap.xml と Data.xml は、Cisco Secure Firewall 移行ツールの [確認と検証 (Review and Validate)] > [リモートアクセス VPN (Remote Access VPN)] > [AnyConnect ファイル (AnyConnect File)] セクションから管理センターにアップロードする必要があります。
2. AnyConnect プロファイルは、管理センターに直接アップロードするか、または Cisco Secure Firewall 移行ツールの [確認と検証 (Review and Validate)] > [リモートアクセス VPN (Remote Access VPN)] > [AnyConnect ファイル (AnyConnect File)] セクションを介してアップロードできます。

手動でアップロードされたファイルが Cisco Secure Firewall 移行ツールで使用できるようになりました。

移行の実行

Cisco Secure Firewall 移行ツールの起動

このタスクは、デスクトップバージョンの Cisco Secure Firewall 移行ツールを使用している場合にのみ適用されます。CDO でホストされている移行ツールのクラウドバージョンを使用している場合は、[ASA 構成ファイルのアップロード \(11 ページ\)](#)に進みます。



- (注) Cisco Secure Firewall 移行ツールを起動すると、別のウィンドウでコンソールが開きます。移行が進むのに合わせて、Cisco Secure Firewall 移行ツールの現在のステップの進行状況がコンソールに表示されます。画面にコンソールが表示されない場合は、Cisco Secure Firewall 移行ツールの背後にある可能性があります。

始める前に

- [Cisco.com](#) からの Cisco Secure Firewall 移行ツールのダウンロード
- サポートされる移行先の管理センターセクションで要件を確認します。
- Cisco Secure Firewall 移行ツールを実行するために、最新バージョンの Google Chrome ブラウザがコンピュータにインストールされていることを確認します。Google Chrome をデフォルトのブラウザとして設定する方法については、「[Set Chrome as your default web browser](#)」を参照してください。
- 大規模な構成ファイルを移行する場合は、移行プッシュ中にシステムがスリープ状態にならないようにスリープ設定を構成します。

手順

ステップ 1 コンピュータで、Cisco Secure Firewall 移行ツールをダウンロードしたフォルダに移動します。

ステップ 2 次のいずれかを実行します。

- Windows マシンで、Cisco Secure Firewall 移行ツールの実行可能ファイルをダブルクリックして、Google Chrome ブラウザで起動します。

プロンプトが表示されたら、[はい (Yes)] をクリックして、Cisco Secure Firewall 移行ツールがシステムに変更を加えることができるようにします。

Cisco Secure Firewall 移行ツールは、すべての関連ファイルを作成し、Cisco Secure Firewall 移行ツールの存在するフォルダに保存します (ログおよびリソースのフォルダを含む)。

- Mac では、Cisco Secure Firewall 移行ツールの *.command ファイルを目的のフォルダに移動し、ターミナルアプリケーションを起動して、Cisco Secure Firewall 移行ツールがインストールされているフォルダを参照し、次のコマンドを実行します。

```
# chmod 750 Firewall_Migration_Tool-version_number.command  
# ./Firewall_Migration_Tool-version_number.command
```

Cisco Secure Firewall 移行ツールは、すべての関連ファイルを作成し、Cisco Secure Firewall 移行ツールの存在するフォルダに保存します (ログおよびリソースのフォルダを含む)。

ヒント Cisco Secure Firewall 移行ツールを開こうとすると、警告ダイアログが表示されます。これは、身元が明らかな開発者によって Cisco Secure Firewall 移行ツールが Apple に登録されていないためです。身元不明の開発者によるアプリケーションを開く方法については、「[Open an app from an unidentified developer](#)」を参照してください。

(注) MAC のターミナルの zip メソッドを使用します。

ステップ 3 [エンドユーザライセンス契約 (End User License Agreement)] ページで、テレメトリ情報をシスコと共有する場合は、[Cisco Success Network と情報を共有することに同意 (I agree to share data with Cisco Success Network)] をクリックし、それ以外の場合は [後で行う (I'll do later)] をクリックします。

Cisco Success Network に統計を送信することに同意すると、Cisco.com アカウントを使用してログインするように求められます。Cisco Success Network に統計を送信しないことを選択した場合は、ローカルログイン情報を使用して Cisco Secure Firewall 移行ツールにログインします。

ステップ 4 Cisco Secure Firewall 移行ツールのログインページで、次のいずれかを実行します。

- Cisco Success Network と統計を共有するには、[CCOでログイン (Login with CCO)] リンクをクリックし、シングルサインオンログイン情報を使用して Cisco.com アカウントにログインします。Cisco.com アカウントがない場合は、Cisco.com のログインページで作成します。

Cisco.com アカウントを使用してログインしている場合は、[ステップ 8](#) に進みます。

- インターネットにアクセスできないエアギャップネットワークにファイアウォールを展開した場合は、Cisco TAC に連絡して、管理者のログイン情報で動作するビルドを入手してください。このビルドでは使用状況の統計がシスコに送信されず、TAC がログイン情報を提供できることに注意してください。

ステップ 5 [パスワードのリセット (Reset Password)] ページで、古いパスワードと新しいパスワードを入力し、新しいパスワードを確認します。

新しいパスワードは 8 文字以上で、大文字と小文字、数字、および特殊文字を含める必要があります。

ステップ 6 [リセット (Reset)] をクリックします。

ステップ 7 新しいパスワードでログインします。

(注) パスワードを忘れた場合は、既存のすべてのデータを `<migration_tool_folder>` から削除し、Cisco Secure Firewall 移行ツールを再インストールします。

ステップ 8 移行前チェックリストを確認し、記載されているすべての項目を完了していることを確認します。

チェックリストの項目を 1 つ以上完了していない場合は、完了するまで続行しないでください。

ステップ 9 [新規移行 (New Migration)] をクリックします。

ステップ 10 [ソフトウェアアップデートの確認 (Software Update Check)] 画面で、Cisco Secure Firewall 移行ツールの最新バージョンを実行しているかどうか不明な場合は、リンクをクリックし、Cisco.com でバージョンを確認します。

ステップ 11 [続行 (Proceed)] をクリックします。

次のタスク

次のステップに進むことができます。

- ASA 構成をコンピュータにエクスポートした場合は、「[ASA 構成ファイルのアップロード](#)」に進みます。
- Cisco Secure Firewall 移行ツールを使用して ASA から情報を抽出する場合は、[Cisco Secure Firewall 移行ツールから ASA への接続 \(11 ページ\)](#)に進みます。

Cisco Secure Firewall 移行ツールでのデモモードの使用

Cisco Secure Firewall 移行ツールを起動し、[送信元設定の選択 (Select Source Configuration)] ページで、[移行の開始 (Start Migration)] を使用して移行を開始するか、[デモモード (Demo Mode)] に入るかを選択できます。

デモモードでは、ダミーデバイスを使用してデモ移行を実行し、実際の移行フローがどのようになるかを可視化できます。移行ツールは、[送信元ファイアウォールベンダー (Source Firewall Vendor)] ドロップダウンでの選択に基づいてデモモードをトリガーします。構成ファイルをアップロードするか、ライブデバイスに接続して移行を続行することもできます。デモ FMC デバイスやデモ FTD デバイスなどのデモのソースデバイスとターゲットデバイスを選択して、デモ移行の実行を進められます。



注意 [デモモード (Demo Mode)] を選択すると、既存の移行ワークフローがあれば消去されます。[移行の再開 (Resume Migration)] にアクティブな移行があるときにデモモードを使用すると、アクティブな移行は失われ、デモモードを使用した後に最初から再開する必要があります。

また、実際の移行ワークフローと同様に、移行前レポートのダウンロードと確認、インターフェイスのマッピング、セキュリティゾーンのマッピング、インターフェイスグループのマッピングなどのすべてのアクションを実行することもできます。ただし、デモ移行は設定の検証までしか実行できません。これはデモモードにすぎないため、選択したデモターゲットデバイスに設定をプッシュすることはできません。検証ステータスと概要を確認し、[デモモードの終了 (Exit Demo Mode)] をクリックして [送信元設定の選択 (Select Source Configuration)] ページに再度移動し、実際の移行を開始できます。



- (注) デモモードでは、設定のプッシュを除く Cisco Secure Firewall 移行ツールのすべての機能セットを活用して、実際の移行を行う前にエンドツーエンドの移行手順のトライアルを実行できます。

ASA 構成ファイルのアップロード

始める前に

送信元 ASA デバイスから構成ファイルを .cfg または .txt としてエクスポートします。



- (注) 手動でコード化された構成ファイルや手動で変更した構成ファイルはアップロードしないでください。テキストエディタは、移行に失敗する原因となる空白行やその他の問題をファイルに追加します。

手順

ステップ 1 [ASA Fortinet情報の抽出 (Extract ASA Fortinet Information)] ページの [手動アップロード (Manual Upload)] セクションで、[アップロード (Upload)] をクリックして ASA 構成ファイルをアップロードします。

ステップ 2 ASA 構成ファイルの場所を参照し、[開く (Open)] をクリックします。

Cisco Secure Firewall 移行ツールが構成ファイルをアップロードします。大規模な構成ファイルの場合、この手順には時間がかかります。コンソールには、解析中の ASA 構成行など、行ごとに進行状況のログが表示されます。コンソールが表示されない場合は、Cisco Secure Firewall 移行ツールの背後にある別のウィンドウで確認できます。[コンテキストの選択 (Context Selection)] セクションで、アップロードされた構成がマルチコンテキスト ASA に対応するかが識別されます。

ステップ 3 [コンテキストの選択 (Context Selection)] セクションを確認し、移行する ASA を選択します。

次のタスク

[Cisco Secure Firewall 移行ツールの接続先パラメータの指定 \(15 ページ\)](#)

Cisco Secure Firewall 移行ツールから ASA への接続

Cisco Secure Firewall 移行ツールは、移行する ASA デバイスに接続し、必要な構成情報を抽出できます。

始める前に

- Cisco Secure Firewall 移行ツールをダウンロードして起動します。
- シングルコンテキスト ASA の場合、管理 IP アドレス、管理者ログイン情報、およびイネーブルパスワードを取得します。
- マルチコンテキストモード ASA の場合は、**管理**コンテキストの IP アドレス、管理者ログイン情報、およびイネーブルパスワードを取得します。



(注) ASA にイネーブルパスワードが構成されていない場合は、Cisco Secure Firewall 移行ツールでこのフィールドを空白のままにしておくことができます。

手順

ステップ 1 [ASA情報の抽出 (Extract ASA Information)] 画面の [ASAへの接続 (Connect to ASA)] セクションで、[接続 (Connect)] をクリックして、移行する ASA デバイ스에接続します。

ステップ 2 [ASA ログイン (ASA Login)] 画面で、次の情報を入力します。

1. [ASA IP アドレス/ホスト名 (ASA IP Address/Hostname)] フィールドに、管理 IP アドレスまたはホスト名 (シングルコンテキスト ASA の場合) か、管理コンテキストの IP アドレスまたはホスト名 (マルチコンテキスト ASA の場合) を入力します。
2. [ユーザ名 (Username)]、[パスワード (Password)]、および[イネーブルパスワード (Enable Password)] フィールドに、適切な管理者用のログイン資格情報を入力します。

(注) ASA にイネーブルパスワードが構成されていない場合は、Cisco Secure Firewall 移行ツールでこのフィールドを空白のままにしておくことができます。

3. [ログイン (Login)] をクリックします。

Cisco Secure Firewall 移行ツールが ASA に接続すると、ASA に正常に接続されたというメッセージが表示されます。マルチコンテキスト ASA の場合、Cisco Secure Firewall 移行ツールはコンテキストを識別してリストします。

ステップ 3 [コンテキスト (Context)] ドロップダウンリストから、移行する ASA コンテキストを選択します。

ステップ 4 (任意) [ヒットカウントの収集 (Collect Hitcounts)] を選択します。

オンにすると、このツールは ASA ルールが使用された回数と、ASA 稼働時間以降または最後の ASA 再起動以降にルールが使用された最後の時刻を計算し、[確認と検証 (Review and Validate)] ページにこの情報を表示します。これにより、移行前にルールの有効性と関連性を評価できます。

ステップ 5 [抽出を開始 (Start Extraction)] をクリックします。

Cisco Secure Firewall 移行ツールが ASA に接続し、構成情報の抽出を開始します。抽出が正常に完了すると、[コンテキストを選択 (Context Selection)] セクションで、アップロードされた構成がシングルコンテキストまたはマルチコンテキスト ASA のどちらに対応するかが識別されます。

次のタスク

[Cisco Secure Firewall 移行ツールの接続先パラメータの指定 \(15 ページ\)](#)

ASA セキュリティコンテキストの選択

始める前に

単一の ASA デバイスは複数の仮想デバイスにパーティション化でき、このパーティションはセキュリティコンテキストと呼ばれます。各セキュリティコンテキストは、独自のセキュリティポリシー、インターフェイス、および管理者を持つ独立したデバイスとして機能します。マルチコンテキストは、複数のスタンドアロンデバイスを使用することに似ていますが、実際にあるデバイスは 1 台だけです。セキュリティコンテキストの詳細については、『Cisco ASA Series General Operations CLI Configuration Guide』の「[Common Uses for Security Contexts](#)」を参照してください。

このタスク手順は、Cisco Secure Firewall ASA で 2 つ以上のセキュリティコンテキストを設定している場合に適用されます。ASA の設定をアップロードすると、Cisco Secure Firewall 移行ツールはデバイス上のセキュリティコンテキストを検出し、コンテキストに関連するすべての設定情報を解析して、[コンテキストの選択 (Context Selection)] ページに表示します。

手順

- ステップ 1** ASA 構成ファイルをアップロードします。構成ファイルにコンテキストが含まれている場合、移行ツールにすべてのセキュリティコンテキストの名前が表示されます。

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

Extraction Methods >

Context Selection ▾

Choose (One from below)

Context Migration (One at a time) Merge Multi-Context to Single Instance

Note - Choose at least two contexts of the same type (routed or transparent) for merging.

Context Selection	Context Name	#Config Lines	#ACLs	#Objects	#NATs	#Routes	#Interfaces	#VPN
<input type="checkbox"/>	FMT2	189	75	0	0	0	4	0
<input type="checkbox"/>	FMT3	154	24	0	0	0	7	0
<input type="checkbox"/>	FMT1	154	14	3	3	6	4	0

ステップ2 (任意) いずれかのコンテキストから設定を移行するには、[コンテキスト移行 (1つずつ) (Context Migration (One at a time))] オプションボタンをクリックし、コンテキストを選択して移行を続行します。

ステップ3 (任意) マルチコンテキストの設定を単一インスタンスにマージして移行するには、[マルチコンテキストを単一インスタンスにマージ (Merge Multi-Context to Single Instance)] オプションボタンをクリックします。マルチコンテキストのマージを選択すると、設定行、ACL、オブジェクト、ルート (スタティックルート、PBR、ECMP を含む)、インターフェイスの数などのコンテキスト情報を表示できます。マルチコンテキストを単一インスタンスにマージすることは、トランスペアレントファイアウォールモードコンテキストとルーテッドファイアウォールモードコンテキストの両方でサポートされています。ただし、マージ対象には同じタイプのコンテキストを選択してください。トランスペアレントモードコンテキストをルーテッドモードコンテキストとマージすることはできません。システムコンテキストと管理コンテキストはサポートされておらず、移行ツールで検出されません。

(注) マルチコンテキストをマージする前に、次の前提条件を確認してください。

- ASA でポートチャネルが設定されている場合は、ターゲット脅威に対する防御デバイスでもそれらが設定されていることを確認します。
- 2つのインターフェイスの VLAN ID とサブインターフェイス ID が同じである場合、移行ツールにより新しいインターフェイスに新しい VLAN ID とサブインターフェイス ID が自動的に追加されます。これらの ID に関する情報は、移行前レポートに含まれています。移行ツールによって作成されたこれらの新しいインターフェイスが、対応するデバイスのトランクポートオブジェクトに設定されていることを確認します。脅威に対する防御デバイスでは、2つのインターフェイスが同じ VLAN ID とサブインターフェイス ID を持つことはできないためです。
- AS パスオブジェクトは、移行されるすべてのコンテキストで一意である必要があります。重複していると移行されません。

(注) マルチコンテキストをマージするときに、マージ対象に選択した2つ以上のコンテキストで VPN が設定されている場合は、移行ツールにより、VPN が設定されているいずれかのコンテキストを選択するよう求められます。選択したコンテキストの VPN 設定のみが移行され、他のコンテキストの VPN 設定は無視されます。ただし、選択されていないコンテキスト内の他のすべての設定 (オブジェクト、拡張 ACL、NAT ルール、参照されていない VPN オブジェクトなど) は変わらず移行されることに注意してください。

ステップ4 [解析を開始 (Start Parsing)] をクリックします。コンテキストを選択して解析を開始すると、移行ツールはすべてのコンテキストの設定をマージして解析し、[解析サマリー (Parsed Summary)] を表示します。マージされたコンテキストの移行を実行する場合は、移行対象に選択したコンテキストの数が、解析サマリーの VRF の数と同じであることを注意してください。ただし、VPN 設定を持つコンテキストがある場合は、VPN 設定を持つ VRF がグローバルルータに直接プッシュされるため、解析サマリーに表示される VRF は1つ少なくなります。

- (注) [解析を開始 (Start Parsing)] をクリックしていて、別のコンテキストを選択する場合は、戻って別のコンテキストを選択することはできません。[戻る (Back)] をクリックして構成ファイルのアップロードから開始し、別のコンテキストを選択することができます。

ステップ 5 アップロードされた構成ファイルで、Cisco Secure Firewall 移行ツールが検出して解析した要素の概要を確認します。

ステップ 6 [次へ (Next)] をクリックして、ターゲットパラメータを選択します。

Cisco Secure Firewall 移行ツールの接続先パラメータの指定

始める前に

- オンプレミス Firewall Management Center の Management Center の IP アドレスを取得します。
- Cisco Secure Firewall 移行ツール 3.0 以降では、オンプレミスの Firewall Management Center またはクラウド提供型 Firewall Management Center を選択できます。
- クラウド提供型 Firewall Management Center の場合、リージョンと API トークンを指定する必要があります。詳細については、「[サポートされる移行先の管理センター](#)」を参照してください。
- 「[User Accounts for Management Access](#)」の説明に従って、REST API にアクセスするための十分な権限で、Management Center に Cisco Secure Firewall 移行ツールの専用アカウントを作成します。
- (任意) インターフェイスやルートなどのデバイス固有の構成を移行する場合は、ターゲット脅威に対する防御を Management Center に追加します。「[Adding Devices to the Firewall Management Center](#)」を参照してください。
- [確認と検証 (Review and Validate)] ページで IPS またはファイルポリシーを ACL に適用する必要がある場合は、移行前に Management Center でポリシーを作成することを強くお勧めします。Cisco Secure Firewall 移行ツールは接続された Management Center からポリシーを取得するため、同じポリシーを使用します。新しいポリシーを作成して複数のアクセス制御リストに割り当てると、パフォーマンスが低下し、プッシュが失敗する可能性があります。

手順

ステップ 1 [ターゲットの選択 (Select Target)] 画面の [ファイアウォール管理 (Firewall Management)] セクションで、次の手順を実行します。オンプレミスのファイアウォール管理センターまたはクラウド提供型ファイアウォール管理センターへの移行を選択できます。

- オンプレミスのファイアウォール管理センターに移行するには、次の手順を実行します。

- a) [オンプレミス FMC (On-Prem FMC)] オプションボタンをクリックします。
- b) 管理センターの IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。
- c) [Domain] ドロップダウンリストで、移行先のドメインを選択します。
脅威に対する防御 デバイスに移行する場合は、選択したドメインで使用可能な脅威に対する防御 デバイスにのみ移行できます。
- d) [接続 (Connect)] をクリックして、手順 2 に進みます。
 - クラウド提供型 Firewall Management Center に移行するには、次の手順を実行します。
 - a) [クラウド提供型 FMC (Cloud-delivered FMC)] オプションボタンをクリックします。
 - b) リージョンを選択し、CDO API トークンを貼り付けます。CDO から API トークンを生成するため、以下の手順に従います。
 1. CDO ポータルにログインします。
 2. [設定 (Settings)] > [全般設定 (General Settings)] に移動して、API トークンをコピーします。
- c) [接続 (Connect)] をクリックして、手順 2 に進みます。

ステップ 2 [Firewall Management Center へのログイン (Firewall Management Center Login)] ダイアログボックスで、Cisco Secure Firewall 移行ツール専用アカウントのユーザー名とパスワードを入力し、[ログイン (Login)] をクリックします。

Cisco Secure Firewall 移行ツールは Management Center にログインし、その Management Center による管理対象脅威に対する防御 デバイスのリストを取得します。この手順の進行状況はコンソールで確認できます。

ステップ 3 [続行 (Proceed)] をクリックします。

[Threat Defense の選択 (Choose Threat Defense)] セクションでは、移行先の脅威に対する防御 デバイスを選択できます。また、脅威に対する防御 デバイスがない場合は、ASA 構成の共有ポリシー (アクセス制御リスト、NAT、およびオブジェクト) を Management Center に移行できます。

ステップ 4 [Threat Defense の選択 (Choose Threat Defense)] セクションで、次のいずれかを実行します。

- [Firewall Threat Defense デバイスの選択 (Select Firewall Threat Defense Device)] ドロップダウンリストをクリックし、ASA 構成を移行するデバイスをオンにします。
選択した Management Center ドメイン内のデバイスが、IP アドレスと名前ですらリストされません。

- (注) 少なくとも、選択するネイティブ 脅威に対する防御 デバイスには、移行する ASA 構成と同じ数の物理インターフェイスまたはポートチャネルインターフェイスが必要です。少なくとも、脅威に対する防御デバイスのコンテナインスタンスには、同じ数の物理インターフェイスまたはポートチャネルインターフェイスとサブインターフェイスが必要です。ASA 構成と同じファイアウォールモードでデバイスを構成する必要があります。ただし、これらのインターフェイスは、両方のデバイスで同じ名前である必要はありません。
- (注) サポートされているターゲット Threat Defense プラットフォームが、管理センターバージョン 6.5 以降を備えた Firewall 1010 である場合にのみ、FDM 5505 移行サポートは共有ポリシーに適用され、デバイス固有のポリシーには適用されません。Threat Defense なしで続行すると、Cisco Secure Firewall 移行ツールは構成またはポリシーを Threat Defense にプッシュしません。したがって、Threat Defense のデバイス固有の構成であるインターフェイスとルート、およびサイト間 VPN は移行されません。ただし、NAT、ACL、ポートオブジェクトなど、サポートされている他のすべての構成（共有ポリシーとオブジェクト）は移行されます。リモートアクセス VPN は共有ポリシーであり、Threat Defense なしでも移行できます。

表 1: ASA ファイアウォール機能とサポートされている Management Center または Threat Defense のバージョン

ファイアウォール機能	サポートされている管理センターまたは Threat Defense のバージョン
ASA とリモート展開	6.7 以降
暗号マップサイト間 VPN	6.6 以降
仮想トンネルインターフェイス (VTI) とルートベース (VTI)	6.7 以降
動的ルートオブジェクトと BGP	7.1 以降
リモート アクセス VPN	<ul style="list-style-type: none"> • Management Center 7.2 以降 • Threat Defense 7.0 以降
EIGRP	<ul style="list-style-type: none"> • Management Center 7.2 以降 • Threat Defense 7.0 以降
PBR	<ul style="list-style-type: none"> • Management Center 7.3 以降 • Threat Defense 7.3 以降
ECMP	<ul style="list-style-type: none"> • Management Center 7.1 以降 • Threat Defense 6.5 以降

ファイアウォール機能	サポートされている管理センターまたは Threat Defense のバージョン
WebVPN	<ul style="list-style-type: none"> • Management Center 7.4 以降 • Threat Defense 7.4 以降
SNMP	<ul style="list-style-type: none"> • Management Center 7.4 以降 • Threat Defense 7.4 以降
DHCP リレー、サーバー、および DDNS	<ul style="list-style-type: none"> • Management Center 7.4 以降 • Threat Defense 7.4 以降

(注) サイト間 VPN、VTI、およびルートベース (VTI) インターフェイスを移行するには、Management Center で脅威に対する防御を構成する必要があります。

- ASA 5505 の場合、デバイス固有の構成 (インターフェイスおよびルータ) と共有ポリシー (NAT、ACL、オブジェクト) は、サポートされているターゲット脅威に対する防御プラットフォームが Management Center バージョン 6.5 以降を備えた Firewall 1010 の場合にのみ移行できます。

(注)

- ターゲット脅威に対する防御が FPR-1010 でない場合、またはターゲット Management Center が 6.5 よりも前の場合は、ASA 5505 の移行サポートは共有ポリシーにのみ適用されます。デバイス固有の設定は移行されません。
- 送信元構成は ASA 5505 であるため、[デバイスの選択 (Select Device)] ドロップダウンリストから FPR-1010 のみを選択できます。
- ASA-SM 移行のサポートは、共有ポリシーのみを対象としています。デバイス固有の設定は移行されません。

- [FTD を使用せず続行 (Proceed without FTD)] をクリックして、構成を Management Center に移行します。

脅威に対する防御なしで続行すると、Cisco Secure Firewall 移行ツールは脅威に対する防御に構成またはポリシーをプッシュしません。したがって、脅威に対する防御のデバイス固有の校正であるインターフェイスとルート、およびサイト間 VPN は移行されず、Management Center で手動で構成する必要があります。ただし、NAT、ACL、ポートオブジェクトなど、サポートされている他のすべての構成 (共有ポリシーとオブジェクト) は移行されます。リモートアクセス VPN は共有ポリシーであり、Threat Defense なしでも移行できます。

ステップ 5 [続行 (Proceed)] をクリックします。

移行先に応じて、Cisco Secure Firewall 移行ツールを使用して移行する機能を選択できます。

ステップ 6 [機能の選択 (Select Features)]セクションをクリックして、移行先に移行する機能を確認して選択します。

- 接続先 脅威に対する防御 デバイスに移行する場合、Cisco Secure Firewall 移行ツールは、[デバイスの構成 (Device Configuration)]セクションと [共有構成 (Shared Configuration)]セクションで、ASA 構成から移行できる機能を自動的に選択します。要件に応じて、デフォルトの選択をさらに変更できます。
- Management Center に移行する場合、Cisco Secure Firewall 移行ツールは、[デバイス設定 (Device Configuration)]、[共有構成 (Shared Configuration)]、および [最適化 (Optimization)]セクションで、ASA 構成から移行できる機能を自動的に選択します。要件に応じて、デフォルトの選択をさらに変更できます。
- Cisco Secure Firewall 移行ツールでは、移行中に次のアクセス制御がサポートされています。

- 宛先セキュリティゾーンの指定：移行中の ACL の宛先ゾーンのマッピングを有効にします。

ルートルックアップロジックは静的ルートと接続ルートに限定される一方、PBR、動的ルート、および NAT は考慮されません。インターフェイス ネットワーク構成は、接続ルート情報を取得するために使用されます。

送信元および接続先のネットワーク オブジェクト グループの性質によっては、この操作によりルールが急増することがあります。

- トンネル化されたルールのプレフィルタとしての移行：ASA カプセル化トンネルプロトコルルールをプレフィルタトンネルルールにマッピングすると、次のような利点があります。
 - ディープインスペクションの調整：カプセル化トラフィックの場合に、ファストパス処理でのパフォーマンスを向上させます。
 - パフォーマンスの向上：早期処理のメリットがあるその他の接続についても、ファストパスやブロックをすることができます。

Cisco Secure Firewall 移行ツールは、送信元構成でカプセル化されたトンネルトラフィックルールを識別し、プレフィルタトンネルルールとして移行します。プレフィルタポリシーで移行されたトンネルルールを確認できます。プレフィルタポリシーは、Management Center で移行されたアクセス コントロール ポリシーに関連付けられます。

プレフィルタトンネルルールとして移行されるプロトコルは次のとおりです。

- GRE (47)
- IPv4 カプセル化 (4)
- IPv6 カプセル化 (41)
- Teredo トンネリング (UDP:3544)

(注) プレフィルタオプションを選択しない場合、すべてのトンネルトラフィックルールがサポートされていないルールとして移行されます。

ASA 構成の ACL トンネルルール (GRE および IPnIP) は、現在、デフォルトで双方向として移行されます。アクセスコントロールの状態オプションで、接続先のルール方向を双方向または単方向に指定できるようになりました。

- Cisco Secure Firewall 移行ツールは、VPN トンネル移行用に次のインターフェイスとオブジェクトをサポートしています。
 - ポリシーベース (暗号マップ) : ターゲット Management Center と脅威に対する防御がバージョン 6.6 以降の場合
 - ルートベース (VTI) : ターゲット Management Center と脅威に対する防御がバージョン 6.7 以降の場合
- Cisco Secure Firewall 移行ツールは、ターゲット管理センターが 7.2 以降の場合はリモートアクセス VPN の移行をサポートします。リモートアクセス VPN は、Threat Defense なしで移行できる共有ポリシーです。Threat Defense を使用する移行を選択した場合、Threat Defense のバージョンは 7.0 以降である必要があります。
- (任意) [Optimization] セクションで、[Migrate only referenced objects] を選択して、アクセスコントロールポリシーと NAT ポリシーで参照されているオブジェクトのみを移行します。
 - (注) このオプションを選択すると、ASA 構成内の参照されていないオブジェクトは移行されません。これにより、移行時間が最適化され、未使用のオブジェクトが構成から消去されます。
- (任意) [最適化 (Optimization)] セクションで、脅威に対する防御のアクセスポリシーによる最適なメモリ使用率を実現する場合は、[オブジェクトグループの検索 (Object group search)] を選択します。
- (任意) [インライングループ化 (Inline Grouping)] セクションでは、Cisco Secure Firewall 移行ツールを使用して、CSM または DM で始まる定義済みのネットワークおよびサービスオブジェクト名のアクセスルールをクリアできます。このオプションをオフにすると、定義済みのオブジェクト名が移行時に保持されます。詳細については、「[インライングループ化](#)」を参照してください。
 - (注) デフォルトでは、インライングループ化のオプションが有効になっています。
- 送信元 ASA デバイスに [SNMP] および [DHCP]、[サーバー (Server)]、[リレー (Relay)]、および [DDNS] 設定がある場合、対応するチェックボックスがデフォルトでオンになっています。これらの設定を移行しない場合は、手動でオフにします。DHCP が選択されている場合は、[サーバー (Server)] をオンにするか、[リレー (Relay)] と [DDNS] の両方をオンにできます。
- SSL クライアントレス VPN トンネルプロトコルが設定されたグループポリシーと、SAML 認証を使用するグループポリシーが設定されたトンネルグループがある場合、移行ツールはデフォルトで [WebVPN] チェックボックスをオンにします。これらの設定を移行しない場合は、手動でオフにしてください。

- ステップ 7** [続行 (Proceed)] をクリックします。
- ステップ 8** [Rule Conversion/ Process Config] セクションで、[Start Conversion] をクリックして変換を開始します。
- ステップ 9** Cisco Secure Firewall 移行ツールによって変換された要素の概要を確認します。
構成ファイルが正常にアップロードおよび解析されたかどうかを確認するには、移行を続行する前に**移行前レポート**をダウンロードして確認します。
- ステップ 10** [レポートのダウンロード (Download Report)] をクリックし、**移行前レポート**を保存します。
移行前レポートのコピーも、Cisco Secure Firewall 移行ツールと同じ場所にある Resources フォルダに保存されます。

次のタスク

[移行前レポートの確認 \(22 ページ\)](#)

インライングループ化

ASDM および CSM マネージド ASA によるオブジェクトグループ化

送信元または接続先のアドレス、あるいは送信元または接続先のサービスに複数の項目 (オブジェクトまたはインラインの値) を入力すると、CSM または ASDM でオブジェクトグループが自動的に作成されます。各 ASA デバイスに構成を展開する際に、CSM および ASDM で使用されるこれらのオブジェクトグループの命名規則は、それぞれ CSM_INLINE および DM_INLINE です。



- (注) オブジェクトグループ化の動作を変更するには、[ツール (Tools)] > [設定 (Preferences)] から、[指定したプレフィックスを持つネットワークおよびサービスオブジェクトを自動展開する (Auto-expand network and service objects with specified prefix)] ルールテーブル設定を選択します。

次に、ASDM によって管理される ASA で **show run** コマンドを使用して抽出された構成スニペットを示します。

```
object network host1
 host 10.1.1.100
object network fqdn_obj1
 fqdn abc.cisco.com
object-group network DM_INLINE_NETWORK_1
 network-object 10.21.44.189 255.255.255.255
 network-object 10.21.44.190 255.255.255.255
object-group network DM_INLINE_NETWORK_2
 network-object 10.21.44.191 255.255.255.255
 network-object object host1
 network-object object fqdn_obj1
```

```
access-list CSM_DM_ACL extended permit tcp object-group DM_INLINE_NETWORK_1 object-group
DM_INLINE_NETWORK_2
```

上記の例では、ASDM UI の access-list CSM_DM_ACL は、ルールの送信元および接続先のネットワークとして DM_INLINE グループを表示せず、代わりに DM_INLINE グループの内容を表示します。

インライングループ化 : ASDM/CSM

Cisco Secure Firewall 移行ツールのインライングループ化機能を使用すると、ASDM または CSM のマネージド ASA デバイスの **show running-configuration** を解析できます。ASDM または CSM と同じアクセスリストルールの UI 表現を保持するオプションがあります。オプトアウトした場合、移行されたルールは、ASA **show running-configuration** で記録されている DM_INLINE グループを参照します。



- (注) Cisco Secure Firewall 移行ツールへの送信元 ASA 構成ファイル入力は、引き続き ASA からまたは ASA デバイス (SSH) へのライブ接続を介して収集された **show run** または **show tech** になります。Cisco Secure Firewall 移行ツールは、他の形式の構成ファイルまたは方式をサポートしていません。

次の図は、ACE または RULE の [送信元ネットワーク (Source Network)] フィールドと [接続先ネットワーク (Destination Network)] フィールドが、それぞれインライングループ化オプションの有効化または無効化に基づいてどのように変化するかを示しています。

図 1: インライングループ化あり : ASDM/CSM が有効

Name	SOURCE			DESTINATION			State	Action
	Zone	Network	Port	Zone	Network	Port		
CSM_DM_ACL_#1	outside	10.21.44.189, 10.21.44.190	ANY	ANY	10.21.44.191, host1, fqrn_obj1	ANY	✓	Allow

図 2: インライングループ化あり : ASDM/CSM が無効

Name	SOURCE			DESTINATION			State	Action
	Zone	Network	Port	Zone	Network	Port		
CSM_DM_ACL_#1	outside	DM_INLINE_NETWORK_1	ANY	ANY	DM_INLINE_NETWORK_2	ANY	✓	Allow

移行前レポートの確認

移行中に移行前レポートをダウンロードし忘れた場合は、次のリンクを使用してダウンロードしてください。

移行前レポートのダウンロードエンドポイント : http://localhost:8888/api/downloads/pre_migration_summary_html_format



- (注) レポートは、Cisco Secure Firewall 移行ツールの実行中にのみダウンロードできます。

手順

ステップ 1 移行前レポートをダウンロードした場所に移動します。

移行前レポートのコピーも、Cisco Secure Firewall 移行ツールと同じ場所にある Resources フォルダに保存されます。

ステップ 2 移行前レポートを開き、その内容を慎重に確認して、移行が失敗する原因となる問題を特定します。

移行前レポートには、次の情報が含まれています。

- [全体のサマリー (Overall Summary)] : ASA 構成情報を抽出するため、またはライブ ASA 構成に接続するために使用される方法。

ライブ ASA に接続している場合は、ASA で検出されたファイアウォールモード。マルチコンテキストモードの場合は、移行用に選択したコンテキスト。

脅威に対する防御に正常に移行できるサポート対象 ASA 構成要素と、移行対象として選択された特定の ASA 機能のサマリー。

ライブ ASA に接続している場合、サマリーにはヒットカウント情報 (ASA ルールが検出された回数とそのタイムスタンプ情報) が含まれます。

- [エラーのある構成行 (Configuration Lines with Errors)] : Cisco Secure Firewall 移行ツールが解析できなかったために正常に移行できない ASA の構成要素の詳細。ASA 構成でこれらのエラーを修正し、新しい構成ファイルをエクスポートしてから、新しい構成ファイルを Cisco Secure Firewall 移行ツールにアップロードし、続行してください。
- [部分的なサポート構成 (Partially Supported Configuration)] : 部分的にのみ移行可能な ASA 構成要素の詳細。これらの構成要素には、詳細オプションを含むルールとオブジェクトが含まれているため、詳細オプションを使用せずにルールまたはオブジェクトを移行できません。これらの行を確認し、詳細オプションが Management Center でサポートされているかどうかを確認します。サポートされている場合は、Cisco Secure Firewall 移行ツールを使用して移行を完了した後に、これらのオプションを手動で構成することを計画します。
- [オブジェクトおよびオブジェクトグループの競合解決 (Object and Object Groups Conflict Resolution)] : 移行しようとしているコンテキスト間で競合している ASA ネットワークオブジェクトとサービスオブジェクト、およびオブジェクト、サービス、プロトコルオブジェクトグループの詳細。これらのオブジェクトの競合に関する詳細を表示するには、**[競合数のリンク (Link for Conflict Count)]** をクリックします。競合の理由を確認し、移行ツールが競合をどのように処理しているかを知ることができます。
- [未サポートの構成 (Unsupported Configuration)] : Cisco Secure Firewall 移行ツールがこれらの機能の移行をサポートしていないため、移行できない ASA 構成要素の詳細。これらの行を確認し、各機能が Management Center でサポートされているかどうかを確認します。サポートされている場合は、Cisco Secure Firewall 移行ツールを使用して移行を完了した後に、機能を手動で構成することを計画します。

- [無視される構成 (Ignored Configuration)] : Management Center または Cisco Secure Firewall 移行ツールでサポートされていないために無視される ASA 構成要素の詳細。Cisco Secure Firewall 移行ツールはこれらの行を解析しません。これらの行を確認し、各機能が Management Center でサポートされているかどうかを確認します。サポートされている場合は、機能を手動で構成することを計画します。[無視された設定行のリンク (Link for the ignored configuration lines)] をクリックして、無視されたすべての行を表示します。

Management Center と脅威に対する防御でサポートされる機能の詳細については、『[Management Center Configuration Guide](#)』 [英語] を参照してください。

- ステップ 3** 移行前レポートで修正措置が推奨されている場合は、ASA インターフェイスで修正を完了し、ASA 構成ファイルを再度エクスポートしてから、更新された構成ファイルをアップロードし、続行してください。
- ステップ 4** ASA 構成ファイルが正常にアップロードおよび解析されたら、Cisco Secure Firewall 移行ツールに戻り、[次へ (Next)] をクリックして移行を続行します。

次のタスク

[ASA 構成と Threat Defense インターフェイスのマッピング](#)

ASA 構成と Threat Defense インターフェイスのマッピング

脅威に対する防御 デバイスには、ASA 構成で使用されている数以上の物理インターフェイスとポート チャネルインターフェイスが必要です。これらのインターフェイスは、両方のデバイスで同じ名前である必要はありません。インターフェイスのマッピング方法を選択できます。

[FTDインターフェイスのマップ (Map FTD Interface)] 画面で、Cisco Secure Firewall 移行ツールは、脅威に対する防御デバイス上のインターフェイスのリストを取得します。デフォルトでは、Cisco Secure Firewall 移行ツールは ASA のインターフェイスと脅威に対する防御 デバイスをインターフェイス ID に従ってマッピングします。たとえば、ASA インターフェイスの「管理専用」インターフェイスは、脅威に対する防御デバイスの「管理専用」インターフェイスに自動的にマッピングされ、変更できません。

ASA インターフェイスから脅威に対する防御 インターフェイスへのマッピングは、脅威に対する防御 デバイスタイプによって異なります。

- ターゲット脅威に対する防御 がネイティブタイプの場合は次のようになります。
 - 脅威に対する防御には、使用する ASA インターフェイスまたはポートチャネル (PC) データインターフェイスが同数以上必要です (ASA 構成の管理専用とサブインターフェイスを除く)。同数未満の場合は、ターゲット脅威に対する防御に必要なタイプのインターフェイスを追加します。
 - サブインターフェイスは、物理インターフェイスまたはポートチャネルマッピングに基づいて Cisco Secure Firewall 移行ツールによって作成されます。

- ターゲット 脅威に対する防御 がコンテナタイプの場合は次のようになります。
 - 脅威に対する防御 には、使用する ASA インターフェイス、物理サブインターフェイス、ポートチャンネル、またはポート チャンネル サブインターフェイスが同数以上必要です（ASA 構成の管理専用を除く）。同数未満の場合は、ターゲット 脅威に対する防御に必要なタイプのインターフェイスを追加します。たとえば、ターゲット脅威に対する防御の物理インターフェイスと物理サブインターフェイスの数が ASA での数より 100 少ない場合、ターゲット 脅威に対する防御 に追加の物理または物理サブインターフェイスを作成できます。
 - サブインターフェイスは、Cisco Secure Firewall 移行ツールでは作成されません。物理インターフェイス、ポートチャンネル、またはサブインターフェイス間のインターフェイスマッピングのみが許可されます。

始める前に

Management Center に接続し、接続先として 脅威に対する防御 を選択していることを確認します。詳細については、「[Cisco Secure Firewall 移行ツールの接続先パラメータの指定（15 ページ）](#)」を参照してください。



- (注) 脅威に対する防御 デバイスなしで Management Center に移行する場合、この手順は適用されません。

手順

- ステップ 1** インターフェイスマッピングを変更する場合は、**[FTDインターフェイス名 (FTD Interface Name)]** のドロップダウンリストをクリックし、その ASA インターフェイスにマッピングするインターフェイスを選択します。

管理インターフェイスのマッピングは変更できません。脅威に対する防御インターフェイスがすでに ASA インターフェイスに割り当てられている場合は、ドロップダウンリストからそのインターフェイスを選択できません。割り当て済みのすべてのインターフェイスはグレー表示され、使用できません。

サブインターフェイスをマッピングする必要はありません。Cisco Secure Firewall 移行ツールは、ASA 構成内のすべてのサブインターフェイスについて 脅威に対する防御 デバイスのサブインターフェイスをマッピングします。
- ステップ 2** 各 ASA インターフェイスを 脅威に対する防御 インターフェイスにマッピングしたら、**[次へ (Next)]** をクリックします。
- ステップ 3** **[マップ済みのNameif (Mapped Nameif)]** 列を使用して、対象の管理センターに同じ名前の既存の設定があるかどうかを検証します。移行ツールが同じ名前を設定を検出した場合は、これ

らの名前を変更できます。または、検証後にこの列のすべてのエントリが緑色に変わった場合は、そのまま続行できます。

次のタスク

ASA インターフェイスを適切な脅威に対する防御 インターフェイスオブジェクト、セキュリティゾーン、およびインターフェイスグループにマッピングします。詳細については、「[セキュリティゾーン、インターフェイスグループ、および VRF への ASA インターフェイスのマッピング](#)」を参照してください。

セキュリティゾーン、インターフェイスグループ、および VRF への ASA インターフェイスのマッピング



(注) ASA 構成にアクセスリストと NAT ルールが含まれていない場合、またはこれらのポリシーを移行しない場合は、この手順をスキップして「[最適化、構成の確認と検証 \(28 ページ\)](#)」に進むことができます。

ASA 構成が正しく移行されるように、ASA インターフェイスを適切な脅威に対する防御 インターフェイス オブジェクト、セキュリティゾーン、インターフェイスグループ、および VRF にマッピングします。ASA 構成では、アクセス コントロール ポリシーと NAT ポリシーはインターフェイス名 (nameif) を使用します。Management Center では、これらのポリシーはインターフェイスオブジェクトを使用します。さらに、Management Center ポリシーはインターフェイスオブジェクトを次のようにグループ化します。

- セキュリティゾーン：インターフェイスは、1つのセキュリティゾーンにのみ属することができます。
- インターフェイスグループ：インターフェイスは複数のインターフェイスグループに属することができます。
- VRF：インターフェイスは1つの VRF 設定にのみ属することができます。

Cisco Secure Firewall 移行ツールでは、セキュリティゾーン、インターフェイスグループ、および VRF とインターフェイスを 1 対 1 でマッピングできます。セキュリティゾーンまたはインターフェイスグループがインターフェイスにマッピングされている場合、他のインターフェイスへのマッピングには使用できませんが、Management Center では許可されます。Management Center のセキュリティゾーンとインターフェイスグループの詳細については、『[Cisco Secure Firewall Management Center Device Configuration Guide](#)』の「[Security Zones and Interface Groups](#)」を参照してください。

手順

- ステップ 1** [セキュリティゾーン、インターフェイスグループ、および VRF のマッピング (Map Security Zones, Interface Groups and VRFs)] 画面で、使用可能なインターフェイス、セキュリティゾーン、インターフェイスグループ、および VRF 設定を確認します。
- ステップ 2** セキュリティゾーンおよびインターフェイスグループが Management Center に存在する場合、またはセキュリティゾーンタイプオブジェクトとして ASA 構成ファイルに存在し、ドロップダウンリストで使用可能な場合、これらにインターフェイスをマッピングするには、次の手順を実行します。
- [セキュリティゾーン (Security Zones)] 列で、インターフェイスのセキュリティゾーンを選択します。
 - [インターフェイスグループ (Interface Groups)] 列で、インターフェイスのインターフェイスグループを選択します。
 - [VRF] 列で、インターフェイスの VRF 設定を選択します。
- ステップ 3** セキュリティゾーン、インターフェイスグループ、および VRF は、手動でマッピングすることも自動で作成することもできます。
- ステップ 4** セキュリティゾーン、インターフェイスグループ、VRF を手動でマッピングするには、次の手順を実行します。
- [セキュリティゾーン、インターフェイスグループ、VRF の追加 (Add SZ, IG & VRF)] をクリックします。
 - [セキュリティゾーン、インターフェイスグループ、VRF の追加 (Add SZ, IG & VRF)] ダイアログボックスで、編集アイコンをクリックし、VRF に付ける名前を入力して、緑色のチェックマークをクリックします。編集アイコンを再度クリックして、VRF 名を編集することもできます。

(注) マージされた設定の移行を実行していて、いずれかのコンテキストに VPN 設定があった場合、それはグローバルルータに直接移行されるため、ここには表示されずインターフェイスにマッピングされます。
 - [セキュリティゾーン (Security Zone)] 列にセキュリティゾーン名を入力します。使用できる最大文字数は 48 です。同様に、インターフェイスグループを追加できます。
 - [閉じる (Close)] をクリックします。
- セキュリティゾーンとインターフェイスグループを自動作成によってマッピングするには、次の手順を実行します。
- [自動作成 (Auto-Create)] をクリックします。
 - [自動作成 (Auto-Create)] ダイアログボックスで、[インターフェイスグループ (Interface Groups)] または [ゾーンマッピング (Zone Mapping)] のいずれかまたは両方をオンにします。
 - [自動作成 (Auto-Create)] をクリックします。
- Cisco Secure Firewall 移行ツールは、これらのセキュリティゾーンに ASA インターフェイスと同じ名前 (**outside** や **inside** など) を付け、名前の後に "(A)" を表示して、Cisco Secure Firewall

移行ツールによって作成されたことを示します。インターフェイスグループには、**outside_ig** や **inside_ig** などの **_ig** サフィックスが追加されます。また、セキュリティゾーンとインターフェイスグループには、ASA インターフェイスと同じモードがあります。たとえば、ASA 論理インターフェイスが L3 モードの場合、そのインターフェイス用に作成されたセキュリティゾーンとインターフェイスグループも L3 モードになります。

ステップ 5 すべてのインターフェイスを適切なセキュリティゾーン、インターフェイスグループ、VRF にマッピングしたら、**[次へ (Next)]** をクリックします。

最適化、構成の確認と検証

移行した ASA 構成を Management Center にプッシュする前に、構成を慎重に確認し、それが適切で脅威に対する防御 デバイスの構成内容と一致することを確認します。点滅しているタブは、次の一連のアクションを実行する必要があることを示しています。



(注) [構成の最適化、確認および検証 (Optimize, Review and Validate Configuration)] 画面で Cisco Secure Firewall 移行ツールを閉じると、進行状況が保存され、後で移行を再開できます。この画面の前に Cisco Secure Firewall 移行ツールを閉じると、進行状況は保存されません。解析後に障害が発生した場合、[インターフェイスマッピング (Interface Mapping)] 画面から Cisco Secure Firewall 移行ツールを再起動します。

これで、Cisco Secure Firewall 移行ツールは、Management Center にすでに存在する侵入防御システム (IPS) ポリシーとファイルポリシーを取得し、移行するアクセスコントロールルールにそれらに関連付けることができます。

ファイルポリシーは、システムが全体的なアクセス制御設定の一環として、ネットワークの高度なマルウェア防御とファイル制御を実行するために使用する一連の設定です。この関連付けにより、アクセスコントロールルールの条件と一致するトラフィック内のファイルを通過させる前に、システムは必ずファイルを検査するようになります。

同様に、トラフィックが接続先に向かうことを許可する前に、システムの最終防御ラインとして IPS ポリシーを使用できます。侵入ポリシーは、セキュリティ違反に関するトラフィックの検査方法を制御し、インライン展開では、悪意のあるトラフィックをブロックまたは変更することができます。システムが侵入ポリシーを使用してトラフィックを評価する場合、システムは関連付けられた変数セットを使用します。セット内の大部分の変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスとポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。

タブで特定の構成項目を検索するには、列の上部にあるフィールドに項目名を入力します。テーブルの行はフィルタ処理され、検索語に一致する項目のみが表示されます。

送信元 ASA デバイスは、CSM または ASDM で管理できます。送信元または接続先のアドレス、あるいは送信元または接続先のサービスに複数の項目 (オブジェクトまたはインラインの値) を入力すると、CSM または ASDM でオブジェクトグループが自動的に作成されます。

CSM および ASDM で使用されるこれらのオブジェクトグループの命名規則は、それぞれ CSM_INLINE および DM_INLINE です。

インライングループ化 CSM または ASDM 管理型設定をクリアすることを選択すると、事前に定義されたオブジェクトが実際のオブジェクトまたはメンバー名に置き換えられます。CSM または ASDM 管理型設定をクリアしない場合、事前に定義されたオブジェクト名は移行のために保持されます。

たとえば、10.21.44.189 と 10.21.44.190 はオブジェクトグループのメンバーであり、オブジェクトグループ DM_INLINE_NETWORK_1 やオブジェクトグループ DM_INLINE_NETWORK_2 などの定義済みの名前に変更されます。



- (注) デフォルトでは、[インライングループ化 (Inline Grouping)] オプションが有効になっています。

[構成の最適化、確認および検証 (Optimize, Review and Validate Configuration)] 画面で Cisco Secure Firewall 移行ツールを閉じると、進行状況が保存され、後で移行を再開できます。この画面の前に閉じると、進行状況は保存されません。解析後に障害が発生した場合、[インターフェイスマッピング (Interface Mapping)] 画面から Cisco Secure Firewall 移行ツールを再起動します。

Cisco Secure Firewall 移行ツールの ACL 最適化の概要

Cisco Secure Firewall 移行ツールは、ネットワーク機能に影響を与えることなく、ファイアウォールルールベースから最適化（無効化または削除）できる ACL を識別および分離するサポートを提供します。

ACL 最適化は、次の ACL タイプをサポートします。

- 冗長 ACL : 2つの ACL の構成とルールのセットが同じ場合、基本以外の ACL を削除してもネットワークに影響はありません。たとえば、2つのルールが同じネットワーク上で FTP および IP トラフィックを許可し、アクセスを拒否するルールが定義されていない場合、最初のルールを削除できます。
- シャドウ ACL : 最初の ACL は、2番目の ACL の設定を完全にシャドウイングします。2つのルールに同様のトラフィックがある場合、2番目のルールはアクセスリストの後半に表示されるため、どのトラフィックにも適用されません。2つのルールがトラフィックに対して異なるアクションを指定している場合、シャドウイングされたルールを移動するか、いずれかのルールを編集して必要なポリシーを実装できます。たとえば、特定の送信元または宛先に対して、基本ルールで IP トラフィックを拒否し、シャドウイングされたルールで FTP トラフィックを許可できます。

Cisco Secure Firewall 移行ツールは、ACL 最適化のルールを比較する際に次のパラメータを使用します。



- (注) ASA では ACP ルールアクションに対してのみ最適化を使用できます

- 無効化された ACL は、最適化プロセス中に考慮されません。
- 送信元の ACL は、対応する ACE（インライン値）に展開された後、次のパラメータについて比較されます。
 - 送信元と宛先のゾーン
 - 送信元と宛先のネットワーク
 - 送信元/宛先ポート

[レポートのダウンロード (Download Report)] をクリックして、ACL 名と、対応する冗長 ACL およびシャドウされた ACL を Excel ファイルで表形式で確認します。ACL の詳細情報を表示するには、[詳細な ACL 情報 (Detailed ACL Information)] シートを使用します。

オブジェクトの最適化

次のオブジェクトは、移行プロセス中にオブジェクトの最適化について考慮されます。

- 未参照のオブジェクト：移行の開始時に、未参照のオブジェクトを移行しないように選択できます。
- 重複したオブジェクト：オブジェクトがすでに Management Center に存在する場合、重複したオブジェクトを作成する代わりに、ポリシーが再利用されます。

手順

ステップ 1 (オプション) [構成の最適化、確認および検証 (Optimize, Review and Validate Configuration)] 画面で、[ACL の最適化 (Optimize ACL)] をクリックして最適化コードを実行し、以下の操作を実行します。

- a) [はい (Yes)] をクリックして、ACL の最適化を続行します。特定された移行の冗長 ACL ルールとシャドウ ACL ルールが表示されます。

ACL 最適化の分析にかかる時間は、移行元の構成ファイルのサイズによって異なります。予測時間が表示されます。

最適化が考慮された ACL ルールの合計数の概要を示すレポートが表示されます。最適化レポートとそのコンポーネントの詳細については、[ACL 最適化のレポート \(41 ページ\)](#) を参照してください。

[冗長 ACL (Redundant ACL)] および [シャドウ ACL (Shadow ACL)] タブは、ACL 最適化レポートにデータがある場合にのみ表示されます。

ACL は、[冗長 ACL (Redundant ACL)] と [シャドウ ACL (Shadow ACL)] 両方の異なる基本ルールに表示されます。

(注) 冗長またはシャドウ ACL の下に表示される ACL エントリは、基本 ACL とは見なされません。

- b) 特定された ACL 最適化ルールをダウンロードするには、[ダウンロード (Download)] をクリックします。
- c) ルールを選択し、[アクション (Actions)] > [無効として移行 (Migrate as disabled)] または [移行しない (Do not migrate)] を選択して、いずれかのアクションを適用します。
- d) [保存 (Save)] をクリックします。
移行操作が [移行しない (Do not migrate)] から [無効として移行 (Migrate as disabled)] またはその逆になります。

次のオプションを使用して、ルールの一括選択を実行できます。

- [移行 (Migrate)] : デフォルトの状態に移行します。
- [移行しない (Do not migrate)] : ACL の移行を無視します。
- [無効として移行 (Migrate as disabled)] : [状態 (State)] フィールドが [無効 (Disable)] に設定されている ACL を移行します。
- [有効として移行 (Migrate as enabled)] : [状態 (State)] フィールドが [有効 (Enable)] に設定されている ACL を移行します。

ステップ 2 [設定の最適化、確認、および検証 (Optimize, Review and Validate Configuration)] 画面で、[アクセス制御ルール (Access Control Rules)] をクリックし、次の手順を実行します。

- a) テーブル内の各エントリについて、マッピングを確認し、それらが正しいことを確認します。

移行されたアクセスポリシールールは、プレフィックスとして ACL 名を使用し、それに ACL ルール番号を追加することで、ASA 構成ファイルにマッピングしやすくします。たとえば、ASA ACL の名前が "inside_access" の場合、ACL の最初のルール (または ACE) 行の名前は "inside_access_#1" になります。TCP または UDP の組み合わせ、拡張サービスオブジェクト、またはその他の理由でルールを拡張する必要がある場合、Cisco Secure Firewall 移行ツールは名前に番号付きサフィックスを追加します。たとえば、許可ルールが移行のために 2 つのルールへ拡張される場合、それらのルールには "inside_access_#1-1" と "inside_access_#1-2" という名前が付けられます。

サポートされていないオブジェクトを含むルールの場合、Cisco Secure Firewall 移行ツールは名前に "_UNSUPPORTED" というサフィックスを追加します。

- b) 1 つ以上のアクセス制御リストポリシーを移行しない場合は、ポリシーのボックスをオンにして行を選択し、[アクション (Actions)] > [移行しない (Do not migrate)] を選択して、[保存 (Save)] をクリックします。

移行しないことを選択したすべてのルールは、テーブルでグレー表示されます。

- c) Management Center ファイルポリシーを 1 つ以上のアクセスコントロールポリシーに適用する場合は、該当する行のボックスをオンにし、[アクション (Actions)] > [ファイルポリシー (File Policy)] を選択します。

[ファイルポリシー (File Policy)] ダイアログで、適切なファイルポリシーを選択し、選択したアクセスコントロールポリシーに適用して、[保存 (Save)] をクリックします。

- d) Management Center IPS ポリシーを 1 つ以上のアクセス コントロール ポリシーに適用する場合は、該当する行のボックスをオンにし、**[アクション (Actions)] > [IPS ポリシー (IPS Policy)]** を選択します。

[IPS ポリシー (IPS Policy)] ダイアログで、適切な IPS ポリシーと対応する変数セットを選択し、選択したアクセスコントロールポリシーに適用して、**[保存 (Save)]** をクリックします。

- e) ログイングが有効になっているアクセスコントロールルールのログイングオプションを変更する場合は、該当する行のボックスをオンにし、**[アクション (Actions)] > [ログ (Log)]** を選択します。

[ログ (Log)] ダイアログでは、接続の開始時または終了時、またはその両方でイベントのログイングを有効にできます。ログイングを有効にする場合は、接続イベントを**イベントビューア**または**Syslog**のいずれか、または両方に送信することを選択する必要があります。接続イベントをsyslogサーバに送信することを選択した場合、Management Centerですでに構成されているsyslogポリシーを**[Syslog]** ドロップダウンメニューから選択できます。

- f) [アクセスコントロール (Access Control)] テーブル内の移行されたアクセスコントロールルールのアクションを変更する場合は、該当する行のボックスをオンにし、**[アクション (Actions)] > [ルールアクション (Rule Action)]** を選択します。

[ルールアクション (Rule Action)] ダイアログの**[アクション (Actions)]** ドロップダウンで、**[ACP]** タブまたは**[プレフィルタ (Prefilter)]** タブを選択できます。

- **ACP** : アクセスコントロールルールには、システムが一致するトラフィックをどのように処理し、ログに記録するのかが指定するアクションがあります。アクセスコントロールルールに対して許可、信頼、モニタ、ブロック、またはリセット付きブロックのいずれかのアクションを実行できます。
- **Prefilter** : ルールのアクションによって、一致したトラフィックの処理とログ記録の方法が決まります。ファストパスとブロックを実行できます。

ヒント アクセス制御ルールにアタッチされている IPS およびファイルのポリシーは、**[許可 (Allow)]** オプションを除くすべてのルールアクションに対して自動的に削除されます。

ACL Rule Category : Cisco Secure Firewall 移行ツールは、CSM マネージド ASA 構成の**[ルール (Rule)]** セクションを保持し、Management Center の ACL カテゴリとして移行します。

ポリシーのキャパシティと制限の警告 : Cisco Secure Firewall 移行ツールは、移行したルールの合計 ACE カウントを、ターゲットプラットフォームでサポートされている ACE 制限と比較します。

Cisco Secure Firewall 移行ツールは比較の結果に基づいて、移行された ACE の総数がしきい値を超えた場合や、ターゲットデバイスのサポートされている制限のしきい値に近づいている場合は、視覚インジケータと警告メッセージを表示します。

ルールが**[ACE カウント (ACE Count)]** 列を超える場合は、最適化することも、移行しないことを決定することもできます。移行を完了してからこの情報を使用して、Management Center でプッシュしてから展開するまでの間に、ルールを最適化することもできます。

- (注) Cisco Secure Firewall 移行ツールは、警告があっても移行をブロックしません。ACE カウントは、昇順、降順、等しい、大なり、および小なりのフィルタリング順序シーケンスでフィルタ処理できます。
- フィルタリング条件をクリアするには、[フィルタのクリア (Clear Filter)] をクリックします。
- (注) ACE に基づいた ACL のソート順序は、表示のみを目的としています。ACL は、発生した時間順に基づいてプッシュされます。

ステップ 3 次のタブをクリックし、構成項目を確認します。

- **アクセス制御**
- [オブジェクト (Objects)] ([アクセスリストオブジェクト (Access List Objects)], [ネットワークオブジェクト (Network Objects)], [ポートオブジェクト (Port Objects)], [VPN オブジェクト (VPN Objects)], および[動的ルートオブジェクト (Dynamic-Route-Objects)])
- **NAT**
- [インターフェイス (Interfaces)]
- [ルート (Routes)]
- **DHCP**
- **SNMP**
- [サイト間 VPN トンネル (Site-to-Site VPN Tunnels)]
- [リモートアクセス VPN (Remote Access VPN)]
- **WebVPN**

(注) サイト間およびリモートアクセス VPN の設定では、VPN フィルタ設定とそれらに関連する拡張アクセスリストオブジェクトが移行され、それぞれのタブで確認できます。

アクセスリストオブジェクトには、BGP、EIGRP、および RA VPN で使用される標準 ACL と拡張 ACL が表示されます。

1つ以上の NAT ルールまたはルートインターフェイスを移行しない場合は、該当する行のボックスをオンにし、[アクション (Actions)] > [移行しない (Do not migrate)] を選択して、[保存 (Save)] をクリックします。

移行しないことを選択したすべてのルールは、テーブルでグレー表示されます。

ステップ 4 (任意) 構成の確認中に、[ネットワークオブジェクト (Network Objects)] タブ、[ポートオブジェクト (Port Objects)] タブ、または [VPN オブジェクト (VPN Objects)] タブで [アクション (Actions)] > [名前の変更 (Rename)] を選択して、ネットワークオブジェクト、ポートオブジェクト、または VPN オブジェクトの名前を変更することができます。

名前が変更されたオブジェクトを参照するアクセスルールと NAT ポリシーも、新しいオブジェクト名で更新されます。

ステップ 5 [動的ルートオブジェクト (Dynamic-Route Objects)] セクションには、移行されるすべてのサポートされているオブジェクトが表示されます。

- ポリシーリスト
- プレフィックスリスト
- ルートマップ
- コミュニティ リスト
- AS パス
- アクセス リスト

ステップ 6 [ルート (Routes)] セクションには、次のルートが表示されます。

- [スタティック (Static)] : すべての IPv4 および IPv6 スタティックルートを表示します。
- [BGP] : すべての BGP ルートを表示します。
- [EIGRP] : すべての EIGRP ルートを表示します。

EIGRP では、`more system:running` 構成がアップロードされ、キーが暗号化されていない場合、認証キーが取得されます。ソース構成でキーが暗号化されている場合は、EIGRP のインターフェイスセクションでキーを手動で指定できます。認証タイプ (暗号化、非暗号化、認証、またはなし) を選択し、それに応じてキーを指定できます。

- ECMP : すべての ECMP ゾーンおよび関連付けられた VRF を表示します。

(注) このセクションで実行できる唯一のアクションは、ECMP ゾーンの名前を変更することです。

- PBR : すべての PBR ルートを表示します。

ステップ 7 [DHCP] タブでは、次のタブを確認および検証できます。

- [DHCPサーバー (DHCP Server)] : すべての IP アドレスプールと対応するインターフェイスを確認します。
- [DHCPリレー (DHCP Relay)] : DHCP リレーサーバーの IP アドレス、DHCP サーバーが関連付けられているインターフェイス、およびリレー対応インターフェイスを確認します。
- [DDNS] : [DDNS更新方式 (DDNS Update Methods)] タブで、DDNS 方式名、タイプ、DDNS 更新間隔、および DHCP サーバーによって更新されるように設定されているレコード (A または PTR レコード) を確認します。

(注) [機能の選択 (Select Features)] ページでは、DHCP サーバーのみ、またはリレーと DDNS を一緒に選択できます。したがって、[設定の最適化、確認、検証 (Optimize, Review and Validate Configuration)] ページの [DHCPサーバー (DHCP Server)] タブに設定が表示されている場合、[DHCPリレー (DHCP Relay)] タブと [DDNS] タブは空です。

ステップ 8 [SNMP] タブでは、次のタブを確認、検証、および操作できます。

ASA デバイスに SNMPV1/V2 または SNMPV3 設定があるかどうかに基づいて、設定は [SNMPV1/V2] タブまたは [SNMPV3] タブに表示されます。

SNMPV1/V2 :

- [ホストサーバー名 (Host Server Name)] : SNMP ホストの名前
- [IPアドレス (IP Address)] : SNMP ホストの IP アドレス
- [コミュニティストリング (Community String)] : 手動で指定する必要がある SNMP コミュニティストリング。ホストを選択し、[アクション (Actions)] > [コミュニティストリングの更新 (Update Community String)] に移動して、コミュニティストリングを指定します。これは、SNMP サービスに設定されたコミュニティまたはユーザ名と同じである必要があります。
- [検証状態 (Validation State)] : ターゲット管理センターで作成されるホストサーバーの検証状態

SNMPv3 :

- [ユーザー名 (User Name)] : SNMP ホストのユーザー名
- [認証パスワード (Authentication Password)] : [アクション (Actions)] をクリックして、ユーザーの認証パスワードを指定します
- [暗号化パスワード (Encryption Password)] : [アクション (Actions)] をクリックして、ユーザーのプライバシーパスワードを指定します
- [検証状態 (Validation State)] : ターゲット管理センターで作成されるユーザーの検証状態

ステップ 9 [サイト間VPNトンネル (Site-to-Site VPN Tunnels)] セクションには、ASA から Management Center に移行されるサポート対象の VPN トンネルがすべて表示され、次のリストが示されます。

- クリプトマップとルートベース (VTI) の VPN トンネル。
- 認証タイプの VPN トンネルの事前共有キーおよび証明書ベースの認証。

すべての行を検証するために、各 VPN トポロジの事前共有キーと PKI オブジェクトの値を入力する必要があります。更新に失敗すると不完全とマークされ、Cisco Secure Firewall 移行ツールは検証に進むことができません。

(注) ライブ接続 ASA の場合、事前共有キーは移行ツールによって自動的に取得されます。手動でアップロードされた設定の場合は、**more system: running-config** を使用して非表示のキーを取得し、[事前共有キー (Pre-shared Key)]列に手動で入力します。

(注) ASA から Management Center へのトラストポイントまたは PKI オブジェクトの移行は、移行前アクティビティの一環であり、証明書ベースの VPN 移行を正常に実行するために不可欠です。

ステップ 10 [リモートアクセスVPN (Remote Access VPN)] セクションでは、リモートアクセス VPN に対応するすべてのオブジェクトが ASA から管理センターに移行され、次のように表示されます。

- Anyconnect パッケージ : AnyConnect パッケージ、Hostscan ファイル (Dap.xml、Data.xml、Hostscan Package)、外部ブラウザパッケージ、および AnyConnect プロファイルは、移行用に送信元 ASA デバイスから取得する必要があります。

移行前のアクティビティの一環として、すべての AnyConnect パッケージを管理センターにアップロードします。AnyConnect プロファイルは、管理センターに直接アップロードするか、Cisco Secure Firewall 移行ツールからアップロードすることができます。

管理センターから取得した既存の Anyconnect、Hostscan、または外部ブラウザパッケージを選択します。1 つ以上の AnyConnect パッケージを選択する必要があります。送信元の構成で使用可能な場合は、Hostscan、dap.xml、data.xml、または外部ブラウザを選択する必要もあります。AnyConnect プロファイルはオプションです。

正しい dap.xml ファイルが、送信元のファイアウォールから取得されている必要があります。検証は、構成ファイルで使用可能な dap.xml で実行されます。検証に必要なすべてのファイルを選択してアップロードする必要があります。更新に失敗すると不完全とマークされ、Cisco Secure Firewall 移行ツールは検証に進みません。

- [AAA] : Radius、LDAP、AD、LDAP、SAML、およびローカルレルムタイプの認証サーバーが表示されます。すべての AAA サーバーのキーを更新します。Cisco Secure Firewall 移行ツール 3.0 以降、Live Connect ASA の事前共有キーは自動的に取得されます。**more system: running-config** ファイルを使用して、隠しキーを含む送信元の構成をアップロードすることもできます。AAA 認証キーをクリアテキスト形式で取得するには、次の手順を実行します。

(注) これらの手順は、Cisco Secure Firewall 移行ツールの外部で実行する必要があります。

1. SSH コンソールを介して ASA に接続します。
2. `more system:running-config` コマンドを入力します。
3. **aaa-server and local user** セクションに移動してクリアテキスト形式のすべての AAA 構成と対応するキー値を見つけます。

```
ciscoASA#more system:running-config
```

```
!
```

```

aaa-server Test-RADIUS (inside) host 2.2.2.2

key <key in clear text> <-----The radius key is now displayed in clear text
format.

aaa-server Test-LDAP (inside) host 3.3.3.3

ldap-login-password <クリアテキストのパスワード> <-----LDAP/AD/LDAPS パスワードがクリア
テキスト形式で表示されるようになりました。

username Test_User password <Password in clear text> <-----The Local user
password is shown in clear text.

```

(注) ローカルユーザーのパスワードが暗号化されている場合は、パスワードを内部で確認するか、または Cisco Secure Firewall 移行ツールで新しいパスワードを構成できます。

- LDAPS では、管理センターにドメインが必要です。暗号化タイプ LDAPS のドメインを更新する必要があります。
- AD サーバーの Management Center には、一意の AD プライマリドメインが必要です。一意のドメインが識別されると、Cisco Secure Firewall 移行ツールに表示されます。競合が見つかった場合、オブジェクトを正常にプッシュするには、一意の AD プライマリドメインを入力する必要があります。

暗号化が LDAPS に設定されている AAA サーバーの場合、ASA は IP とホスト名またはドメインをサポートしますが、管理センターはホスト名またはドメインのみをサポートしません。ASA 構成にホスト名またはドメインが含まれている場合、それらが取得されて表示されます。ASA 構成に LDAPS の IP アドレスが含まれている場合は、[リモートアクセス VPN (Remote Access VPN)] の下の [AAA] セクションにドメインを入力します。AAA サーバーの IP アドレスに解決できるドメインを入力する必要があります。

タイプが AD の AAA サーバー（サーバータイプは ASA 構成で Microsoft）の場合、[AD プライマリドメイン (AD Primary Domain)] は管理センターで構成する必須フィールドです。このフィールドは ASA では個別に構成されず、ASA の LDAP-base-dn 構成から抽出されます。

If the ldap-base-dn is: ou=Test-Ou,dc=gcevpn,dc=com

[AD プライマリドメイン (AD Primary Domain)] は、プライマリドメインを形成する dc、dc=gcevpn、dc=com で始まるフィールドです。AD プライマリドメインは gcevpn.com になります。

LDAP-base-dn のサンプルファイル：

cn=asa,OU=ServiceAccounts,OU=abc,dc=abc,dc=com:

ここで、dc=abc と dc=com が abc.com として結合され、AD プライマリドメインが形成されます。

cn=admin, cn=users, dc=fwsecurity, dc=cisco, dc=com:

AD プライマリドメインは fwsecurity.cisco.com です。

AD プライマリドメインは自動的に取得され、Cisco Secure Firewall 移行ツールに表示されます。

(注) AD プライマリドメインの値は、レムオブジェクトごとに一意である必要があります。競合が検出された場合か、または Firewall 移行ツールが ASA 構成で値を見つけられない場合は、特定のサーバーの AD プライマリドメインを入力するように求められます。AD プライマリドメインを入力して構成を検証します。

- [アドレスプール (Address Pool)] : ここに表示されるすべての IPv4 プールと IPv6 プールを確認します。
- [グループポリシー (Group-Policy)] : この領域からユーザープロファイル、管理プロファイル、およびクライアント モジュール プロファイルを選択または削除します。この領域には、クライアントプロファイルを持つグループポリシー、管理プロファイル、クライアントモジュール、およびプロファイルを持たないグループポリシーが表示されます。プロファイルが [AnyConnectファイル (AnyConnect file)] 領域に追加されている場合は、事前に選択された状態で表示されます。ユーザープロファイル、管理プロファイル、およびクライアント モジュール プロファイルを選択または削除できます。

特定のグループポリシーに関連するカスタム属性は、[AnyConnectカスタム属性 (AnyConnect Custom Attribute)] タブに表示されます。カスタム属性を選択して検証できます。

- [接続プロファイル (Connection Profile)] : ここに表示されるすべての接続プロファイル/トンネルグループを確認します。
- [トラストポイント (Trustpoints)] : ASAから管理センターへのトラストポイントまたは PKI オブジェクトの移行は、移行前アクティビティの一環であり、リモートアクセス VPN の移行を正常に実行するために不可欠です。[リモートアクセスインターフェイス (Remote Access Interface)] セクションでグローバル SSL、IKEv2、およびインターフェイスのトラストポイントをマッピングして、移行を続行します。LDAPS プロトコルが有効になっている場合、グローバル SSL と IKEv2 トラストポイントは必須です。

SAML オブジェクトが存在する場合、SAML IDP と SP のトラストポイントを SAML セクションでマッピングできます。SP 証明書のアップロードはオプションです。特定のトンネルグループについては、トラストポイントをオーバーライドすることもできます。オーバーライドされた SAML トラストポイント構成が送信元 ASA で使用可能な場合は、[SAML のオーバーライド (Override SAML)] で選択できます。

ASA からの PKI 証明書のエクスポートについては、「[ASA からの PKI 証明書のエクスポートと管理センターへのインポート](#)」を参照してください。

- [証明書マップ (Certificate Maps)] : ここに証明書マップが表示されます。
- [VPNロードバランシング (VPN Load Balancing)] : VPN ロードバランシングの構成がここに表示されます。

VPN ロードバランシングでは、**more system: running-config** 構成がアップロードされた場合、Cisco Secure Firewall 移行ツールは暗号化キーをフェッチします。[アクション

(Actions)]> [キーの更新 (Update Keys)]を使用して、暗号化キーを手動で更新できません。

- 移行ツールは、[WebVPN] タブの下に、送信元 ASA デバイスで検出されたすべての WebVPN ポリシーを一覧表示します。WebVPN ポリシーには、SSL クライアントレス VPN トンネルプロトコルが設定された ASA グループポリシーと、SAML 認証を使用するポリシーを参照するトンネルグループが含まれます。続行する前に、WebVPN 設定に関連付けられているタブを確認してください。
 - [ゼロトラストアプリケーションポリシー (Zero Trust Application Policy)] : ポリシーを選択し、[アクション (Actions)]> [ゼロトラストポリシーの更新 (Update Zero Trust Policy)] フィールドに移動して、別の値を指定します
 - [ポリシー名 (Policy Name)] : 移行されるポリシーの名前。
 - [ドメイン名 (Domain Name)] : 手動で指定する必要があるユーザー定義のドメイン名。このドメイン名は、プライベートアプリケーションにアクセスする Threat Defense インターフェイスを解決します。このドメイン名は、アプリケーショングループ内のすべてのプライベートアプリケーションの ACS URL を生成するために使用されます。
 - [アイデンティティ証明書 (Identity Certificate)] : 移行前にターゲット管理センターにインポートしたアイデンティティ証明書。これは、移行前タスクの一部として実行する必要があります。
 - [セキュリティゾーン (Security Zones)] : ポリシーに関連付けられている対応するセキュリティゾーン。
 - [グローバルポートプール (Global Port Pool)] : ポリシーのポート範囲。このプールの一意のポートは、各プライベートアプリケーションに割り当てられます。
 - Application Group
 - [アプリケーショングループ (Application Group)] : アプリケーショングループ名、再認証間隔、セキュリティゾーンなどの [アプリケーショングループ設定 (Application Group Settings)] を確認します。

[SAML IdP メタデータ (SAML IdP Metadata)] タブでは、アプリケーショングループ名、サービスプロバイダーのエンティティ ID、SAML アイデンティティプロバイダー (IdP) のシングルサインオン URL、および IdP 証明書を手動で設定するか、[後で設定 (Configure Later)] を選択できます

[アプリケーション (Applications)] タブでは、アプリケーション名、外部 URL、アプリケーション URL、アプリケーション証明書、アプリケーショングループなどのアプリケーション固有の設定を確認または設定できます。
 - [スタンドアロンアプリケーション (Standalone Applications)] : アプリケーション名、外部 URL、アプリケーション URL、アプリケーション証明書、再認証間隔、セキュリティゾーンなど、スタンドアロンアプリケーションの [アプリケーション設定 (Application Settings)] を確認または設定します。[SAML IdP メタデータ (SAML IdP

Metadata)] タブでは、スタンドアロンアプリケーションの IdP メタデータ設定を手動で設定するか、後で設定できます。タブには、アプリケーショングループ名、エンティティ ID、シングルサインオン URL、および IdP 証明書が含まれます。

フィールドを更新するには、[アクション (Actions)] をクリックし、さまざまなフィールドの更新を選択します。

移行が成功したら、管理センターに移行した設定をすべて確認し、準備ができれば Threat Defense デバイスに展開します。

ステップ 11 (任意) グリッド内の各構成項目の詳細をダウンロードするには、[ダウンロード (Download)] をクリックします。

ステップ 12 確認が完了したら、[検証 (Validate)] をクリックします。注意が必要な必須フィールドは、値を入力するまで点滅し続けることに注意してください。[検証 (Validate)] ボタンは、すべての必須フィールドに入力した後にのみ有効になります。

検証中、Cisco Secure Firewall 移行ツールは Management Center に接続し、既存のオブジェクトを確認し、それらのオブジェクトを移行対象オブジェクトのリストと比較します。オブジェクトがすでに Management Center に存在する場合、Cisco Secure Firewall 移行ツールは次の処理を実行します。

- オブジェクトの名前と構成が同じ場合、Cisco Secure Firewall 移行ツールは既存のオブジェクトを再利用し、Management Center に新しいオブジェクトを作成しません。
- オブジェクトの名前が同じで構成が異なる場合、Cisco Secure Firewall 移行ツールはオブジェクトの競合を報告します。

検証の進行状況はコンソールで確認できます。

ステップ 13 検証が完了し、[検証ステータス (Validation Status)] ダイアログボックスに 1 つ以上のオブジェクトの競合が表示された場合は、次の手順を実行します。

a) [競合の解決 (Resolve Conflicts)] をクリックします。

Cisco Secure Firewall 移行ツールは、オブジェクトの競合が報告された場所に応じて、[ネットワークオブジェクト (Network Objects)] タブまたは [ポートオブジェクト (Port Objects)] タブのいずれかまたは両方に警告アイコンを表示します。

b) タブをクリックし、オブジェクトを確認します。

c) 競合がある各オブジェクトのエントリを確認し、[アクション (Actions)] > [競合の解決 (Resolve Conflicts)] を選択します。

d) [競合の解決 (Resolve Conflicts)] ウィンドウで、推奨アクションを実行します。

たとえば、既存の Management Center オブジェクトとの競合を避けるために、オブジェクト名にサフィックスを追加するように求められる場合があります。デフォルトのサフィックスを受け入れるか、独自のサフィックスに置き換えることができます。

e) [解決 (Resolve)] をクリックします。

f) タブ上のすべてのオブジェクトの競合を解決したら、[保存 (Save)] をクリックします。

- g) [検証 (Validate)]をクリックして構成を再検証し、すべてのオブジェクトの競合を解決したことを確認します。

ステップ 14 検証が完了し、[検証ステータス (Validation Status)]ダイアログボックスに「Successfully Validated」というメッセージが表示されたら、移行された構成の以下へのプッシュ：[Management Center \(42 ページ\)](#)に進みます。

ACL 最適化のレポート

ACL 最適化レポートには、次の情報が表示されます。

- **Summary シート**：ACL 最適化のサマリーが表示されます。

Sl.no	ACL name	Redundant ACLs	Shadowed ACLs
1	outsideACL_#1		outsideACL_#2, outsideACL_#3, outsideACL_#4, outsideACL_#5, outsideACL_#6, outsideACL_#7, outsideACL_#8, outsideACL_#9, outsideACL_#10, outsideACL_#11, outsideACL_#12
2	outsideACL_#13		outsideACL_#17, outsideACL_#18
3	outsideACL_#14		outsideACL_#15, outsideACL_#16, outsideACL_#17, outsideACL_#18
4	outsideACL_#19		outsideACL_#20, outsideACL_#21, outsideACL_#22, outsideACL_#23, outsideACL_#24
5	outsideACL_#25		outsideACL_#27, outsideACL_#28, outsideACL_#29, outsideACL_#30
6	outsideACL_#26		
7	outsideACL_#31		outsideACL_#32, outsideACL_#33
8	outsideACL_#34		
9	dmzACL_#1		
10	dmzACL_#2	dmzACL_#5	
11	dmzACL_#3		dmzACL_#5
12	dmzACL_#4		
13	dmzACL_#6		dmzACL_#7, dmzACL_#8, dmzACL_#9, dmzACL_#10
14	dmzACL_#11		dmzACL_#13
15	dmzACL_#12		
16	extACL_#1		
17	extACL_#2		
18	extACL_#3		extACL_#4, extACL_#5, extACL_#6
19	extACL_#7		
20	extACL_#8	extACL_#9, extACL_#10	
21	extACL_#11		
22	extACL_#12	extACL_#13	
23	extACL_#14		
24	extACL_#15		
25	extACL_#16		
26	extACL_#17		extACL_#18, extACL_#19
27	localtoremove_#1		
28	opt_#1		opt_#3
29	opt_#2	opt_#4	opt_#5
30	opt_#6-1	opt_#17-1	opt_#7-1, opt_#8-1
31	opt_#9-1	opt_#10-1	
32	opt_#11-1	opt_#12-1	opt_#13-1
33	opt_#14-1		opt_#15-1, opt_#16-1
34	opt_#18		
35	opt_#19		opt_#20, opt_#21
36	opt_#22-1	opt_#23-1	
37			

- **Detailed ACL Information**：ベース ACL の詳細が表示されます。各 ACL には、比較対象の基本の ACL と最適化カテゴリとの関連付けを識別する ACL タイプ（シャドウまたは冗長）のタグが付いています。

移行された構成の以下へのプッシュ : Management Center

Sl.no	ACL name	Source zone	Destination zone	Source network	Destination network	Source port	Destination port	Action	ACL type
1	1 outsideACL_#1	outside	ANY	any	10.0.0.0/8	ANY	ANY	permit	
2	outsideACL_#2	outside	ANY	any	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
4	outsideACL_#3	outside	ANY	192.168.0.1	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
5	outsideACL_#4	outside	ANY	192.168.0.10	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
6	outsideACL_#5	outside	ANY	any	10.1.1.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
7	outsideACL_#6	outside	ANY	any	10.1.1.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
8	outsideACL_#7	outside	ANY	any	10.1.1.0/24	ANY	tcp:80	permit	Shadowed by outsideACL_#1
9	outsideACL_#8	outside	ANY	any	10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
10	outsideACL_#9	outside	ANY	200.200.200.1	10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
11	outsideACL_#10	outside	ANY	10.10.10.10, 10.10.0.0/16	10.10.0.0/19, 10.99.99.99, 10.99.99.90, 10.99.99.99, 10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
12	outsideACL_#11	outside	ANY	any	10.99.99.90, 10.99.99.99, 10.10.10.10, 10.10.0.0/16, 10.99.99.99, 10.10.10.10, 10.10.0.0/16, 10.99.99.99, 10.10.10.10, 10.10.0.0/16, 10.10.0.0/16, 10.10.0.0/19	ANY	ANY	permit	Shadowed by outsideACL_#1
14	2 outsideACL_#13	outside	ANY	any	192.168.0.0/16	ANY	ANY	permit	
15	outsideACL_#17	outside	ANY	10.10.1.1	192.168.0.0/16	ANY	tcp:443	permit	Shadowed by outsideACL_#13
16	outsideACL_#18	outside	ANY	10.10.1.1	192.168.0.0/16	ANY	tcp:80	permit	Shadowed by outsideACL_#13

移行された構成の以下へのプッシュ : Management Center

構成の検証に成功せず、すべてのオブジェクトの競合を解決していない場合は、移行された ASA 構成を Management Center にプッシュできません。

移行プロセスのこのステップでは、移行された構成を Management Center に送信します。脅威に対する防御 デバイスに構成を展開しません。ただし、脅威に対する防御 上の既存の構成はこのステップで消去されます。



(注) Cisco Secure Firewall 移行ツールが移行された構成を Management Center に送信している間は、構成を変更したり、デバイスに展開したりしないでください。

手順

ステップ 1 [検証ステータス (Validation Status)] ダイアログボックスで、検証の概要を確認します。

ステップ 2 [構成のプッシュ (Push Configuration)] をクリックして、移行した ASA 構成を Management Center に送信します。

Cisco Secure Firewall 移行ツールの新しい最適化機能を使用すると、検索フィルタを使用して移行結果を迅速に取得できます。

Cisco Secure Firewall 移行ツールは、CSV ダウンロードを最適化し、ページビューごとにまたはすべてのルールにアクションを適用することもできます。

Cisco Secure Firewall 移行ツールに、移行の進行状況の概要が表示されます。コンソールに、Management Center にプッシュされているコンポーネントの詳細な進行状況を行ごとに表示できます。

ステップ 3 移行が完了したら、[レポートのダウンロード (Download Report)] をクリックして、移行後レポートをダウンロードして保存します。

移行後レポートのコピーも、Cisco Secure Firewall 移行ツールと同じ場所にある Resources フォルダに保存されます。

ステップ 4 移行が失敗した場合は、移行後レポート、ログファイル、および未解析ファイルを慎重に確認して、失敗の原因を把握します。

トラブルシューティングについては、サポートチームに問い合わせることもできます。

移行の失敗のサポート

移行に失敗する場合は、サポートにお問い合わせください。

1. [移行完了 (Complete Migration)] 画面で、[サポート (Support)] ボタンをクリックします。

ヘルプサポートページが表示されます。

2. [サポートバンドル (Support Bundle)] チェックボックスをオンにして、ダウンロードする構成ファイルを選択します。

(注) ログファイルと DB ファイルは、デフォルトでダウンロード用に選択されています。

3. [ダウンロード (Download)] をクリックします。

サポートバンドルファイルは、ローカルパスに .zip としてダウンロードされます。Zip フォルダを抽出して、ログファイル、DB、および構成ファイルを表示します。

4. [Email us] をクリックして、テクニカルチームに障害の詳細を電子メールで送信します。

ダウンロードしたサポートファイルを電子メールに添付することもできます。

5. [TAC ページに移動 (Visit TAC page)] をクリックして、シスコのサポートページで TAC ケースを作成します。

(注) TAC ケースは、移行中にいつでもサポートページからオープンできます。

移行後レポートの確認と移行の完了

移行後のレポートには、さまざまなカテゴリの ACL カウント、ACL 最適化、および構成ファイルで実行された最適化の全体的なビューに関する詳細が表示されます。詳細については、[最適化、構成の確認と検証 \(28 ページ\)](#) を参照してください。

オブジェクトを確認して検証します。

• カテゴリ

• ACL ルール合計数 (移行元の構成)

• 最適化の対象とみなされる ACL ルールの合計数。冗長、シャドウなどがあります。

- 最適化の ACL カウントは、最適化の前後にカウントされた ACL ルールの合計数を示します。

移行中に移行後レポートをダウンロードし忘れた場合は、次のリンクを使用してダウンロードしてください。

移行後レポートのダウンロードエンドポイント：http://localhost:8888/api/downloads/post_migration_summary_html_format



(注) レポートは、Cisco Secure Firewall 移行ツールの実行中にのみダウンロードできます。

手順

ステップ 1 移行後レポートをダウンロードした場所に移動します。

ステップ 2 移行後レポートを開き、その内容を慎重に確認して、ASA 構成がどのように移行されたかを理解します。

- **Migration Summary** : ASA から脅威に対する防御へ正常に移行された構成の概要。ASA インターフェイス、Management Center ホスト名とドメイン、ターゲット脅威に対する防御デバイス（該当する場合）、および正常に移行された構成要素に関する情報が含まれます。
- **Selective Policy Migration** : 移行用に選択された特定の ASA 機能の詳細は、[デバイス構成機能 (Device Configuration Features)]、[共有構成機能 (Shared Configuration Features)]、および [最適化 (Optimization)] の 3 つのカテゴリ内で使用できます。
- **ASA Interface to Threat Defense Interface Mapping** : 正常に移行されたインターフェイスの詳細と、ASA 構成のインターフェイスを脅威に対する防御デバイスのインターフェイスにマッピングした方法。これらのマッピングが期待どおりであることを確認します。

(注) このセクションは、宛先脅威に対する防御デバイスを使用しない移行、または移行にインターフェイスが選択されていない場合には適用されません。
- **Source Interface Names to Threat Defense Security Zones and Interface Groups** : 正常に移行された ASA 論理インターフェイスと名前の詳細、およびそれらを脅威に対する防御のセキュリティゾーンとインターフェイスグループにマッピングした方法。これらのマッピングが期待どおりであることを確認します。

(注) アクセス制御リストと NAT が移行に選択されていない場合、このセクションは適用されません。
- **Object Conflict Handling** : Management Center の既存のオブジェクトと競合していると識別された ASA オブジェクトの詳細。オブジェクトの名前と設定が同じ場合、Cisco Secure Firewall 移行ツールは Management Center オブジェクトを再利用しています。オブジェクトの名前が同じで構成が異なる場合は、管理者がそれらのオブジェクトの名前を変更してい

ます。これらのオブジェクトを慎重に確認し、競合が適切に解決されたことを確認します。

- **Access Control Rules, NAT, and Routes You Chose Not to Migrate** : Cisco Secure Firewall 移行ツールで移行しないように選択したルールの詳細。Cisco Secure Firewall 移行ツールによって無効化され、移行されなかったこれらのルールを確認します。これらの行を確認し、選択したすべてのルールがこのセクションにリストされていることを確認します。必要に応じて、これらのルールを手動で構成できます。
- **Partially Migrated Configuration** : 詳細オプションなしでもルールを移行できる詳細オプション付きルールを含む、一部のみ移行された ASA ルールの詳細。これらの行を確認し、詳細オプションが Management Center でサポートされているかどうかを確認します。サポートされている場合は、これらのオプションを手動で構成します。
- **Unsupported Configuration** : Cisco Secure Firewall 移行ツールがこれらの機能の移行をサポートしていないため、移行されなかった ASA 構成要素の詳細。これらの行を確認し、各機能が脅威に対する防御でサポートされているかどうかを確認します。その場合は、Management Center でこれらの機能を手動で構成します。
- **Expanded Access Control Policy Rules** : 移行時に単一の ASA Point ルールから複数の脅威に対する防御ルールに拡張された ASA アクセスコントロールポリシールールの詳細。
- **Actions Taken on Access Control Rules**
 - **Access Rules You Chose Not to Migrate** : Cisco Secure Firewall 移行ツールで移行しないように選択した ASA アクセスコントロールルールの詳細。これらの行を確認し、選択したすべてのルールがこのセクションにリストされていることを確認します。必要に応じて、これらのルールを手動で構成できます。
 - **Access Rules with Rule Action Change** : Cisco Secure Firewall 移行ツールを使用して「ルールアクション」が変更されたすべてのアクセスコントロールポリシールールの詳細。ルールアクションの値は、Allow、Trust、Monitor、Block、Block with reset です。これらの行を確認し、選択したすべてのルールがこのセクションにリストされていることを確認します。必要に応じて、これらのルールを手動で構成できます。
 - **Access Control Rules that have IPS Policy and Variable Set Applied** : IPS ポリシーが適用されているすべての ASA アクセスコントロールポリシールールの詳細。これらのルールを慎重に確認し、この機能が脅威に対する防御でサポートされているかどうかを確認します。
 - **Access Control Rules that have File Policy Applied** : ファイルポリシーが適用されているすべての ASA アクセスコントロールポリシールールの詳細。これらのルールを慎重に確認し、この機能が脅威に対する防御でサポートされているかどうかを確認します。
 - **Access Control Rules that have Rule 'Log' Setting Change** : Cisco Secure Firewall 移行ツールを使用して「ログ設定」が変更された ASA アクセスコントロールルールの詳細。ログ設定の値は、False、Event Viewer、Syslog です。これらの行を確認し、選択したすべてのルールがこのセクションにリストされていることを確認します。必要に応じて、これらのルールを手動で構成できます。

- **Access Control Rules that have failed Zone-lookup** : ルートルックアップ操作に失敗し、**移行後レポート**に入力される ASA アクセスコントロールルールの詳細。Cisco Secure Firewall 移行ツールは、送信元構成のルート（静的および接続）情報に基づいてルートルックアップ操作を実行し、アクセスルールに宛先セキュリティゾーンを設定します。
- **Access Control Rules for Tunneled Protocols** : 移行時にプレフィルタトンネルルールとして移行されるトンネルルールの詳細。

- (注) サポートされていないルールが移行されなかった場合、不要なトラフィックがファイアウォールを通過する問題が発生します。このトラフィックが脅威に対する防御によってブロックされるように、**Management Center** でルールを構成することを推奨します。
- (注) [確認と検証 (Review and Validate)] ページで IPS またはファイルポリシーを ACL に適用する必要がある場合は、移行前に管理センターでポリシーを作成することを強くお勧めします。Cisco Secure Firewall 移行ツールは接続された管理センターからポリシーを取得するため、同じポリシーを使用します。新しいポリシーを作成して複数のポリシーに割り当てると、パフォーマンスが低下し、プッシュが失敗する可能性があります。

Management Center と脅威に対する防御でサポートされる機能の詳細については、『[Management Center Configuration Guide, Version 6.2.3](#)』 [英語] を参照してください。

ステップ 3 移行前レポートを開き、脅威に対する防御 デバイスで手動で移行する必要がある ASA 構成項目をメモします。

ステップ 4 Management Center で、次の手順を実行します。

- a) 脅威に対する防御デバイスの移行された構成を確認し、次を含むすべての期待されるルールおよびその他の構成項目が移行されたことを確認します。
- アクセス制御リスト (ACL)
 - ネットワークアドレス変換規則
 - ポートおよびネットワークオブジェクト
 - ルート (Routes)
 - インターフェイス
 - IP SLA オブジェクト
 - オブジェクトグループの検索
 - 時間ベースのオブジェクト
 - VPN オブジェクト
 - [サイト間 VPN トンネル (Site-to-Site VPN Tunnels)]
 - 動的ルートオブジェクト

- b) 一部がサポートされている、サポートされていない、無視された、無効化された、および移行されなかったすべての構成項目とルールを構成します。

これらの項目とルールを構成する方法の詳細については、『[Management Center Configuration Guide](#)』[英語]を参照してください。手動構成が必要な構成項目の例を次に示します。

- プラットフォーム設定 (SSH アクセスと HTTPS アクセスを含む) (「[Threat Defense プラットフォーム設定](#)」を参照)
- Syslog 設定 (「[Configure Syslog](#)」を参照)
- 動的ルーティング (「[Routing Overview for Threat Defense](#)」を参照)
- サービスポリシー (「[FlexConfig Policies](#)」を参照)
- VPN 構成 (「[Threat Defense VPN](#)」を参照)
- 接続ログ設定 (「[Connection Logging](#)」を参照)

ステップ 5 確認が完了したら、Management Center から脅威に対する防御 デバイスに移行された構成を展開します。

サポートされていないルールと一部がサポートされているルールについて、データが**移行後レポート**に正しく反映されていることを確認します。

Cisco Secure Firewall 移行ツールは、ポリシーを脅威に対する防御 デバイスに割り当てます。変更が実行中の構成に反映されていることを確認します。移行されるポリシーを識別しやすくするために、これらのポリシーの説明には ASA 構成のホスト名が含まれています。

Cisco Secure Firewall 移行ツールのアンインストール

すべてのコンポーネントは、Cisco Secure Firewall 移行ツールと同じフォルダに保存されます。

手順

ステップ 1 Cisco Secure Firewall 移行ツールを配置したフォルダに移動します。

ステップ 2 ログを保存する場合は、log フォルダを切り取りまたはコピーして別の場所に貼り付けます。

ステップ 3 移行前レポートと移行後レポートを保存する場合は、resources フォルダを切り取りまたはコピーして別の場所に貼り付けます。

ステップ 4 Cisco Secure Firewall 移行ツールを配置したフォルダを削除します。

ヒント ログファイルはコンソールウィンドウに関連付けられています。Cisco Secure Firewall 移行ツールのコンソールウィンドウが開いている場合、ログファイルとフォルダは削除できません。

移行例 : ASA から Threat Defense 2100 へ



(注) 移行の完了後にターゲットデバイスで実行できるテスト計画を作成します。

- [メンテナンス期間前のタスク](#)
- [メンテナンス期間のタスク](#)

メンテナンス期間前のタスク

始める前に

Management Center をインストールして展開していることを確認します。詳細については、適切な『[Management Center Hardware Installation Guide](#)』[英語] および適切な『[Management Center Getting Started Guide](#)』[英語] を参照してください。

手順

- ステップ 1** 移行する ASA デバイスまたはコンテキストに対して **show running-config** コマンドを使用し、ASA 構成のコピーを保存します。「[View the Running Configuration](#)」を参照してください。
- または、移行する ASA デバイスまたはコンテキストに対して Adaptive Security Device Manager (ASDM) を使用し、[ファイル (File)] > [新しいウィンドウに実行構成を表示する (Show Running Configuration in New Window)] を選択して、構成ファイルを取得します。
- (注) マルチコンテキスト ASA の場合は、**show tech-support** コマンドを使用して、すべてのコンテキストの構成を単一ファイルに取得できます。
- ステップ 2** ASA 構成ファイルを確認します。
- ステップ 3** ネットワークに Firepower 2100 シリーズデバイスを展開し、インターフェイスを接続してアプライアンスの電源をオンにします。
- 詳細については、『[Cisco Threat Defense for the 2100 Series Using Management Center Quick Start Guide](#)』[英語] を参照してください。
- ステップ 4** Management Center によって管理される Firepower 2100 シリーズデバイスを登録します。
- 詳細については、「[Add Devices to the Management Center](#)」を参照してください。
- ステップ 5** (任意) 送信元 ASA 構成にポートチャネルがある場合は、ターゲット Firepower 2100 シリーズデバイスでポートチャネル (EtherChannel) を作成します。
- 詳細については、「[Configure EtherChannels and Redundant Interfaces](#)」を参照してください。

- ステップ 6** Cisco Secure Firewall 移行ツールの最新バージョンを <https://software.cisco.com/download/home/286306503/type> からダウンロードして実行します。
- 詳細については、[Cisco.com](#) からの [Cisco Secure Firewall 移行ツールのダウンロード \(4 ページ\)](#) を参照してください。
- ステップ 7** Cisco Secure Firewall 移行ツールを起動し、接続先パラメータを指定する場合は、Management Center に登録した Firepower 2100 シリーズ デバイスを選択します。
- 詳細については、[Cisco Secure Firewall 移行ツールの接続先パラメータの指定 \(15 ページ\)](#) を参照してください。
- ステップ 8** ASA インターフェイスを 脅威に対する防御 インターフェイスにマッピングします。
- (注) Cisco Secure Firewall 移行ツールを使用すると、ASA インターフェイスタイプを 脅威に対する防御 インターフェイスタイプにマッピングできます。
- たとえば、ASA のポートチャネルを 脅威に対する防御 の物理インターフェイスにマッピングできます。
- 詳細については、「[ASA 構成と Threat Defense インターフェイスのマッピング](#)」を参照してください。
- ステップ 9** 論理インターフェイスをセキュリティゾーンにマッピングするときに、[自動作成 (Auto-Create)] をクリックして、Cisco Secure Firewall 移行ツールで新しいセキュリティゾーンを作成できるようにします。既存のセキュリティゾーンを使用するには、手動で ASA 論理インターフェイスをセキュリティゾーンにマッピングします。
- 詳細については、「[セキュリティゾーン、インターフェイスグループ、および VRF への ASA インターフェイスのマッピング](#)」を参照してください。
- ステップ 10** このガイドの手順に従って、移行する構成を順に確認および検証し、構成を Management Center にプッシュします。
- ステップ 11** 移行後レポートを確認し、手動で他の構成をセットアップして 脅威に対する防御 に展開し、移行を完了します。
- 詳細については、「[移行後レポートの確認と移行の完了 \(43 ページ\)](#)」を参照してください。
- ステップ 12** 移行の計画時に作成したテスト計画を使用して、Firepower 2100 シリーズ デバイスをテストします。

メンテナンス期間のタスク

始める前に

メンテナンスウィンドウの前に実行する必要があるすべてのタスクが完了していることを確認します。「[メンテナンス期間前のタスク \(48 ページ\)](#)」を参照してください。

手順

- ステップ 1** SSH コンソールを介して ASA に接続し、インターフェイス構成モードに切り替えます。
- ステップ 2** **shutdown** コマンドを使用して、ASA インターフェイスをシャットダウンします。
- ステップ 3** (任意) Management Center にアクセスし、Firepower 2100 シリーズデバイスの動的ルーティングを構成します。
- 詳細については、「[Dynamic Routing](#)」を参照してください。
- ステップ 4** 周辺スイッチング インフラストラクチャの Address Resolution Protocol (ARP) キャッシュをクリアします。
- ステップ 5** 周辺スイッチング インフラストラクチャから Firepower 2100 シリーズ デバイス インターフェイスの IP アドレスに対して基本的な ping テストを実行し、アクセス可能であることを確認します。
- ステップ 6** Firepower 2100 シリーズ デバイス インターフェイスの IP アドレスに対するレイヤ 3 ルーティングが必要なデバイスから基本的な ping テストを実行します。
- ステップ 7** Firepower 2100 シリーズ デバイスに新しい IP アドレスを割り当て、ASA に割り当てられた IP アドレスを再利用しない場合は、次の手順を実行します。
1. IP アドレスを参照する静的ルートを更新し、Firepower 2100 シリーズ デバイスの IP アドレスを指すようにします。
 2. ルーティングプロトコルを使用している場合は、ネイバーが Firepower 2100 シリーズ デバイスの IP アドレスを予期される接続先のネクストホップとして認識していることを確認します。
- ステップ 8** 包括的なテスト計画を実行し、Firepower 2100 デバイスの管理 Management Center 内でログをモニタリングします。
-

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。