ASA 設定を Firepower Threat Defense 設定に移行する

移行のための ASA の準備

ステップ 1 ASA デバイスが設定の移行に関する要件を満たしていることを確認します（ASA デバイスの要件 を参照）。

ステップ 2 エクスポートするアクセス コントロール リスト（ACL）と NAT ポリシーを確認します。

ステップ 3 設定から不必要なルールをできるだけ取り除きます。変換する前に、ASA 設定の複雑さとサイズを可能な限り削減しておくことを推奨します。ACL 内にあるエントリの数を確認する方法：

```
show access-list acl_name | i elements
```

移行ツールのインストール

注意 実稼働 Firepower Management Center に移行ツールをインストール**しない**でください。このツールの使用は、実稼働デバイスではサポートされません。移行ツールのインストール後は、指定した Firepower Management Center を再イメージ化することによってのみ、ツールをアンインストールできます。

ステップ 1 サポートから次のいずれかのイメージをダウンロードします。

- Firepower Management Center Virtual for VMware
- Firepower Management Center Virtual for KVM

ステップ 2 適切なガイドに説明されているように、イメージ ファイルを使用して専用の Firepower Management Center Virtual をインストールします。

- *Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide*
- *Cisco Firepower Management Center Virtual for KVM Deployment Quick Start Guide*

ステップ 3 `admin` ユーザ名を使用して、`ssh` 経由で Firepower Management Center に接続します。

ステップ 4 ルート シェルにログインします。

```
sudo su -
```

ステップ 5 次のコマンドを実行します。

```
enableMigrationTool.pl
```

（注） プロセスの完了後、移行ツールを使用する Firepower Management Center で実行している Web インターフェイス セッションを更新します。

ASA 設定ファイルの保存

移行ツールは、ASA 設定ファイルを .cfg または .txt 形式で変換できます。

ステップ 1 設定を保存します。

この設定を保存するために使用するコマンドは、ASA デバイスのバージョンによって異なる場合があります。詳細については、http://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asaroadmap.html#pgfId-126642 の ASA ドキュメンテーション ロードマップにリストされている、適切なバージョンの ASA 構成ガイドを参照してください。

ステップ 2 保存した設定ファイルを移行ツールからアクセスできる場所（たとえば、ローカル コンピュータやネットワーク上の共有ドライブ）に移動します。

ASA 設定ファイルの変換

ASA 設定ファイル（.cfg または .txt）を Firepower 設定ファイル（.sfo）に変換するには、次の手順を実行します。

⚠

注意 移行ツール UI は、Firepower Management Center UI を拡張したものです。ただし、この手順に記載されている機能のみを実行できます。

ステップ 1 お使いのブラウザで `https://hostname/` に直接移動します。*Hostname* 要素は、移行ツールをインストールする専用の Firepower Management Center Virtual のホスト名に対応します。

ステップ 2 `admin` ユーザとしてログインします。

ステップ 3 **[システム（System）] > [ツール（Tools）] > [インポート/エクスポート（Import/Export）]** を選択します。

ステップ 4 [パッケージのアップロード（Upload Package）] をクリックします。

ステップ 5 [参照（Browse）] をクリックし、ASA からエクスポートした設定ファイルを選択します。

ステップ 6 [Next] をクリックします。

ステップ 7 アクセス ルールを変換するときにシステムに使用させるポリシーを選択します。

- [プレフィルタ ポリシー（Prefilter Policy）]：アクセス ルールをプレフィルタ ルールに変換します。
- [アクセス コントロール ポリシー（Access Control Policy）]：アクセス ルールをアクセス コントロール ルールに変換します。

ステップ 8 [プレフィルタ ポリシー（Prefilter Policy）] を選択した場合は、許可アクションを使用してシステムがアクセス ルールに割り当てるアクションを選択します。

- [高速パス（Fastpath）]：アクセス制御、ID 要件、レート制限を含む、すべての詳細な検査および制御から一致するトラフィックを免除します。トンネルを高速パス化すると、すべてのカプセル化された接続が高速パス化されます。
- [分析（Analyze）]：残りのアクセス制御によってトラフィックが引き続き分析されるようにします。アクセス制御および関連するディープ インスペクションによって渡された場合、このトラフィックはレート制限も行われる場合があります。

ステップ 9 [アクセス コントロール ポリシー（Access Control Policy）] を選択した場合は、許可アクションを使用してシステムにルールを割り当てさせるアクションを選択します。

- [信頼する（Trust）]：トラフィックはディープ インスペクションまたはネットワーク検出なしで通過できます。信頼できるトラフィックは、引き続き ID ポリシーによって課される認証要件、およびレート制限の対象となります。

- [許可（Allow）]：一致するトラフィックの通過を許可します。許可されたトラフィックは、引き続き ID ポリシーによって課される認証要件、レート制限、およびディープ インスペクション（設定されている場合）の対象となります。

ステップ 10 [次へ（Next）] を選択します。

システムは、移行をタスクとしてキューに登録します。メッセージ センターでタスクのステータスを表示できます。

ステップ 11 [システム ステータス（System Status）] アイコンをクリックして、メッセージ センターを表示します。

ステップ 12 [タスク（Tasks）] タブをクリックします。

中間 Firepower Management Center で実行できるのは移行ツールのタスクのみなので、移行タスクはトップ メッセージとしてリストされます。

ステップ 13 移行が失敗した場合は、適切なログでエラー メッセージを確認してください。詳細については、変換失敗のトラブルシューティング （4 ページ） を参照してください。

ステップ 14 移行が成功した場合：

- [.sfo をダウンロード（Download .sfo）] を選択し、変換されたファイルをローカル コンピュータにコピーします。
- [移行レポート（Migration Report）] をクリックして、移行レポートを表示します。

ステップ 15 移行レポートを確認します。

移行レポートには、移行ツールが Firepower Threat Defense 設定に正常に変換できた、または変換できなかった ASA 設定の概要が示されています。変換に失敗した設定には次のものがあります。

- Firepower システムでサポートされていない ASA 設定
- Firepower システムでサポートされている（Firepower 同等要素がある）が、移行ツールは変換しない ASA 設定

Firepower 同等要素がある変換に失敗した設定の場合は、変換されたポリシーを実稼働Firepower Management Centerにインポートした後に、手動で追加できます。

変換失敗のトラブルシューティング

変換が専用の Firepower Management Center で失敗すると、移行ツールは、トラブルシューティング ファイルにエラーデータを記録します。このデータはローカル コンピュータにダウンロードできます。

ステップ 1 **[システム（System）] > [ヘルス（Health）] > [モニタ（Monitor）]**を選択します。

ステップ 2 アプライアンス リストの [アプライアンス（Appliance）] 列で、専用の Firepower Management Center の名前をクリックします。

ステップ 3 [トラブルシューティング ファイルの生成（Generate Troubleshooting Files）] をクリックします。

ステップ 4 [すべてのデータ（All Data）] チェックボックスをオンにします。

ステップ 5 [生成（Generate）] をクリックします。
システムは、トラブルシューティング ファイルの生成をタスクとしてキューに登録します。

ステップ 6 タスクの進捗をメッセージ センターで表示して追跡します。

ステップ 7 システムがトラブルシューティング ファイルを生成し、タスク ステータスが [完了（Completed）] に変ったら、[クリックして生成されたファイルを取得（Click to retrieve generated files）] をクリックします。

ステップ 8 圧縮ファイルをローカル コンピュータに保存し、ファイルを解凍します。

ステップ 9 エラー メッセージについては、次のファイルを確認してください。

- `dir-archives/var-log/action_queue.log.#.gz`
- `dir-archives/var-log/mojo/mojo.log.#`
- `dir-archives/var-opt-CSCOpx-MDC-log-operation/usmsharedsvcs.log`
- `dir-archives/var-opt-CSCOpx-MDC-log-operation/vmsbesvcs.log`
- `dir-archives/var-opt-CSCOpx-MDC-log-operation/vmssharedsvcs.log`

変換済み ASA 設定のインポート

Firepower Management Center のマルチドメイン展開では、システムは、変換された ASA 設定を、それをインポートするドメインに割り当てます。インポート時に、変換されたオブジェクトの [ドメイン（Domain）] フィールドに値が読み込まれます。

ステップ 1 実稼働Firepower Management Centerで、**[システム（System）] > [ツール（Tools）] > [インポート/エクスポート（Import/Export）]**を選択します。

ステップ 2 [パッケージのアップロード（Upload Package）] をクリックします。

ステップ 3 [ファイルの選択（Choose File）] をクリックし、参照を使用してローカル コンピュータ上の適切な .sfo ファイルを選択します。

ステップ 4 [アップロード（Upload）] をクリックします。

ステップ 5 インポートするポリシーを選択します。ポリシーには、以前の移行の選択内容に応じて、アクセス コントロール ポリシー、プレフィルタ ポリシー、または NAT ポリシーが含まれている場合があります。

ステップ 6 [インポート（Import）] をクリックします。
システムによってファイルが分析され、[インポートの競合（Import Conflict）] ページが表示されます。

ステップ 7 [インポートの競合（Import Conflict）] ページで：

- 設定の競合を解決します。Firepower Management Center コンフィギュレーション ガイド の「Import Conflict Resolution」を参照してください。
- ルールが元の ASA 設定のインターフェイス別にどのようにグループ化されたかを再現するか、またはそのグループの関連付けを新しいものに置き換えます。これを行うには、次のように、アクセス

コントロール ルールをセキュリティ ゾーンに割り当て、プレフィルタ ルールまたは NAT ルールをインターフェイス グループに割り当てる必要があります。

タイプ（Type）	ソース（Source）	次の場合にこのゾーンまたはグループを選択します
システムによって生成されたセキュリティ ゾーン/インターフェイス グループ	移行ツールは、変換時に自動的にこのセキュリティ ゾーン/インターフェイス グループを作成します。	ルールが元の ASA 設定のインターフェイス別にどのようにグループ化されたかを再現する場合。
変換された ASA 設定をインポートする前に作成されたセキュリティ ゾーン/インターフェイス グループ	変換された ASA 設定をインポートする前にこのセキュリティ ゾーン/インターフェイス グループを作成します。	Firepower Management Center にすでに存在するセキュリティ ゾーン/インターフェイス グループにルールを関連付ける場合。
インポート プロセス中にその場で作成されたセキュリティ ゾーン/インターフェイス グループ	ルール セットの横にあるドロップダウン リストから [新規...（New...）] を選択して、このセキュリティ ゾーン/インターフェイス グループを作成します。	Firepower Management Center の新しいセキュリティ ゾーン/インターフェイス グループにルールを関連付ける場合。

ヒント セットに関する詳細を展開するには、ルール セットの横にある矢印を使用します。

（注） 移行ツールはインターフェイス設定を変換しません。変換された ASA 設定をインポートした後に、手動でデバイスを追加して、それらのデバイスでインターフェイスを設定する必要があります。ただし、このインポートの手順では、ACL または NAT ポリシーと単一のエンティティ（セキュリティ ゾーンまたはインターフェイス グループ）との間の関連付けを保持できるので、新しい Firepower Threat Defense デバイスのインターフェイスと素早く関連付けることができます。セキュリティ ゾーン/インターフェイス グループをインターフェイスに関連付ける方法の詳細については、移行済みポリシーの設定 （7 ページ） を参照してください。

ステップ 8 [インポート（Import）] をクリックします。
インポートが完了すると、メッセージ センターに移動させるメッセージが表示されます。

ステップ 9 [システム ステータス（System Status）] アイコンをクリックして、メッセージ センターを表示します。

ステップ 10 [タスク（Tasks）] タブをクリックします。

ステップ 11 インポート タスクのリンクをクリックして、インポート レポートをダウンロードします。

Firepower Threat Defense のインストール

次の表に示す適切なクイック スタート ガイドを使用して Firepower Threat Defense をインストールします。

（注） クイック スタート ガイドの手順には、デバイスへの新しいイメージのインストールが含まれているので、新しいデバイスに Firepower Threat Defense をインストールするのか、または元の ASA を Firepower Threat Defense に再イメージ化するのかにかかわらず、同じ手順を使用できます。

プラットフォーム	クイック スタート ガイド
Firepower Threat Defense：ASA 5506-X、ASA 5506H-X、ASA 5506W-X、ASA 5508-X、ASA 5512-X、ASA 5515-X、ASA 5516-X、ASA 5525-X、ASA 5545-X、および ASA 5555-X	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/5500X/ftd-55xx-X-qsg.html
Firepower 4100 Series with Threat Defense：4110、4120、および 4140	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fp4100/ftd-4100-qsg.html
Firepower 9300 with Threat Defense	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fp9300/ftd-9300-qsg.html
Firepower Threat Defense Virtual：VMware	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/ftdv/ftdv-vmware-qsg.html
Firepower Threat Defense Virtual：AWS クラウド	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/aws/ftdv-aws-qsg.html

移行済みポリシーの設定

この手順では、移行されたポリシーを Firepower Management Center に設定するための手順の概要について説明します。各手順の詳細については、Firepower Management Center コンフィギュレーション ガイド で関連する手順を参照してください。

ステップ 1 Firepower Threat Defense デバイスのインターフェイスを、変換プロセス中に作成されたセキュリティ ゾーンまたはインターフェイス グループに割り当てます。

ステップ 2 ASA アクセス ルールをアクセス コントロール ポリシーに移行した場合：

- 必要に応じて、無効になっているルールの有効化または編集、ルールの追加、ルールの削除、およびルールの順序の変更によって、ポリシーのルールを調整します。たとえば、異なる送信元と宛先のプロトコルまたは複数のプロトコルを指定するルールを編集することができます（複数のプロトコルを指定するアクセス ルール を参照）。
- 必要に応じて、ツールが変換しない ASA パラメータの Firepower 同等要素を設定します。

アクセス ルールのパラメータ	アクセス コントロール ルールのパラメータ
ユーザ（User）	選択されたユーザの状態

アクセス ルールのパラメータ	アクセス コントロール ルールのパラメータ
セキュリティ グループ（送信元）（Security Group (Source)）	カスタム SGT の状態

- アクセス コントロール ポリシーを Firepower Threat Defense デバイスに割り当てます。

ステップ 3 ASA アクセス ルールをプレフィルタ ポリシーに移行した場合：

- 必要に応じて、無効になっているルールの有効化または編集、ルールの追加、ルールの削除、およびルールの順序の変更によって、ポリシーのルールを調整します。たとえば、異なる送信元と宛先のプロトコルまたは複数のプロトコルを指定するルールを編集することができます（複数のプロトコルを指定するアクセス ルール を参照）。
- 必要に応じて、ツールが変換しない ASA パラメータの Firepower 同等要素を設定します。

アクセス ルールのパラメータ	プレフィルタ ルールのパラメータ
ユーザ（User）	選択されたユーザの状態
セキュリティ グループ（送信元）（Security Group (Source)）	カスタム SGT の状態

- システムが変換時に作成した新しいアクセス コントロール ポリシーを設定するか、または、プレフィルタ ポリシーを別のアクセス コントロール ポリシーに関連付けます。

  警告 移行ツールにより、移行されたアクセス コントロール ポリシーのデフォルトの動作が [すべてのトラフィックをブロック（Block All Traffic）] に設定されます。これは ACL での暗黙の拒否に相当します。移行プレフィルタ ポリシーと一緒に異なるアクセス コントロール ポリシーを使用する場合は、デフォルトの動作を [すべてのトラフィックをブロック（Block All Traffic）] に設定することを考慮してください。そうしないと、セキュリティ ホールが作成される恐れがあります。

- 関連付けられたアクセス コントロール ポリシーを Firepower Threat Defense デバイスに割り当てます。

ステップ 4 NAT ポリシーを移行した場合：

- 必要に応じて、無効になっているルールの有効化または編集、ルールの追加、ルールの削除、およびルールの順序の変更によって、ポリシーのルールを調整します。
- NAT ポリシーを Firepower Threat Defense デバイスに割り当てます。

ステップ 5 必要に応じて、Application Visibility and Control、侵入からの保護、URL フィルタリング、および高度なマルウェア防御（AMP）を含む、次世代ファイアウォール機能を設定します。

ステップ 6 設定変更を展開します。設定変更の展開 （9 ページ）を参照してください。

設定変更の展開

移行した設定を展開するには、次の手順を使用します。展開プロセスの詳細については、『*Firepower Management Center Configuration Guide*』の「Deploying Configuration Changes」を参照してください。

ステップ 1 Firepower Management Center メニュー バーで、[展開（Deploy）] をクリックします。

[ポリシーの展開（Deploy Policies）] ダイアログに、設定の期限が切れているデバイスがリストされます。ダイアログの上部の [バージョン（Version）] は、最後に設定変更を行った時期を示します。デバイス テーブルの [現在のバージョン（Current Version）] 列は、変更を各デバイスに最後に展開した時期を示します。

ステップ 2 設定変更を展開するデバイスを特定して選択します。

- [ソート（Sort）]：列ヘッダーをクリックすることで、デバイス リストをソートします。
- [展開（Expand）]：デバイス リストを展開して展開される設定変更を表示するには、プラス アイコン（⊞）をクリックします。システムは、期限切れのポリシーをインデックス（🕘）アイコンでマーキングします。
- [フィルタ（Filter）]：デバイス リストをフィルタリングします。ディスプレイの列ヘッダーの右上隅にある矢印をクリックし、[フィルタ（Filters）] テキスト ボックスにテキストを入力し、Enter を押します。チェックボックスをオンまたはオフにして、フィルタをアクティブまたは非アクティブにします。
- 調整：マウス カーソルを列ヘッダーの上に移動し、列をドラッグ アンド ドロップして希望の順序にします。

ステップ 3 [展開（Deploy）] をクリックします。

ステップ 4 変更の展開時にエラーまたは警告が出された場合には、次の選択肢があります。

- [続行（Proceed）]：警告状態を解決せずに展開を続行します。システムがエラーを確認した場合は続行できません。
- [キャンセル（Cancel）]：展開せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。