Firepower Threat Defense 構成に Cisco ASA 構成を移行する

移行に向けて Cisco ASA を準備する

手順

ステップ 1 Cisco ASA デバイスが構成の移行要件を満たしているかどうかを確認するには、「Cisco ASA デバイスの要件」を参照してください。

ステップ 2 エクスポートするアクセス制御リスト（ACL）と NAT ポリシーを特定します。

ステップ 3 できるだけ多くの重要でないルールを構成からプルーニングします。シスコでは、変換前に Cisco ASA 構成の複雑さとサイズを可能な限り軽減することを推奨しています。ACL に含まれているエントリの数を確認するには：

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

移行ツールのインストール

⚠

注意 本運用 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、本運用デバイスではサポートされていません。移行ツールをインストールしたら、指名された Firepower Management Center を再イメージ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。

手順

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 該当するガイドの説明に従って、イメージファイルを使用して指名された Firepower Management Center Virtual をインストールします。

- 『*VMware* 導入向け *Cisco Firepower Management Center Virtual* クイックスタートガイド』
- *Cisco Firepower Management Center Virtual for KVM Deployment* クイックスタートガイド

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

ステップ 4 Root Shell 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）
プロセスが完了したら、Firepower Management Center で実行中の Web インターフェイスセッションを更新して、移行ツールを使用します。

Cisco ASA 構成ファイルを保存する

移行ツールは、Cisco ASA 構成ファイルを .cfg または .txt 形式に変換できます。

手順

ステップ 1 設定を保存します。

この構成を保存するために使用するコマンドは、Cisco 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 Cisco ASA のドキュメントロードマップに一覧されている該当するバージョンの『Cisco ASA 構成ガイド』を参照してください。

ステップ 2 保存した構成ファイルを、移行ツールからアクセス可能な場所（たとえば、ローカルコンピュータまたはネットワーク上の共有ドライブ）に転送します。

Cisco ASA 構成ファイルを変換する

次の手順を実行して、Cisco ASA 構成ファイル（.cfg または .txt）を Firepower 構成ファイル（.sfo）に変換します。

注意 移行ツールの UI は、Firepower Management Center UI の拡張機能です。ただし、この手順で説明されている機能のみを実行できます。

手順

ステップ 1 ブラウザで `https://hostname/` にアクセスします。*hostname* 要素は、移行ツールがインストールされている専用の Firepower Management Center Virtual のホスト名に対応しています。

ステップ 2 `admin` ユーザーとしてログインします。

ステップ 3 **[System]** > **[Tools]** > **[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、Cisco ASA からエクスポートした構成ファイルを選択します。

ステップ 6 **[次へ（Next）]** をクリックします。

ステップ 7 アクセスルールの変換時にシステムが使用するポリシーを選択します。

- **プレフィルタポリシー** - 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** - 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**を選択した場合、Permit アクションを持つアクセスルールに対して、システムに割り当てるアクションを選択します。

- **Fastpath**—アクセスコントロール、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** - トラフィックが残りのアクセスコントロールによって引き続き分析されることを許可します。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**を選択した場合、Permit アクションを持つルールに対して、システムに割り当てるアクションを選択します。

- **信頼** - ディープインスペクションやネットワーク検出をせずにトラフィックを通過させます。信頼されたトラフィックは、アイデンティティポリシーによって強制される認証要件、およびレート制限が適用され続けます。
- **許可** - 一致するトラフィックの通過を許可します。許可されるトラフィックには、アイデンティティ ポリシーによって強制される認証要件が適用され続けます。レート制限、および詳細検査（設定されている場合）も適用され続けます。

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します。タスクの状態は、メッセージセンタ - で表示できます。

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。

移行タスクは最上位のメッセージとして表示されます。これは、中間 Firepower Management Center で実行できるタスクが移行ツールのタスクに限られているためです。

ステップ 13 移行が失敗した場合は、該当するログでエラーメッセージを確認します。詳細については、「変換エラーをトラブルシューティングする （5 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）]** をクリックして、ローカルコンピュータに変換したファイルをコピーします。
- **[移行レポート（Migration Report）]** をクリックすると、移行レポートを表示できます。

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、Firepower Threat Defense 構成に変換できた Cisco ASA 構成および正常に変換できなかった Cisco ASA 構成が要約されています。正常に変換できなかった構成として、次が挙げられます。

- Firepower システムでサポートされていない Cisco ASA 構成
- Firepower システム（Firepower に相当する機能がある）でサポートされているが、移行ツールが変換しない Cisco ASA 構成

Firepower に相当する機能があるにもかかわらず変換に失敗した構成については、変換済みポリシーを本運用Firepower Management Center にインポートした後で手動で追加します。

変換エラーをトラブルシューティングする

専用 Firepower Management Center で変換が失敗した場合、移行ツールは、ローカルコンピュータにダウンロードできる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。

手順

ステップ 1 **[System]** > **[Health]** > **[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します。

ステップ 6 メッセージセンターを表示するとタスクの進捗状況を追跡できます。

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、タスク状態が [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ーに保存して、ファイルを解凍します。

ステップ 9 次のファイルでエラーメッセージを確認します。

- `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`

変換した Cisco ASA 構成をインポートする

Firepower Management Center のマルチドメインデプロイメントで、システムは、変換した Cisco ASA 構成をそれをインポートするドメインに変換します。インポート時に、システムは、変換したオブジェクトの **[ドメイン（Domain）]** フィールドに値を入力します。

手順

ステップ 1 本運用 Firepower Management Center で、[**[System]** > **[Tools]** > **[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 **[ファイルを選択（Choose File）]** をクリックし、[参照（browse）] 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、以前の移行で選択した選択肢に応じて、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。
システムはファイルを分析し、[競合をインポート（Import Conflict）] ページを表示します。

ステップ 7 [競合をインポート（Import Conflict）] ページで、次の手順を実行します。

- 構成の競合を解決します。Firepower Management Center Configuration Guide の「競合解決をインポート」を参照してください。
- 元の Cisco ASA 構成でインターフェイスごとにルールがグループ化されていた方法を複製するか、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	ソース	次の場合、このゾーンまたはグループを選択します。
システム生成の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、変換中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自動作成します。	元の Cisco ASA 構成のインターフェイスごとにルールがグループ化された方法を複製します。
変換された Cisco ASA 構成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 Cisco ASA 構成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。	ルールを、Firepower Management Center ですでに既存するセキュリティゾーン/インターフェイスグループに関連付けます。
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	ルール一式の横にあるドロップダウンリストで、[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。	ルールを、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関連付けます。

ヒント
ルール一致機の横にある矢印を使用して、セットに関する追加情報を展開します。

（注）
移行ツールはインターフェイス構成を変換しません。デバイスを手動で追加し、変換された Cisco ASA 構成をインポートした後、それらのデバイスのインターフェイスを構成する必要があります。ただし、このインポート手順により、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）との関連付けを保持し、新しい Firepower Threat Defense デバイスのインターフェイスとすぐに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とインターネットへの関連付けの詳細については、「移行したポリシーを構成する （8 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、システムにメッセージセンターに誘導するメッセージが表示されます。

ステップ 9 [システム状態（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 インポートレポートをダウンロードするには、インポートタスク内のリンクをクリックします。

Firepower Threat Defense をインストールする

手順

次の表に記載されている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記載されているため、同じ手順を使用して、新しいデバイスに Firepower Threat Defense をインストールしたり、Firepower Threat Defense に元の Cisco ASA を再イメージすることもできます。

プラットフォーム	クイック スタート ガイド
Firepower Threat Defense：Cisco ASA 5506-X、Cisco ASA 5506H-X、Cisco ASA 5506W-X、Cisco ASA 5508-X、Cisco ASA 5512-X、Cisco ASA 5515-X、Cisco ASA 5516-X、Cisco ASA 5525-X、Cisco ASA 5545-X、Cisco ASA 5555-X	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/5500X/ftd-55xx-X-qsg.html
Threat Defense を搭載した Firepower 4100 シリーズ：4110、4120、および 4140	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fp4100/ftd-4100-qsg.html
Threat Defense を搭載した Firepower 9300	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 Cloud	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/aws/ftdv-aws-qsg.html

移行したポリシーを構成する

この手順では、Firepower Management Center に移行したポリシーを構成するための大まかな手順を説明します。各手順の詳細については、Firepower Management Center Configuration Guide に記載されている関連手順を参照してください。

手順

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インターフェイスグループのセキュリティゾーンに割り当てます。

ステップ 2 Cisco ASA アクセスルールをアクセス コントロール ポリシーに移行する場合：

- 必要に応じて、無効なルールを有効または無効にし、ポリシーのルールを調整、追加、削除できます。またルールの順番を変更できます。たとえば、別の送信元プロトコルおよび接続先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変更する場合は、「複数のプロトコルを指定するアクセスルール」を参照してください。
- 必要に応じて、ツールが変換しない Cisco ASA パラメータに Firepower と同等の機能を構成します。

Access Rule パラメータ	Access Control Rule パラメータ
ユーザー	選択されたユーザー条件
セキュリティグループ（送信元）	カスタム SGT 条件

- 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 Cisco ASA アクセスルールをプレフィルタポリシーに移行する場合：

- 必要に応じて、無効なルールを有効または無効にし、ポリシーのルールを調整、追加、削除できます。またルールの順番を変更できます。たとえば、別の送信元プロトコルおよび接続先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変更する場合は、「複数のプロトコルを指定するアクセスルール」を参照してください。
- 必要に応じて、ツールが変換しない Cisco ASA パラメータに Firepower と同等の機能を構成します。

Access Rule パラメータ	Prefilter Rule パラメータ
ユーザー	選択されたユーザー条件
セキュリティグループ（送信元）	カスタム SGT 条件

- 変換中にシステムが作成するアクセス コントロール ポリシーを構成するか、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
移行ツールは、移行済みアクセス コントロール ポリシーのデフォルトアクションを **[すべてのトラフィックをブロック（Block All Traffic）]** に設定します。これは、ACL における暗黙の拒否と同等の

設定です。移行したプレフィルタポリシーがある別の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 **[すべてのトラフィックをブロック（Block All Traffic）]** に設定することを検討します。そうしないと、セキュリティホールが生じる場合があります。

- 関連するアクセス 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、無効なルールを有効または無効にし、ポリシーのルールを調整、追加、削除できます。またルールの順番を変更できます。
- 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、アプリケーションの可視性と制御、侵入保護、URL フィルタ処理、Cisco Advanced Malware Protection（AMP）を含む NGFW 機能を構成します。

ステップ 6 設定変更を展開します。設定変更をデプロイする （9 ページ）を参照してください。

設定変更をデプロイする

移行した構成をデプロイするには、次の手順を実行します。詳細については、『*Firepower Management Center* 構成ガイド』の「構成変更をデプロイする」を参照してください。

手順

ステップ 1 FMC 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、**プラス記号**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**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 [Deploy] をクリックします。

ステップ 4 展開する変更に関するエラーや警告がシステムによって識別された場合は、[要求された展開のエラーと警告（Errors and Warnings for Requested Deployment）] ウィンドウにその内容が表示されます。

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。

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。

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。