Cisco ASAから Firepower Threat Defense への移行の概要

このガイドでは、シスコの移行ツールを使用して、Cisco ASA から Firepower Threat Defense デバイスへファイアウォールポリシー設定を移行する方法について説明します。

Cisco ASA は、高度なステートフル ファイアウォールと VPN コンセントレータの機能を 1 つの装置に組み合わせたものです。これは、ファイアウォールの業界標準規格です。この製品の詳細については、「http://www.cisco.com/go/asa」を参照してください。

Firepower Threat Defense は、ファイアウォールの進化における次のステップです。これは、統合した NGFW と次世代 IPS 機能を提供します。Firepower ソフトウェアモデルで利用可能な IPS 機能に加え、ファイアウォールとプラットフォーム機能には、サイト間 VPN、堅牢なルーティング、NAT、クラスタリングおよび、アプリケーション可視化やアクセスコントロールにおける各種最適化が含まれます。Firepower Threat Defense は、Cisco Advanced Malware Protection（AMP）と URL フィルタリングもサポートします。この製品の詳細については、「http://www.cisco.com/go/ngfw」を参照してください。

シスコの移行ツールを使用すると、Cisco ASA 構成の特定の機能を Firepower Threat Defense 構成の同等の機能に変換できます。変換後、変換されたポリシーを調整し、追加の Firepower Threat Defense ポリシーを構成して移行を手動で構成することをシスコはお勧めします。

Cisco ASA 構成は、新しい Firepower Threat Defense デバイス、または、更新後、Firepower Threat Defense デバイスとして元の Cisco ASA デバイスに移行できます。

移行プロセスの概要については、https://www.youtube.com/watch?v=N06xXat59B0 のリンクにある動画をご視聴ください。

Firepower Management Center およびサポートされる移行ツール

次の表に、Firepower Management Center のさまざまなバージョンでサポートされている移行ツールを示します。

Firepower Management Center	Cisco ASA から Firepower Threat Defense への移行ツール	FirePOWER 移行ツール
バージョン 6.2、6.2.1、6.2.2	はい	いいえ

Firepower Management Center	Cisco ASA から Firepower Threat Defense への移行ツール	FirePOWER 移行ツール
バージョン 6.2.3 ～ 6.4	はい	はい
バージョン 6.5 以降	いいえ	はい

Cisco ASA から Firepower Threat Defense への移行ツール

Cisco ASA 構成を Firepower Threat Defense 構成 Firepower Management Center に移行するには、「専用の Firepower Management Center Virtual for VMware を準備するために Cisco ASA から Firepower Threat Defense 以降ツールイメージを使用する」を参照してください。この専用の FMC は、デバイスと通信しません。代わりに、移行ツールを使用して、.cfg または .txt 形式の Cisco ASA 構成ファイルを.sfo 形式の Firepower インポートファイルに変換できます。その後、本運用 FMC をインポートします。

移行ツールは、Cisco ASA 構成形式でデータのみを変換できます（つまり、適切な順番の Cisco ASA CLI コマンドのフラットファイル）。移行ツールを使用すると、システムがファイル形式を検証します。たとえば、ファイルには ASA version コマンドを含める必要があります。システムがファイルを検証できない場合、変換は失敗します。

Cisco ASA デバイスの要件

移行ツールは、次の Cisco ASA デバイスから構成データを移行できます。

表 *1* : バージョン *6.2.1* でサポートされているプラットフォームと環境

サポートされるプラットフォーム	対応環境
任意	ASA バージョン 9.8/ASDM バージョン 7.8 ASA バージョン 9.7/ASDM バージョン 7.7 ASA バージョン 9.6/ASDM バージョン 7.6 Cisco ASA バージョン 9.5/ASDMバージョン 7.5 ASA バージョン 9.4/ASDM バージョン 7.4 Cisco ASA バージョン 9.3/ASDMバージョン 7.3 ASA バージョン 9.2/ASDM バージョン 7.2 ASA バージョン 9.1/ASDM バージョン 7.1 Cisco ASA バージョン 9.0/ ASDMバージョン 7.0 ASA バージョン 8.4/ASDM バージョン 6.4

さらに、Cisco ASA デバイスは次の条件を満たしている必要があります。

- シングルコンテキストモードを実行する。
- フェイルオーバーペアの一部である場合のアクティブユニット。
- クラスターの一部である場合のマスターユニット。

Cisco ASA デバイスは、透過的なモードまたはルーテッドモードで実行できます。

Firepower デバイスの要件

このドキュメントで説明する移行プロセスでは、次の Firepower デバイスが必要です。

- 専用の Firepower Management Center Virtual for VMware で実行されている移行ツール。
- 本運用 Firepower Management Center。サポートされているプラットフォームでサポートされている環境を実行する必要があります。

サポートされている Firepower Management Center プラットフォーム	サポートされている Firepower Management Center 環境
Firepower Management Center：FS750、FS1000、FS1500、FS2000、FS2500、FS3500、FS4000、Virtual	移行ツールと同じバージョンである必要があります。

- 本運用 Firepower Threat Defense デバイス（Cisco ASA デバイスで再イメージ可能）。Firepower Threat Defense でサポートされているプラットフォームと環境の一覧については、「Cisco Firepower Compatibility Guide」を参照してください。

ライセンス要件

このドキュメントに記載されている移行された構成を使用するには、Base Firepower Threat Defense ライセンスが必要です。詳細については、「http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html」を参照してください。

Cisco ASA デバイスには、Firepower Threat Defense デバイスとは異なるライセンスが必要なため、移行ツールは、ライセンス情報を移行しません。Firepower Threat Defense デバイス向けに新しいライセンスを購入する必要があります。移行コンテキストのライセンス価格については、セールス担当者にお問い合わせください。

移行でサポートされる Cisco ASA 機能

移行ツールを使用すると、次の Cisco ASA 機能を移行できます。

- 拡張済みアクセスルール（インターフェイスへの割り当ておよびグローバルな割り当てが可能）
- Twice NAT およびネットワークオブジェクト NAT ルール
- ツールが変換する拡張済みアクセスルールと NAT ルールに関連付けられたネットワークオブジェクト/グループまたはサービスオブジェクト/グループ

このツールが Cisco ASA 構成を Firepower Threat Defense 構成に変換する方法の詳細については、「変換マッピングの概要」を参照してください。

移行制限

Cisco ASA に移行時は、次の制限に注意します。

Cisco ASA 構成のみ
移行ツールは、Cisco ASA 構成のみを変換します。既存の ASA FirePOWER 構成は変換されません。既存の ASA FirePOWER 構成を Firepower Threat Defense 構成に手動で変換する必要があります。

ACL と ACE の制限
移行ツールが変換できる Cisco ASA 構成ファイルのサイズには具体的な制限はありません。ただし、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。複雑なポリシーやルールは、重要なリソースを消費し、パフォーマンスに悪影響を与える可能性があります。Firepower で構成変更をデプロイする際、システムはすべてのルールをまとめて評価し、ターゲット デバイスでネットワーク トラフィックを評価するために使用する拡張基準セットを作成します。それらの基準がターゲットデバイスのリソース（物理メモリ、プロセッサなど）を上回っている場合、そのデバイスに構成をデプロイできません。

適用されるルールとオブジェクトのみ

移行ツールは、インターフェイスに適用される ACL のみを変換します。つまり、Cisco ASA 構成ファイルには、ペアになっている**access-list** および **access-group** コマンドが含まれます。

オブジェクトが、アクティブに適用される ACL または NAT ルールのいずれかに関連付けられている場合、移行ツールは、そのオブジェクトのみを変換します。つまり、Cisco ASA 構成ファイルには、適切に関連付けられている **object**、**access-list**、**access-group** および **nat** コマンドが含まれます。ネットワークオブジェクトとサービスオブジェクトのみを移行できません。

サポートされていない ACL および NAT 構成

移行ツールは、具体的な例外を除き、ほとんどの ACL および NAT 構成をサポートしています。サポートされていない ACL および NAT 構成は次のように処理されます。

[変換するが無効にする（Converts but Disables）] - 移行ツールは次を使用する ACE を完全に変換できません。

- 時間範囲オブジェクト
- 完全修飾ドメイン名（FQDN）
- ローカルユーザーとユーザーグループ
- セキュリティグループ（SGT）オブジェクト
- 送信元ポートと宛て先ポートの両方に対するネストされたサービスグループ

  サポート対象外の要素に対して Firepower の同等の機能がないため、これらのルールの特定の要素は変換できません。これらの場合、ツールは Firepower の同等のものがあるルール要素（ソースネットワークなど）を変換し、Firepower の同等のものがないルール要素（時間範囲など）を除外し、作成される新しいアクセス コントロール ポリシーまたはプレフィルタポリシーでルールを無効にします。

  Cisco ASA 構成から移行されるエグレス ACL ルールは、サポートされないルールです。これらは無効な状態で表示されます。

  無効化された各ルールの場合、システムはルール名に `(unsupported)` と追加し、移行中にルールが無効化された理由を示すコメントもルールに追加します。 で無効化されたルールをインポートしたら、Firepower Management CenterFirepower システムでデプロイメントを成功させるためにルールを手動で編集したり、置き換えたりできます。

[除外（Excludes）] - 移行ツールは、作成するポリシーから、EtherType ACL または WebType ACL、ホストアドレス名のエイリアスを使用する ACE（**name** コマンドで指定）、事前定義された（デフォルト）サービスオブジェクトを使用する ACE の構成を除外します。これらの除外された構成の詳細については、『*CLI* ブック *2*：*Cisco ASA* シリーズファイアウォール *CLI* 構成ガイド』または『*ASDM* ブック *2*：*Cisco ASA* シリーズファイアウォール *ASDM* 構成ガイド』を参照してください。

サポートされていないその他の Cisco ASA 構成

移行ツールは、このドキュメントで指定されていない Cisco ASA 機能の移行をサポートしていません。このツールは、Cisco ASA 構成ファイルを処理する際に、サポートされていない機能の構成データを無視します。

移行のチェックリスト

移行ツールを使用する前に、次を確認します。

- Cisco ASA デバイスが移行のすべての条件を満たしているかを確認するには、「Cisco ASA デバイスの要件 （2 ページ）」を参照してください。
- Cisco ASA 構成ファイルは、.cfg または .txt のいずれかの形式です。
- Cisco ASA 構成ファイルには、サポートされている構成のみが含まれます。移行に必要な制限を満たしていることを確認するには、「移行制限 （4 ページ）」を参照してください。
- Cisco ASA 構成ファイルには、有効な Cisco ASA CLI 構成のみを含めます。続行する前に、誤ったコマンドまたは不完全なコマンドを修正します。ファイルに無効な構成が含まれている場合、移行は失敗します。
- 変換された Cisco ASA 構成ファイルをインポートするには、Firepower Management Center を構成を変換する移行ツールと同じバージョンで実行する必要があります。この制限は、メジャーリリースとマイナーリリースの両方で適用されます。たとえば、移行ツールがバージョン 6.2.1 を実行していて、ファイルをインポートする Firepower Management Center がバージョン 6.1.0.2 を実行している場合、変換した Cisco ASA 構成ファイルをインポートする前に、Firepower Management Center 6.2.1 にアップグレードする必要があります。

表記法

このドキュメントでは、Firepower Threat Defense 構成に変換された Cisco ASA 構成の例を示します。これらの例のほとんどの列は、関連するルールエディタまたは Firepower Management Center のオブジェクトマネージャのコンポーネントに直接マップします。次の表に、Firepower UI コンポーネントに直接マッピングされない列を示します。

表 *2:* 間接値を使用する列

列	値	説明
有効化	True/False	アクセスコントロールまたはプレフィルタルールで、**[有効化（Enabled）]** チェックボックスをオンにするかオフにするかを指定します。

列	値	説明
アクション	同等に許可	次のように、変換時に選択した選択肢に応じて、決定される値を指定します。 • アクセスルールをアクセスコントロールルールに変換する場合は、この値を **[許可（Allow）]** または **[True]** のどちらにするかも選択します。 • アクセスルールをプレフィルタルールに変換する場合は、この値を **[許可Fastpath]** または **[分析（Analyze）]** のどちらにするかも選択します。
ドメイン	なし	変換時点では、このフィールドは空欄です。これは、システムが、本運用 Firepower Management Center にインポートするまで、システムがドメインを割り当てないためです。インポート時に、システムは、変換された構成をインポートするドメインに基づいてドメインを割り当てます。
オーバーライド	True/False	オブジェクトで **[オーバーライドを許可（Allow Overrides）]** チェックボックスをオンにするかオフにするかを指定します。

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。