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、ご自身の Cisco ASA から Firepower Threat Defense デバイスにファイアウォール ポリシーの設定を移行する方法について説明します。

Cisco ASA では、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が提供されます。これは長い間、ファイアウォールの業界標準でした。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を表しています。これによって、統合型次世代ファイアウォールおよび次世代IPS機能が提供されます。Firepower ソフトウェアのモデルで使用可能なIPS機能に加えて、ファイアウォールおよび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の可視性とアクセス制御におけるその他の最適化が含まれています。Firepower Threat Defense は、高度なマルウェア防御（AMP）および URL フィルタリングもサポートしています。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して、ASA 設定内の特定の機能を Firepower Threat Defense 設定の同等機能に変換することができます。この変換後、ご自身で変換したポリシーを調整して、追加の Firepower Threat Defense ポリシーを設定することで、移行を手動で完了させることを推奨します。

ASA 設定を新しい Firepower Threat Defense デバイスに移行したり、Firepower Threat Defense デバイスとして更新した後の元の ASA デバイスに移行することができます。

移行プロセスの概要については、こちらのリンク（https://www.youtube.com/watch?v=N06xXat59B0）でビデオをご覧ください。

• 表記法 （6 ページ）

移行ツール

ASA 設定を Firepower Threat Defense 設定の Firepower Management Center に移行するには、ASA から Firepower Threat Defense への移行ツールイメージを使用して、専用の Firepower Management Center Virtual for VMware を準備します。この専用の Management Center 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 ASA 設定ファイルを .sfo 形式の Firepower インポート ファイルに変換することができ、そのファイルを実稼働Management Centerにインポートできます。

移行ツールが変換できるのは、ASA 設定形式のデータ（つまり、適切な順序の ASA CLI コマンドのフラットファイル）のみです。移行ツールを使用すると、システムはファイルの形式を検証します。たとえば、ファイルには、ASA version コマンドが含まれている必要があります。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。

ASA デバイスの要件

移行ツールは、次の ASA デバイスから設定データを移行することができます。

表 *1:* バージョン *6.2.2* でサポートされ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	サポートされる環境
任意（Any）	バージョン 6.2.1 および 6.2.2 の移行ツール： 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 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 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 ASA バージョン 9.0/ASDM バージョン 7.0 ASA バージョン 8.7/ASDM バージョン 6.7 ASA バージョン 8.6/ASDM バージョン 6.6 ASA バージョン 8.5/ASDM バージョン 6.5 ASA バージョン 8.4/ASDM バージョン 6.4

また、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 モードで実行している。
- フェールオーバー ペアの一部である場合は、アクティブなユニット。

- クラスタの一部である場合は、マスター ユニット。

ASA デバイスは、トランスペアレント モードまたはルーテッド モードで動作できます。

Firepower デバイスの要件

このマニュアルに記載されている移行プロセスには、次の Firepower デバイスが必要です。

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

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

- 実稼働Firepower Threat Defenseデバイス（再イメージ化されたASAデバイス可）。Firepower Threat Defenseでサポートされるプラットフォームおよび環境のリストについては、Firepower システム互換性ガイドを参照してください。

ライセンス要件

このマニュアルに記載されている移行済みの設定を使用するには、基本の 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。

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。ご使用の Firepower Threat Defense デバイス用の新しいライセンスを購入する必要があります。移行におけるライセンス価格について質問がある場合は、セールス担当者にお問い合わせください。

移行がサポートされる ASA 機能

移行ツールを使用して、次の ASA 機能を移行することができます。

- 拡張アクセス ルール（インターフェイスへの割り当てと、グローバルな割り当てが可能です）
- Twice NAT ルール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アクセス ルールおよび NAT ルールに関連付けられているネットワーク オブジェクトとグループまたはサービス オブジェクトとグループ

ツールが ASA 設定を Firepower Threat Defense 設定に変換する仕組みについては、変換マッピングの概要 を参照してください。

移行の制限

ASA の設定を移行するときは、次の制限事項に注意してください。

ASA の設定のみ

移行ツールは ASA の設定のみ変換します。既存の ASA FirePOWER 設定は変換しません。既存の ASA FirePOWER 設定を Firepower Threat Defense 設定に手動で変換する必要があります。

ACL および ACE の制限

移行ツールで変換可能な ASA 設定ファイルのサイズに特定の制限はありません。ただし、変換する前に、可能な限り ASA 設定の複雑さとサイズを削減しておくことを推奨します。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 で設定の変更を展開すると、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、そのデバイスに設定を展開することはできません。

適用済みルールおよびオブジェクトのみ

移行ツールは、インターフェイスに適用されている ACL のみを変換します。つまり、ASA 設定ファイルには、ペアリングされた **access-list** および **access-group** コマンドが含まれている必要があります。

移行ツールは、アクティブに適用された ACL または NAT ルールに関連付けられているオブジェクトのみを変換します。つまり、ASA 設定ファイルには、適切に関連付けられた **object**、**access-list**、**access-group**、および **nat** コマンドが含まれている必要があります。ネットワーク オブジェクトおよびサービス オブジェクトを単独で移行することはできません。

サポート対象外の ACL および NAT の設定

移行ツールは、特定の例外を除き、ほとんどの ACL および NAT の設定をサポートします。サポート対象外の ACL および NAT の設定は次のように処理します。

[変換するが無効にする（Converts but Disables）]：移行ツールは、以下を使用する 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 ユーザまたはユーザ グループ
- セキュリティ グループ（SGT）オブジェクト

- 送信元ポートおよび宛先ポート両方について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 と同等の機能がないため、これらのルールの特定の要素を変換できません。このような場合、ツールは Firepower と同等のルール要素（たとえば、送信元ネットワーク）を変換し、Firepower と同等でないルール要素（たとえば、時間範囲）を除外し、作成した新しいアクセス コントロール ポリシーまたはプレフィルタ ポリシーでそのルールを無効にします。

  ASA 設定から移行された出力 ACL ルールはサポートされていないルールです。それらは無効化された状態で表示されます。

  無効化された各ルールに対し、システムは `(unsupported)` をルール名に追加し、システムが移行時にルールを無効にした理由を示すコメントをルールに追加します。ご自身のFirepower Management Centerで無効化されたルールをインポートした後、手動でルールを編集または置き換えることで、Firepower システムに正常に展開することができます。

[除外する（Excludes）]：移行ツールは、作成するポリシーから次の設定を除外します：EtherType または WebType ACL、ホストのアドレス名エイリアスを使用する ACE（**name** コマンドで指定）、および定義済み（デフォルト）サービス オブジェクトを使用する ACE。これらの除外される設定の詳細については、『*CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide*』または『*ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide*』を参照してください。

その他のサポート対象外の ASA 設定

移行ツールは、このマニュアルで指定されているもの以外の ASA 機能の移行をサポートしません。ツールは ASA 設定ファイルを処理する際に、サポート対象外の機能に関する設定データを無視します。

移行チェックリスト

移行ツールを使用する前に、以下について確認してください。

- ASA デバイスが移行に関するすべての要件を満たしている（ASA デバイスの要件 （2 ページ） を参照）。
- ASA 設定ファイルが .cfg または .txt 形式である。
- ASA設定ファイルにはサポート対象の設定のみが含まれており、移行に必要な制限事項を満たしている（移行の制限 （4 ページ） を参照）。
- ASA 設定ファイルには、有効な ASA CLI 設定のみが含まれている。正しくないコマンドまたは不完全なコマンドは続行する前に修正してください。ファイルに無効な設定が含まれている場合、移行は失敗します。
- 変換された ASA 設定ファイルをインポートするには、Firepower Management Center が、設定を変換する移行ツールと同じバージョンを実行している必要があります。この制約事項は、メジャー リリースとマイナー リリースの両方に適用されます。たとえば、移行ツー

ルはバージョン 6.2.1 を実行しているが、ファイルをインポートする Firepower Management Center はバージョン 6.1.0.2 を実行している場合は、変換された ASA 設定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

このマニュアルには、Firepower Threat Defense 設定に変換される ASA 設定の例が記載されています。これらの例にあるカラムのほとんどは、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ピングします。次の表に、Firepower UI コンポーネントに直接マッピングしないカラムを示します。

表 *2:* 間接値を使用するカラム

カラム	値	説明
[有効（Enabled）]	true/false（True/False）	アクセス コントロール ルールまたはプレフィルタ ルールで [有効（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。
操作（Action）	同等の許可	次のように、変換時の選択内容によっ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 ルールに変換するように選択した場合は、この値を [許可（Allow）] にするか [信頼する（Trust）] にするかも選択します。 • アクセス ルールをプレフィルタ ルールに変換するように選択した場合は、この値を [高速パス（Fastpath）] にするか [分析（Analyze）] にするかも選択します。
ドメイン（Domain）	None	実稼働Firepower Management Center時にインポートされるまでシステムはドメインを割り当てないので、変換の時点ではこのフィールドは空になっています。インポート時に、変換された設定をインポートするドメインに基づいて、ドメインがシステムによって割り当てられます。
オーバーライド（Override）	true/false（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。