Cisco ASA から Firepower Threat Defense へのバージョン 6.2 移行ガイド

初版：2017 年 01 月 23 日

最終更新：2017 年 02 月 08 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

Text Part Number:

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 1 章

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*：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）	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

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 Center：FS750、FS1500、FS2000、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 System Compatibility Guide* 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, （19 ページ） 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

移行ツールは、最大 2000000 の合計アクセス ルールの要素を含む ASA 設定ファイルをサポートできます。変換された設定ファイルがこの制限を超えると、移行は失敗します。

1 つの ACL の要素数ではなく、ASA 設定ファイル内のすべてのアクセス ルールの要素の合計を考慮する必要があります。1 つの ACL の要素を表示するには、ASA CLI コマンド `show access-list | i elements` を使用します。

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。

  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 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 6.2.0 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	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。

カラム	値	説明
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	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。

第 2 章

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，（2 ページ）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 ACL 内にあるエントリの数を確認します。

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

ステップ 4 設定に 2000000 を超える要素が含まれている場合は、できるだけ多くの不要な要素をプルーニングします。

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 CenterUI 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 移行ツールで、[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 [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 4 [次へ（Next）]をクリックします。

ステップ 5 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（PrefilterPolicy）] : 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（AccessControl 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 6 [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 7 [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 8 システムがサポートされていないルールを処理する方法を指定します。

- 無効ルールとして変換する（Convert as disabled rules）
- 変換せず移行レポートに追加しない（Do not convert and add to migration report）

ステップ 9 ロギングの有効時にアクセス ルールを変換する際に、システムが割り当てる必要があるアクションを選択します。

- 接続の開始時（At the start of connection）
- 接続の終了時（At the end of connection）
- 両方

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，（13 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）] > [状況（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 TAC の指示に従って、トラブルシューティング ファイルをシスコに送信します。

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 Configuration Guide*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, （16 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 Configuration Guide*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，（31 ページ）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
セキュリティ グループ（送信元）（Security Group (Source)）	カスタム SGT の状態
Enable Logging	[接続開始時にロギング（Log at Beginning of Connection）]および/または[接続終了時にロギング（Log at End of Connection）] オプション
ログ レベル（Logging Level）	接続イベント ロギング
ロギング間隔（Logging Interval）	接続イベント ロギング

- 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，（31 ページ）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
Enable Logging	[接続開始時にロギング（Log at Beginning of Connection）] および/または [接続終了時にロギング（Log at End of Connection）] オプション
ログ レベル（Logging Level）	接続イベント ロギング
ロギング間隔（Logging Interval）	接続イベント ロギング

- 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。
- 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, （17 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（Filter）]テキスト ボックスにテキストを入力し、Enter を押します。

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。

付 録 A

変換マッピング

以下のトピックでは、移行ツールが ASA 設定を FirePOWER Threat Defense設定に変換する仕組みについて説明します。

変換マッピングの概要

移行ツールは、次のように ASA 設定を FirePOWER Threat Defense設定に変換します。

表 *3*：変換マッピングの概要

エンティティ	ASA の設定	FirePOWER Threat Defenseの設定
ネットワーク オブジェクト	ネットワーク オブジェクト ネットワーク オブジェクト グループ ネストされたネットワーク オブジェクト グループ	ネットワーク オブジェクト ネットワーク オブジェクト グループ ネストされたネットワーク オブジェクト グループ

エンティティ	ASA の設定	FirePOWER Threat Defenseの設定
サービス オブジェクト	サービス オブジェクト サービス オブジェクト グループ ネストされたサービスオブジェクト グループ	ポート オブジェクト ポート オブジェクト グループ フラット化されたポート オブジェクト グループ
アクセス ルール	アクセス ルール	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（選択されているとおり）
NAT ルール	Twice NAT ルール ネットワーク オブジェクト NAT ルール	手動 NAT ルール 自動 NAT ルール

変換された設定の命名規則

移行ツールは、ASA アクセス ルール、NAT ルール、および関連オブジェクトを FirePOWER Threat Defense相当に変換する際に、以下に記載する命名規則を使用します。

オブジェクト名およびオブジェクト グループ名

オブジェクトおよびオブジェクト グループを変換する際、移行ツールは ASA 設定ファイルからのオブジェクトおよびグループの名前を保持します。

次に、例を示します。

```
object network obj1
 host 1.2.3.4
object network obj2
 range 1.2.3.7 1.2.3.10
 subnet 10.83.0.0 255.255.0.0
object-group network obj_group1
 network-object object obj1
 network-object object obj2
```

ツールは、この設定を `obj1` および `obj2` という名前のネットワーク オブジェクトと、`obj_group1` という名前のネットワーク オブジェクト グループに変換します。

サービス オブジェクトとサービス グループをポート オブジェクトとポート オブジェクト グループに変換する際、ツールでは特定の場合において、次の拡張子を元のオブジェクト名またはグループ名に追加できます。

表 *4*：変換されたサービス オブジェクトおよびグループの拡張子

内線番号	追加する理由
_dst	送信元ポートおよび宛先ポートを含むサービス オブジェクトを2つのポート オブジェクトに分割します。システムは、変換された宛先ポート データを保存するために使用されるサービス オブジェクトにこの拡張子を追加します。詳細については、送信元ポートと宛先ポートを含むサービス オブジェクト, （41 ページ）を参照してください。
_src	送信元ポートおよび宛先ポートを含むサービス オブジェクトを2つのポート オブジェクトに分割します。システムは、変換された送信元ポート データを保存するために使用されるサービス オブジェクトにこの拡張子を追加します。詳細については、送信元ポートと宛先ポートを含むサービス オブジェクト, （41 ページ）を参照してください。
_#	ネストされたサービス グループを変換します（ネストされたサービス グループの変換, （44 ページ）を参照）。

ポリシー名

ASA 設定ファイルには、ASA のホスト名を指定する `hostname` パラメータが含まれています。移行ツールは、この値を使用して、ファイルを変換するときに作成するポリシーに名前を付けます。

- アクセス コントロール ポリシー：*hostname*-AccessPolicy-*conversion_date*
- プレフィルタ ポリシー：*hostname*-PrefilterPolicy-*conversion_date*
- NAT ポリシー：*hostname*-NATPolicy-*conversion_date*

ルール名

変換されたアクセス コントロール ルール、プレフィルタ ルール、および NAT ルールに対し、システムは次の形式を使用して新しい各ルールに名前を付けます。

ACL_name-#rule_index

引数の説明

- *ACL_name*：ルールが属していた ACL の名前。
- *rule_index*：ルールが ACL 内の他のルールと比較して変換された順序を指定するシステムによって生成された整数。

次に、例を示します。

```
acl1#1
```

システムがサービス オブジェクトの変換中に複数のルールに単一のアクセス ルールを展開する必要がある場合、システムは次の拡張子を追加します。

ACL_name#rule_index_sub_index

ここで、追加された # は、拡張された順序における新しいルールの位置を表します。

次に、例を示します。

```
acl1#1_1
```

```
acl1#1_2
```

ルール名が 30 文字より長いとシステムが判断した場合、システムは ACL 名を短縮し、圧縮された名前をチルダ（~）を使用して終了します。

```
ACL Name~#rule index
```

たとえば、元の ACL 名が `accesslist_for_outbound_traffic` の場合、システムは ACL 名を次のように切り捨てます。

```
accesslist_for_outbound_tr~#1
```

セキュリティ ゾーン名およびインターフェイス グループ名

移行ツールは、ASA 設定ファイルの `access-group` コマンドを変換する際に、セキュリティ ゾーンまたはインターフェイス グループ（変換時の選択内容による）を作成することで、コマンド内のイングレスとイーグレスの情報をキャプチャします。ツールは、次の形式を使用して、これらの新しいセキュリティ ゾーンまたはインターフェイス グループに名前を付けます。

*ACL_name_interface_name_direction_keyword*_zone

引数の説明

- *ACL_name*：`access-group` コマンドからの ACL の名前。
- *interface_name*：`access-group` コマンドからのインターフェイスの名前。
- *direction_keyword*：`access-group` コマンドからの方向キーワード（`in` または `out`）。

次に例を示します。

```
access-list acp1 permit tcp any host 209.165.201.3 eq 80
access-group acp1 in interface outside
```

ツールは、この設定を `acp1_outside_in_zone` という名前のセキュリティ ゾーンまたはインターフェイス グループに変換します。

Firepower オブジェクトおよびオブジェクト グループに固有のフィールド

Firepower ネットワークおよびポート オブジェクトとポート グループには、ASA オブジェクトおよびグループには存在しないいくつかのフィールドがあります。移行ツールによって、変換されたネットワークおよびポート オブジェクトとポート グループのこれらの Firepower 固有フィールドには次のデフォルト値が読み込まれます。

表 *5* : ***Firepower*** オブジェクトとグループに固有のフィールドに対するデフォルト値

Firepower オブジェクトおよびグループのフィールド	変換済み **ASA** オブジェクトおよびグループに対するデフォルト値
ドメイン（Domain）	なし
オーバーライド（Override）	いいえ（False）

これらのデフォルト値の詳細については、表記法, （6 ページ）を参照してください。

アクセス ルールの変換

移行ツールは、移行時にユーザが選択した内容に応じて、ASA アクセス ルールをアクセス コントロール ルールまたはプレフィルタ ルールに変換できます。

アクセス コントロール ルールへのアクセス ルールの変換

ASA アクセス ルールを FirePOWER Threat Defense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：

- システムは、変換されたルールを、アクセスコントロールポリシーの[デフォルト（Default）] ルール セクションに追加します。
- システムは、[説明（Description）] フィールドの内容を、ルールの [コメント履歴（Comment History）]にエントリとして保持します。
- システムは、変換されたルールを識別するエントリを [コメント履歴（Comment History）]に追加します。
- システムは、アクセス コントロール ルールの [アクション（Action）]を次のように設定します。

アクセス ルールのアクション	アクセス コントロール ルールのアクション
許可（Permit）	移行時の選択内容に応じて、[許可（Allow）] または [信頼する（Trust）]
拒否（Deny）	ブロック

- システムは、アクセス コントロール ルールの [送信元ゾーン（Source Zones）]および [宛先ゾーン（Destination Zones）] を次のように設定します。

ACL タイプ（ACL Type）	送信元ゾーン（Source Zones）	宛先ゾーン（Destination Zones）
グローバル（任意のインターフェイスに適用されます）	任意（Any）	任意（Any）
特定のインターフェイスに適用されます	インポート時に選択したセキュリティ ゾーン	任意（Any）

- アクセス ルールが非アクティブの場合、ツールはそのルールを無効なアクセス コントロール ルールに変換します。

移行ツールは、次のデフォルトのパラメータを使用して、変換されたルールをアクセス コントロール ポリシーに割り当てます。

- システムは、新しいアクセス 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。
- システムは、アクセス コントロール ポリシーをデフォルトのプレフィルタ ポリシーに関連付けます。

アクセスコントロールルールフィールドにマッピングされるアクセスルールフィールド

移行ツールは、次の表で説明するように、ASAアクセス ルールのフィールドをFirePOWER Threat Defenseアクセス コントロール ルールのフィールドに変換します。

（注）

- カラム 1（ASA アクセス ルール フィールド）のフィールド名は、ASDM インターフェイスのフィールド ラベルに対応します。
- カラム2（Firepowerアクセス コントロール ルール フィールド）のフィールド名は、Firepower Management Centerインターフェイスのフィールド ラベルに対応します。

表 *6*：*Firepower* アクセス コントロール ルール フィールドにマッピングされる *ASA* アクセス ルール フィールド

ASA アクセス ルール フィールド	Firepower アクセス コントロール ルール フィールド
インターフェイス（Interface）	対応するフィールドなし
操作	操作
ソース（Source）	送信元ネットワーク

ASA アクセス ルール フィールド	Firepower アクセス コントロール ルール フィールド
ユーザ（User）	変換しません。[選択されたユーザ（Selected Users）] の条件と同等
セキュリティ グループ（送信元）（Security Group (Source)）	変換しません。カスタム SGT の条件と同等
[接続先（Destination）]	宛先ネットワーク
セキュリティ グループ（宛先）（Security Group (Destination)）	対応するフィールドなし
サービス	[選択済み宛先ポート（Selected Destination Port）]。事前定義済みのサービス オブジェクトが指定されている場合は変換しません。
説明	コメント
Enable Logging	変換しません。[接続開始時にロギング（Log at Beginning of Connection）] または [接続終了時にロギング（Log at End of Connection）] と同等
ログ レベル（Logging Level）	変換しません。接続イベントのロギングと同等
ルールの有効化（Enable Rule）	有効（Enabled）
トラフィックの方向	対応するフィールドなし
送信元サービス（Source Service）	[選択済み送信元ポート（Selected Source Port）]。事前定義済みのサービス オブジェクトが指定されている場合は変換しません。
ロギング間隔（Logging Interval）	変換しません。接続イベントのロギングと同等
時間範囲（Time Range）	対応するフィールドなし

アクセス コントロール ルールに固有のフィールド

FirePOWER Threat Defenseアクセス コントロール ルールには、ASA アクセス ルールには存在しないいくつかのフィールドがあります。移行ツールによって、変換されたアクセス コントロール ルールのこれらの Firepower 固有フィールドには次のデフォルト値が読み込まれます。

表 *7*：***Firepower*** アクセス コントロール ルールに固有のフィールドに対するデフォルト値

アクセス コントロール ルール フィールド	変換されたアクセス ルールのデフォルト値
[名前（Name）]	システムによって生成されます（変換された設定の命名規則, （20 ページ）を参照）
送信元ゾーン（Source Zone）	• ACLがグローバルに適用される場合は、[いずれか（Any）] • ACL が特定のインターフェイスに適用される場合は、ツールが変換時に作成するセキュリティ ゾーン
宛先ゾーン（Destination Zone）	[いずれか（Any）]（すべてのアクセス コントロールルールのデフォルト）
選択された VLAN タグ（Selected VLAN Tags）	デフォルトなし（インポートした後に手動で条件を追加できます）
選択されたアプリケーションとフィルタ（Selected Applications and Filters）	デフォルトなし（インポートした後に手動で条件を追加できます）
選択された URL（Selected URLs）	デフォルトなし（インポートした後に手動で条件を追加できます）

プレフィルタ ルールへのアクセス ルールの変換

ASA アクセス ルールを FirePOWER Threat Defenseプレフィルタ ルールに変換するように選択した場合：

- システムは、[説明（Description）] フィールドの内容を、ルールの [コメント履歴（Comment History）]にエントリとして保持します。
- 変換されたルールを識別するエントリを [コメント履歴（Comment History）]に追加します。
- システムは、プレフィルタ ルールの [アクション（Action）]を次のように設定します。

アクセス ルールのアクション	プレフィルタ ルールのアクション
許可（Permit）	移行時の選択内容に応じて、[高速パス（Fastpath）]または [分析（Analyze）]
拒否（Deny）	ブロック

- システムは、プレフィルタ ルールの [送信元インターフェイス オブジェクト（Source Interface Objects）]および [宛先インターフェイス オブジェクト（Destination Interface Objects）] を次のように設定します。

ACL タイプ（ACL Type）	送信元インターフェイス オブジェクト（Source Interface Objects）	宛先インターフェイス オブジェクト（Destination Interface Objects）
グローバル（任意のインターフェイスに適用されます）	任意（Any）	任意（Any）
特定のインターフェイスに適用されます	インポート時に選択したインターフェイス グループ	任意（Any）

- アクセス ルールが非アクティブの場合、ツールはそのルールを無効なプレフィルタ ルールに変換します。

移行ツールは、次のデフォルトのパラメータを使用して、変換されたルールをプレフィルタ ポリシーに割り当てます。

- システムは、新しいプレフィルタ ポリシーのデフォルト アクションを [すべてのトンネル トラフィックを分析（Analyze All Tunnel Traffic）]に設定します。
- システムは、プレフィルタ ポリシーと同じ名前のアクセス コントロール ポリシーを作成し、次にプレフィルタ ポリシーをそのアクセス コントロール ポリシーに関連付けます。システムは、新しいアクセス 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。

プレフィルタ ルール フィールドにマッピングされるアクセス ルール フィールド

移行ツールは、次の表で説明するように、ASA アクセス ルールのフィールドを FirePOWER Threat Defenseプレフィルタ ルールのフィールドに変換します。

（注）

- カラム 1（ASA アクセス ルール フィールド）のフィールド名は、ASDM インターフェイスのフィールド ラベルに対応します。
- カラム 2（Firepower プレフィルタ ルール フィールド）のフィールド名は、Firepower Management Centerインターフェイスのフィールド ラベルに対応します。

表 *8*：*Firepower* プレフィルタ ルール フィールドにマッピングされる *ASA* アクセス ルール フィールド

ASA アクセス ルール フィールド	Firepower プレフィルタ ルール フィールド
インターフェイス（Interface）	対応するフィールドなし

ASA アクセス ルール フィールド	Firepower プレフィルタ ルール フィールド
ルールの有効化（Enable Rule）	有効（Enabled）
操作	操作
ソース（Source）	送信元ネットワーク
ユーザ（User）	対応するフィールドなし
セキュリティ グループ（送信元）（Security Group (Source)）	対応するフィールドなし
[接続先（Destination）]	宛先ネットワーク
セキュリティ グループ（宛先）（Security Group (Destination)）	対応するフィールドなし
サービス	選択済み送信元ポート（Selected Source Port） 選択済み宛先ポート（Selected Destination Port）
説明	コメント
Enable Logging	変換しません。[接続開始時にロギング（Log at Beginning of Connection）] または [接続終了時にロギング（Log at End of Connection）] と同等
ログ レベル（Logging Level）	変換しません。接続イベントのロギングと同等
トラフィックの方向	対応するフィールドなし
送信元サービス（Source Service）	[選択済み送信元ポート（Selected Source Port）]。事前定義済みのサービス オブジェクトが指定されている場合は変換しません。
ロギング間隔（Logging Interval）	変換しません。接続イベントのロギングと同等
時間範囲（Time Range）	対応するフィールドなし

Firepower プレフィルタ ルールに固有のフィールド

FirePOWER Threat Defenseプレフィルタ ルールには、ASA アクセス ルールには存在しないいくつかのフィールドがあります。移行ツールによって、変換されたプレフィルタ ルールのこれらの Firepower 固有フィールドには次のデフォルト値が読み込まれます。

表 *9*：***Firepower*** プレフィルタ ルールに固有のフィールドに対するデフォルト値

プレフィルタ ルール フィールド	変換されたアクセス ルールのデフォルト値
[名前（Name）]	システムによって生成されます（変換された設定の命名規則, （20 ページ）を参照）
送信元インターフェイス オブジェクト（Source Interface Objects）	• ACLがグローバルに適用される場合は、[いずれか（Any）] • ACL が特定のインターフェイスに適用される場合は、ツールが変換時に作成するインターフェイス グループ
宛先インターフェイス オブジェクト（Destination Interface Objects）	[いずれか（Any）]（すべてのプレフィルタルールのデフォルト）
選択された VLAN タグ（Selected VLAN Tags）	デフォルトなし（インポートした後に手動で条件を追加できます）

アクセス ルールのポート引数演算子

拡張アクセス ルールには、サービス オブジェクトで使用されるものと同じ演算子を使用する `port_argument` 要素が含まれている可能性があります。移行ツールは、アクセス ルールに単一のポート引数演算子が含まれているか、または複数のポート引数演算子が含まれているかによって、サービス オブジェクトを変換するときに同じ演算子を変換するのとは若干異なる方法で、アクセス ルール内のこれらの演算子を変換します。

次の表に、使用可能な演算子と、単一演算子の使用例を示します。

表 *10*：アクセス ルールのポート引数演算子

演算子	説明	例
lt	次の値より小さい。	access-list acp1 extended permit tcp any lt 300
gt	次の値より大きい。	access-list acp2 extended permit tcp any gt 300
eq	次の値と等しい。	access-list acp3 extended permit tcp any eq 300
neq	次の値と等しくない。	access-list acp4 extended permit tcp any neq 300
range	値の包括的な範囲。この演算子を使用する場合は、2つのポート番号を指定します（例：range 100 200）。	access-list acp5 extended permit tcp any range 9000 12000

アクセス ルールに単一のポート引数演算子が含まれている場合、移行ツールは、次のようにアクセス ルールを単一のアクセス コントロール ルールまたはプレフィルタ ルールに変換します。

表 *11*：アクセス コントロール ルールまたはプレフィルタ ルールに変換される単一のポート引数演算子を含むアクセス ルール

Op	名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	操作	有効（Enabled）
lt	acp1#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	1 ～ 299	任意（Any）	同等の許可	はい（True）
gt	acp2#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	301 ～ 65535	任意（Any）	同等の許可	はい（True）
eq	acp3#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	300	任意（Any）	同等の許可	はい（True）
neq	acp4#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	1 ～ 299、301 ～ 65535	任意（Any）	同等の許可	はい（True）
range	acp5#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	9000 ～ 2000	任意（Any）	同等の許可	はい（True）

この表の[元の演算子（Original Operator）]（[Op]）列は、わかりやすくするために示されており、アクセス コントロール ルールのフィールドを表すものではありません。

アクセス ルールに複数のポート演算子（たとえば、`access-list acp6 extended permit tcp any neq 300 any neq 400`）が含まれている場合、移行ツールは、次のように単一のアクセス ルールを複数のアクセス コントロール ルールまたはプレフィルタ ルールに変換します。

表 *12*：アクセス コントロール ルールに変換される複数のポート引数演算子を含むアクセス ルール

Op	名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	操作	有効（Enabled）
neq	acp6#1_1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	1 ～ 299	1 ～ 399	同等の許可	はい（True）
neq	acp6#1_2	任意（Any）	任意（Any）	任意（Any）	任意（Any）	301 ～ 65535	1 ～ 399	同等の許可	はい（True）
neq	acp6#1_3	任意（Any）	任意（Any）	任意（Any）	任意（Any）	1 ～ 299	401 ～ 65535	同等の許可	はい（True）
neq	acp6#1_4	任意（Any）	任意（Any）	任意（Any）	任意（Any）	301 ～ 65535	401 ～ 65535	同等の許可	はい（True）

この表の[元の演算子（Original Operator）]（[Op]）列は、わかりやすくするために示されており、アクセス コントロール ルールのフィールドを表すものではありません。

複数のプロトコルを指定するアクセス ルール

ASA では、複数のプロトコルを指定するプロトコル サービス オブジェクトを使用するように、アクセス ルールの送信元ポートおよび宛先ポートを設定できます（たとえば、TCP や UDP）。次に、例を示します。

```
object-group protocol TCPUDP
 protocol-object udp
 protocol-object tcp
access-list acp1 extended permit object-group TCPUDP any any
```

ただし、Firepower システムでは、アクセス コントロール ルールまたはプレフィルタ ルールは次のとおりにのみ設定できます。

- 送信元ポートおよび宛先ポートの両方が同じプロトコルを指定する必要があります。
- 宛先ポートは複数のプロトコルを指定できますが、送信元ポートは何も指定できません。

プロトコル オブジェクト グループ tcp および udp を含むアクセス ルールは、サポートされていないルールとして移行されます。そのため、ルールはコメント「**tcp および udp の両方を含むオブジェクト グループ プロトコルはサポートされていません（Object Group Protocol containing both tcp and udp is not supported）**」とともに無効になります。

NAT ルールの変換

次の表に要約しているように、ASA 向けの NAT および FirePOWER Threat Defense向けの NAT は、同等の機能をサポートしています。

表 *13*：*FirePOWER Threat DefenseNAT* ポリシーにマッピングされる *ASA NAT* ポリシー

ASA NAT ポリシー	FirePOWER Threat DefenseNAT ポリシー	特性の定義
Twice NAT	手動 NAT	• 1 つのルールで送信元と宛先両方のアドレスを指定します。 • 直接設定されます。 • ネットワーク オブジェクト グループを使用できます。 • NAT テーブルで手動で順序付けします（自動 NAT ルールの前または後）。
ネットワーク オブジェクト NAT	自動 NAT	• 送信元アドレスまたは宛先アドレスを指定します。 • ネットワーク オブジェクトのパラメータとして設定されます。 • ネットワーク オブジェクト グループは使用できません。 • NAT テーブルで自動的に順序付けされます。

移行ツールは、ASA NAT 設定をFirePOWER Threat DefenseNAT 設定に変換します。ただし、ツールは、サポートされていないネットワーク オブジェクトを使用している ASA NAT 設定は変換できません。そのような場合、変換は失敗します。

FirePOWER Threat Defenseルール フィールドにマッピングされる ASA NAT ルール フィールド

移行ツールは、次の表で説明するように、ASA NAT ルールのフィールドを FirePOWER Threat DefenseNAT ルールのフィールドに変換します。

（注）

- カラム 1（ASA NAT ルール フィールド）のフィールド名は、ASDM インターフェイスのフィールド ラベルに対応します。
- カラム 2（Firepower Threat Defense ルール フィールド）のフィールド名は、Firepower Management Centerインターフェイスのフィールド ラベルに対応します。

表 *14*：*FirePOWER Threat DefenseNAT* ルール フィールドにマッピングされる *ASA NAT* ルール フィールド

ASA NAT ルール フィールド	FirePOWER Threat Defenseルール フィールド
[元のパケット（Original Packet）] - [送信元インターフェイス（Source Interface）]	[インターフェイス オブジェクト（Interface Objects）] - [送信元インターフェイス オブジェクト（Source Interface Objects）]
[元のパケット（Original Packet）] - [送信元アドレス（Source Address）]	[元のパケット（Original Packet）] - [元の送信元（Original Source）]
[元のパケット（Original Packet）] - [宛先インターフェイス（Destination Interface）]	[インターフェイス オブジェクト（Interface Objects）] - [宛先インターフェイス オブジェクト（Destination Interface Objects）]
[元のパケット（Original Packet）] - [宛先アドレス（Destination Address）]	[元のパケット（Original Packet）] - [元の宛先（Original Destination）] - [アドレス タイプ（Address Type）] [元のパケット（Original Packet）] - [元の宛先（Original Destination）] - [ネットワーク（Network）]
[元のパケット（Original Packet）] - [サービス（Service）]	[元のパケット（Original Packet）] - [元の送信元ポート（Original Source Port）] [元のパケット（Original Packet）] - [元の宛先ポート（Original Destination Port）]
[変換されたパケット（Translated Packet）] - [送信元 NAT タイプ（Source NAT Type）]	タイプ（Type）
[変換されたパケット（Translated Packet）] - [送信元アドレス（Source Address）]	[変換されたパケット（Translated Packet）] - [変換された送信元（Translated Source）] - [アドレス タイプ（Address Type）] [変換されたパケット（Translated Packet）] - [変換された送信元（Translated Source）] - [ネットワーク（Network）]
[変換されたパケット（Translated Packet）] - [宛先アドレス（Destination Address）]	[変換されたパケット（Translated Packet）] - [変換された宛先（Translated Destination）]

ASA NAT ルール フィールド	FirePOWER Threat Defenseルール フィールド
[変換されたパケット（Translated Packet）] - [サービス（Service）]	[変換されたパケット（Translated Packet）] - [変換された送信元ポート（Translated Source Port）] [変換されたパケット（Translated Packet）] - [変換された宛先ポート（Translated Destination Port）]
1 対 1 アドレス変換を使用（Use one-to-one address translation）	[詳細設定（Advanced）] - [Net 間マッピング（Net to Net Mapping）]
PAT プール変換済みアドレス（PAT Pool Translated Address）	[PAT プール（PAT Pool）] - [PAT] - [アドレス タイプ（Address Type）] [PAT プール（PAT Pool）] - [PAT] - [ネットワーク（Network）]
ラウンドロビン	[PAT プール（PAT Pool）] - [ラウンド ロビン割り当てを使用（Use Round Robin Allocation）]
インターフェイス単位ではなく宛先単位の拡張 PAT 一意性（Extend PAT uniqueness to per destination instead of per interface）	[PAT プール（PAT Pool）] - [拡張 PAT テーブル（Extended PAT Table）]
TCP および UDP ポートをフラットな範囲 1024 ～ 65535 に変換する（Translate TCP and UDP ports into flat range 1024-65535）	[PAT プール（PAT Pool）] - [フラットなポート範囲（Flat Port Range）]
1 ～ 1023 の範囲を含む（Include range 1-1023）	[PAT プール（PAT Pool）] - [予約ポートを含む（Include Reserve Ports）]
ブロック割り当ての有効化（Enable Block Allocation）	対応なし
送信元インターフェイス PAT に IPv6 を使用する（Use IPv6 for source interface PAT）	対応なし
宛先インターフェイス PAT に IPv6 を使用する（Use IPv6 for destination interface PAT）	[詳細設定（Advanced）] - [IPv6]
ルールの有効化（Enable rule）	有効（Enable）
このルールに一致する DNS 応答を変換（Translate DNS replies that match this rule）	[詳細設定（Advanced）] - [このルールに一致する DNS 応答を変換（Translate DNS replies that match this rule）]

ASA NAT ルール フィールド	FirePOWER Threat Defenseルール フィールド
出力インターフェイスでプロキシ ARP を無効にする（Disable Proxy ARP on egress interface）	[詳細設定（Advanced）] - [宛先インターフェイスで ARP をプロキシしない（Do not proxy ARP on Destination Interface）]
ルートテーブルを検索して出力インターフェイスを見つける（Lookup route table to locate egress interface）	対応なし
方向（Direction）	[詳細設定（Advanced）] - [単方向（Unidirectional）]
説明	説明

ネットワークオブジェクトおよびネットワークオブジェクト グループの変換

ネットワーク オブジェクトおよびネットワーク オブジェクト グループは、IP アドレスまたはホスト名を識別します。ASA と FirePOWER Threat Defenseの両方で、これらのオブジェクトおよびグループをアクセス ルールと NAT ルールの両方に使用できます。

ASA では、1 つのネットワーク オブジェクトには、1 つのホスト、ネットワーク IP アドレス、IP アドレスの範囲、または完全修飾ドメイン名（FQDN）を入れることができます。Firepower システムでは、ネットワーク オブジェクトは、FQDN を除くこれらの同じ値をサポートしています。

オブジェクトが複数のアクセス ルールまたは NAT ルールで使用されているかどうかにかかわらず、移行ツールは ASA ネットワーク オブジェクトまたはグループを 1 回変換します。

ネットワーク オブジェクトの変換

変換する各 ASA ネットワーク オブジェクトに対し、移行ツールは Firepower ネットワーク オブジェクトを作成します。

移行ツールは、次のように ASA ネットワーク オブジェクトのフィールドを Firepower ネットワーク オブジェクトのフィールドに変換します。

表 *15*：*Firepower* ネットワーク オブジェクト フィールドにマッピングされる *ASA* ネットワーク オブジェクト フィールド

ASA ネットワーク オブジェクト フィールド	Firepower ネットワーク オブジェクト フィールド
[名前（Name）]	システムによって生成されます（を参照） 変換された設定の命名規則, （20 ページ）
タイプ（Type）	タイプ（Type）
IPバージョン	対応するフィールドなし
[IPアドレス（IP Address）]	値
ネットマスク	[値（Value）]（CIDR 表記に含まれている）
説明	説明
オブジェクト NAT アドレス（Object NAT Address）	対応するフィールドなし

例：アクセス コントロール リストのネットワーク オブジェクト

次のコマンドが ASA 設定ファイルにある場合：

```
object network obj1
 host 1.2.3.4
object network obj2
 range 1.2.3.7 1.2.3.10
object network obj3
 subnet 10.83.0.0 255.255.0.0
access-list sample_acl extended permit ip object obj1 object obj2
access-list sample_acl extended permit ip object obj3 object obj1
access-group gigabitethernet_access_in in interface gigabitethernet1/1
```

システムは、これらのオブジェクトを次のように変換します。

名前	ドメイン	値（ネットワーク）	タイプ（Type）	オーバーライド（Override）
obj1	None	1.2.3.4	ホスト	いいえ（False）
obj2	None	1.2.3.7 ～ 1.2.3.10	アドレス範囲（Address Range）	いいえ（False）
obj3	None	10.83.0.0/16	[ネットワーク（Network）]	いいえ（False）

例：NAT ルールのネットワーク オブジェクト

次のコマンドが ASA 設定ファイルにある場合：

```
nat (gigabitethernet1/1,gigabitethernet1/2) source static obj1 obj1
```

システムは、上記の例でアクセス ルール内のオブジェクト `obj1` を変換するのと同じ方法で、このルール内のオブジェクト `obj1` を変換します。

ネットワーク オブジェクト グループの変換

変換する各 ASA ネットワーク オブジェクト グループに対し、移行ツールは Firepower ネットワーク オブジェクト グループを作成します。また、グループに含まれているオブジェクトがまだ変換されていない場合は、そのオブジェクトも変換します。

移行ツールは、次のように ASA ネットワーク オブジェクト グループのフィールドを Firepower ネットワーク オブジェクト グループのフィールドに変換します。

表 *16*：*Firepower* ネットワーク オブジェクト グループ フィールドにマッピングされる *ASA* ネットワーク オブジェクト グループ フィールド

ASA ネットワーク オブジェクト グループ フィールド	Firepower ネットワーク オブジェクト グループ フィールド
グループ名（Group Name）	名前
説明	説明
グループ内のメンバー（Members In Group）	値（選択されたネットワーク）（Value (Selected Networks)）

例：アクセス コントロール リストのネットワーク オブジェクト グループ

次のコマンドが ASA 設定ファイルにある場合：

```
object network obj1
 host 1.2.3.4
object network obj2
 range 1.2.3.7 1.2.3.10
object network obj3
 subnet 10.83.0.0 255.255.0.0
object-group network obj_group1
 network-object object obj1
 network-object object obj2
 network-object object obj3
access-list sample_acl extended permit ip object-group obj_group1 any
access-group gigabitethernet_access_in in interface gigabitethernet1/1
```

システムは、次のネットワーク グループを作成します。

名前	ドメイン	値（ネットワーク）	タイプ（Type）	オーバーライド（Override）
obj_group1	なし	obj1 obj2 obj3	グループ	いいえ（False）

関連付けられているオブジェクトがまだ変換されていない場合、ネットワーク オブジェクトの変換, （35 ページ）で説明するように、システムはそのオブジェクトを変換します。

例：NAT ルールのネットワーク オブジェクト グループ

次のコマンドが ASA 設定ファイルにある場合：

```
nat (interface1,interface2) source static obj_group1 obj_group1
```

システムは、上記の例でアクセス ルール内の `obj_group1` を変換するのと同じ方法で、このルール内の `obj_group1` を変換します。

サービス オブジェクトおよびサービス グループの変換

ASA では、サービス オブジェクトおよびサービス グループがプロトコルとポートを指定し、それらのポートを送信元ポートまたは宛先ポートとして指定します。サービス オブジェクトおよびグループは、アクセス ルールおよび NAT ルールの両方で使用できます。

Firepower システムでは、ポート オブジェクトおよびポート オブジェクト グループがプロトコルとポートを指定しますが、システムがそれらのポートを送信元ポートまたは宛先ポートとして指定するのは、ユーザがオブジェクトをアクセス コントロール ルール、プレフィルタ ルール、または NAT ルールに追加する場合のみです。サービス オブジェクトを Firepower システムの同等機能に変換するために、移行ツールは、サービス オブジェクトをポート オブジェクトまたはポート グループに変換し、関連するアクセス コントロール ルール、プレフィルタ ルール、または NAT ルールに特定の変更を行います。その結果、変換中に、移行ツールは、単一のセキュリティ オブジェクトおよび関連するアクセス ルールまたは NAT ルールを複数のポート オブジェクトとグループおよび関連するアクセス コントロール ルール、プレフィルタ ルール、または NAT ルールに展開する場合があります。

サービス オブジェクトの変換

移行ツールは、1 つ以上のポート オブジェクトと、それらのポート オブジェクトを参照する 1 つ以上のアクセス コントロール ルールまたはプレフィルタ ルールを作成することによって、ASA サービス オブジェクトを変換します。

移行ツールは、次のサービス オブジェクト タイプを変換できます。

- [プロトコル（Protocol）]
- TCP/UDP

- ICMP/ICMPv6

移行ツールは、次のようにASAサービス オブジェクトのフィールドをFirepowerポート オブジェクトのフィールドに変換します。

表 *17*：*Firepower* ポート オブジェクト フィールドにマッピングされる *ASA* サービス オブジェクト フィールド

ASA サービス オブジェクト フィールド	ASA サービス オブジェクト タイプ	Firepower ポート オブジェクト フィールド
[名前（Name）]	任意（Any）	システムによって生成されます（変換された設定の命名規則, （20 ページ）を参照）
サービス タイプ（Service Type）	TCP/UDP、ICMP/ICMPv6	[プロトコル（Protocol）]
[プロトコル（Protocol）]	プロトコルのみ	[プロトコル（Protocol）]
説明	任意（Any）	対応なし、コンテンツは破棄されます
宛先ポート/範囲（Destination Port/Range）	TCP/UDP のみ	[ポート（Port）]
送信元ポート/範囲（Source Port/Range）	TCP/UDP のみ	[ポート（Port）]
ICMP タイプ（ICMP Type）	ICMP/ICMPv6 のみ	タイプ（Type）
ICMP コード（ICMP Code）	ICMP/ICMPv6 のみ	コード（Code）

サービス オブジェクトのポート リテラル値

ASAサービス オブジェクトは、ポート番号の代わりにポート リテラル値を指定できます。次に、例を示します。

```
object service http
 service tcp destination eq www
```

Firepowerシステムはこれらのポート リテラル値をサポートしていないため、移行ツールは、ポート リテラル値をその値が表すポート番号に変換します。ツールは、上記の例を次のポート オブジェクトに変換します。

名前	タイプ（Type）	ドメイン	値（プロトコル/ポート）	オーバーライド（Override）
http	オブジェクト	なし	TCP(6)/80	いいえ（False）

ポート リテラル値と関連付けられているポート番号の完全なリストについては、『*CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide*』の「TCP and UDP Ports」を参照してください。

サービス オブジェクトのポート引数演算子

ASA サービス オブジェクトは、ポート引数に次の演算子を使用できます。

表 *18*：サービス オブジェクトのポート引数演算子

演算子	説明	例
`lt`	次の値より小さい。	`object service testOperator` ` service tcp source lt 100`
`gt`	次の値より大きい。	`object service testOperator` ` service tcp source gt 100`
`eq`	次の値と等しい。	`object service http-proxy` ` service tcp source eq 8080`
`neq`	次の値と等しくない。	`object service testOperator` ` service tcp source neq 200`
`range`	値の包括的な範囲。	`object service http-proxy` ` service tcp source range 9000 12000`

移行ツールは、次のようにこれらの演算子を変換します。

表 *19*：ポート オブジェクトとグループに変換されるポート引数演算子を含むサービス オブジェクト

演算子	変換先	ポートオブジェクト値の例（プロトコル/ポート）
lt	指定した番号未満のポート番号の範囲を指定する単一のポート オブジェクト。	TCP(6)/1-99
gt	指定した番号より大きいポート番号の範囲を指定する単一のポート オブジェクト。	TCP(6)/101-65535
eq	単一のポート番号を指定する単一のポートオブジェクト。	TCP(6)/8080
neq	2 つのポート オブジェクトおよび 1 つのポート オブジェクト グループ。最初のポート オブジェクトは、指定されたポートよりも低い範囲を指定します。2番目のポートオブジェクトは、指定されたポートよりも高い範囲を指定します。ポート オブジェクト グループには、両方のポートオブジェクトが含まれています。	最初のオブジェクト（testOperator_src_1）： TCP(6)/1-199 2 番目のオブジェクト（testOperator_src_2）： TCP(6)/201-65535 オブジェクト グループ（testOperator_src）： testOperator_src_1 testOperator_src_2
range	値の包括的な範囲を指定する単一のポートオブジェクト。	TCP(6)/9000-12000

送信元ポートと宛先ポートを含むサービス オブジェクト

ASA では、単一のサービス オブジェクトで、送信元と宛先の両方にポートを指定できます。Firepowerシステムでは、ポートオブジェクトはポート値のみを指定します。アクセス コントロール ルールまたはプレフィルタ ルールでポート オブジェクトが使用されるまで、システムはポートを送信元または宛先として指定しません。

この違いに対応するために、移行ツールは、送信元と宛先の両方を指定する ASA サービス オブジェクトを変換する際に、単一のオブジェクトを 2 つのポート オブジェクトに展開します。元の指定を示すための拡張子がオブジェクト名に追加されます。送信元ポートの場合は *_src*、宛先ポートの場合は *_dst* です。

例

```
object service http-proxy
 service tcp source range 9000 12000 destination eq 8080
```

ツールは、このサービス オブジェクトを次のポート オブジェクトに変換します。

名前	タイプ（Type）	ドメイン	値（プロトコル/ポート）	オーバーライド（Override）
http-proxy_src	オブジェクト	なし	TCP(6)/9000 ～ 12000	いいえ（False）
http-proxy_dst	オブジェクト	なし	TCP(6)/8080	いいえ（False）

例：プロトコル サービス オブジェクトの変換

ASA の設定：

```
object service protocolObj1
 service snp
 description simple routing
```

変換先：

表 *20*：ポート オブジェクト

名前	タイプ（Type）	ドメイン	値（プロトコル）	オーバーライド（Override）
protocolObj1	オブジェクト	なし	SNP（109）	いいえ（False）

例：TCP/UDP サービス オブジェクトの変換

ASA の設定：

```
object service servObj1
 service tcp destination eq ssh
```

変換先：

表 *21*：ポート オブジェクト

名前	タイプ（Type）	ドメイン	値（プロトコル/ポート）	オーバーライド（Override）
servObj1	オブジェクト	なし	TCP(6)/22	いいえ（False）

例：ICMP/ICMPv6 サービス オブジェクトの変換

ICMP

ASA の設定：

```
object service servObj1
 service icmp alternate-address 0
```

変換先：

表 *22*：ポート オブジェクト

名前	タイプ（Type）	ドメイン	値（プロトコル/タイプ：コード）	オーバーライド（Override）
servObj1	オブジェクト	なし	ICMP(1)/代替ホストアドレス：ホストの代替アドレス	いいえ（False）

ICMPv6

ASA の設定：

```
object service servObj1
 service icmp6 unreachable 0
```

変換先：

表 *23*：ポート オブジェクト

名前	タイプ（Type）	ドメイン	値（プロトコル/タイプ：コード）	オーバーライド（Override）
servObj1	オブジェクト	なし	IPV6-ICMP (58)/宛先到達不能：接続先へのルートなし	いいえ（False）

サービス グループの変換

移行ツールは、関連するアクセス コントロール ルールまたはプレフィルタ ルールを使用して、ポート オブジェクト グループおよび関連するポート オブジェクト グループを作成することで、ASA サービス グループを変換します。

移行ツールは、次のサービス グループ タイプを変換できます。

- [プロトコル（Protocol）]
- TCP/UDP

- ICMP/ICMPv6

移行ツールは、次のようにASAサービス オブジェクトのフィールドをFirepowerポート オブジェクトのフィールドに変換します。

表 *24*：*Firepower* ポート オブジェクト フィールドにマッピングされる *ASA* サービス グループ フィールド

ASA サービス グループ フィールド	ポート オブジェクト グループ フィールド
[名前（Name）]	システムによって生成されます（変換された設定の命名規則, （20 ページ）を参照）
説明	説明
グループ内のメンバー（Members In Group）	選択したポート（Selected Ports）

ネストされたサービス グループの変換

ASAは、ネストされたサービス グループ（つまり、他のサービス グループを含むサービス グループ）をサポートしています。Firepowerシステムは、ネストされたポート オブジェクト グループをサポートしていませんが、複数のグループを単一のアクセス コントロール ルールまたはプレフィルタ ルールに関連付けることで同等の機能を実現できます。ネストされたサービス グループを変換する場合、移行ツールはグループ構造をフラット化し、最深部のサービス オブジェクトおよびグループをポート オブジェクトおよびポート オブジェクト グループに変換し、それらの変換されたグループをアクセス コントロール ルールまたはプレフィルタ ルールに関連付けます。

最大50のポート オブジェクトを単一のアクセス コントロール ルールまたはプレフィルタ ルールに関連付けることができます。新しいポート オブジェクトの数が50を超えると、ツールによって、新しいすべてのポート オブジェクトがルールに関連付けられるまで、重複アクセス コントロール ルールまたはプレフィルタ ルールが作成されます。

送信元と宛先両方のサービスとして使用されるネストされたサービス オブジェクトを含むFirepowerシステムのルールはサポートされていません。

例

```
object-group service http-8081 tcp
 port-object eq 80
 port-object eq 81

object-group service http-proxy tcp
 port-object eq 8080

object-group service all-http tcp
 group-object http-8081
 group-object http-proxy

access-list FMC_inside extended permit tcp host 33.33.33.33 object-group all-http host
33.33.33.33 object-group all-http
```

上記の例では、サービス オブジェクト *http-8081* および *http-proxy* は *all-http* サービス グループ内にネストされます。

このようなシナリオでは、ポート オブジェクトに関連するルールは無視されます。システムは、オブジェクトをインポートしますが、関連するアクセス コントロール ルールまたはプレフィルタ ルールは無効にし、次のコメントをルールに追加します。**Nested service groups at both Source and Destination are not supported**。

変換されたサービス オブジェクト、サービス グループ、およびシステムが変換時に作成する可能性がある重複ルールに対しツールが使用する命名規則の説明については、を参照してください。変換された設定の命名規則, （20 ページ）

例

ASA の設定：

```
object-group service legServGroup1 tcp
 port-object eq 78
 port-object eq 79
object-group service legServGroup2 tcp
 port-object eq 80
 port-object eq 81
object-group service legacyServiceNestedGrp tcp
 group-object legServGroup1
 group-object legServGroup2
access-list  acp1 extended permit tcp  3.4.5.0  255.255.255.0  5.6.7.0 255.255.255.0
object-group legacyServiceNestedGrp
access-group acp1 global
```

変換先：

表 *25*：ポート オブジェクト グループ

名前	タイプ（**Type**）	ドメイン	値（プロトコル/ポート）	オーバーライド（**Override**）
legServGroup1_1	オブジェクト	なし	TCP(6)/78	いいえ（False）
legServGroup1_2	オブジェクト	なし	TCP(6)/79	いいえ（False）
legServGroup2_1	オブジェクト	なし	TCP(6)/80	いいえ（False）
legServGroup2_2	オブジェクト	なし	TCP(6)/81	いいえ（False）
legServGroup1	グループ	なし	legServGroup1_1 legServGroup1_2	いいえ（False）
legServGroup2	グループ	なし	legServGroup2_1 legServGroup2_2	いいえ（False）

表 *26*：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

名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	操作	有効（Enabled）
acp1#1	任意（Any）	任意（Any）	3.4.5.0/24	5.6.7.0/24	TCP(6)	legServGroup1 legServGroup2	同等の許可	はい（True）

例：プロトコル サービス グループの変換

ASA の設定：

```
object-group protocol TCPUDP
 protocol-object udp
 protocol-object tcp
```

変換先：

表 *27*：ポート オブジェクトおよびグループ

名前	タイプ（Type）	ドメイン	値（プロトコル/ポート）	オーバーライド（Override）
TCPUDP_1	オブジェクト	なし	TCP(6)	いいえ（False）
TCPUDP_2	オブジェクト	なし	UDP(17)	いいえ（False）
TCPUDP	グループ	なし	TCPUDP_1 TCPUDP_2	いいえ（False）

例：TCP/UDP サービス グループの変換

グループの作成時に作成されるオブジェクト

ASA では、サービス グループの作成中にオブジェクトをその場で作成できます。これらのオブジェクトは、サービス オブジェクトとして分類されますが、ASA 設定ファイル内のエントリは `object service` の代わりに `port-object` を使用します。これらのオブジェクトは個別に作成されないため、移行ツールは、グループの作成とは関係なく作成されるオブジェクト用のものとは若干異なる命名規則を使用します。

ASA の設定：

```
object-group service servGrp5 tcp-udp
 port-object eq 50
 port-object eq 55
```

変換先：

表 *28*：ポート オブジェクトおよびグループ

名前	タイプ（**Type**）	ドメイン	値（プロトコル/ポート）	オーバーライド（**Override**）
servGrp5_1	オブジェクト	なし	TCP(6)/50	いいえ（False）
servGrp5_2	オブジェクト	なし	TCP(6)/55	いいえ（False）
servGrp5	グループ	なし	servGrp5_1 servGrp5_2	いいえ（False）

グループから独立して作成されるオブジェクト

ASA の設定：

```
object service servObj1
 service tcp destination eq ssh
object service servObj2
 service udp destination eq 22
object service servObj3
 service tcp destination eq telnet
object-group service servGrp1
 service-object object servObj1
 service-object object servObj2
 service-object object servObj3
```

変換先：

表 *29*：ポート オブジェクトおよびグループ

名前	タイプ（**Type**）	ドメイン	値（プロトコル/ポート）	オーバーライド（**Override**）
servObj1	オブジェクト	なし	TCP(6)/22	いいえ（False）
servObj2	オブジェクト	なし	UDP(17)/22	いいえ（False）
servObj3	オブジェクト	なし	TCP(6)/23	いいえ（False）
servGrp1	グループ	なし	servObj1 servObj2 servObj3	いいえ（False）

例：ICMP/ICMPv6 サービス グループの変換

ICMP

ASA の設定：

```
object-group icmp-type servGrp4
 icmp-object echo-reply
```

変換先：

表 *30*：ポート オブジェクトおよびグループ

名前	タイプ（Type）	ドメイン	値（プロトコル/ポート）	オーバーライド（Override）
servGrp4_1	オブジェクト	なし	ICMP(1)/Echo 応答	いいえ（False）
servGrp4	グループ	なし	servGrp4_1	いいえ（False）

ICMPv6

ASA の設定：

```
object-group service servObjGrp3
 service-object icmp6 packet-too-big
 service-object icmp6 parameter-problem
```

変換先：

表 *31*：ポート オブジェクトおよびグループ

名前	タイプ（Type）	ドメイン	値（プロトコル/ポート）	オーバーライド（Override）
servObjGrp3_1	オブジェクト	なし	IPV6-ICMP(58)/2	いいえ（False）
servObjGrp3_2	オブジェクト	なし	IPV6-ICMP(58)/4	いいえ（False）
servObjGrp3	グループ	なし	servObjGrp3_1 servObjGrp3_2	いいえ（False）

アクセス グループの変換

ASA で ACL を適用するには、CLI で `access-group` コマンドを入力するか、または ASDM アクセス ルール エディタで [適用（Apply）]を選択します。これらの操作はどちらも、ASA 設定ファイル内に `access-group` エントリを生成します（次の例を参照）。

access-group コマンドは、システムが ACL を適用するインターフェイスと、システムがそのインターフェイスのインバウンド（入力）またはアウトバウンド（出力）トラフィックのどちらに ACL を適用するかを指定します。

Firepower システムで同等の機能を設定するには、次の手順を実行します。

- セキュリティ ゾーンを作成し、セキュリティ ゾーンをインターフェイスに関連付け、セキュリティ ゾーンを送信元ゾーン条件（着信トラフィック用）または宛先ゾーン条件（発信トラフィック用）としてアクセス コントロール ルールに追加します。
- インターフェイス グループを作成し、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、インターフェイス グループを送信元インターフェイス グループ条件（着信トラフィック用）または宛先インターフェイス グループ条件（発信トラフィック用）としてプレフィルタ ルールに追加します。

access-group コマンドを変換すると、移行ツールは、セキュリティ ゾーンまたはインターフェイス グループを作成し、セキュリティ ゾーンおよびインターフェイス グループを関連するアクセス コントロール ルールまたはプレフィルタ ルールに条件として追加することで、イングレスとイーグレスの情報をキャプチャします。ただし、移行ツールは、セキュリティ ゾーンまたはインターフェイス グループの名前にインターフェイス情報を保持しますが、関連付けられているインターフェイスまたはデバイスの設定は変換しないので、変換されたポリシーをインポートした後に手動で追加する必要があります。変換されたポリシーをインポートした後、ポリシーをデバイスに、セキュリティ ゾーンまたはインターフェイス グループをインターフェイスに手動で関連付ける必要があります。

ACL を変換すると、ルールが特定のインターフェイスに適用された後でシステムはグローバルに適用されるルールを配置します。

特殊ケース

ASA の設定によって、単一の ACL が入力と出力両方のインターフェイスに適用される場合、ツールは ACL をアクセス コントロール ルールまたはプレフィルタ ルールの次の 2 つのセットに変換します。

- 入力ルールのセット（有効）
- 出力ルールのセット（無効）

ASA の設定によって、単一の ACL がグローバルに適用され、かつ特定のインターフェイスにも適用される場合、ツールは ACL をアクセス コントロール ルールまたはプレフィルタ ルールの次の 2 つのセットに変換します。

- 特定のインターフェイスに関連付けられているルールのセット（有効）
- 送信元と宛先のゾーンが [いずれか（Any）]に設定されているルールのセット（有効）

例：グローバルに適用される ACL

ASA の設定：

```
access-list global_access extended permit ip any any
access-group global_access global
```

移行ツールはこの設定を以下に変換します。

表 *32*：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

名前	送信元ゾーン/Int Grp	宛先ゾーン/Int Grp	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	操作	有効（Enabled）
global_access#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	任意（Any）	任意（Any）	同等の許可	はい（True）

例：特定のインターフェイスに適用される ACL

ASA の設定：

```
access-list acp1 permit tcp any host 209.165.201.3 eq 80
access-group acp1 in interface outside
```

この例では、`access-group` コマンドは、`acp1` という名前の ACL を `outside` という名前のインターフェイスの着信トラフィックに適用しています。

移行ツールはこの設定を以下に変換します。

表 *33*：セキュリティ ゾーン/インターフェイス グループ

名前	インターフェイス タイプ	ドメイン	選択されたインターフェイス
acp1_outside_in_zone	• ルーテッド（ASA デバイスがルーテッド モードで動作している場合） • スイッチド（ASA デバイスがトランスペアレント モードで動作している場合）	None	任意（Any）

表 *34*：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

名前	送信元ゾーン/Int Grp	宛先ゾーン/Int Grp	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	操作	有効（Enabled）
acp1#1	acp1_outside_in_zone	任意（Any）	任意（Any）	209.165.201.3	任意（Any）	TCP(6)/80	同等の許可	はい（True）

付 録 B

変換の例

この項には、ASA 設定の例と、移行ツールが変換先とする FirePOWER Threat Defenseのルールおよびオブジェクトの例が含まれています。

- 例，51 ページ

例

個々のネットワークを指定するアクセス ルール

ASA の設定：

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 5.6.7.0 255.255.255.0
access-group acp1 global
```

変換先：

表 *35*：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

名前	送信元ゾーン（Source Zone）	宛先ゾーン（Destination Zone）	送信元ネットワーク	宛先ネットワーク	送信元ポート	接続先ポート	操作	有効（Enabled）
acp1#1	任意（Any）	任意（Any）	3.4.5.0/24	5.6.7.0/24	TCP(6)	任意（Any）	同等の許可	はい（True）

ネットワーク オブジェクト グループによるアクセス ルール

ASA の設定：

```
access-list acp1 extended permit ip object-group host1 object-group host2
access-group acp1 global
```

変換先：

表 *36*：ネットワーク オブジェクト グループ

名前	ドメイン	値（ネットワーク）	タイプ（**Type**）	オーバーライド（**Override**）
host1	なし	obj1 obj2	グループ	いいえ（False）
host2	None	obj3 obj4	グループ	いいえ（False）

表 *37*：ネットワーク オブジェクト グループを使用したアクセス ルール

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン（**Destination Zone**）	送信元ネットワーク	宛先ネットワーク	送信元ポート（**Source Port**）	宛先ポート（**Destination Port**）	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	host1	host2	任意（Any）	任意（Any）	同等の許可	はい（True）

個々のネットワークおよびポートを指定するアクセス ルール

ASA アクセス ルール

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 eq 90 5.6.7.0 255.255.255.0 eq
80
access-group acp1 global
```

変換先：

表 *38*：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

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン（**Destination Zone**）	送信元ネットワーク	宛先ネットワーク	送信元ポート（**Source Port**）	宛先ポート（**Destination Port**）	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	3.4.5.0/32	5.6.7.0/32	TCP(6)/90	TCP(6)/80	同等の許可	はい（True）

サービス オブジェクトによるアクセス ルール

ASA の設定：

```
object service servObj1
 service tcp destination eq 78
access-list acp1 extended permit object servObj1 any any
access-group acp1 in interface outside
```

変換先：

表 *39*：ポート オブジェクト

名前	タイプ（**Type**）	ドメイン	値（プロトコル/ポート）	オーバーライド（**Override**）
servObj1	オブジェクト	なし	TCP(6)/78	いいえ（False）

表 *40*：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

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン（**Destination Zone**）	送信元ネットワーク	宛先ネットワーク	送信元ポート（**Source Port**）	宛先ポート（**Destination Port**）	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	任意（Any）	servObj1	同等の許可	はい（True）

サービス オブジェクト グループによるアクセス ルール

ASA の設定：

```
object-group service legServGroup tcp
 port-object eq 78
access-list  acp1 extended permit tcp  3.4.5.0  255.255.255.0  5.6.7.0 255.255.255.0
object-group legServGroup
access-group acp1 global
```

変換先：

表 *41*：ポート オブジェクト

名前	タイプ（**Type**）	ドメイン	値（プロトコル/ポート）	オーバーライド（**Override**）
legServGroup	オブジェクト	None	TCP(6)/78	いいえ（False）

表 *42*：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

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン（**Destination Zone**）	送信元ネットワーク	宛先ネットワーク	送信元ポート（**Source Port**）	[接続先ポート（**Destination Port**）]	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	3.4.5.0/24	5.6.7.0/24	TCP(6)	legServGroup	同等の許可	はい（True）

ネストされたサービス オブジェクト グループによるアクセス ルール

ASA の設定：

```
object-group service legServGroup1 tcp
 port-object eq 78
 port-object eq 79
object-group service legServGroup2 tcp
 port-object eq 80
 port-object eq 81
object-group service legacyServiceNestedGrp tcp
 group-object legServGroup1
 group-object legServGroup2
access-list  acp1 extended permit tcp  3.4.5.0  255.255.255.0  5.6.7.0 255.255.255.0
object-group legacyServiceNestedGrp
access-group acp1 global
```

変換先：

表 *43*：ポート オブジェクトおよびグループ

名前	タイプ（**Type**）	ドメイン	値（プロトコル/ポート）	オーバーライド（**Override**）
legServGroup1_1	オブジェクト	None	TCP(6)/78	いいえ（False）
legServGroup1_2	オブジェクト	なし	TCP(6)/79	いいえ（False）
legServGroup2_1	オブジェクト	なし	TCP(6)/80	いいえ（False）
legServGroup2_2	オブジェクト	None	TCP(6)/81	いいえ（False）
legServGroup1	グループ	なし	legServGroup1_1 legServGroup1_2	いいえ（False）
legServGroup2	グループ	なし	legServGroup2_1 legServGroup2_2	いいえ（False）

変換された設定には、ネストされたグループ legacyServiceNestedGrp に相当するものは含まれていないことに注意してください。そのグループはフラット化されていないためです。

表 *44*：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

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン（**Destination Zone**）	送信元ネットワーク	宛先ネットワーク	送信元ポート	[接続先ポート（**Destination Port**）]	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	3.4.5.0/24	5.6.7.0/24	TCP(6)	legServGroup1 legServGroup2	同等の許可	はい（True）

ネストされた拡張サービス オブジェクト グループによるアクセス ルール

ASA の設定：

```
object service http
 service tcp source range 9000 12000 destination eq www
object service http-proxy
 service tcp source range 9000 12000 destination eq 8080
object-group service all-http
 service-object object http
 service-object object http-proxy
object-group service all-httpz
 group-object all-http
 service-object tcp destination eq 443
access-list acp1 extended permit object-group all-httpz any any
access-group acp1 in interface inside
```

変換先：

表 *45*：ポート オブジェクト

名前	タイプ（**Type**）	ドメイン	値（プロトコル/ポート）	オーバーライド（**Override**）
http_src	オブジェクト	None	TCP(6)/9000 ～ 12000	いいえ（False）
http_dst	オブジェクト	None	TCP(6)/80	いいえ（False）
http-proxy_src	オブジェクト	None	TCP(6)/9000 ～ 12000	いいえ（False）
http-proxy_dst	オブジェクト	None	TCP(6)/8080	いいえ（False）
all-httpz-dst	グループ	なし	TCP(6)/443	いいえ（False）

変換された設定には、ネストされたグループ all-httpz に相当するものは含まれていないことに注意してください。そのグループはフラット化されていないためです。

表 *46*：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

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	[接続先ポート（**Destination Port**）]	操作	有効（**Enabled**）
acp1#1_1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	http_src	http_dst	同等の許可	はい（True）
acp1#1_2	任意（Any）	任意（Any）	任意（Any）	任意（Any）	http-proxy_src	http-proxy_dst	同等の許可	はい（True）

名前	送信元ゾーン（Source Zone）	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	[接続先ポート（Destination Port）]	操作	有効（Enabled）
acp1#1_3	任意（Any）	任意（Any）	任意（Any）	任意（Any）	任意（Any）	all-httpz-dst	同等の許可	はい（True）

「gt」および「neq」演算子を使用したサービス オブジェクトによるアクセス ルール

ASA の設定：

```
object service testOperator
 service tcp source gt 100 destination neq 200
access-list acp1 extended permit object testOperator any any
```

変換先：

表 *47*：ポート オブジェクト

名前	タイプ（Type）	ドメイン	値（プロトコル/ポート）	オーバーライド（Override）
testOperator_src	オブジェクト	なし	TCP(6)/101 ～ 65535	いいえ（False）
testOperator_dst_1	オブジェクト	なし	TCP(6)/1 ～ 199	いいえ（False）
testOperator_dst_2	オブジェクト	None	TCP(6)/201 ～ 65535	いいえ（False）
testOperator_dst	グループ	なし	testOperator_dst_1、testOperator_dst_2	いいえ（False）

表 *48*：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

名前	送信元ゾーン（Source Zone）	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	接続先ポート	操作	有効（Enabled）
acp1#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	testOperator_src	testOperator_dst	同等の許可	はい（True）

「lt」および「gt」演算子を使用したセキュリティ オブジェクトによるアクセス ルール

ASA の設定：

```
object service testOperator
 service tcp source gt 100 destination lt 200
access-list acp1 extended permit object testOperator any any
```

変換先：

表 *49*：ポート オブジェクト

名前	タイプ（**Type**）	ドメイン	値（プロトコル/ポート）	オーバーライド（**Override**）
testOperator_src	オブジェクト	なし	TCP(6)/101 ～ 65535	いいえ（False）
testOperator_dst	オブジェクト	なし	TCP(6)/1 ～ 199	いいえ（False）

表 *50*：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

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	[接続先ポート（**Destination Port**）]	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	testOperator_src	testOperator_dst	同等の許可	はい（True）

「eq」演算子とポート リテラル値を使用した TCP サービス オブジェクトによるアクセス ルール

ASA の設定：

```
object service svcObj1
 service tcp source eq telnet destination eq ssh
access-list acp1 extended permit object testOperator any any
```

変換先：

表 *51*：ポート オブジェクト

名前	タイプ（**Type**）	ドメイン	値（プロトコル/ポート）	オーバーライド（**Override**）
svcObj1_src	オブジェクト	なし	TCP(6)/21	いいえ（False）
svcObj1_dst	オブジェクト	なし	TCP(6)/22	いいえ（False）

表 *52*：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

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート（**Destination Port**）	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	svcObj1_src	svcObj1_dst	同等の許可	はい（True）

ICMP サービス オブジェクトによるアクセス ルール

ASA の設定：

```
object-group service icmpObj
 service-object icmp echo-reply 8
 access-list acp1 extended permit object icmpObj any any
```

変換先：

表 *53*：ポート オブジェクト

名前	タイプ（**Type**）	ドメイン	値（プロトコル/ポート）	オーバーライド（**Override**）
icmpObj	オブジェクト	なし	ICMP(1)/Echo 応答	いいえ（False）

表 *54*：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

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン（**Destination Zone**）	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート（**Destination Port**）	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	任意（Any）	icmpObj	同等の許可	はい（True）

プロトコル サービス オブジェクトによるアクセス ルール

ASA の設定：

```
object-group protocol testProtocol
 protocol-object tcp
access-list acp1 extended permit object testProtocol any any
```

変換先：

表 *55*：ポート オブジェクト

名前	タイプ（**Type**）	ドメイン	値（プロトコル/ポート）	オーバーライド（**Override**）
testProtocol	オブジェクト	なし	TCP(6)	いいえ（False）

表 *56*：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

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート（**Destination Port**）	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	任意（Any）	testProtocol	同等の許可	はい（True）

拡張サービス オブジェクトによるアクセス ルール（送信元のみ）

ASA の設定：

```
object service serviceObj
 service tcp source eq 300
 service tcp source eq 800
access-list acp1 extended permit object serviceObj any any
```

変換先：

表 *57*：ポート オブジェクト

名前	タイプ（**Type**）	ドメイン	値（プロトコル/ポート）	オーバーライド（**Override**）
serviceObj_src_1	オブジェクト	None	TCP(6)/300	いいえ（False）
serviceObj_src_2	オブジェクト	None	TCP(6)/800	いいえ（False）
serviceObj	グループ	なし	serviceObj_src_1 serviceObj_src_2	いいえ（False）

表 *58*：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

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン（**Destination Zone**）	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート（**Destination Port**）	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	任意（Any）	serviceObj	同等の許可	はい（True）

拡張サービス オブジェクトによるアクセス ルール（送信元と宛先）

ASA の設定：

```
object service serviceObj
 service tcp source eq 300 destination eq 400
access-list acp1 extended permit tcp object serviceObj any any
```

変換先：

表 *59*：ポート オブジェクト

名前	タイプ（**Type**）	ドメイン	値（プロトコル/ポート）	オーバーライド（**Override**）
serviceObj_src	オブジェクト	なし	TCP(6)/300	いいえ（False）
serviceObj_dst	オブジェクト	なし	TCP(6)/400	いいえ（False）

表 *60*：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

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート（**Destination Port**）	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	serviceObj_src	serviceObj_dst	同等の許可	はい（True）

送信元ポートでポート引数演算子「**neq**」を使用したアクセス ルール

ASA の設定：

```
access-list acp1 extended permit tcp any neq 300
```

変換先：

表 *61*：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

名前	送信元ゾーン（Source Zone）	宛先ゾーン（Destination Zone）	送信元ネットワーク	宛先ネットワーク	送信元ポート	接続先ポート（Destination Port）	アクション（Action）	有効（Enabled）
acp1#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	1 ～ 299、301 ～ 65535	任意（Any）	同等の許可	はい（True）

送信元ポートおよび宛先ポートでポート引数演算子「neq」を使用したアクセス ルール

ASA の設定：

```
access-list acp1 extended permit tcp any neq 300 any neq 400
```

変換先：

表 *62*：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

名前	送信元ゾーン（Source Zone）	宛先ゾーン（Destination Zone）	送信元ネットワーク	宛先ネットワーク	送信元ポート	接続先ポート（Destination Port）	操作	有効（Enabled）
acp1#1_1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	1 ～ 299	1 ～ 399	同等の許可	はい（True）
acp1#1_2	任意（Any）	任意（Any）	任意（Any）	任意（Any）	301 ～ 65535	1 ～ 399	同等の許可	はい（True）
acp1#1_3	任意（Any）	任意（Any）	任意（Any）	任意（Any）	1 ～ 299	401 ～ 65535	同等の許可	はい（True）
acp1#1_4	任意（Any）	任意（Any）	任意（Any）	任意（Any）	301 ～ 65535	401 ～ 65535	同等の許可	はい（True）

非アクティブ アクセス ルール

ASA の設定：

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 5.6.7.0 255.255.255.0 inactive
access-group acp1 global
```

変換先：

表 *63*：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

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン（**Destination Zone**）	送信元ネットワーク	宛先ネットワーク	送信元ポート	接続先ポート（**Destination Port**）	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	3.4.5.0/24	5.6.7.0/24	TCP(6)	任意（Any）	同等の許可	いいえ（False）

着信トラフィックに適用されるアクセス コントロール リスト

ASA の設定：

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 eq 90 any eq 80
access-group acp1 in inside
```

変換先：

表 *64*：セキュリティ ゾーン/インターフェイス グループ

名前	インターフェイス タイプ	ドメイン	選択されたインターフェイス
acp1_inside_in_zone	• ルーテッド（ASA デバイスがルーテッドモードで動作している場合） • スイッチド（ASAデバイスがトランスペアレントモードで動作している場合）	なし	任意（Any）

表 *65*：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

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート（**Destination Port**）	アクション	有効（**Enabled**）
acp1#1	acp1_inside_in_zone	任意（Any）	3.4.5.0/24	任意（Any）	TCP(6)/90	TCP(6)/80	同等の許可	はい（True）

発信トラフィックに適用されるアクセス コントロール リスト

ASA の設定：

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 eq 90 any eq 80
access-group acp1 out outside
```

変換先：

表 *66*：セキュリティ ゾーン/インターフェイス グループ

名前	インターフェイス タイプ	ドメイン	選択されたインターフェイス
acp1_outside_out_zone	• ルーテッド（ASA デバイスがルーテッドモードで動作している場合） • スイッチド（ASAデバイスがトランスペアレントモードで動作している場合）	なし	任意（Any）

表 *67*：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

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート（**Destination Port**）	操作	有効（**Enabled**）
acp1#1	acp1_outside_out_zone	任意（Any）	3.4.5.0/24	任意（Any）	TCP(6)/90	TCP(6)/80	同等の許可	はい（True）