Firewall 移行ツールの実行

Cisco.com から Firewall 移行ツールのダウンロード

始める前に

Cisco.com へのインターネット接続が可能な Windows 10 64 ビットまたは macOS バージョン 10.13 以降のマシンが必要です。

手順

ステップ 1 コンピュータで、Firewall 移行ツール用のフォルダを作成します。

このフォルダには、他のファイルを保存しないことをお勧めします。Firewall 移行ツールを起動すると、ログ、リソース、およびその他すべてのファイルがこのフォルダに配置されます。

（注） Firewall 移行ツールの最新バージョンをダウンロードする場合は、必ず新しいフォルダを作成し、既存のフォルダは使用しないでください。

ステップ 2 https://software.cisco.com/download/home/286306503/type を参照し、[Firewall移行ツール（Firewall Migration Tool）] をクリックします。

上記のリンクをクリックすると、[Firewall NGFWバーチャル（Firewall NGFW Virtual）] の [Firewall移行ツール（Firewall Migration Tool）] に移動します。脅威に対する防御デバイスのダウンロード領域から Firewall 移行ツールをダウンロードすることもできます。

ステップ 3 Firewall 移行ツールの最新バージョンを、作成したフォルダにダウンロードします。

Windows 用または macOS マシン用の適切な Firewall 移行ツール実行可能ファイルをダウンロードします。

次のタスク

ASA 構成ファイルの取得

ASA 構成ファイルの取得

ASA 構成ファイルを取得するには、次のいずれかの方法を使用できます。

- ASA 構成ファイルのエクスポート （2 ページ）
- Firewall 移行ツールから ASA への接続 （6 ページ）

ASA 構成ファイルのエクスポート

このタスクは、ASA 構成ファイルを手動でアップロードする場合にのみ必要です。ASAから Firewall 移行ツール に接続する場合は、Firewall 移行ツールから ASA への接続 （6 ページ）に進みます。

（注） ファイルをエクスポートした後、ASA 構成を手動でコーディングしたり、変更を加えたりしないでください。これらの変更は Secure Firewall Threat Defense に移行されず、移行でエラーが発生するか、移行が失敗します。たとえば、端末で構成ファイルを開いて保存すると、 Firewall 移行ツールで解析できない空白または空白行が追加されることがあります。

エクスポートされた ASA 構成ファイルに "--More--" キーワードがテキストとして含まれていないことを確認します。含まれていると、移行が失敗する可能性があります。

手順

ステップ 1 移行する ASA デバイスまたはコンテキストに対して **show running-config** コマンドを使用し、そこから構成をコピーします。「View the Running Configuration」を参照してください。

または、移行する ASA デバイスまたはコンテキストに対して Adaptive Security Device Manager（ASDM）を使用し、**[ファイル（File）] > [新しいウインドウに実行コンフィギュレーションを表示（Show Running Configuration in New Window）]** を選択して、構成ファイルを取得します。

（注） マルチコンテキスト ASA の場合は、**show tech-support** コマンドを使用して、単一ファイル内のすべてのコンテキストの構成を取得できます。

ステップ 2 構成を `.cfg` または `.txt` として保存します。

異なる拡張子の Firewall 移行ツール 構成を ASAにアップロードすることはできません。

ステップ 3 ASAをダウンロードしたコンピュータに Firewall 移行ツール 構成ファイルを転送します。

次のタスク

Firewall 移行ツールの起動 （3 ページ）

Firewall 移行ツールの起動

（注） Firewall 移行ツールを起動すると、別のウィンドウでコンソールが開きます。移行が進むのに合わせて、Firewall 移行ツールの現在のステップの進行状況がコンソールに表示されます。画面にコンソールが表示されない場合は、Firewall 移行ツールの背後にある可能性があります。

始める前に

- Cisco.com から Firewall 移行ツールのダウンロード
- Firewall 移行ツールに関する注意事項と制約事項セクションで要件を確認します。
- Firepower 移行ツールを実行するために、最新バージョンの Google Chrome ブラウザがコンピュータにインストールされていることを確認します。Google Chrome をデフォルトのブラウザとして設定する方法については、「Set Chrome as your default web browser」を参照してください。
- 大規模な構成ファイルを移行する場合は、移行プッシュ中にシステムがスリープ状態にならないようにスリープ設定を構成します。

手順

ステップ 1 コンピュータで、Firewall 移行ツールをダウンロードしたフォルダに移動します。

ステップ 2 次のいずれかを実行します。

- Windows マシンで、Firewall 移行ツールの実行可能ファイルをダブルクリックして、Google Chrome ブラウザで起動します。

  プロンプトが表示されたら、[はい（Yes）] をクリックして、Firewall 移行ツールがシステムに変更を加えることができるようにします。

  Firewall 移行ツールは、すべての関連ファイルを作成し、Firepower 移行ツールの存在するフォルダに保存します（ログおよびリソースのフォルダを含む）。

- Mac では、Firewall 移行ツールの `*.command` ファイルを目的のフォルダに移動し、ターミナルアプリケーションを起動して、Firewall 移行ツールがインストールされているフォルダを参照し、次のコマンドを実行します。

  ```
  # chmod 750 Firewall_Migration_Tool-version_number.command
  ```

  ```
  # ./Firewall_Migration_Tool-version_number.command
  ```

  Firewall 移行ツールは、すべての関連ファイルを作成し、Firepower 移行ツールの存在するフォルダに保存します（ログおよびリソースのフォルダを含む）。

  ヒント Firewall 移行ツールを開こうとすると、警告ダイアログが表示されます。これは、身元が明らかな開発者によって Firewall 移行ツールが Apple に登録されていないためです。身元不明の開発者によるアプリケーションを開く方法については、「Open an app from an unidentified developer」を参照してください。

  （注） MAC のターミナルの zip メソッドを使用します。

ステップ 3 [エンドユーザライセンス契約（End User License Agreement）] ページで、テレメトリ情報をシスコと共有する場合は、[Cisco Success Network と情報を共有することに同意（I agree to share data with Cisco Success Network）] をクリックし、それ以外の場合は [後で行う（I'll do later）] をクリックします。

Cisco Success Network に統計を送信することに同意すると、Cisco.com アカウントを使用してログインするように求められます。Cisco Success Network に統計を送信しないことを選択した場合は、ローカルログイン情報を使用して Firewall 移行ツールにログインします。

ステップ 4 Firewall 移行ツールのログインページで、次のいずれかを実行します。

- Cisco Success Network と統計を共有するには、[CCO でログイン（Login with CCO）] リンクをクリックし、シングルサインオンログイン情報を使用して Cisco.com アカウントにログインします。

  （注） Cisco.com アカウントがない場合は、Cisco.com のログインページで作成します。

- 次のデフォルトログイン情報でログインします。

  - ユーザー名：admin

- パスワード：Admin123

Cisco.com アカウントを使用してログインしている場合は、ステップ 8 に進みます。

ステップ 5 [パスワードのリセット（Reset Password）]ページで、古いパスワードと新しいパスワードを入力し、新しいパスワードを確認します。

新しいパスワードは8 文字以上で、大文字と小文字、数字、および特殊文字を含める必要があります。

ステップ 6 [リセット（Reset）] をクリックします。

ステップ 7 新しいパスワードでログインします。

（注） パスワードを忘れた場合は、既存のすべてのデータを <*migration_tool_folder*> から削除し、Firewall 移行ツールを再インストールします。

ステップ 8 移行前チェックリストを確認し、記載されているすべての項目を完了していることを確認します。

チェックリストの項目を 1 つ以上完了していない場合は、完了するまで続行しないでください。

ステップ 9 [新規移行（New Migration）] をクリックします。

ステップ 10 [ソフトウェアアップデートの確認（Software Update Check）] 画面で、Firewall 移行ツールの最新バージョンを実行しているかどうかが不明な場合は、リンクをクリックし、Cisco.com でバージョンを確認します。

ステップ 11 [続行（Proceed）] をクリックします。

次のタスク

次のステップに進むことができます。

- ASA 構成をコンピュータにエクスポートした場合は、「ASA 構成ファイルのアップロード」に進みます。
- Firewall 移行ツールを使用して ASA から情報を抽出する場合は、Firewall 移行ツールから ASA への接続 （6 ページ）に進みます。

ASA 構成ファイルのアップロード

始める前に

送信元 ASA デバイスから構成ファイルを `.cfg` または `.txt` としてエクスポートします。

（注） ハードコーディングした構成ファイルや手動で変更した構成ファイルはアップロードしないでください。テキストエディタは、移行に失敗する原因となる空白行やその他の問題をファイルに追加します。

手順

ステップ 1 [**Extract ASA Information**] 画面の [手動アップロード（Manual Upload）] セクションで、[アップロード（Upload）] をクリックして ASA 構成ファイルをアップロードします。

ステップ 2 ASA 構成ファイルの場所を参照し、[開く（Open）] をクリックします。

Firewall 移行ツールは構成ファイルをアップロードします。大規模な構成ファイルの場合、この手順には時間がかかります。コンソールには、解析中の ASA 構成行など、行ごとに進行状況のログが表示されます。コンソールが表示されない場合は、 Firewall 移行ツールの背後にある別のウィンドウで確認できます。[コンテキストの選択（Context Selection）] セクションで、アップロードされた構成がマルチコンテキスト ASA に対応するかが識別されます。

ステップ 3 [コンテキストの選択（Context Selection）] セクションを確認し、移行する ASA を選択します。

ステップ 4 [解析を開始（Start Parsing）] をクリックします。

[解析サマリー（Parsed Summary）] セクションに解析ステータスが表示されます。

ステップ 5 アップロードされた構成ファイルで、 Firewall 移行ツールが検出および解析した要素の概要を確認します。

ステップ 6 [次へ（Next）] をクリックして、ターゲットパラメータを選択します。

次のタスク

Firewall 移行ツールの接続先パラメータの指定 （8 ページ）

Firewall 移行ツールから ASA への接続

Firewall 移行ツールは、移行する ASA デバイスに接続し、必要な構成情報を抽出できます。

始める前に

- Firewall 移行ツールをダウンロードして起動します。
- シングルコンテキスト ASA の場合、管理 IP アドレス、管理者ログイン情報、およびイネーブルパスワードを取得します。
- マルチコンテキストモード ASA の場合は、**管理**コンテキストの IP アドレス、管理者ログイン情報、およびイネーブルパスワードを取得します。

（注） ASA に**イネーブルパスワード**が構成されていない場合は、Firewall 移行ツールでこのフィールドを空白のままにしておくことができます。

手順

ステップ 1 [ASA情報の抽出（Extract ASA Information）] 画面の [ASAへの接続（Connect to ASA）] セクションで、[接続（Connect）] をクリックして、移行する ASA デバイスに接続します。

ステップ 2 [ASA ログイン（ASA Login）] 画面で、次の情報を入力します。

1. [ASA IP アドレス/ホスト名（ASA IP Address/Hostname）] フィールドに、管理 IP アドレスまたはホスト名（シングルコンテキスト ASA の場合）か、管理コンテキストの IP アドレスまたはホスト名（マルチコンテキスト ASA の場合）を入力します。
2. [ユーザ名（Username）]、[パスワード（Password）]、および[イネーブルパスワード（Enable Password）] フィールドに、適切な管理者用のログイン資格情報を入力します。

   （注） ASA に**イネーブルパスワード**が構成されていない場合は、Firewall 移行ツールでこのフィールドを空白のままにしておくことができます。
3. [ログイン（Login）] をクリックします。

Firewall 移行ツールが ASA に接続すると、ASA に正常に接続されたというメッセージが表示されます。マルチコンテキスト ASA の場合、Firewall 移行ツールはコンテキストを識別してリストします。

ステップ 3 [コンテキスト（Context）] ドロップダウンリストから、移行する ASA コンテキストを選択します。

ステップ 4 （任意）[ヒットカウントの収集（Collect Hitcounts）] を選択します。

オンにすると、このツールは ASA ルールが使用された回数と、ASA 稼働時間以降または最後の ASA 再起動以降にルールが使用された最後の時刻を計算し、[確認と検証（Review and Validate）] ページにこの情報を表示します。これにより、移行前にルールの有効性と関連性を評価できます。

ステップ 5 [抽出を開始（Start Extraction）] をクリックします。

Firewall 移行ツールが ASA に接続し、構成情報の抽出を開始します。抽出が正常に完了すると、[コンテキストを選択（Context Selection）] セクションで、アップロードされた構成がシングルコンテキストまたはマルチコンテキスト ASA のどちらに対応するかが識別されます。

ステップ 6 [コンテキストを選択（Context Selection）] セクションを確認し、移行する ASA コンテキストを選択します。

ステップ 7 [解析を開始（Start Parsing）] をクリックします。

[解析サマリー（Parsed Summary）] セクションに解析ステータスが表示されます。Firewall 移行ツールは構成ファイルを解析し、ASA から切断します。

ステップ 8 アップロードされた構成ファイルで、Firewall 移行ツールが検出および解析した要素の概要を確認します。

ステップ 9 [次へ（Next）] をクリックして、ターゲットパラメータを選択します。

次のタスク

Firewall 移行ツールの接続先パラメータの指定 （8 ページ）

Firewall 移行ツールの接続先パラメータの指定

始める前に

- オンプレミス Firewall Management Center の Management Center の IP アドレスを取得します。
- Firewall Migration Tool 3.0 以降では、オンプレミスの Firewall Management Center またはクラウド提供型 Firewall Management Center を選択できます。
- クラウド提供型 Firewall Management Center の場合、クラウド提供型 Firewall Management Center の移行で説明されているように、リージョンと API トークンを指定する必要があります。
- 「User Accounts for Management Access」の説明に従って、REST API にアクセスするための十分な権限で、Management Center に Firewall 管理ツールの専用アカウントを作成します。
- （任意）インターフェイスやルートなどのデバイス固有の構成を移行する場合は、ターゲット 脅威に対する防御 デバイスを Management Center に追加します。「Adding Devices to the Firewall Management Center」を参照してください。
- [確認と検証（Review and Validate）] ページで IPS またはファイルポリシーを ACL に適用する必要がある場合は、移行前に Management Center でポリシーを作成することを強くお勧めします。Firewall 移行ツールは接続された Management Center からポリシーを取得するため、同じポリシーを使用します。新しいポリシーを作成して複数のアクセス制御リストに割り当てると、パフォーマンスが低下し、プッシュが失敗する可能性があります。

手順

ステップ 1 [ターゲットの選択（Select Target）] 画面の [ファイアウォール管理（Firewall Management）] セクションで、次の手順を実行します。オンプレミスのファイアウォール管理センターまたはクラウド提供型ファイアウォール管理センターへの移行を選択できます。

- オンプレミスのファイアウォール管理センターに移行するには、次の手順を実行します。

a) [オンプレミス FMC（On-Prem FMC）] オプションボタンをクリックします。
b) 管理センターの IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。
c) [Domain] ドロップダウンリストで、移行先のドメインを選択します。

脅威に対する防御 デバイスに移行する場合は、選択したドメインで使用可能な 脅威に対する防御 デバイスにのみ移行できます。

d) [接続（Connect）] をクリックして、**手順 2** に進みます。

- クラウド提供型 Firewall Management Center に移行するには、次の手順を実行します。

a) [クラウド提供型 FMC（Cloud-delivered FMC）] オプションボタンをクリックします。
b) リージョンを選択し、CDO API トークンを貼り付けます。CDO API トークンの生成については、クラウド提供型 Firewall Management Center の移行を参照してください。
c) [接続（Connect）] をクリックして、**手順 2** に進みます。

ステップ 2 [Firewall Management Centerへのログイン（Firewall Management Center Login）] ダイアログボックスで、Firewall 移行ツール専用アカウントのユーザー名とパスワードを入力し、[ログイン（Login）] をクリックします。

Firewall 移行ツールは Management Center にログインし、その Management Center による管理対象 脅威に対する防御 デバイスのリストを取得します。この手順の進行状況はコンソールで確認できます。

ステップ 3 [続行（Proceed）] をクリックします。

[Threat Defense の選択（Choose Threat Defense）] セクションでは、移行先の 脅威に対する防御 デバイスを選択できます。また、脅威に対する防御 デバイスがない場合は、ASA 構成の共有ポリシー（アクセス制御リスト、NAT、およびオブジェクト）を Management Center に移行できます。

ステップ 4 [Threat Defense の選択（Choose Threat Defense）] セクションで、次のいずれかを実行します。

- [Firewall Threat Defenseデバイスの選択（Select Firewall Threat Defense Device）] ドロップダウンリストをクリックし、ASA 構成を移行するデバイスをオンにします。

選択した Management Center ドメイン内のデバイスが、**IP アドレス**と**名前**でリストされます。

（注） 少なくとも、選択するネイティブ 脅威に対する防御デバイスには、移行する ASA 構成と同じ数の物理インターフェイスまたはポート チャネル インターフェイスが必要です。少なくとも、脅威に対する防御デバイスのコンテナインスタンスには、同じ数の物理インターフェイスまたはポート チャネル インターフェイスとサブインターフェイスが必要です。ASA 構成と同じファイアウォールモードでデバイスを構成する必要があります。ただし、これらのインターフェイスは、両方のデバイスで同じ名前である必要はありません。

表 *1 : ASA* ファイアウォール機能とサポートされている *Management Center* または *Threat Defense* のバージョン

ファイアウォール機能	サポートされている管理センターまたは Threat Defense のバージョン
ASA とリモート展開	6.7 以降
暗号マップサイト間 VPN	6.6 以降
仮想トンネルインターフェイス（VTI）とルートベース（VTI）	6.7 以降
動的ルートオブジェクトと BGP	7.1 以降
リモート アクセス VPN	Management Center 7.2 以降と Threat Defense 7.0 以降。

（注） サイト間 VPN、VTI、およびルートベース（VTI）インターフェイスを移行するには、Management Center で 脅威に対する防御 を構成する必要があります。

- ASA 5505 の場合、デバイス固有の構成（インターフェイスおよびルータ）と共有ポリシー（NAT、ACL、オブジェクト）は、サポートされているターゲット 脅威に対する防御 プラットフォームが Management Center バージョン 6.5 以降を備えた Firewall 1010 の場合にのみ移行できます。

  （注） ターゲット 脅威に対する防御 が FPR-1010 でない場合、またはターゲット Management Center が 6.5 よりも前の場合は、ASA 5505 の移行サポートは共有ポリシーにのみ適用されます。デバイス固有の設定は移行されません。

  （注） 送信元構成は ASA 5505 であるため、[Select Device] ドロップダウンリストから FPR-1010 のみを選択できます。

  （注） ASA-SM移行のサポートは、共有ポリシーのみを対象としています。デバイス固有の設定は移行されません。

- [Threat Defense を使用せず続行（Proceed without Threat Defense）] をクリックして、構成を Management Center に移行します。

  脅威に対する防御 なしで続行すると、Firewall 移行ツールは 脅威に対する防御 に構成またはポリシーをプッシュしません。したがって、脅威に対する防御のデバイス固有の構成であるインターフェイスとルート、およびサイト間 VPN は移行されません。ただし、NAT、ACL、ポートオブジェクトなど、サポートされている他のすべての構成（共有ポリシーとオブジェクト）は移行されます。リモートアクセス VPN は共有ポリシーであり、Threat Defense なしでも移行できます。

ステップ 5 [続行（Proceed）] をクリックします。

移行先に応じて、Firewall 移行ツールを使用して移行する機能を選択できます。

ステップ 6 [機能の選択（Select Features）] セクションをクリックして、移行先に移行する機能を確認して選択します。

- 接続先 脅威に対する防御 デバイスに移行する場合、Firewall 移行ツールは、[デバイス設定（Device Configuration）] セクションと [共有設定（Shared Configuration）] セクションで、ASA 構成から移行できる機能を自動的に選択します。要件に応じて、デフォルトの選択をさらに変更できます。
- Management Center に移行する場合、Firewall 移行ツールは、[共有設定（Shared Configuration）] セクションで、ASA 構成から移行できる機能を自動的に選択します。要件に応じて、デフォルトの選択をさらに変更できます。

（注） [デバイスの構成（Device Configuration）] セクションは、移行先 脅威に対する防御 デバイスを選択していない場合は使用できません。

- Firewall 移行ツールでは、移行中に次のアクセス制御がサポートされています。
  - 宛先セキュリティゾーンの指定：移行中の ACL の宛先ゾーンのマッピングを有効にします。

    ルートルックアップロジックは静的ルートと接続ルートに限定され、PBR、動的ルート、および NAT は考慮されません。インターフェイス ネットワーク構成は、接続ルート情報を取得するために使用されます。

    送信元および接続先のネットワーク オブジェクト グループの性質によっては、この操作によりルールが急増することがあります。

  - トンネル化されたルールのプレフィルタとしての移行：ASA カプセル化トンネルプロトコルルールをプレフィルタトンネルルールにマッピングすると、次のような利点があります。
    - ディープインスペクションの調整：カプセル化トラフィックの場合に、ファストパス処理でのパフォーマンスを向上させます。
    - パフォーマンスの向上：早期処理のメリットがあるその他の接続についても、ファストパスやブロックをすることができます。

    Firewall 移行ツールは、送信元構成でカプセル化されたトンネルトラフィックルールを識別し、プレフィルタトンネルルールとして移行します。プレフィルタポリシーで移行されたトンネルルールを確認できます。プレフィルタポリシーは、Management Center で移行されたアクセス コントロール ポリシーに関連付けられます。

    プレフィルタトンネルルールとして移行されるプロトコルは次のとおりです。
    - GRE（47）
    - IPv4 カプセル化（4）
    - IPv6 カプセル化（41）
    - Teredo トンネリング（UDP:3544）

    （注） プレフィルタオプションを選択しない場合、すべてのトンネルトラフィックルールがサポートされていないルールとして移行されます。

ASA 構成の ACL トンネルルール（GRE および IPnIP）は、現在、デフォルトで双方向として移行されます。アクセスコントロールの状態オプションで、接続先のルール方向を双方向または単方向に指定できるようになりました。

- Firewall 移行ツールは、VPN トンネル移行用に次のインターフェイスとオブジェクトをサポートしています。
  - ポリシーベース（暗号マップ）：ターゲット Management Center と 脅威に対する防御 がバージョン 6.6 以降の場合
  - ルートベース（VTI）：ターゲット Management Center と 脅威に対する防御 がバージョン 6.7 以降の場合
- ファイアウォール移行ツールは、ターゲットの管理センターが 7.2 以降の場合はリモートアクセス VPN の移行をサポートします。リモートアクセス VPN は、Threat Defense なしで移行できる共有ポリシーです。Threat Defense を使用する移行を選択した場合、Threat Defense のバージョンは 7.0 以降である必要があります。
- （任意）[Optimization] セクションで、[Migrate only referenced objects] を選択して、アクセス コントロール ポリシーと NAT ポリシーで参照されているオブジェクトのみを移行します。

  （注） このオプションを選択すると、ASA 構成内の参照されていないオブジェクトは移行されません。これにより、移行時間が最適化され、未使用のオブジェクトが構成から消去されます。
- （任意）[最適化（Optimization）] セクションで、脅威に対する防御 のアクセスポリシーによる最適なメモリ使用率を実現する場合は、[オブジェクトグループの検索（Object group search）] を選択します。
- （任意）[インライングループ化（Inline Grouping）] セクションでは、Firewall 移行ツールを使用して、CSM または DM で始まる定義済みのネットワークおよびサービスオブジェクト名のアクセスルールをクリアできます。このオプションをオフにすると、定義済みのオブジェクト名が移行時に保持されます。詳細については、「インライングループ化」を参照してください。

  （注） デフォルトでは、インライングループ化のオプションが有効になっています。

ステップ 7 [続行（Proceed）] をクリックします。

ステップ 8 [Rule Conversion/ Process Config] セクションで、[Start Conversion] をクリックして変換を開始します。

ステップ 9 Firewall 移行ツールによって変換された要素の概要を確認します。

構成ファイルが正常にアップロードおよび解析されたかどうかを確認するには、移行を続行する前に**移行前レポート**をダウンロードして確認します。

ステップ 10 [レポートのダウンロード（Download Report）] をクリックし、**移行前レポート**を保存します。

移行前レポートのコピーも、Firewall 移行ツールと同じ場所にある Resources フォルダに保存されます。

次のタスク

移行前レポートの確認 （14 ページ）

インライングループ化

ASDM および CSM マネージド ASA によるオブジェクトグループ化

送信元または接続先のアドレス、あるいは送信元または接続先のサービスに複数の項目（オブジェクトまたはインラインの値）を入力すると、CSM または ASDM でオブジェクトグループが自動的に作成されます。各 ASA デバイスに構成を展開する際に、CSM および ASDM で使用されるこれらのオブジェクトグループの命名規則は、それぞれCSM_INLINE およびDM_INLINE です。

（注） オブジェクトグループ化の動作を変更するには、**[ツール（Tools）]** > **[設定（Preferences）]** から、[指定したプレフィックスを持つネットワークおよびサービスオブジェクトを自動展開する（Auto-expand network and service objects with specified prefix）] ルールテーブル設定を選択します。

次に、ASDM によって管理される ASA で **show run** コマンドを使用して抽出された構成スニペットを示します。

```
object network host1
 host 10.1.1.100
object network fqdn_obj1
 fqdn abc.cisco.com
object-group network DM_INLINE_NETWORK_1
 network-object 10.21.44.189 255.255.255.255
 network-object 10.21.44.190 255.255.255.255
object-group network DM_INLINE_NETWORK_2
 network-object 10.21.44.191 255.255.255.255
 network-object object host1
 network-object object fqdn_obj1


access-list CSM_DM_ACL extended permit tcp object-group DM_INLINE_NETWORK_1 object-group
 DM_INLINE_NETWORK_2
```

上記の例では、ASDM UI の access-list CSM_DM_ACL は、ルールの送信元および接続先のネットワークとして DM_INLINE グループを表示せず、代わりに DM_INLINE グループの内容を表示します。

インライングループ化：ASDM/CSM

Firewall 移行ツールのインライングループ化機能を使用すると、ASDM または CSM のマネージド ASA デバイスの **show running-configuration** を解析できます。ASDM または CSM と同じアクセスリストルールの UI 表現を保持するオプションがあります。オプトアウトした場合、移行されたルールは、ASA **show running-configuration** で記録されている DM_INLINE グループを参照します。

（注） 引き続き Firewall 移行ツールへの送信元 ASA 構成ファイル入力は、ASA からまたは ASA デバイス（SSH）へのライブ接続を介して収集された **show run** または **show tech** になります。Firewall 移行ツールは、他形式の構成のファイルまたは方式をサポートしていません。

次の図は、ACE または RULE の [送信元ネットワーク（Source Network）] フィールドと [接続先ネットワーク（Destination Network）] フィールドが、それぞれインライングループ化オプションの有効化または無効化に基づいてどのように変化するかを示しています。

図 *1:* インライングループ化あり：*ASDM/CSM* が有効

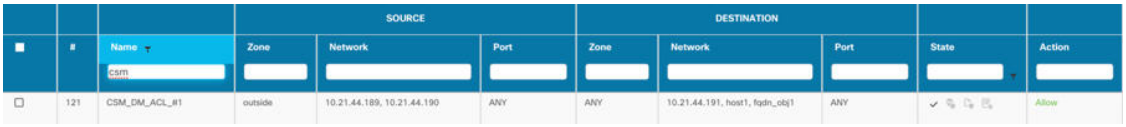


図 *2:* インライングループ化あり：*ASDM/CSM* が無効

移行前レポートの確認

移行中に移行前レポートをダウンロードし忘れた場合は、次のリンクを使用してダウンロードしてください。

移行前レポートのダウンロードエンドポイント：http://localhost:8888/api/downloads/pre_migration_summary_html_format

（注） レポートは、 Firewall 移行ツールの実行中にのみダウンロードできます。

手順

ステップ 1 移行前レポートをダウンロードした場所に移動します。

移行前レポートのコピーも、 Firewall 移行ツールと同じ場所にある `Resources` フォルダに保存されます。

ステップ 2 移行前レポートを開き、その内容を慎重に確認して、移行が失敗する原因となる問題を特定します。

移行前レポートには、次の情報が含まれています。

- [全体のサマリー（Overall Summary）]：ASA 構成情報を抽出するため、またはライブ ASA 構成に接続するために使用される方法。

  ライブ ASA に接続している場合は、ASA で検出されたファイアウォールモード。マルチコンテキストモードの場合は、移行用に選択したコンテキスト。

  脅威に対する防御 に正常に移行できるサポート対象 ASA 構成要素と、移行対象として選択された特定の ASA 機能のサマリー。

  ライブ ASA に接続している場合、サマリーにはヒットカウント情報（ASA ルールが検出された回数とそのタイムスタンプ情報）が含まれます。

- [エラーのある構成行（Configuration Lines with Errors）]： Firewall 移行ツール が解析できなかったために正常に移行できない ASA の構成要素の詳細。ASA 構成でこれらのエラーを修正し、新しい構成ファイルをエクスポートしてから、新しい構成ファイルを Firewall 移行ツールにアップロードし、続行してください。

- [部分的なサポート構成（Partially Supported Configuration）]：部分的にのみ移行可能な ASA 構成要素の詳細。これらの構成要素には、詳細オプションを含むルールとオブジェクトが含まれているため、詳細オプションを使用せずにルールまたはオブジェクトを移行できます。これらの行を確認し、詳細オプションが Management Center でサポートされているかどうかを確認します。サポートされている場合は、 Firewall 移行ツールを使用して移行を完了した後に、これらのオプションを手動で構成することを計画します。

- [未サポートの構成（Unsupported Configuration）]： Firewall 移行ツールがこれらの機能の移行をサポートしていないため、移行できない ASA 構成要素の詳細。これらの行を確認し、各機能が Management Center でサポートされているかどうかを確認します。サポートされている場合は、 Firewall 移行ツールを使用して移行を完了した後に、機能を手動で構成することを計画します。

- [無視される構成（Ignored Configuration）]： Management Center または Firewall 移行ツールでサポートされていないために無視される ASA 構成要素の詳細。 Firewall 移行ツールはこれらの行を解析しません。これらの行を確認し、各機能が Management Center でサポートされているかどうかを確認します。サポートされている場合は、機能を手動で構成することを計画します。

Management Center と 脅威に対する防御 でサポートされる機能の詳細については、『Management Center Configuration Guide』[英語] を参照してください。

ステップ 3 **移行前レポート**で修正措置が推奨されている場合は、ASA インターフェイスで修正を完了し、ASA 構成ファイルを再度エクスポートしてから、更新された構成ファイルをアップロードし、続行してください。

ステップ 4 ASA構成ファイルが正常にアップロードおよび解析されたら、Firewall移行ツールに戻り、[次へ（Next）] をクリックして移行を続行します。

次のタスク

ASA 構成と Secure Firewall Device Manager Threat Defense インターフェイスのマッピング

ASA 構成と Secure Firewall Device Manager Threat Defense インターフェイスのマッピング

脅威に対する防御 デバイスには、ASA 構成で使用されている数以上の物理インターフェイスとポート チャネル インターフェイスが必要です。これらのインターフェイスは、両方のデバイスで同じ名前である必要はありません。インターフェイスのマッピング方法を選択できます。

[Threat Defense インターフェイスのマップ（Map Threat Defense Interface）] 画面で、脅威に対する防御 デバイス上のインターフェイスのリストを取得します。デフォルトでは、Firewall 移行ツールは ASA のインターフェイスと 脅威に対する防御 デバイスをインターフェイス ID に従ってマッピングします。たとえば、ASAインターフェイスの「管理専用」インターフェイスは、脅威に対する防御デバイスの「管理専用」インターフェイスに自動的にマッピングされ、変更できません。

ASA インターフェイスから 脅威に対する防御 インターフェイスへのマッピングは、脅威に対する防御 デバイスタイプによって異なります。

- ターゲット 脅威に対する防御 がネイティブタイプの場合は次のようになります。
  - 脅威に対する防御には、使用するASAインターフェイスまたはポートチャネル（PC）データインターフェイスが同数以上必要です（ASA 構成の管理専用とサブインターフェイスを除く）。同数未満の場合は、ターゲット 脅威に対する防御 に必要なタイプのインターフェイスを追加します。
  - サブインターフェイスは、物理インターフェイスまたはポートチャネルマッピングに基づいて Firewall 移行ツールによって作成されます。
- ターゲット 脅威に対する防御 がコンテナタイプの場合は次のようになります。
  - 脅威に対する防御 には、使用する ASA インターフェイス、物理サブインターフェイス、ポートチャネル、またはポート チャネル サブインターフェイスが同数以上必要です（ASA 構成の管理専用を除く）。同数未満の場合は、ターゲット 脅威に対する防御 に必要なタイプのインターフェイスを追加します。たとえば、ターゲット 脅威に対する防御 の物理インターフェイスと物理サブインターフェイスの数が ASA での数より 100 少ない場合、ターゲット 脅威に対する防御 に追加の物理または物理サブインターフェイスを作成できます。

- サブインターフェイスは、Firewall移行ツールでは作成されません。物理インターフェイス、ポートチャネル、またはサブインターフェイス間のインターフェイスマッピングのみが許可されます。

始める前に

Management Center に接続し、接続先として 脅威に対する防御 を選択していることを確認します。詳細については、「Firewall 移行ツールの接続先パラメータの指定 （8 ページ）」を参照してください。

（注） 脅威に対する防御 デバイスなしで Management Center に移行する場合、この手順は適用されません。

手順

ステップ 1 インターフェイスマッピングを変更する場合は、[Threat Defenseインターフェイス名（Threat Defense Interface Name）] のドロップダウンリストをクリックし、その ASA インターフェイスにマッピングするインターフェイスを選択します。

管理インターフェイスのマッピングは変更できません。脅威に対する防御インターフェイスがすでに ASA インターフェイスに割り当てられている場合は、ドロップダウンリストからそのインターフェイスを選択できません。割り当て済みのすべてのインターフェイスはグレー表示され、使用できません。

サブインターフェイスをマッピングする必要はありません。Firewall 移行ツールは、ASA 構成内のすべてのサブインターフェイスについて 脅威に対する防御 デバイスのサブインターフェイスをマッピングします。

ステップ 2 各 ASA インターフェイスを 脅威に対する防御 インターフェイスにマッピングしたら、[次へ（Next）] をクリックします。

次のタスク

ASA インターフェイスを適切な 脅威に対する防御 インターフェイス オブジェクト、セキュリティゾーン、およびインターフェイスグループにマッピングします。詳細については、「セキュリティゾーン とインターフェイスグループへの ASA インターフェイスのマッピング」を参照してください。

セキュリティゾーン とインターフェイスグループへの ASA インターフェイスのマッピング

（注） ASA 構成にアクセスリストと NAT ルールが含まれていない場合、またはこれらのポリシーを移行しない場合は、この手順をスキップして「最適化、 移行する構成の確認と検証 （19 ページ）」に進むことができます。

ASA 構成が正しく移行されるように、ASA インターフェイスを適切な 脅威に対する防御 インターフェイス オブジェクト、セキュリティゾーン、およびインターフェイスグループにマッピングします。ASA 構成では、アクセス コントロール ポリシーと NAT ポリシーはインターフェイス名（nameif）を使用します。Management Center では、これらのポリシーはインターフェイス オブジェクトを使用します。さらに、Management Center ポリシーはインターフェイス オブジェクトを次のようにグループ化します。

- セキュリティゾーン：インターフェイスは、1つのセキュリティゾーンにのみ属することができます。
- インターフェイスグループ：インターフェイスは複数のインターフェイスグループに属することができます。

Firewall移行ツールでは、セキュリティゾーンおよびインターフェイスグループとインターフェイスを 1 対 1 でマッピングできます。セキュリティゾーンまたはインターフェイスグループがインターフェイスにマッピングされている場合、他のインターフェイスへのマッピングには使用できませんが、Management Center では許可されます。Management Center のセキュリティゾーンとインターフェイスグループの詳細については、「Interface Objects: Interface Groups and Security Zones」を参照してください。

手順

ステップ 1 [セキュリティゾーンとインターフェイスグループへのマッピング（Map Security Zones and Interface Groups）] 画面で、使用可能なインターフェイス、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確認します。

ステップ 2 セキュリティゾーンおよびインターフェイスグループが Management Center に存在する場合、またはセキュリティ ゾーン タイプ オブジェクトとして ASA 構成ファイルに存在し、ドロップダウンリストで使用可能な場合、これらにインターフェイスをマッピングするには、次の手順を実行します。

a) [セキュリティゾーン（Security Zones）] 列で、そのインターフェイスのセキュリティゾーンを選択します。

b) [インターフェイスグループ（Interface Groups）] 列で、そのインターフェイスのインターフェイスグループを選択します。

ステップ 3 セキュリティゾーンとインターフェイスグループは、手動でマッピングすることも自動で作成することもできます。

ステップ 4 セキュリティゾーンとインターフェイスグループを手動でマッピングするには、次の手順を実行します。

a) [セキュリティゾーンとインターフェイスグループの追加（Add SZ & IG）] をクリックします。
b) [セキュリティゾーンとインターフェイスグループの追加（Add SZ & IG）] ダイアログボックスで、[追加（Add）] をクリックして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を追加します。
c) [セキュリティゾーン（Security Zone）] 列にセキュリティゾーン名を入力します。使用できる最大文字数は 48 です。同様に、インターフェイスグループを追加できます。
d) [閉じる（Close）] をクリックします。

セキュリティゾーンとインターフェイスグループを自動作成によってマッピングするには、次の手順を実行します。

a) [自動作成（Auto-Create）] をクリックします。
b) [自動作成（Auto-Create）] ダイアログボックスで、[インターフェイスグループ（Interface Groups）] または [ゾーンマッピング（Zone Mapping）] のいずれかまたは両方をオンにします。
c) [自動作成（Auto-Create）] をクリックします。

Firewall 移行ツールは、これらのセキュリティゾーンに ASA インターフェイスと同じ名前（**outside** や **inside** など）を付け、名前の後に "(A)" を表示して、 Firewall 移行ツールによって作成されたことを示します。インターフェイスグループには、**outside_ig** や **inside_ig** などの `_ig` サフィックスが追加されます。また、セキュリティゾーンとインターフェイスグループには、ASA インターフェイスと同じモードがあります。たとえば、ASA 論理インターフェイスが L3 モードの場合、そのインターフェイス用に作成されたセキュリティゾーンとインターフェイスグループも L3 モードになります。

ステップ 5 すべてのインターフェイスを適切なセキュリティゾーンとインターフェイスグループにマッピングしたら、[次へ（Next）] をクリックします。

最適化、 移行する構成の確認と検証

移行した ASA 構成を Management Center にプッシュする前に、構成を慎重に確認し、それが適切で 脅威に対する防御 デバイスの構成内容と一致することを確認します。点滅しているタブは、次の一連のアクションを実行する必要があることを示しています。

これで、 Firewall 移行ツールは、Management Center にすでに存在する侵入防御システム（IPS）ポリシーとファイルポリシーを取得し、移行するアクセスコントロールルールにそれらを関連付けることができます。

ファイルポリシーは、システムが全体的なアクセス制御設定の一環として、ネットワークの高度なマルウェア防御とファイル制御を実行するために使用する一連の設定です。この関連付け

により、アクセス コントロール ルールの条件と一致するトラフィック内のファイルを通過させる前に、システムは必ずファイルを検査するようになります。

同様に、トラフィックが接続先に向かうことを許可する前に、システムの最終防御ラインとしてIPSポリシーを使用できます。侵入ポリシーは、セキュリティ違反に関するトラフィックの検査方法を制御し、インライン展開では、悪意のあるトラフィックをブロックまたは変更することができます。システムが侵入ポリシーを使用してトラフィックを評価する場合、システムは関連付けられた変数セットを使用します。セット内の大部分の変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先のIPアドレスとポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。

タブで特定の構成項目を検索するには、列の上部にあるフィールドに項目名を入力します。テーブルの行はフィルタ処理され、検索語に一致する項目のみが表示されます。

送信元 ASA デバイスは、CSM または ASDM で管理できます。送信元または接続先のアドレス、あるいは送信元または接続先のサービスに複数の項目（オブジェクトまたはインラインの値）を入力すると、CSM または ASDM でオブジェクトグループが自動的に作成されます。CSM および ASDM で使用されるこれらのオブジェクトグループの命名規則は、それぞれ CSM_INLINE および DM_INLINE です。

インライン グループ化CSMまたはASDM管理型設定をクリアすることを選択すると、事前に定義されたオブジェクトが実際のオブジェクトまたはメンバー名に置き換えられます。CSM または ASDM 管理型設定をクリアしない場合、事前に定義されたオブジェクト名は移行のために保持されます。

たとえば、10.21.44.189 と 10.21.44.190 はオブジェクトグループのメンバーであり、オブジェクトグループ DM_INLINE_NETWORK_1 やオブジェクトグループ DM_INLINE_NETWORK_2 などの定義済みの名前に変更されます。

（注） デフォルトでは、[Inline Grouping] オプションが有効になっています。

[構成の最適化、確認および検証（Optimize, Review and Validate Configuration）] 画面で Firewall 移行ツールを閉じると、進行状況が保存され、後で移行を再開できます。この画面の前に Firewall 移行ツールを閉じると、進行状況は保存されません。解析後に障害が発生した場合、[インターフェイスマッピング（Interface Mapping）] 画面から Firewall 移行ツールを再起動します。

Firewall 移行ツール ACL 最適化の概要

は、ネットワーク機能に影響を与えることなく、ファイアウォール ルール ベースから最適化（無効化または削除）できる ACL を識別および分離するサポートを提供します。

ACL 最適化は、次の ACL タイプをサポートします。

- 冗長 ACL：2 つの ACL の構成とルールのセットが同じ場合、基本以外の ACL を削除してもネットワークに影響はありません。たとえば、2 つのルールが同じネットワーク上で FTP および IP トラフィックを許可し、アクセスを拒否するルールが定義されていない場合、最初のルールを削除できます。

- シャドウ ACL：最初の ACL は、2 番目の ACL の設定を完全にシャドウイングします。2 つのルールに同様のトラフィックがある場合、2 番目のルールはアクセスリストの後半に表示されるため、どのトラフィックにも適用されません。2 つのルールがトラフィックに対して異なるアクションを指定している場合、シャドウイングされたルールを移動するか、いずれかのルールを編集して必要なポリシーを実装できます。たとえば、特定の送信元または宛先に対して、基本ルールで IP トラフィックを拒否し、シャドウイングされたルールで FTP トラフィックを許可できます。

は、ACL 最適化のルールを比較する際に次のパラメータを使用します。

（注） ASA ではACP ルールアクションに対してのみ最適化を使用できます。

- 無効化された ACL は、最適化プロセス中に考慮されません。
- 送信元の ACL は、対応する ACE（インライン値）に展開された後、次のパラメータについて比較されます。
  - 送信元と宛先のゾーン
  - 送信元と宛先のネットワーク
  - [送信元/宛先ポート（Source and Destination Port）]

オブジェクトの最適化

次のオブジェクトは、移行プロセス中にオブジェクトの最適化について考慮されます。

- 未参照のオブジェクト：移行の開始時に、未参照のオブジェクトを移行しないように選択できます。
- 重複したオブジェクト：オブジェクトがすでに Management Center に存在する場合、重複したオブジェクトを作成する代わりに、ポリシーが再利用されます。

手順

ステップ 1 （任意）[構成の最適化、確認および検証（Optimize, Review and Validate Configuration）] 画面で、[ACLの最適化（Optimize ACL）] をクリックして最適化コードを実行し、以下の操作を実行します。

a) 特定された ACL 最適化ルールをダウンロードするには、[ダウンロード（Download）] をクリックします。
b) ルールを選択し、**[アクション（Actions）]** > **[無効として移行（Migrate as disabled）]** または **[移行しない（Do not migrate）]** を選択して、いずれかのアクションを適用します。
c) **[保存（Save）]** をクリックします。
移行操作が [移行しない（Do not migrate）] から [無効として移行（Migrate as disabled）] またはその逆に変わります。

次のオプションを使用して、ルールの一括選択を実行できます。

- [移行（Migrate）]：デフォルトの状態で移行します。
- [移行しない（Do not migrate）]：ACL の移行を無視します。
- [無効として移行（Migrate as disabled）]：[状態（State）]フィールドが[無効（Disable）]に設定されている ACL を移行します。
- [有効として移行（Migrate as enabled）]：[状態（State）]フィールドが[有効（Enable）]に設定されている ACL を移行します。

ステップ 2 [構成の確認と検証（Review and Validate Configuration）]画面で、[アクセス制御ルール（Access Control Rules）]をクリックし、次の手順を実行します。最適化、

a) テーブル内の各エントリについて、マッピングを確認し、それらが正しいことを確認します。

移行されたアクセスポリシールールは、プレフィックスとして ACL 名を使用し、それに ACL ルール番号を追加することで、ASA 構成ファイルにマッピングしやすくします。たとえば、ASA ACL の名前が "inside_access" の場合、ACL の最初のルール（または ACE）行の名前は "inside_access_#1" になります。TCP または UDP の組み合わせ、拡張サービスオブジェクト、またはその他の理由でルールを拡張する必要がある場合、Firewall 移行ツールは名前に番号付きサフィックスを追加します。たとえば、許可ルールが移行のために 2 つのルールへ拡張される場合、それらのルールには "inside_access_#1-1" と "inside_access_#1-2" という名前が付けられます。

サポートされていないオブジェクトを含むルールの場合、 Firewall 移行ツールは名前に "_UNSUPPORTED" というサフィックスを追加します。

b) 1 つ以上のアクセス制御リストポリシーを移行しない場合は、該当する行のボックスをオンにし、**[アクション（Actions）]** > **[移行しない（Do not migrate）]** を選択して、[保存（Save）] をクリックします。

移行しないことを選択したすべてのルールは、テーブルでグレー表示されます。

c) Management Center ファイルポリシーを 1 つ以上のアクセス コントロール ポリシーに適用する場合は、該当する行のボックスをオンにし、**[アクション（Actions）]**>**[ファイルポリシー（File Policy）]** を選択します。

[ファイルポリシー（File Policy）]ダイアログで、適切なファイルポリシーを選択し、選択したアクセス コントロール ポリシーに適用して、[保存（Save）] をクリックします。

d) Management Center IPS ポリシーを 1 つ以上のアクセス コントロール ポリシーに適用する場合は、該当する行のボックスをオンにし、**[アクション（Actions）]**>**[IPS ポリシー（IPS Policy）]** を選択します。

[IPS ポリシー（IPS Policy）]ダイアログで、適切な IPS ポリシーと対応する変数セットを選択し、選択したアクセスコントロールポリシーに適用して、[保存（Save）]をクリックします。

e) ロギングが有効になっているアクセスコントロールルールのロギングオプションを変更する場合は、該当する行のボックスをオンにし、**[アクション（Actions）]** > **[ログ（Log）]** を選択します。

[ログ（Log）] ダイアログでは、接続の開始時または終了時、またはその両方でイベントのロギングを有効にできます。ロギングを有効にする場合は、接続イベントを**イベントビューア**または **Syslog** のいずれか、または両方に送信することを選択する必要があります。接続イベントを syslog サーバに送信することを選択した場合、Management Center ですでに構成されている syslog ポリシーを [Syslog] ドロップダウンメニューから選択できます。

f) [アクセスコントロール（Access Control）] テーブル内の移行されたアクセスコントロールルールのアクションを変更する場合は、該当する行のボックスをオンにし、**[アクション（Actions）]** > **[ルールアクション（Rule Action）]** を選択します。

[ルールアクション（Rule Action）] ダイアログの [アクション（Actions）] ドロップダウンで、[ACP] タブまたは [プレフィルタ（Prefilter）] タブを選択できます。

- ACP：アクセスコントロールルールには、システムが一致するトラフィックをどのように処理し、ログに記録するのかを指定するアクションがあります。アクセスコントロールルールに対して許可、信頼、モニタ、ブロック、またはリセット付きブロックのいずれかのアクションを実行できます。
- Prefilter：ルールのアクションによって、一致したトラフィックの処理とログ記録の方法が決まります。ファストパスとブロックを実行できます。

ヒント アクセスコントロールルールにアタッチされている IPS およびファイルのポリシーは、[許可（Allow）] オプションを除くすべてのルールアクションに対して自動的に削除されます。

[ACLルールカテゴリ（ACL Rule Category）]： Firewall 移行ツールは、CSM マネージド ASA 構成の [ルール（Rule）] セクションを保持し、Management Center の ACL カテゴリとして移行します。

ポリシーのキャパシティと制限の警告： Firewall 移行ツールは、移行したルールの合計 ACE カウントを、ターゲットプラットフォームでサポートされている ACE 制限と比較します。

Firewall 移行ツールは比較の結果に基づいて、移行された ACE の総数がしきい値を超えた場合や、ターゲットデバイスのサポートされている制限のしきい値に近づいている場合は、視覚インジケータと警告メッセージを表示します。

ルールが [ACE カウント（ACE Count）] 列を超える場合は、最適化することも、移行しないことを決定することもできます。移行を完了してからこの情報を使用して、Management Center でプッシュしてから展開するまでの間に、ルールを最適化することもできます。

（注） Firewall 移行ツールは、警告にもかかわらず移行をブロックしません。

ACE カウントを、昇順、降順、等しい、大なり、および小なりのフィルタリング順序シーケンスでフィルタリングできるようになりました。

フィルタリング条件をクリアするには、[フィルタのクリア（Clear Filter）] をクリックします。

（注） ACE に基づいた ACL のソート順序は、表示のみを目的としています。ACL は、発生した時間順に基づいてプッシュされます。

ステップ 3 次のタブをクリックし、構成項目を確認します。

- [NAT ルール（NAT Rules）]
- [オブジェクト（Objects）]（[アクセスリストオブジェクト（Acess List Objects）]、[ネットワークオブジェクト（Network Objects）]、[ポートオブジェクト（Port Objects）]、[VPN オブジェクト（VPN Objects）]、および[動的ルートオブジェクト（Dynamic-Route-Objects）]）
- [インターフェイス（Interfaces）]
- [ルート（Routes）]
- [サイト間 VPN トンネル（Site-to-Site VPN Tunnels）]
- [リモートアクセス VPN（Remote Access VPN）]

アクセスリストオブジェクトには、BGP と RA VPN で使用される標準 ACL と拡張 ACL が表示されます。

1つ以上のNATルールまたはルートインターフェイスを移行しない場合は、該当する行のボックスをオンにし、**[アクション（Actions）] > [移行しない（Do not migrate）]** を選択して、[保存（Save）] をクリックします。

移行しないことを選択したすべてのルールは、テーブルでグレー表示されます。

ステップ 4 （任意）構成の確認中に、[ネットワークオブジェクト（Network Objects）] タブ、[ポートオブジェクト（Port Objects）] タブ、または [VPNオブジェクト（VPN Objects）] タブで **[アクション（Actions）] > [名前の変更（Rename）]** を選択して、ネットワークオブジェクト、ポートオブジェクト、または VPN オブジェクトの名前を変更することができます。

名前が変更されたオブジェクトを参照するアクセスルールとNATポリシーも、新しいオブジェクト名で更新されます。

ステップ 5 [動的ルートオブジェクト（Dynamic-Route-Objects）] セクションには、移行されるすべてのサポートされているオブジェクトが表示されます。

- ポリシーリスト
- プレフィックスリスト
- ルートマップ
- コミュニティ リスト
- AS パス
- アクセス リスト

ステップ 6 [ルート（Routes）] セクションには、次のルートが表示されます。

- [スタティック（Static）]：すべての IPv4 および IPv6 スタティックルートを表示します。
- [BGP]：すべての BGP ルートを表示します。

ステップ 7 [リモートアクセス VPN（Remote Access VPN）] セクションでは、リモートアクセス VPN に対応するすべてのオブジェクトが ASA から管理センターに移行され、次のように表示されます。

- **Anyconnect ファイル**：AnyConnect パッケージ、Hostscan ファイル（Dap.xml、Data.xml、Hostscan Package）、外部ブラウザパッケージ、および AnyConnect プロファイルは、送信元 ASA デバイスから取得する必要があり、また、移行に使用できる必要があります。

  移行前のアクティビティの一環として、すべての AnyConnect パッケージを管理センターにアップロードします。AnyConnect プロファイルは、管理センターに直接アップロードしたり、Firewall 移行ツールからアップロードしたりできます。

  管理センターから取得した既存の Anyconnect、Hostscan、または外部ブラウザパッケージを選択します。1 つ以上の AnyConnect パッケージを選択する必要があります。送信元の構成で使用可能な場合は、Hostscan、dap.xml、data.xml、または外部ブラウザを選択する必要があります。AnyConnect プロファイルはオプションです。

  dap.xml は、ASA から取得した正しいファイルである必要があります。検証は、構成ファイルで使用可能な dap.xml で実行されます。検証に必要なすべてのファイルをアップロードして選択する必要があります。更新に失敗すると不完全とマークされ、Firewall 移行ツールは検証に進みません。

- [AAA]：Radius、LDAP、AD、LDAP、SAML、およびローカルレルムタイプの認証サーバーが表示されます。すべての AAA サーバーのキーを更新します。Firewall 移行ツール 3.0 以降、Live Connect ASA の事前共有キーは自動的に取得されます。**more system: running-config** ファイルを使用して、隠しキーを含む送信元の構成をアップロードすることもできます。ASA からクリアテキスト形式でキーを取得する方法については、「リモートアクセス VPN の移行」を参照してください。
- LDAPS では、管理センターにドメインが必要です。暗号化タイプ LDAPS のドメインを更新する必要があります。
- AD サーバーの Management Center には、一意の AD プライマリドメインが必要です。一意のドメインが識別されると、Firewall 移行ツールに表示されます。競合が見つかった場合、オブジェクトを正常にプッシュするには、一意の AD プライマリドメインを入力する必要があります。ドメインと AD プライマリドメインの取得については、「リモートアクセス VPN の移行」を参照してください。
- [アドレスプール（Address Pool）]：すべての IPv4 プールと IPv6 プールがここに表示されます。
- [グループポリシー（Group-Policy）]：このセクションには、クライアントプロファイル、管理プロファイル、クライアントモジュール、およびプロファイルのないグループポリシーを含むグループポリシーが表示されます。プロファイルが [AnyConnect ファイル（AnyConnect file）] セクションに追加されている場合は、事前に選択された状態で表示されます。ユーザープロファイル、管理プロファイル、およびクライアント モジュール プロファイルを選択または削除できます。

- [接続プロファイル（Connection Profile）] ：すべての接続プロファイル/トンネルグループがここに表示されます。
- [トラストポイント（Trustpoint）] : ASA から管理センターへのトラストポイントまたは PKI オブジェクトの移行は、移行前アクティビティの一環であり、RA VPN の移行を正常に実行するために不可欠です。[リモート アクセス インターフェイス（Remote Access Interface）] セクションでグローバル SSL、IKEv2、およびインターフェイスのトラストポイントをマッピングして、移行の次の手順に進みます。LDAPS プロトコルが有効になっている場合、グローバル SSL と IKEv2 トラストポイントは必須です。SAML オブジェクトが存在する場合、SAML IDP と SP のトラストポイントを SAML セクションでマッピングできます。SP 証明書はオプションです。特定のトンネルグループについては、トラストポイントをオーバーライドすることもできます。オーバーライドされた SAML トラストポイント構成が送信元 ASA で使用可能な場合は、[SAML のオーバーライド（Override SAML）] オプションで選択できます。

  ASA からの PKI 証明書のエクスポートについては、「リモートアクセス VPN の移行」を参照してください。
- [証明書マップ（Certificate Maps）] : ここに証明書マップが表示されます。

ステップ 8 （任意）グリッド内の各構成項目の詳細をダウンロードするには、[ダウンロード（Download）] をクリックします。

ステップ 9 確認が完了したら、[検証（Validate）] をクリックします。

検証中、 Firewall 移行ツールは Management Center に接続し、既存のオブジェクトを確認して、それらのオブジェクトを移行対象オブジェクトのリストと比較します。オブジェクトが Management Center にすでに存在する場合、 Firewall 移行ツールは次のことを行います。

- オブジェクトの名前と構成が同じ場合、 Firewall 移行ツールは既存のオブジェクトを再利用し、 Management Center に新しいオブジェクトを作成しません。
- オブジェクトの名前が同じで構成が異なる場合、 Firewall 移行ツールはオブジェクトの競合を報告します。

検証の進行状況はコンソールで確認できます。

ステップ 10 検証が完了し、[検証ステータス（Validation Status）] ダイアログボックスに 1 つ以上のオブジェクトの競合が表示された場合は、次の手順を実行します。

a) [競合の解決（Resolve Conflicts）] をクリックします。

Firewall 移行ツールは、オブジェクトの競合が報告された場所に応じて、[ネットワークオブジェクト（Network Objects）] タブまたは [ポートオブジェクト（Port Objects）] タブのいずれかまたは両方に警告アイコンを表示します。

b) タブをクリックし、オブジェクトを確認します。

c) 競合がある各オブジェクトのエントリを確認し、**[アクション（Actions）] > [競合の解決（Resolve Conflicts）]** を選択します。

d) [競合の解決（Resolve Conflicts）] ウィンドウで、推奨アクションを実行します。

たとえば、既存の Management Center オブジェクトとの競合を避けるために、オブジェクト名にサフィックスを追加するように求められる場合があります。デフォルトのサフィックスを受け入れるか、独自のサフィックスに置き換えることができます。

e) [解決（Resolve）] をクリックします。
f) タブ上のすべてのオブジェクトの競合を解決したら、[保存（Save）] をクリックします。
g) [検証（Validate）] をクリックして構成を再検証し、すべてのオブジェクトの競合を解決したことを確認します。

ステップ 11 検証が完了し、[検証ステータス（Validation Status）] ダイアログボックスに「Successfully Validated」というメッセージが表示されたら、移行された構成の Management Center へのプッシュ （28 ページ）に進みます。

ACL 最適化のレポート

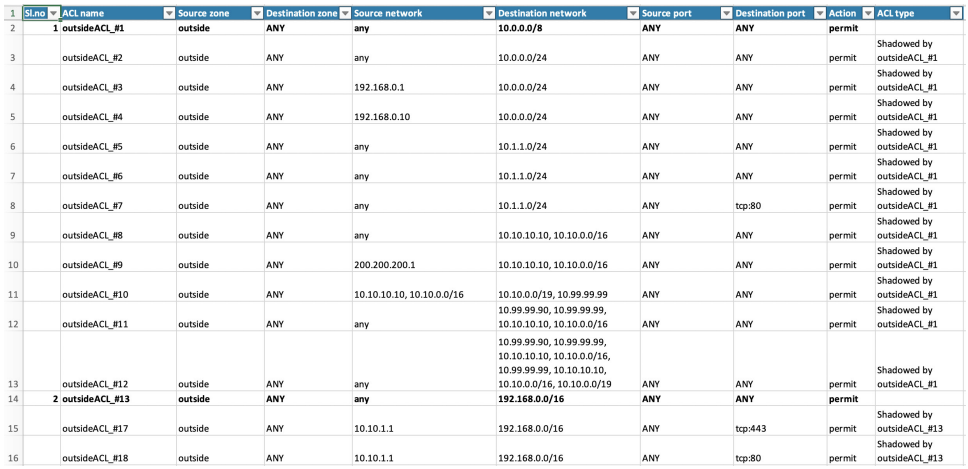
ACL 最適化レポートには、次の情報が表示されます。

- Summary シート：ACL 最適化のサマリーが表示されます。

	A	B	C	D
1	Sl.no	ACL name	Redundant ACLs	Shadowed ACLs
2	1	outsideACL_#1		outsideACL_#2, outsideACL_#3, outsideACL_#4, outsideACL_#5, outsideACL_#6, outsideACL_#7, outsideACL_#8, outsideACL_#9, outsideACL_#10, outsideACL_#11, outsideACL_#12
3	2	outsideACL_#13		outsideACL_#17, outsideACL_#18
4	3	outsideACL_#14		outsideACL_#15, outsideACL_#16, outsideACL_#17, outsideACL_#18
5	4	outsideACL_#19		outsideACL_#20, outsideACL_#21, outsideACL_#22, outsideACL_#23, outsideACL_#24
6	5	outsideACL_#25		outsideACL_#27, outsideACL_#28, outsideACL_#29, outsideACL_#30
7	6	outsideACL_#26		
8	7	outsideACL_#31		outsideACL_#32, outsideACL_#33
9	8	outsideACL_#34		
10	9	dmzACL_#1		
11	10	dmzACL_#2	dmzACL_#5	
12	11	dmzACL_#3		dmzACL_#5
13	12	dmzACL_#4		
14	13	dmzACL_#6		dmzACL_#7, dmzACL_#8, dmzACL_#9, dmzACL_#10
15	14	dmzACL_#11		dmzACL_#13
16	15	dmzACL_#12		
17	16	extACL_#1		
18	17	extACL_#2		
19	18	extACL_#3		extACL_#4, extACL_#5, extACL_#6
20	19	extACL_#7		
21	20	extACL_#8	extACL_#9, extACL_#10	
22	21	extACL_#11		
23	22	extACL_#12	extACL_#13	
24	23	extACL_#14		
25	24	extACL_#15		
26	25	extACL_#16		
27	26	extACL_#17		extACL_#18, extACL_#19
28	27	localtoremote_#1		
29	28	opt_#1		opt_#3
30	29	opt_#2	opt_#4	opt_#5
31	30	opt_#6-1	opt_#17-1	opt_#7-1, opt_#8-1
32	31	opt_#9-1	opt_#10-1	
33	32	opt_#11-1	opt_#12-1	opt_#13-1
34	33	opt_#14-1		opt_#15-1, opt_#16-1
35	34	opt_#18		
36	35	opt_#19		opt_#20, opt_#21
37	36	opt_#22-1	opt_#23-1	

Summary | Detailed ACL Information | +

- Detailed ACL Information：ベース ACL の詳細が表示されます。各 ACL には、比較対象の基本の ACL と最適化カテゴリとの関連付けを識別する ACL タイプ（シャドウまたは冗長）のタグが付いています。



Sl.no	ACL name	Source zone	Destination zone	Source network	Destination network	Source port	Destination port	Action	ACL type
1	**outsideACL_#1**	**outside**	**ANY**	**any**	**10.0.0.0/8**	**ANY**	**ANY**	**permit**	
	outsideACL_#2	outside	ANY	any	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#3	outside	ANY	192.168.0.1	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#4	outside	ANY	192.168.0.10	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#5	outside	ANY	any	10.1.1.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#6	outside	ANY	any	10.1.1.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#7	outside	ANY	any	10.1.1.0/24	ANY	tcp:80	permit	Shadowed by outsideACL_#1
	outsideACL_#8	outside	ANY	any	10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#9	outside	ANY	200.200.200.1	10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#10	outside	ANY	10.10.10.10, 10.10.0.0/16	10.10.0.0/19, 10.99.99.99	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#11	outside	ANY	any	10.99.99.90, 10.99.99.99, 10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#12	outside	ANY	any	10.99.99.90, 10.99.99.99, 10.10.10.10, 10.10.0.0/16, 10.99.99.99, 10.10.10.10, 10.10.0.0/16, 10.10.0.0/19	ANY	ANY	permit	Shadowed by outsideACL_#1
2	**outsideACL_#13**	**outside**	**ANY**	**any**	**192.168.0.0/16**	**ANY**	**ANY**	**permit**	
	outsideACL_#17	outside	ANY	10.10.1.1	192.168.0.0/16	ANY	tcp:443	permit	Shadowed by outsideACL_#13
	outsideACL_#18	outside	ANY	10.10.1.1	192.168.0.0/16	ANY	tcp:80	permit	Shadowed by outsideACL_#13

移行された構成の Management Center へのプッシュ

構成の検証に成功せず、すべてのオブジェクトの競合を解決していない場合は、移行された ASA 構成を Secure Firewall Management Center にプッシュできません。

移行プロセスのこのステップでは、移行された構成を Secure Firewall Management Center に送信します。Secure Firewall Threat Defense デバイスに構成を展開しません。ただし、Secure Firewall Threat Defense 上の既存の構成はこのステップで消去されます。

（注） Firewall 移行ツールが移行された構成を Secure Firewall Management Center に送信している間は、構成を変更したり、デバイスに展開したりしないでください。

手順

ステップ 1 [検証ステータス（Validation Status）] ダイアログボックスで、検証の概要を確認します。

ステップ 2 [構成のプッシュ（Push Configuration）] をクリックして、移行された ASA 構成を Secure Firewall Management Center に送信します。

Firewall 移行ツールの新しい最適化機能を使用すると、検索フィルタを使用して移行結果を迅速に取得できます。

Firewall 移行ツールは、CSV ダウンロードを最適化し、ページビューごとにまたはすべてのルールにアクションを適用することもできます。

Firewall 移行ツールに、移行の進行状況の概要が表示されます。コンソールに、Secure Firewall Management Center にプッシュされているコンポーネントの詳細な進行状況を行ごとに表示できます。

ステップ 3 移行が完了したら、[レポートのダウンロード（Download Report）] をクリックして、移行後レポートをダウンロードして保存します。

移行前レポートのコピーも、 Firewall 移行ツールと同じ場所にある `Resources` フォルダに保存されます。

ステップ 4 移行が失敗した場合は、移行後レポート、ログファイル、および未解析ファイルを慎重に確認して、失敗の原因を把握します。

トラブルシューティングについては、サポートチームに問い合わせることもできます。

移行の失敗のサポート

移行に失敗する場合は、サポートにお問い合わせください。

1. [移行完了（Complete Migration）] 画面で、[サポート（Support）] ボタンをクリックします。

   ヘルプサポートページが表示されます。

2. [サポートバンドル（Support Bundle）] チェックボックスをオンにして、ダウンロードする構成ファイルを選択します。

   （注） ログファイルと DB ファイルは、デフォルトでダウンロード用に選択されています。

3. [ダウンロード（Download）] をクリックします。

   サポートバンドルファイルは、ローカルパスに .zip としてダウンロードされます。Zip フォルダを抽出して、ログファイル、DB、および構成ファイルを表示します。

4. [Email us] をクリックして、テクニカルチームに障害の詳細を電子メールで送信します。

   ダウンロードしたサポートファイルを電子メールに添付することもできます。

5. [TAC ページに移動（Visit TAC page）] をクリックして、シスコのサポートページで TAC ケースを作成します。

   （注） TAC ケースは、移行中にいつでもサポートページからオープンできます。

移行後レポートの確認と移行の完了

移行後のレポートには、さまざまなカテゴリの ACL カウント、ACL 最適化、および構成ファイルで実行された最適化の全体的なビューに関する詳細が表示されます。詳細については、最適化、 移行する構成の確認と検証 （19 ページ）を参照してください。

オブジェクトを確認して検証します。

- **カテゴリ**
  - ACL ルール合計数（移行元の構成）
  - 最適化の対象とみなされる ACL ルールの合計数。冗長、シャドウなどがあります。

- 最適化の ACL カウントは、最適化の前後にカウントされた ACL ルールの合計数を示します。

移行中に移行後レポートをダウンロードし忘れた場合は、次のリンクを使用してダウンロードしてください。

移行後レポートのダウンロードエンドポイント：http://localhost:8888/api/downloads/post_migration_summary_html_format

（注） レポートは、 Firewall 移行ツールの実行中にのみダウンロードできます。

手順

ステップ 1 **移行後レポート**をダウンロードした場所に移動します。

ステップ 2 移行後レポートを開き、その内容を慎重に確認して、ASA 構成がどのように移行されたかを理解します。

- Migration Summary：ASA から Threat Defense へ正常に移行された構成の概要。ASA インターフェイス、 Management Center ホスト名とドメイン、ターゲット Threat Defense デバイス（該当する場合）、および正常に移行された構成要素に関する情報が含まれます。
- Selective Policy Migration：移行用に選択された特定の ASA 機能の詳細は、[デバイス構成機能（Device Configuration Features）]、[共有構成機能（Shared Configuration Features）]、および [最適化（Optimization）] の 3 つのカテゴリ内で使用できます。
- ASA Interface to Threat Defense Interface Mapping：正常に移行されたインターフェイスの詳細と、ASA 構成のインターフェイスを Threat Defense デバイスのインターフェイスにマッピングした方法。これらのマッピングが期待どおりであることを確認します。

  （注） このセクションは、宛先 Threat Defense デバイスを使用しない移行、または移行に**インターフェイス**が選択されて**いない**場合には適用されません。

- Source Interface Names to Threat Defense Security Zones and Interface Groups：正常に移行された ASA 論理インターフェイスと名前の詳細、およびそれらを Threat Defense のセキュリティゾーンとインターフェイスグループにマッピングした方法。これらのマッピングが期待どおりであることを確認します。

  （注） **アクセス制御リスト**と **NAT** が移行に選択されて**いない**場合、このセクションは適用されません。

- Object Conflict Handling：Management Center の既存のオブジェクトと競合していると識別された ASA オブジェクトの詳細。オブジェクトの名前と設定が同じ場合、 Firewall 移行ツールは Management Center オブジェクトを再利用しています。オブジェクトの名前が同じで構成が異なる場合は、管理者がそれらのオブジェクトの名前を変更しています。これらのオブジェクトを慎重に確認し、競合が適切に解決されたことを確認します。

- Access Control Rules, NAT, and Routes You Chose Not to Migrate： Firewall 移行ツールで移行しないように選択したルールの詳細。 Firewall 移行ツールによって無効化され、移行されなかったこれらのルールを確認します。これらの行を確認し、選択したすべてのルールがこのセクションにリストされていることを確認します。必要に応じて、これらのルールを手動で構成できます。
- Partially Migrated Configuration：詳細オプションなしでもルールを移行できる詳細オプション付きルールを含む、一部のみ移行された ASA ルールの詳細。これらの行を確認し、詳細オプションが Management Center でサポートされているかどうかを確認します。サポートされている場合は、これらのオプションを手動で構成します。
- Unsupported Configuration： Firewall 移行ツールがこれらの機能の移行をサポートしていないため、移行されなかった ASA 構成要素の詳細。これらの行を確認し、各機能が Threat Defense でサポートされているかどうかを確認します。その場合は、Management Center でこれらの機能を手動で構成します。
- Expanded Access Control Policy Rules：移行時に単一の ASA Point ルールから複数の Threat Defense ルールに拡張された ASA アクセス コントロール ポリシー ルールの詳細。
- **Actions Taken on Access Control Rules**
  - [移行しないアクセスルール（Access Rules You Chose Not to Migrate）]： Firewall 移行ツールで移行しないように選択した ASA アクセスコントロールルールの詳細。これらの行を確認し、選択したすべてのルールがこのセクションにリストされていることを確認します。必要に応じて、これらのルールを手動で構成できます。
  - Access Rules with Rule Action Change： Firewall 移行ツールツールを使用して「ルールアクション」が変更されたすべてのアクセス コントロール ポリシー ルールの詳細。ルールアクションの値は、Allow、Trust、Monitor、Block、Block with reset です。これらの行を確認し、選択したすべてのルールがこのセクションにリストされていることを確認します。必要に応じて、これらのルールを手動で構成できます。
  - Access Control Rules that have IPS Policy and Variable Set Applied：IPS ポリシーが適用されているすべての ASA アクセス コントロール ポリシー ルールの詳細。これらのルールを慎重に確認し、この機能が Threat Defense でサポートされているかどうかを確認します。
  - Access Control Rules that have File Policy Applied：ファイルポリシーが適用されているすべての ASA アクセス コントロール ポリシー ルールの詳細。これらのルールを慎重に確認し、この機能が Threat Defense でサポートされているかどうかを確認します。
  - Access Control Rules that have Rule ‘Log’ Setting Change： Firewall 移行ツールを使用して「ログ設定」が変更された ASA アクセスコントロールルールの詳細。ログ設定の値は、False、Event Viewer、Syslog です。これらの行を確認し、選択したすべてのルールがこのセクションにリストされていることを確認します。必要に応じて、これらのルールを手動で構成できます。
  - Access Control Rules that have failed Zone-lookup：ルートルックアップ操作に失敗し、**移行後レポート**に入力される ASA アクセスコントロールルールの詳細。 Firewall 移

行ツールは、送信元構成のルート（静的および接続）情報に基づいてルートルックアップ操作を実行し、アクセスルールに宛先セキュリティゾーンを設定します。

- Access Control Rules for Tunneled Protocols：移行時にプレフィルタトンネルルールとして移行されるトンネルルールの詳細。

（注） サポートされていないルールが移行されなかった場合、不要なトラフィックがファイアウォールを通過する問題が発生します。このトラフィックが Threat Defense によってブロックされるように、Management Center でルールを構成することを推奨します。

（注） [確認と検証（Review and Validate）] ページで IPS またはファイルポリシーを ACL に適用する必要がある場合は、移行前に管理センターでポリシーを作成することを強くお勧めします。 Firewall 移行ツールは接続された管理センターからポリシーを取得するため、同じポリシーを使用します。新しいポリシーを作成して複数のポリシーに割り当てると、パフォーマンスが低下し、プッシュが失敗する可能性があります。

Management Center と Threat Defense でサポートされる機能の詳細については、『Management Center Configuration Guide, Version 6.2.3』[英語] を参照してください。

ステップ 3 **移行前レポート**を開き、Threat Defense デバイスで手動で移行する必要がある ASA 構成項目をメモします。

ステップ 4 Management Center で、次の手順を実行します。

a) Threat Defense デバイスの移行された構成を確認し、次を含むすべての期待されるルールおよびその他の構成項目が移行されたことを確認します。

- アクセス制御リスト（ACL）
- ネットワークアドレス変換規則
- ポートおよびネットワークオブジェクト
- ルート（Routes）
- インターフェイス
- IP SLA オブジェクト
- オブジェクトグループの検索
- 時間ベースのオブジェクト
- VPN オブジェクト
- サイト間 VPN トンネル
- [動的ルートオブジェクト（Dynamic-Route-Objects）]

b) 一部がサポートされている、サポートされていない、無視された、無効化された、および移行されなかったすべての構成項目とルールを構成します。

これらの項目とルールを構成する方法の詳細については、『Management Center Configuration Guide』[英語] を参照してください。手動構成が必要な構成項目の例を次に示します。

- プラットフォーム設定（SSH アクセスと HTTPS アクセスを含む）（「Threat Defense プラットフォーム設定」を参照）
- Syslog 設定（「Configure Syslog」を参照）
- 動的ルーティング（「Routing Overview for Threat Defense」を参照）
- サービスポリシー（「FlexConfig Policies」を参照）
- VPN 構成（「Threat Defense VPN」を参照）
- 接続ログ設定（「Connection Logging」を参照）

ステップ 5 確認が完了したら、Management Center から Threat Defense デバイスに移行された構成を展開します。

サポートされていないルールと一部がサポートされているルールについて、データが**移行後レポート**に正しく反映されていることを確認します。

Firewall 移行ツールでポリシーが Threat Defense デバイスに割り当てられます。変更が実行中の構成に反映されていることを確認します。移行されるポリシーを識別しやすくするために、これらのポリシーの説明には ASA 構成のホスト名が含まれています。

Firewall 移行ツールのアンインストール

すべてのコンポーネントは、Firewall 移行ツールと同じフォルダに保存されます。

手順

ステップ 1 Firewall 移行ツールを配置したフォルダに移動します。

ステップ 2 ログを保存する場合は、`log` フォルダを切り取りまたはコピーして別の場所に貼り付けます。

ステップ 3 移行前レポートと移行後レポートを保存する場合は、`resources` フォルダを切り取りまたはコピーして別の場所に貼り付けます。

ステップ 4 Firewall 移行ツールを配置したフォルダを削除します。

ヒント ログファイルはコンソールウィンドウに関連付けられています。Firewall 移行ツールのコンソールウィンドウが開いている限り、ログファイルとフォルダは削除できません。