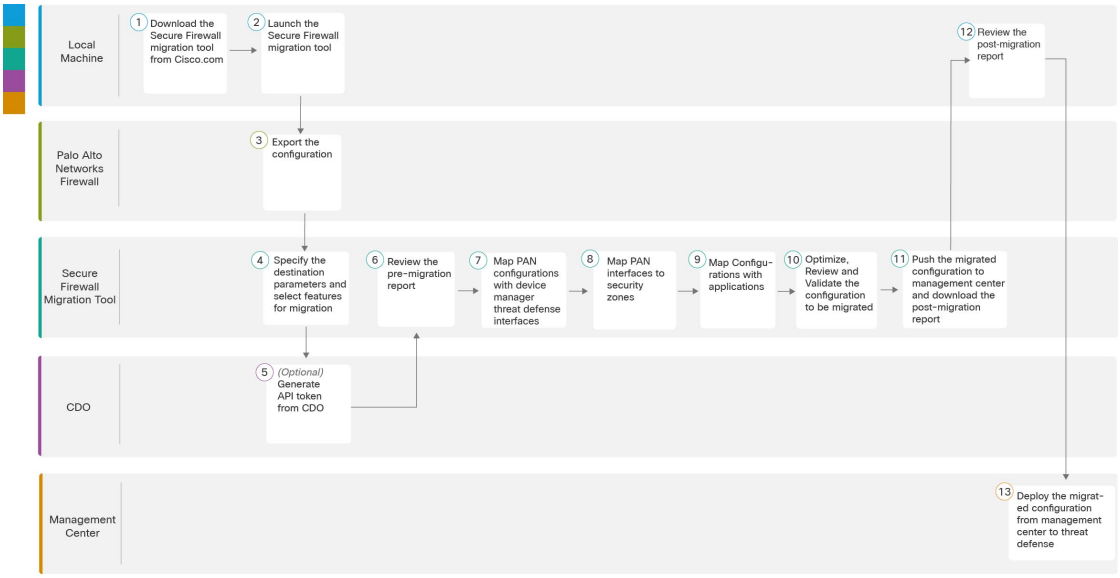
Palo Alto Networks ファイアウォールの Threat Defense への移行ワークフロー

エンドツーエンドの手順

次のフローチャートは、Cisco Secure Firewall 移行ツールを使用して、Palo Alto Networks ファイアウォールを Threat Defense に移行するワークフローを示しています。



	ワークスペース	手順
1	Local Machine	Cisco.com から Cisco Secure Firewall 移行ツールをダウンロードします。詳細な手順については、「Cisco.com からの Cisco Secure Firewall 移行ツールのダウンロード」を参照してください。
2	Local Machine	ローカルマシンで Cisco Secure Firewall 移行ツールを起動します。「Cisco Secure Firewall 移行ツールの起動」を参照してください。
3	Palo Alto Networks ファイアウォール	構成ファイルのエクスポート：Palo Alto Networks ファイアウォールから構成をエクスポートするには、「Palo Alto Networks ファイアウォールからの構成のエクスポート」を参照してください。
4	Cisco Secure Firewall 移行ツール	このステップでは、移行の接続先パラメータを指定できます。詳細な手順については、「Cisco Secure Firewall 移行ツールの接続先パラメータの指定」を参照してください。
5	CDO	（オプション）この手順はオプションであり、クラウドで提供される Firewall Management Center を移行先管理センターとして選択した場合にのみ必要です。詳細な手順については、「Cisco Secure Firewall移行ツールの接続先パラメータの指定」を参照してください。
6	Cisco Secure Firewall 移行ツール	移行前レポートをダウンロードした場所に移動し、レポートを確認します。詳細な手順については、「移行前レポートの確認」を参照してください。
7	Cisco Secure Firewall 移行ツール	PAN 構成が正しく移行されるように、PAN インターフェイスを適切な Threat Defense 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。詳細な手順については、「PAN ファイアウォール 構成と Threat Defense インターフェイスのマッピング」を参照してください。
8	Cisco Secure Firewall 移行ツール	PAN インターフェイスを適切なセキュリティゾーンにマッピングします。詳細な手順については、「セキュリティゾーンインターフェイスグループ への PAN インターフェイスのマッピング」をご覧ください。
9	Cisco Secure Firewall 移行ツール	PAN 構成を対応するターゲットアプリケーションにマップできます。詳細な手順については、「構成とアプリケーションのマッピング」を参照してください。
10	Cisco Secure Firewall 移行ツール	構成を慎重に確認し、それが適切で Threat Defense デバイスの構成内容と一致することを確認します。詳細な手順については、「最適化、 構成の確認と検証」を参照してください。

	ワークスペース	手順
11	Cisco Secure Firewall 移行ツール	移行プロセスのこのステップでは、移行された構成を管理センターに送信し、移行後レポートをダウンロードできるようにします。詳細な手順については、「移行された構成の以下へのプッシュ：Management Center」を参照してください。
12	Local Machine	移行後レポートをダウンロードした場所に移動し、レポートを確認します。詳細な手順については、「移行後レポートの確認と移行の完了」を参照してください。
13	Management Center	移行した構成を管理センターから Threat Defense に展開します。詳細な手順については、「移行後レポートの確認と移行の完了」を参照してください。

移行の前提条件

PAN 構成を移行する前に、次のアクティビティを実行します。

Cisco.com からの Cisco Secure 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。

ステップ 1 コンピュータで、Cisco Secure 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。Cisco Secure 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） Cisco Secure 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 [Cisco Secure 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 Cisco Secure 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 Cisco Secure 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 Cisco Secure Firewall 移行ツール実行可能ファイルをダウンロードします。

移行の実行

Cisco Secure Firewall 移行ツールの起動

このタスクは、デスクトップバージョンの Cisco Secure Firewall 移行ツールを使用している場合にのみ適用されます。CDO でホストされている移行ツールのクラウドバージョンを使用している場合は、「Palo Alto Networks ファイアウォールからの設定のエクスポート」に進みます。

（注） Cisco Secure 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、Cisco Secure 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、Cisco Secure 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 からの Cisco Secure Firewall 移行ツールのダウンロード
- サポートされる移行先の管理センターセクションで要件を確認します。
- Cisco Secure Firewall 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。

ステップ 1 コンピュータで、Cisco Secure 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、Cisco Secure 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、Cisco Secure 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。

Cisco Secure Firewall 移行ツールは、すべての関連ファイルを作成し、Cisco Secure Firewall 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、Cisco Secure 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、Cisco Secure 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
```

Cisco Secure Firewall 移行ツールは、すべての関連ファイルを作成し、Cisco Secure Firewall 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 Cisco Secure 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 Cisco Secure 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 Cisco Secure Firewall 移行ツールにログインします。

ステップ 4 Cisco Secure 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。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。

  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。

- インターネットにアクセスできないエアギャップネットワークにファイアウォールを展開した場合は、Cisco TAC に連絡して、管理者のログイン情報で動作するビルドを入手してください。このビルドでは使用状況の統計がシスコに送信されず、TAC がログイン情報を提供できることに注意してください。

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、Cisco Secure 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、Cisco Secure 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。

- Cisco Secure Firewall 移行ツールを使用して PAN ファイアウォールから情報を抽出する必要がある場合は、「Palo Alto ファイアウォールからの構成ファイル（Panorama の管理対象外）」に進みます。

Cisco Secure Firewall 移行ツールでのデモモードの使用

Cisco Secure Firewall 移行ツールを起動し、**[送信元設定の選択（Select Source Configuration）]** ページで、**[移行の開始（Start Migration）]** を使用して移行を開始するか、**[デモモード（Demo Mode）]** に入るかを選択できます。

デモモードでは、ダミーデバイスを使用してデモ移行を実行し、実際の移行フローがどのようになるかを可視化できます。移行ツールは、**[送信元ファイアウォールベンダー（Source Firewall Vendor）]** ドロップダウンでの選択に基づいてデモモードをトリガーします。構成ファイルをアップロードするか、ライブデバイスに接続して移行を続行することもできます。デモ FMC デバイスやデモ FTD デバイスなどのデモのソースデバイスとターゲットデバイスを選択して、デモ移行の実行を進められます。

⚠

注意 **[デモモード（Demo Mode）]** を選択すると、既存の移行ワークフローは消去されます。**[移行の再開（Resume Migration）]** にアクティブな移行があるときにデモモードを使用すると、アクティブな移行は失われ、デモモードを使用した後に最初から再開する必要があります。

また、実際の移行ワークフローと同様に、移行前レポートのダウンロードと確認、インターフェイスのマッピング、セキュリティゾーンのマッピング、インターフェイスグループのマッピングなどのすべてのアクションを実行することもできます。ただし、デモ移行は設定の検証までしか実行できません。これはデモモードにすぎないため、選択したデモターゲットデバイスに設定をプッシュすることはできません。検証ステータスと概要を確認し、**[デモモードの終了（Exit Demo Mode）]** をクリックして **[送信元設定の選択（Select Source Configuration）]** ページに再度移動し、実際の移行を開始できます。

（注） デモモードでは、設定のプッシュを除く Cisco Secure Firewall 移行ツールのすべての機能セットを活用して、実際の移行を行う前にエンドツーエンドの移行手順のトライアルを実行できます。

Palo Alto Networks ファイアウォールからの構成のエクスポート

構成ファイルは、次の方法でエクスポートできます。

Palo Alto ファイアウォールからの構成ファイル（Panorama の管理対象外）

ゲートウェイから構成を抽出するには、次の手順を実行します。

ステップ 1 [Device] > [Setup] > [Operations] に移動し、[Save Named Configuration <file_name.xml>] を選択します。

ステップ 2 [OK] をクリックします。

ステップ 3 [Device] > [Setup] > [Operations] に移動し、[Export Named Configuration] をクリックします。

ステップ 4 <file_name.xml> ファイルを選択します。

ステップ 5 [OK] をクリックします。

ステップ 6 実行構成 <file_name.xml> を含む XML ファイルを選択し、[Ok] をクリックして構成ファイルをエクスポートします。

ステップ 7 エクスポートしたファイルをファイアウォールの外部の場所に保存します。このバックアップを使用して Cisco Secure Firewall 移行ツールにアップロードし、構成を 脅威に対する防御 に移行できます。

ステップ 8 （任意）接続先 NAT に同じ送信元ゾーンと接続先ゾーンがある NAT ポリシーがある場合は、次の手順を実行します。

a) ファイアウォールで CLI から **show routing route** コマンドを実行します。
b) ルーティングテーブルを .txt ファイルにコピーします。
c) この .txt ファイルをフォルダに追加します。このフォルダで .txt ファイルと .xml ファイル（panconfig.xml を含む）を圧縮します。

これらのステップは、移行に必須ではありません。これらのステップを実行しないと、接続先ゾーンは Cisco Secure Firewall 移行ツールでの移行中にマッピングされず、移行レポートに含まれます。

（注） **show routing route** コマンドを使用して、ルーティングテーブルの詳細を抽出します。抽出した出力をメモ帳に貼り付けます。

Palo Alto ファイアウォールからの構成ファイル（Panorama の管理対象）

デバイスが Panorama で管理されている場合は、ゲートウェイから設定を抽出する必要があります。Panorama 設定をゲートウェイと統合し、設定を抽出します。

Cisco Secure Firewall 移行ツールのユーザーインターフェイスで、次の手順を実行します。

始める前に

スーパーユーザーアカウントを使用して、Palo Alto ファイアウォールの Web UI にログインします。

ステップ 1 **[デバイス（Device）]** > **[サポート（Support）]** > **[テクニカルサポートファイル（Tech Support File）]**に移動します。

ステップ 2 **[テクニカルサポートファイルの生成（Generate Tech Support File）]**をクリックします。

ステップ 3 生成されたファイルが利用可能になったら、[テクニカルサポートファイルのダウンロード（Download Tech Support File）] をクリックします。

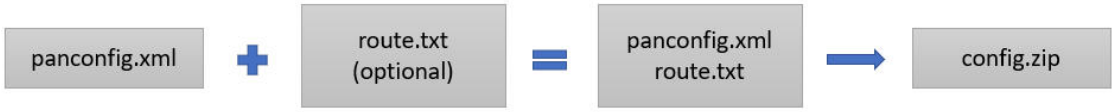
ステップ 4 ファイルを解凍して展開し、パス *\opt\pancfg\mgmt\saved-configs* に移動して、*merged-running-config.xml* ファイルを取得します。

次のタスク

エクスポートされたファイルの圧縮

エクスポートされたファイルの圧縮

Palo Alto Gateway ファイアウォールの panconfig.xml、および route.txt をエクスポートします（同じ送信元ゾーンと宛先ゾーンを持つ NAT ルールがある場合）。



Cisco Secure 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。
- Cisco Secure Firewall 移行ツール 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、リージョンと API トークンを指定する必要があります。詳細については、「サポートされる移行先の管理センター」を参照してください。
- （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 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。Cisco Secure 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。

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 から API トークンを生成するため、以下の手順に従います。

1. CDO ポータルにログインします。
2. **[設定（Settings）] > [全般設定（General Settings）]** に移動して、API トークンをコピーします。

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、Cisco Secure 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。

Cisco Secure 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。

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、 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。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。

（注） サポートされているターゲット Threat Defense プラットフォームが、管理センターバージョン 6.5 以降を備えた Firewall 1010である場合にのみ、FDM 5505 移行サポートは共有ポリシーに適用され、デバイス固有のポリシーには適用されません。Threat Defense なしで続行すると、Cisco Secure Firewall 移行ツールは構成またはポリシーを Threat Defense にプッシュしません。したがって、Threat Defense 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。

リモート展開が有効になっている Management Center または 脅威に対する防御 6.7 以降への Palo Alto Networks ファイアウォールの移行は、Cisco Secure Firewall 移行ツールでサポートされています。インターフェイスとルートの移行は手動で行う必要があります。

- [FTD を使用せず続行（Proceed without FTD）] 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、Cisco Secure 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 のデバイス固有の校正であるインターフェイスとルート、およびサイト間 VPN は移行されず、Management Center で手動で構成する必要があります。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、Cisco Secure 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。

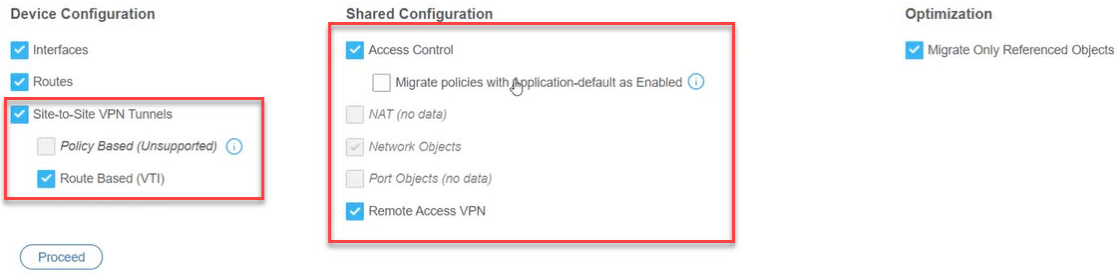
- 接続先 脅威に対する防御 デバイスに移行する場合、Cisco Secure Firewall 移行ツールは、[デバイスの構成（Device Configuration）] セクションと [共有構成（Shared Configuration）] セクションで、 構成から移行できる機能を自動的に選択します。要件に応じて、デフォルトの選択をさらに変更できます。
- Management Center に移行する場合、Cisco Secure Firewall 移行ツールは、[共有構成（Shared Configuration）] セクションで、 構成から移行できる機能を自動的に選択します。要件に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

- PAN の場合は、[Shared Configuration] で、関連する [Access Control] オプションを選択します。

  Migrate policies with Application-Default as Enabled：このオプションを選択すると、PAN アプリケーションが移行されます。このチェックボックスをオンにした場合にのみ、[Migrate policies with Application-Default as Enabled] オプションが表示されます。

  （注） [Application Mapping] は、ポリシーが移行対象として選択されている場合にのみ有効になります。



VPN が設定された Palo Alto Networks ファイアウォールから設定を移行する場合は、**[デバイス設定（Device Configuration）]** ペインで **サイト間 VPN トンネル**を、**[共有設定（Shared Configuration）]** ペインで**リモートアクセス VPN** を選択または選択解除できます。ポリシーベースのサイト間 VPN 設定は、Palo Alto Networks ファイアウォールでサポートされていないため、サポートされないことに注意してください。

サービスが "Application-Default" であるポリシー

サービスが「**application-default**」であり、アプリケーションが参照されているメンバーまたはグループを持つポリシーは、[機能の選択（Feature Selection）] ページでの選択に従って移行されます。Management Center には **application-default** と同等の設定がないため、このようなポリシーはサービス「any」でプッシュされます。**application-default** と同様の機能を複製する場合は、アプリケーションが使用するポートを Palo Alto Networks ファイアウォールから見つけ、Management Center の [ポリシー（Policy）] のポートセクションでそのポートを構成します。

たとえば、"**web-browsing**" を持ち、サービスが"**application-default**" であるポリシーは、アプリケーション HTTP（web-browsing と同等）と "**any**" ポートとして移行されます。"**application-default**" と同じ機能を複製するには、ポートを TCP/80 および TCP/8080 として構成します。web-browsing は、ポート TCP 80 および TCP 8080 を使用します。ポリシーに複数のアプリケーションがある場合は、各アプリケーションで使用されるポートを構成します。

ポリシーに複数のアプリケーションがある場合は、ポートを構成する前にポリシーを分割することを推奨します。これにより、他のアプリケーションへの追加アクセスが許可される可能性があるためです。

"**any**" として構成されたアプリケーションと "**application-default**" として構成されたサービスが設定されているポリシーは、[Feature Selection] ページで選択できる項目（アプリケーションは "**any**"、サービスは"**any**"）に関係なく、無効として移行されます。これが許容可能な動作である場合は、アプリケーションを有効にして変更をコミットします。それ以外の場合は、必要なアプリケーションまたはサービスを選択し、ポリシーを有効にします。

ルールごとのアプリケーションによるアクセス制御リストの分割

複数のアプリケーションに設定された 1 つのルールを含むアクセス制御リストを移行する場合は、ACL の分割を選択できます。これによりそのルールは、1 つのルールにつきアプリケーションが 1 つの複数のルールに分割されます。これを行うには、**[ルールごとにアプリケーションで ACL を分割する（Split ACLs with applications with rules per rule）]** チェックボックスをオンにします。ただし、移行しようとしている設定に、アクセスルールごとに設定された複数のアプリケーションが含まれていない場合、チェックボックスは表示されません。

各ルールは、1 つのルールにつきアプリケーションが 1 つの複数のルールに変換されます。これは、**[設定の最適化、確認、検証（Optimize, Review, and Validate Configuration）]** ページで確認できます。

- Cisco Secure Firewall 移行ツールは、ターゲット管理センターが 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、 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。

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 Cisco Secure 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、Cisco Secure 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。

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、Cisco Secure Firewall 移行ツールの実行中にのみダウンロードできます。

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、Cisco Secure 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。

- 脅威に対する防御 に正常に移行できるサポート対象 構成要素と、移行対象として選択された特定の機能のサマリー。
- [エラーのある構成行（Configuration Lines with Errors）]：Cisco Secure 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 の構成要素の詳細。 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 Cisco Secure 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 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、 Cisco Secure 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）]：Cisco Secure 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 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、 Cisco Secure 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 Cisco Secure 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 構成要素の詳細。Cisco Secure 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、 インターフェイス で修正を完了し、 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 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、Cisco Secure 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

PAN ファイアウォール 構成と Threat Defense インターフェイスのマッピング

PAN ファイアウォール 構成と 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、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。

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 PAN 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またはサブインターフェイスが同数以上必要です（PAN 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。
  - 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 Cisco Secure 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 PAN 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（ 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 PAN 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。

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、「Cisco Secure 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。

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、**[FTDインターフェイス名（FTD Interface Name）]** のドロップダウンリストをクリックし、その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。Cisco Secure Firewall 移行ツールは、 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。

（注） 送信元ファイアウォールのインターフェイスの数がターゲットファイアウォールのインターフェイスの数よりも多い場合は、ターゲットファイアウォールにサブインターフェイスを作成し、移行を再試行します。

ステップ 2 各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

PAN 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 オブジェクトとセキュリティゾーン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インターフェイスグループ への PAN 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インターフェイスグループへのPANインターフェイスのマッピング

構成が正しく移行されるように、 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 にマッピングします。 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。

Cisco Secure Firewall 移行ツールでは、セキュリティゾーン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の詳細については、『*Cisco Secure Firewall Management Center Device Configuration Guide*』の「Security Zones and Interface Groups」を参照してください。

ステップ 1 [セキュリティゾーンのマッピング（Map Security Zones）] 画面で、使用可能なインターフェイスとセキュリティゾーンを確認します。

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 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、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、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 Management Center に存在するセキュリティゾーンにインターフェイスをマッピングするには、[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。

ステップ 4 セキュリティゾーンは、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。

セキュリティゾーン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、[Add] をクリックして新しいセキュリティゾーンを追加します。
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。
d) [閉じる（Close）] をクリックします。

セキュリティゾーン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、[ゾーンマッピング（Zone Mapping）] をオンにします。
c) [自動作成（Auto-Create）] をクリックします。

[自動作成（Auto-Create）] をクリックすると、送信元ファイアウォールゾーンが自動的にマッピングされます。同じ名前のゾーンが Management Center にすでに存在する場合、そのゾーンは再利用されます。マッピングページには、再利用ゾーンに対して "(A)" が表示されます。たとえば、**inside** "(A)" となります。

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にマッピングしたら、[次へ（Next）] をクリックします。

構成とアプリケーションのマッピング

アプリケーションを対応するターゲットアプリケーションにマッピングできます。アプリケーションに基づくルールを移行できます。

Management Center の定義済みアプリケーションと、構成ファイルに含まれる一部のアプリケーションのリストが、このタブにリストされます。Management Center に存在する定義済みマッピングの一部がマップされます。

（注） 定義済みマッピングを編集することはできません。

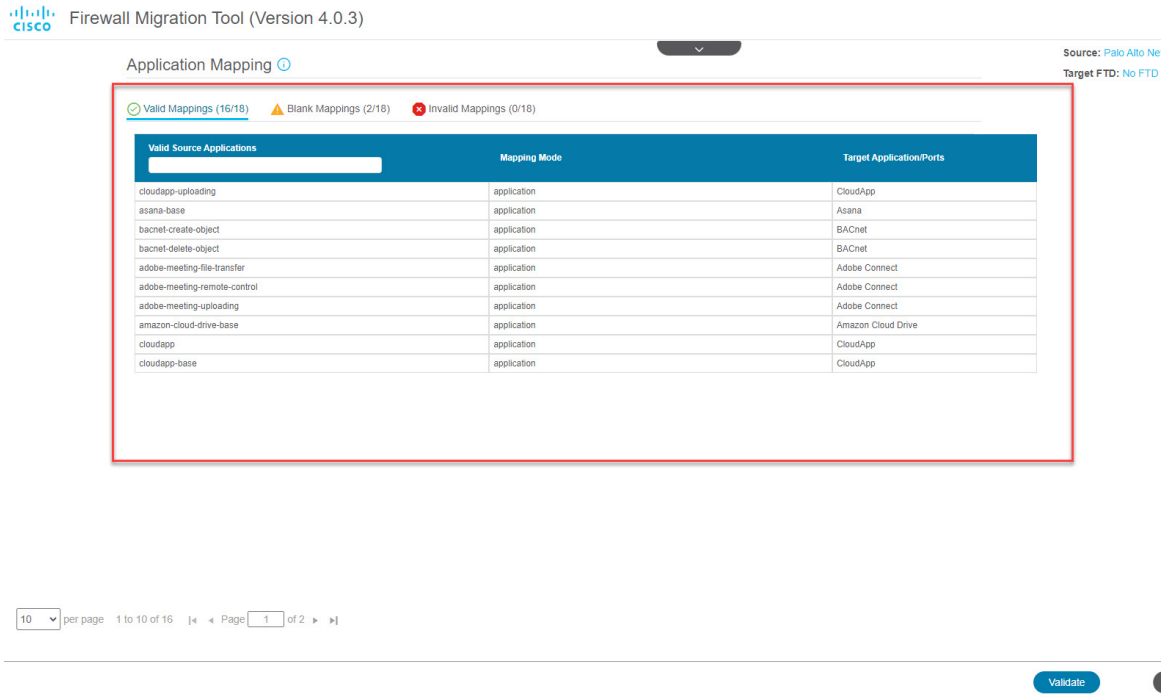
[Application Mapping] ページには、次のタブが表示されます。

- Invalid Mappings：その移行で無効なマッピングのリストを表示します。

  マッピングは、次のシナリオで **Invalid** と呼ばれます。

  - [Mapping Mode] に [Application] または [Port] が選択されているが、[Target] が空の場合。
  - [Mapping Mode] が [Port] で、ポートの構文が正しくない場合。移行を続行するには、[Invalid Mapping] をゼロにする必要があります。

（注） 正しい検証が行われるまで、[Next] ボタンは無効になります。



送信元からマッピングの定義済みリストを取得すると、自動的にマップされる定義済みアプリケーションがあります。マップされていないアプリケーションがある場合は、ポートまたはアプリケーションに手動でマップする必要があります。

- Blank Mappings：マッピングされていないアプリケーションを表示し、ユーザーアクションを要求します。**アプリケーション**は、**アプリケーション**または**ポート**にマッピングされている必要があります。

（注） すべての**アプリケーション**エントリをマッピングすることを推奨しますが、必須ではありません。

マッピングモードが選択され、ターゲットアプリケーションに有効なデータがある場合、それは有効なマッピングです。

（注） デフォルトでは、すべての定義済みマッピングを [Valid Mappings] タブで使用できます。

- Valid Mappings：正しいマッピングを表示します。Cisco Secure Firewall 移行ツールには、一般的に使用されるアプリケーション用に PAN および 脅威に対する防御 のアプリケーションとの定義済みマッピングのデータベースが独自に用意されています。PAN アプリケーションが定義済みマッピング DB と一致する場合、それらのアプリケーションは自動的にマッピングされ、有効なマッピングの下に表示されます。

  アプリケーションが [Blank Mapping] で**アプリケーション**または**ポート**にマッピングされると、検証後に [Valid Mapping] に移動されます。

（注） 定義済みマッピングは編集できません。

無効、有効、およびブランクのマッピング数は、移行に基づいて変化し続けます。

次の表に、アプリケーションマッピングのプロパティを示します。

表 *1*: アプリケーション マッピング テーブル プロパティ

フィールド	説明
送信元アプリケーション（Source Application）	Palo Alto Networks ファイアウォールで使用されているアプリケーションのリストを表示します。
マッピングモード（Mapping Mode）	[Application] または [Port(s)] のいずれかのマッピングモードを選択します。 • Application：マッピングに使用可能なターゲットアプリケーションのリストから選択します。マッピングできるアプリケーションは 1 つだけです。 • Port(s)：マッピングに使用できるポートのリストから選択します。[Ports] を選択する場合は、指定された形式で関連するポート情報を入力します。たとえば、tcp/80 や udp/80 です。 （注） 文字間のスペースは使用できません。

フィールド	説明
対象のアプリケーション（Target Application）	マッピングモードに基づくターゲットアプリケーションまたはポートのリストを表示します。

ICMP および Ping のアプリケーションは、**ICMP** および **ping** のサービスとして移行されます。これは Cisco Secure Firewall 移行ツールによって自動的に実行されるため、[アプリケーションマッピング（Application Mapping）] ページには表示されません。

ステップ 1 [Valid Mappings] タブをクリックして、その移行に有効なマッピング数を表示します。**有効な送信元アプリケーション**と、有効な**マッピングモード**および**ターゲットアプリケーション**をマッピングします。

マッピングが有効になると、有効なマッピング数の増加を確認できます。

ステップ 2 [Blank Mappings] をクリックして、その移行のブランクマッピングのリストを表示します。**ブランク送信元アプリケーション**と、有効な**マッピングモード**および**ターゲットアプリケーション**をマッピングします。

たとえば、マッピングモードを選択し、ターゲット接続先を入力せずに保存すると、ブランクマッピング数が増加します。タブを確認して正しくマッピングし、移行を続行します。

（注） ブランクマッピングがある場合でも、移行を続行できます。

ステップ 3 [Invalid Mappings] タブをクリックして、無効なマッピングのリストを表示します。次の手順を実行します。

a) Invalid Application：移行中に無効なマッピングが表示されます。
b) Mapping Mode：[Application] または [Port] のいずれかのマッピングモードを選択します。
c) Target Application：アプリケーションマッピングのターゲットアプリケーションを選択します。

たとえば、マッピングモードを選択したが、別のターゲット接続先にマップした場合、他のタブに進むことはできません。[Invalid Mappings] タブを確認し、正しいターゲットアプリケーションを入力して、アプリケーションマッピングを実行します。

ステップ 4 各タブで [Validate] をクリックして、その移行の無効なマッピング、ブランクマッピング、または有効なマッピングを検証します。

ステップ 5 [Next] をクリックして続行します。

ステップ 6 検証前に手動で実行したマッピングをクリアするには、**[マップされたデータのクリア（Clear Mapped Data）]** をクリックします。検証をクリックしてマッピングが有効になった後はマッピングを元に戻すことができないため、実行しているマッピングに完全な確信がある場合にのみ**[検証（Validate）]** をクリックすることをお勧めします。

次のタスク

最適化、 構成の確認と検証

最適化、 構成の確認と検証

移行した 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。

（注） [構成の最適化、確認および検証（Optimize, Review and Validate Configuration）] 画面で Cisco Secure 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 Cisco Secure 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 Cisco Secure Firewall 移行ツールを再起動します。

これで、Cisco Secure 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。

（注） デフォルトでは、[インライングループ化（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 Cisco Secure 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 Cisco Secure Firewall 移行ツールを再起動します。

Cisco Secure Firewall 移行ツールの ACL 最適化の概要

Cisco Secure Firewall移行ツールは、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。

Cisco Secure Firewall 移行ツールは、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） PAN 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

ダイナミック IP/ポート フォールバック インターフェイス

Palo Alto Networks から Threat Defense への移行のため、**[設定の最適化、確認、および検証（Optimize, Review and Validate Configuration）]** ページで NAT 設定を確認する場合は、NAT ルールに**ダイナミック IP/ポートフォールバック**設定があるかどうか、およびルールが移行または削除されているかどうかも確認できます。

設定したダイナミック IP またはポート フォールバック インターフェイス アドレスが宛先ゾーンアドレスと同じである場合、Cisco Secure Firewall 移行ツールは NAT ルールを移行します。異なる場合、ルールは移行されず、サポート対象外としてリストされます。これはCisco Secure Firewall Management Center が、ダイナミック IP またはポート フォールバック インターフェイスとして宛先アドレスしか持てないためです。NAT ルールにフォールバック設定がない場合、

移行は検証なしで実行され、**[ダイナミック IP/ポートフォールバック（Dynamic IP/Port-fallback）]** 列には **[適用なし（Not Applicable）]** と表示されます。

ステップ 1 **[設定の最適化、確認、および検証（Optimize, 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。

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。

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、ポリシーのボックスをオンにして行を選択し、**[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。

ヒント アクセス制御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。

ACE カウントは、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処理できます。

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 2 次のタブをクリックし、構成項目を確認します。

- **アクセス制御**
- **オブジェクト（ネットワークオブジェクト、ポートオブジェクト）**
- **NAT**
- [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）]

（注） サイト間およびリモートアクセス VPN の設定では、VPN フィルタ設定とそれらに関連する拡張アクセスリストオブジェクトが移行され、それぞれのタブで確認できます。

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 3 （任意）構成の確認中に、オブジェクトを選択して**[アクション（Actions）]** > **[名前の変更（Rename）]** を選択することで、**[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）]** タブで 1 つ以上のネットワークオブジェクトまたはポートオブジェクトの名前を変更できます。

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 4 エントリを選択して**[アクション（Actions）]** > **[移行しない（Do not migrate）]**を選択することで、**[ルート（Routes）]** セクションからルートを表示し、移行しないルートを 1 つ以上選択できます。

ステップ 5 **[サイト間VPNトンネル（Site-to-Site VPN Tunnels）]** セクションに、サポートされているすべての VPN トポロジが表示されます。すべての行の事前共有キーの値を入力する必要があります。

ステップ 6 **[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 Palo Alto Networks ファイアウォールから管理センターに移行され、次のように表示されます。

- **[ポリシーの割り当て（Policy Assignment）]**：接続プロファイル、その VPN プロトコル、ターゲットデバイス、および VPN インターフェイスの名前を確認および検証します。接続プロファイルの名前を変更する場合は、エントリを選択し、**[アクション（Actions）]** > **[名前の変更（Rename）]**をクリックします。
- **IKEV2**：IKEv2 プロトコル設定（存在する場合）と、それらにマッピングされている送信元インターフェイスを確認および検証します。
- **Anyconnect パッケージ**：AnyConnect 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、Cisco Secure 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、送信元のファイアウォール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、Cisco Secure Firewall 移行ツールは検証に進みません。

- [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（Trustpoints）]**：PAN ファイアウォール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。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。

ステップ 7 （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 8 確認が完了したら、[検証（Validate）] をクリックします。注意が必要な必須フィールドは、値を入力するまで点滅し続けることに注意してください。**[検証（Validate）]** ボタンは、すべての必須フィールドに入力した後にのみ有効になります。

検証中、Cisco Secure 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、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。オブジェクトがすでに Management Center に存在する場合、Cisco Secure Firewall 移行ツールは次の処理を実行します。

- オブジェクトの名前と構成が同じ場合、Cisco Secure 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、Cisco Secure 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 9 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。

Cisco Secure 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 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「Successfully Validated」というメッセージが表示されたら、移行された構成の以下へのプッシュ： Management Center （25 ページ）に進みます。

移行された構成の以下へのプッシュ： Management Center

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、移行された構成を 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 Management Center に送信します。脅威に対する防御 デバイスに構成を展開しません。ただし、脅威に対する防御 上の既存の構成はこのステップで消去されます。

（注） Cisco Secure Firewall 移行ツールが移行された構成を 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。

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、移行した 構成を Management Center に送信します。

Cisco Secure 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、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。

移行後レポートのコピーも、Cisco Secure 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、 構成の確認と検証 （20 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、Cisco Secure Firewall 移行ツールの実行中にのみダウンロードできます。

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、 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 脅威に対する防御 正常に移行された構成の概要。 インターフェイス、Management Center ホスト名とドメイン、ターゲット 脅威に対する防御 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 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。
- 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、 構成のインターフェイスを 脅威に対する防御 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 脅威に対する防御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：正常に移行された PAN 論理インターフェイスと名前の詳細、およびそれらを 脅威に対する防御 のセキュリティゾーン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 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、Cisco Secure 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：Cisco Secure 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。Cisco Secure 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 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：Cisco Secure 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 構成要素の詳細。これらの行を確認し、各機能が 脅威に対する防御 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 Point ルールから複数の 脅威に対する防御 ルールに拡張された 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**
  - Access Rules You Chose Not to Migrate：Cisco Secure Firewall 移行ツールで移行しないように選択した 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：Cisco Secure Firewall 移行ツールを使用して「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 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 脅威に対する防御 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 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 脅威に対する防御 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：Cisco Secure Firewall 移行ツールを使用して「ログ設定」が変更された 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。

（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 脅威に対する防御 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。Cisco Secure 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 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, 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、脅威に対する防御デバイスで手動で移行する必要がある 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) 脅威に対する防御 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
- 動的ルートオブジェクト

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 脅威に対する防御 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。

Cisco Secure Firewall 移行ツールは、ポリシーを 脅威に対する防御 デバイスに割り当てます。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 構成のホスト名が含まれています。

解析のサマリー

解析のサマリーには、オブジェクト、インターフェイス、NAT、ポリシー、およびアプリケーションの数が表示されます。サマリーには、[Pre-parse Summary]、[Parse Summary]、および [Pre-push Summary] の 3 つのコンポーネントがあります。

- Pre-parse Summary：構成のアップロード後に、解析前サマリーが表示されます。この段階で、Cisco Secure Firewall 移行ツールはさまざまなコンポーネントの数を表示します。カスタムアプリケーション、またはグループで使用されているアプリケーションのみが表示されます。構成がマルチ VSYS の場合、完全な VSYS のインターフェイス数が表示されます。ポリシーで直接呼び出されるアプリケーションはカウントされないため、解析前サマリーには一部のアプリケーションが表示されません。したがって、アプリケーション数は解析のサマリーと異なります。同様の動作が NAT にも適用されます。解析前サマリーの一部のコンポーネントにはゼロカウントが表示される場合がありますが、これはこれらの構成の構成要素が 0 であることを意味しません。
- Parse Summary：変換の開始をクリックすると、解析のサマリーが表示されます。この段階で、Cisco Secure Firewall 移行ツールは構成に対してアクションを実行し、サポートされていないすべての構成がサマリーカウントから削除されます。サポートされていないポリシーは無効として Management Center に移行されるため、サポートされていないポリシーはカウントの一部になります。構成の各コンポーネントが解析されます。解析のサマリーで表示されるカウントは、移行される正確な構成カウントです。
- Pre-push Summary：構成を Management Center にプッシュするよう求めるプロンプトが表示される前に、プッシュ前サマリーが表示されます。解析前サマリーのカウントは、Cisco Secure Firewall 移行ツールによって実行されるアクションによって、解析のサマリーと異なる場合があります。NAT で直接参照される IP は、オブジェクトとしてプッシュされます。アプリケーションがポートにマッピングされると、サービスカウントが増加し、アプリケーションがダウンします。アプリケーションマッピングを空白のままにすると、アプリケーション数は減少します。静的ルートに重複するエントリがある場合、そのエントリは削除され、カウントは減少します。

移行の失敗

移行中の解析エラーは次のとおりです。

- **解析の失敗**：構成が Cisco Secure Firewall 移行ツールにアップロードされた後に解析が失敗します。インターフェイスの不良構成が原因です。複数の IP が構成されているか、/32 または /128 の IP がインターフェイスに割り当てられている場合、解析に失敗します。

インターフェイスに複数の IP が割り当てられている場合、またはトンネリング、ループバック、VLANインターフェイスがルーティングの一部である場合は、プッシュの失敗が発生します。

回避策：**移行前レポート**をダウンロードし、移行レポートの [Configuration lines with errors] セクションを参照します。このセクションには、問題の原因となっている構成の詳細が表示されます。問題を修正し、Cisco Secure Firewall 移行ツールに構成を再アップロードする必要があります。

ルート内のトンネル、ループバック、または VLAN インターフェイスによってプッシュの失敗が発生した場合は、そのようなルートを削除して移行を再試行する必要があります。このようなインターフェイスはManagement Center でサポートされていないためです。

- **プッシュの失敗**：Cisco Secure Firewall 移行ツールが構成を移行し、Management Center にプッシュされているときに、プッシュの失敗が発生します。プッシュの失敗は、**移行後レポート**でキャプチャされます。

  回避策：**移行後レポート**をダウンロードし、移行レポートの [Error Reporting] セクションを参照します。このセクションには、問題の原因となっている構成の詳細が表示されます。[確認と検証（Review and Validation）] ページで問題を修正する必要があります。これには、失敗が表示されているセクションで [移行しない（do not migrate）] オプションを選択するか、または送信元構成で問題を修正し、Cisco Secure Firewall 移行ツールに構成を再アップロードします。

Cisco Secure 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、Cisco Secure Firewall 移行ツールと同じフォルダに保存されます。

ステップ 1 Cisco Secure 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 Cisco Secure 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。Cisco Secure Firewall 移行ツールのコンソールウィンドウが開いている場合、ログファイルとフォルダは削除できません。

移行例： PAN から Threat Defense 2100 へ

（注） 移行の完了後にターゲットデバイスで実行できるテスト計画を作成します。

- メンテナンス期間前のタスク
- メンテナンス期間のタスク

メンテナンス期間前のタスク

始める前に

Management Center をインストールして展開していることを確認します。詳細については、適切な『Management Center Hardware Installation Guide』[英語] および適切な『Management Center Getting Started Guide』[英語] を参照してください。

ステップ 1 ネットワークに Firepower 2100 シリーズ デバイスを展開し、インターフェイスを接続してアプライアンスの電源をオンにします。

詳細については、『Cisco Threat Defense for the 2100 Series Using Management Center Quick Start Guide』[英語] を参照してください。

ステップ 2 Management Center によって管理される Firepower 2100 シリーズ デバイスを登録します。

詳細については、「Add Devices to the Management Center」を参照してください。

ステップ 3 Cisco Secure Firewall 移行ツールの最新バージョンを https://software.cisco.com/download/home/286306503/type からダウンロードして実行します。

詳細については、Cisco.com からの Cisco Secure Firewall 移行ツールのダウンロード （3 ページ）を参照してください。

ステップ 4 Cisco Secure Firewall 移行ツールを起動し、接続先パラメータを指定する場合は、Management Center に登録した Firepower 2100 シリーズ デバイスを選択します。

詳細については、Cisco Secure 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。

ステップ 5 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ます。

（注） Cisco Secure Firewall 移行ツールを使用すると、インターフェイスタイプを 脅威に対する防御 インターフェイスタイプにマッピングできます。

詳細については、「PAN ファイアウォール 構成と Threat Defense インターフェイスのマッピング」を参照してください。

ステップ 6 論理インターフェイスをセキュリティゾーンにマッピングするときに、[自動作成（Auto-Create）]をクリックして、Cisco Secure Firewall 移行ツールで新しいセキュリティゾーンを作成できるようにします。既存のセキュリティゾーンを使用するには、手動で論理インターフェイスをセキュリティゾーン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インターフェイスグループ への PAN インターフェイスのマッピング」を参照してください。

ステップ 7 このガイドの手順に従って、移行する構成を順に確認および検証し、構成を Management Center にプッシュします。

ステップ 8 移行後レポートを確認し、手動で他の構成をセットアップして脅威に対する防御に展開し、移行を完了します。

詳細については、「」を参照してください。

ステップ 9 移行の計画時に作成したテスト計画を使用して、Firepower 2100 シリーズ デバイスをテストします。

メンテナンス期間のタスク

始める前に

メンテナンスウィンドウの前に実行する必要があるすべてのタスクが完了していることを確認します。「メンテナンス期間前のタスク （32 ページ）」を参照してください。

ステップ 1 周辺スイッチング インフラストラクチャの Address Resolution Protocol（ARP）キャッシュをクリアします。

ステップ 2 周辺スイッチング インフラストラクチャから Firepower 2100 シリーズ デバイスインターフェイスの IP アドレスに対して基本的な ping テストを実行し、アクセス可能であることを確認します。

ステップ 3 Firepower 2100 シリーズ デバイスインターフェイスの IP アドレスに対するレイヤ 3 ルーティングが必要なデバイスから基本的な ping テストを実行します。

ステップ 4 Firepower 2100 シリーズ デバイスに新しい IP アドレスを割り当て、 に割り当てられた IP アドレスを再利用しない場合は、次の手順を実行します。

1. IP アドレスを参照する静的ルートを更新し、Firepower 2100 シリーズ デバイスの IP アドレスを指すようにします。
2. ルーティングプロトコルを使用している場合は、ネイバーが Firepower 2100 シリーズ デバイスの IP アドレスを予期される接続先のネクストホップとして認識していることを確認します。

ステップ 5 包括的なテスト計画を実行し、 Firepower 2100 デバイスの管理 Management Center 内でログをモニタリングします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。