

# Firewall Migration Manager を使用した Palo Alto Networks ファイアウォールから Cisco Secure Firewall Threat Defense への移行

**最終更新**：2026 年 11 月 17 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/

【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。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. All rights reserved.



# 目 次


第 1 章 **Firewall Migration Manager について** 1

Firewall Migration Manager の概要 1

Firewall Migration Manager の機能 3

Firewall Migration Manager のデフォルトホームページ 8

Palo Alto Networks ファイアウォールから Firewall Threat Defense への移行の仕組み 9

第 2 章 **移行要件** 11

ライセンス要件 11

プラットフォーム要件 11

デバイスの準備状況と要件 12

サポートされるプラットフォームとバージョン 13

Firewall Management Center 要件 13

サポートされている構成 14

第 3 章 **移行前のタスク** 17

ダウンロード： Firewall Migration Manager 17

Palo Alto Networks ファイアウォールからの構成のエクスポート 18

Palo Alto Networks ファイアウォールからの構成ファイルのエクスポート（Panorama の管理対象外） 18

Palo Alto Networks ファイアウォールからの構成ファイルのエクスポート（Panorama の管理対象） 19

第 4 章 **Palo Alto Networks ファイアウォールから Firewall Threat Defense へのワークフロー** 21

Firewall Migration Manager による移行の実行 21

Palo Alto Networks ファイアウォールの構成ファイルのアップロード 22

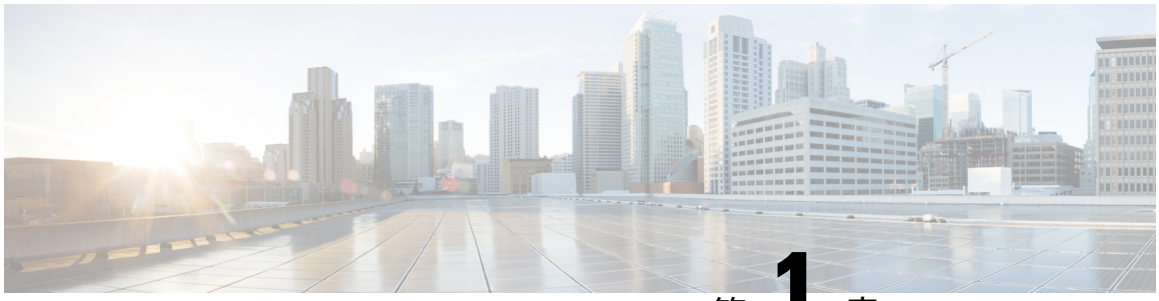
接続先パラメータの指定 23

Palo Alto Networks ファイアウォールの構成と Firewall Threat Defense インターフェイスのマッピング 24

移行構成の確認と検証 25

Firewall Migration Manager 移行前レポートの確認 30

Firewall Migration Manager 移行後レポートの確認 31



第 1 章

# Firewall Migration Manager について


- Firewall Migration Manager の概要 （1 ページ）
- Firewall Migration Manager の機能 （3 ページ）
- Firewall Migration Manager のデフォルトホームページ （8 ページ）
- Palo Alto Networks ファイアウォールから Firewall Threat Defense への移行の仕組み （9 ページ）


## Firewall Migration Manager の概要

Firewall Migration Manager は、サポートされている Palo Alto Networks ファイアウォール構成の Cisco Secure Firewall Threat Defense への移行を自動化するネットワーク セキュリティ アプリケーションです。移行元の構成を解析し、機能をマッピングし、ポリシーを Firewall Management Center にプッシュして、ファイアウォール ソリューションのアップグレードを目指す組織の移行プロセスを効率化します。

### Firewall Migration Manager を選択する理由

ファイアウォールの移行は、計画時には簡単に思えても、多くの場合実行には複雑さが伴います。一般的な課題として、構成の依存関係、大規模なルールセットにおける解析のタイムアウト、予想外に短いカットオーバー期間が挙げられます。多くの組織では、これらのリスクによってセキュリティの最新化の取り組みが遅れています。

Firewall Migration Manager は、これらの課題を克服し、シームレスな移行を実現するために構築された企業向けの製品です。この製品は、Cisco Secure Firewall Threat Defense への移行のあらゆる段階で、予測可能なタイムライン、復元力の高いワークフロー、および明確な可視性を提供することで、お客様とパートナーを支援します。その結果、移行が摩擦の原因ではなく、戦略的な推進力となります。

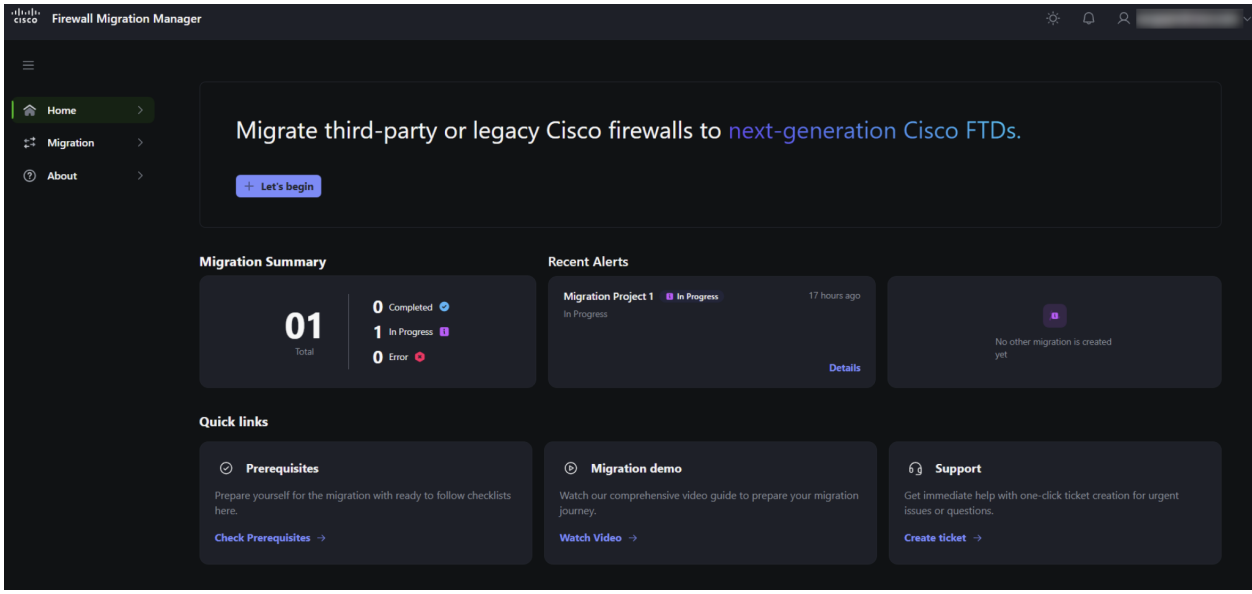
### 主な機能

- **移行効率**：Firewall Migration Manager は、精度と信頼性を維持しつつ、ファイアウォールの移行プロセスを効率化および迅速化します。

- **改良された GUI**：Firewall Migration Manager を使用することで、断片化された手動のワークフローを排除し、代わりにウィザードによるガイド付きのオーケストレーション、視覚的なタスク追跡、並列実行、およびステータスの能動的なモニタリングが可能になります。
- **展開前の検証とテスト**：チームは展開の実行前に移行計画を十分に評価できます。
- **レポートとトレーサビリティの強化**：内容豊富な移行レポートとより明確な監査証跡により、ジョブを実行するエンジニアからシスコのレビュー担当者に至るまで、すべての関係者が必要な可視性を得られます。
- **幅広いプラットフォームに対応**：シスコは、サポート対象となる移行元を継続的に拡張し、より多くのプラットフォームに対応する予定です。これにより、さらに多くのチームを Cisco Secure Firewall Threat Defense に統合できるようになります。

### ダッシュボードの概要

Firewall Migration Manager ダッシュボードは、ネットワークデバイスの移行を追跡およびトラブルシュートするための中央管理インターフェイスです。また、移行プロジェクトの正常性と進行状況を可視化します。




**主な機能エリア**：

- **移行のモニタリング**：[**移行の概要（Migration Summary）**] タイルには、すべての移行タスクのステータス概要がリアルタイムで表示され、完了済み、進行中、およびブロックされたタスクの数を確認できます。
- **問題の識別**：[**最近のアラート（Recent Alerts）**] セクションは問題の診断に役立ちます。失敗した移行タスクにフラグを付け、失敗が発生したステージと原因を正確に特定するとともに、構成シンタックスの問題や接続タイムアウトなど、原因の簡単な説明を提示します。

- **リソースおよびサポートハブ**：[**クイックリンク（Quick links**）] セクションでは、オンボーディングと障害対応に不可欠な、次に挙げるリソースを即座に利用できます。
  - [**前提条件（Prerequisites**）]：チェックリストをレビューし、移行を開始する前にすべての前提条件が満たされていることを確認します。
  - [**移行デモ（Migration demo**）]：移行の全体的な流れを紹介する包括的なビデオを視聴できます。
  - [**サポート（Support**）]：緊急の問題や質問がある場合、ワンクリックでチケットを作成してすぐにサポートを受けられます。

# Firewall Migration Manager の機能

次の表に、Firewall Migration Manager の新機能の概要を示します。

| リリース | 機能 | 詳細 |
|---|---|---|
| 10.0.1 | Palo Alto Networks ファイアウォールから Firewall Threat Defense への移行のサポート。 | Firewall Migration Manager は、 Palo Alto Networks ファイアウォール構成の Firewall Threat Defense デバイスへの移行をサポートしています。 |
| | 移行前および移行後レポートの強化。 | Firewall Migration Manager では、ユーザー体験を向上させ、移行された構成の分析を容易にするために、移行前および移行後レポートの機能が強化されています。 |
| | レイヤ 2 インターフェイスからレイヤ 3 インターフェイスへの移行のサポート。 | Firewall Migration Manager は、互換性のあるインターフェイス構成を Firewall Threat Defense デバイス上のルーテッドインターフェイスに変換することで、レイヤ 2 インターフェイスからレイヤ 3インターフェイスへの移行をサポートしています。 |
| | VRF 移行のサポート | Firewall Migration Manager は VRF の移行をサポートしています。 |
| | BGP 移行のサポート | Firewall Migration Manager は BGP の移行をサポートしています。 |
| | ルーティングテーブルに基づく NAT ゾーンのマッピング | Firewall Migration Manager はルーティングテーブルを使用して、移行中に NAT ゾーンのマッピングを導出します。 |
| | インターフェイスにまたがる複数の IP アドレスの処理 | 移行中、 Palo Alto Networks ファイアウォール インターフェイスに複数の IP アドレスがある場合、Firewall Migration Manager ウィザードによって、そのインターフェイスの IP アドレスを 1 つ選択するよう求められます。 |
| | Panorama からのポリシー階層の移行 | Firewall Migration Manager は Palo Alto Networks ファイアウォールのポリシー階層を、Firewall Threat Defense デバイス内のネストされたアクセス コントロール ポリシーとして移行します。 |
| | 外部ダイナミックリストの移行 | Firewall Migration Manager は外部ダイナミックリストの移行をサポートしています。 |

| リリース | 機能 | 詳細 |
| --- | --- | --- |
| | アクセスポリシールール内のアプリケーションの一括追加のサポート。 | Firewall Migration Manager は、移行中におけるアクセスポリシールール内のアプリケーションの一括追加をサポートしています。これにより、移行後にアプリケーションベースのアクセスポリシーを更新するために必要な労力が削減されます。 |

| リリース | 機能 | 詳細 |
|---|---|---|
| 10.0.0 | Cisco ASA から Firewall Threat Defense への移行のサポート。 | Firewall Migration Manager は、Cisco ASA 構成の Firewall Threat Defense デバイスへの移行をサポートしています。 |
| | ターゲットバージョンの自動検出 | Firewall Management Center および Firewall Threat Defense のターゲットデバイスのバージョンと情報を自動的に識別し、構成の整合性を正確に維持します。 |
| | 自動化された移行ワークフロー | Firewall Migration Manager では、既存の環境から Firewall Threat Defense デバイスへのセキュリティポリシー、ネットワークオブジェクト、およびデバイス構成の自動移行により、手作業が削減されます。 |
| | 中央管理型ダッシュボードのサポート | |

| リリース | 機能 | 詳細 |
| --- | --- | --- |
| | | Firewall Migration Manager ダッシュボードは、移行プロセスを合理化するための一元的かつ直感的なインターフェイスを提供します。可視性と業務効率の向上を目的として設計されたこのダッシュボードには、次の機能が用意されています。<br>• 移行の概要：すべての移行プロジェクトのステータスをリアルタイムでモニターし、完了済み、進行中、およびエラー状態の移行の件数を確認できます。<br>• 能動的なアラート：最新の移行アラートとプロジェクトの詳細を即座に確認できるため、常に最新情報を把握できます。<br>• クイックリンク：移行前チェックリスト、包括的なビデオガイド、ワンクリックでのサポートチケット作成など、重要なリソースにダッシュボードから直接アクセスできます。<br>この一元化されたアプローチにより、サードパーティ製のファイアウォールやレガシーファイアウォールから次世代 Cisco ファイアウォール プラットフォームへの移行が簡単になり、より合理化された整然とした移行プロセスが実現します。 |
| | GUI の改善 | Firewall Migration Manager では、ウィザード形式のオーケストレーション プラットフォームに移行タスクを統合する、改善されたグラフィカル ユーザー インターフェイスが提供されます。このインターフェイスは、視覚的な明瞭さ、並列タスク処理、およびステータスの能動的なモニタリングを重視しています。 |
| | インテリジェントな解析 | |

| リリース | 機能 | 詳細 |
|---|---|---|
| | | この機能では構成を自動的にスキャンして、サポートされていない項目や参照されていない項目を識別します。これにより、注意が必要な項目のみに手動のクリーンアップ作業を集中できるため、時間を節約できます。<br>このツールは、企業規模の構成を効率的に解析し、数千件のルールを数分で処理します。 |
| | 移行履歴の保持 | さまざまなプロジェクト間で移行履歴が保持されるため、以前の移行を追跡して再確認できます。 |
| | 並列移行のサポート | 効率を向上させるために、この機能によって最大 10 件の移行プロセスを同時に実行し、ネットワーク移行を一括処理できます。 |
| | 一時停止と再開 | Firewall Migration Manager ではデータを喪失することなく、任意の時点でタスクの一時停止と再開を行えます。[**進行中（In-Progress**）] には、ホームページの [**最近のアラート（Recent Alerts**）] タイルから、またはメインメニューの [**移行（Migration**）] をクリックすることでアクセスできます。 |

# Firewall Migration Manager のデフォルトホームページ

ログイン後、Firewall Migration Manager のホームページが表示されます。

ホームページには、次の主なエリアがあります。

- [**移行の概要（Migration summary**）]：実行済み、完了済み、進行中、およびエラーにより失敗した移行の合計数を表示します。
- [**最近のアラート（Recent Alerts**）]：移行タスクのステータスの更新をリアルタイムで表示します。タイルには、移行プロジェクト名、移行ステータス、タイムスタンプ、および現在のフェーズまたは必要なアクションの簡単な説明が表示されます。
- [**クイックリンク（Quick links**）]：
  - [**前提条件（Prerequisites**）]：すぐに実行できるチェックリストを使用して、移行に向けた準備を行います。

- [**移行デモ（Migration demo**）]：最新リリースで導入された重要な機能と機能強化を紹介するデモビデオへのリンクを提供します。
- [**サポート（Support**）]：[**チケットの作成（Create ticket**）] リンクを介したワンクリックのチケット作成プロセスを使用して、即座にサポートを受けられます。

表 *1 : Migration Status*

| ステータス | 説明 | 操作 |
|---|---|---|
| 進行中（In-progress） | 移行タスクは現在アクティブです。表示される説明は、実行中の特定の手順を示します。 | ユーザーは進行状況をモニターし、移行の完了を待つことができます。<br>[**詳細（Details**）] リンクをクリックすると、移行ページに移動します。 |
| 完了 | 移行タスクが正常に完了しました。 | なし |
| [エラー（Error）] | 移行タスクが失敗しました。 | [**詳細（Details**）] リンクをクリックして、特定のログまたはエラーを引き起こした構成の問題を調査します。 |

# Palo Alto Networks ファイアウォールから Firewall Threat Defense への移行の仕組み

### process_summary

Firewall Migration Manager は、 Palo Alto Networks ファイアウォールの構成を正確に解析および検証し、Firewall Threat Defense に正しく展開することで、 Palo Alto Networks ファイアウォールの構成の移行を自動化します。

### process_workflow

次の各段階は、 Palo Alto Networks ファイアウォールから Firewall Threat Defense への移行の仕組みについて説明しています。

1. **構成の収集と解析**：Firewall Migration Manager は Palo Alto Networks ファイアウォールデバイスから情報を収集し、その構成を解析します。
2. **Palo Alto Networks ファイアウォールの構成、インターフェイス、セキュリティゾーンの、Firewall Threat Defense へのマッピング**：Firewall Migration Manager によって、インター

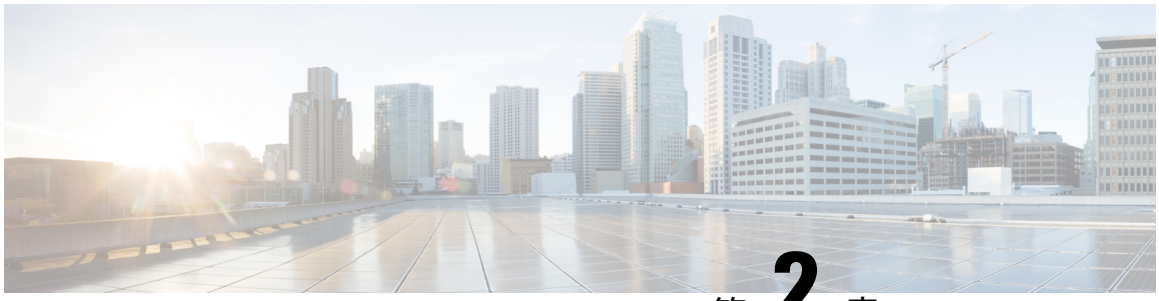
フェイス、セキュリティゾーン、およびインターフェイスグループが Threat Defense デバイスにマッピングされます。マッピングを確認して検証してください。

3. **移行前レポートの確認**：サポートされていない構成、無視される構成、および誤った構成を特定するレポートが Firewall Migration Manager によって生成されます。これにはブロックエラーとその理由が含まれます。

4. **解析エラーの修復**：移行前に解決できるよう、Firewall Migration Manager によって解析エラーが強調表示されます。

5. **検証済みの構成のプッシュ**：Firewall Migration Manager は、検証済みの構成を Firewall Management Center にプッシュし、その構成を接続先デバイスに移行します。

6. **移行後レポートの確認**：完全に移行された構成、部分的に移行された構成、または移行されなかった構成を含む詳細レポートが Firewall Migration Manager によって生成されます。修正内容の一覧を表示し、競合を回避するために行われた変更を特定し、スキップされた項目を示すとともに、移行の失敗や手動対応が必要な事項を文書化します。



第 2 章

# 移行要件


- ライセンス要件 （11 ページ）
- プラットフォーム要件 （11 ページ）
- デバイスの準備状況と要件 （12 ページ）
- サポートされるプラットフォームとバージョン （13 ページ）
- Firewall Management Center 要件 （13 ページ）
- サポートされている構成 （14 ページ）


## ライセンス要件

Firewall Migration Manager は無料ですが、デバイスの登録とポリシーの展開をサポートするために、Management Center に Firewall Threat Defense 機能の適切なライセンスが付与されていることを確認してください。

Firewall Migration Manager および Firewall Management Center を使用するには、次のライセンス要件を満たす必要があります。

- Firewall Management Center に、使用予定の Firewall Threat Defense 機能の適切なライセンスが付与されている必要があります。
- Firewall Threat Defense デバイスを登録してそれらのデバイスにポリシーを展開するには、適切なライセンスが必要です。

詳細については、『*Cisco Secure Firewall Management Center* アドミニストレーション ガイド』の「ライセンス」セクションを参照してください。

## プラットフォーム要件

Firewall Migration Manager を適切に機能させるには、特定のプラットフォームと構成の設定が必要です。サポートされている環境と必要な設定は次のとおりです。

- **システム要件**：
  - Microsoft Windows 11（64 ビット）以降

- MacOS 14 以降

Cisco.com に接続するためのインターネット接続が必要です。

（注） インターネットにアクセスできないエアギャップ環境や隔離された環境で移行を実行する場合は、Cisco TAC に連絡してエアギャップ用の Firewall Migration Manager インストーラを入手してください。

- **電源管理（Windows）**：：移行中は、[**電源とスリープ（Power & Sleep）**] の [**スリープ（Sleep）**] 設定を [**PC をスリープ状態にしない（Never put the PC to sleep）**] に設定して、中断を防ぎます。
- **電源管理（macOS）**：移行プロセス全体を通じてコンピュータとハードディスクがアクティブな状態を維持するように、[**省エネルギー（Energy Saver）**] 設定を構成します。

# デバイスの準備状況と要件

Firewall Management Center に移行する場合、ターゲットの Firewall Threat Defense デバイスが追加されている必要はありません。Firewall Threat Defense デバイスへの今後の展開に備えて、ポリシーを Firewall Management Center に移行できます。

Firewall Threat Defense デバイスが Firewall Management Center に追加されている場合は、移行を開始する前に、ターゲットの Firewall Threat Defense デバイスが次の条件を満たしていることを確認します。

- **登録**：ターゲットの Firewall Threat Defense デバイスが Firewall Management Center に登録されている必要があります。
- **構成の状態**：
  - 高可用性（HA）構成をサポートしている。
  - スタンドアロンまたはコンテナインスタンスをサポートしている。
  - **制限**：ターゲットの Firewall Threat Defense デバイスが、デバイスクラスターの一部ではない必要があります。
- **インターフェイスのマッピング**：
  - コンテナインスタンスを使用する場合、Firewall Threat Defense デバイスの最小インターフェイス数（物理、サブインターフェイス、およびポートチャネル）が、移行元の Palo Alto Networks ファイアウォールデバイスと同じかそれを上回っている必要があります。

- Firewall Migration Manager は、物理インターフェイスからポートチャネル インターフェイスへのマッピングなど、異なるインターフェイスタイプ間のマッピングをサポートしています。

（注） Firewall Migration Manager は、ターゲットのマルチインスタンス Firewall Threat Defense デバイスのサブインターフェイスを作成しません。ターゲットデバイスで事前に構成する必要があります。

警告 移行のプッシュ中に、Firewall Migration Manager は既存のデバイス固有の構成（ルート、インターフェイスなど）を自動的に消去して上書きします。意図しないデータ損失を避けるために、移行前にデバイスを手動でクリーンアップすることを強く推奨します。

# サポートされるプラットフォームとバージョン

移行を正常に完了させるには、ハードウェアとソフトウェアのバージョンが次の仕様に準拠している必要があります。

| コンポーネント | サポートされている最小バージョン |
|---|---|
| 移行元 PAN-OS | 6.1.x 以降 |
| Firewall Management Center | 6.2.3.3 以降 |
| ターゲット Firewall Threat Defense | 6.5 以降 |

### サポートされるターゲットデバイス

- **物理デバイス**：Firepower 1000、2100、4100、9300（SM モジュール）、および Secure Firewall 220、1200、3100、3200、4200、6100 シリーズ
- **仮想デバイス**：VMware（ESXi/vSphere）およびクラウド（Azure/AWS）上の Threat Defense

# Firewall Management Center 要件

Firewall Migration Manager はオンプレミスの Firewall Management Center をサポートしています。

### オンプレミス Firewall Management Center の前提条件

- **スマートライセンス**：移行するすべての機能のスマートライセンスをインストールします。
- **REST API**：REST API が有効になっている（[システム（System）]（⚙） > **[設定（Configuration）] > [REST APIの優先設定（REST API Preferences）]**）。

（注） REST API を有効にするには、Firewall Management Center の管理者ユーザーロールが必要です。Firewall Management Center のユーザーロールの詳細については、「ユーザーロール」を参照してください。

# サポートされている構成

Firewall Migration Manager は、Firewall Threat Defense デバイスとの機能パリティに基づいて Palo Alto Networks ファイアウォールの構成を分類します。

### 完全にサポートされている構成

- ネットワークオブジェクト、グループ、およびゾーン（L2/L3/仮想ワイヤ）
- サービス オブジェクト グループ
- IPv4 および IPv6 FQDN オブジェクト、グループ、およびスタティックルート
- アクセスルール、ID ポリシー、NAT ルール、NAT ゾーン
- インターフェイス:
  - インターフェイスタイプ：物理、サブインターフェイス（VLANマッピング済み）、ループバック、集約
  - 移行では、インターフェイスにまたがる複数の IP アドレスを処理できます。
  - レイヤ 2 インターフェイスからレイヤ 3 インターフェイスへの移行
- VRF および BGP 移行のサポート
- Panorama からのポリシー階層の移行
- 外部ダイナミックリストの移行
- アクセスルールへのアプリケーションの一括追加

### 部分的にサポートされている構成

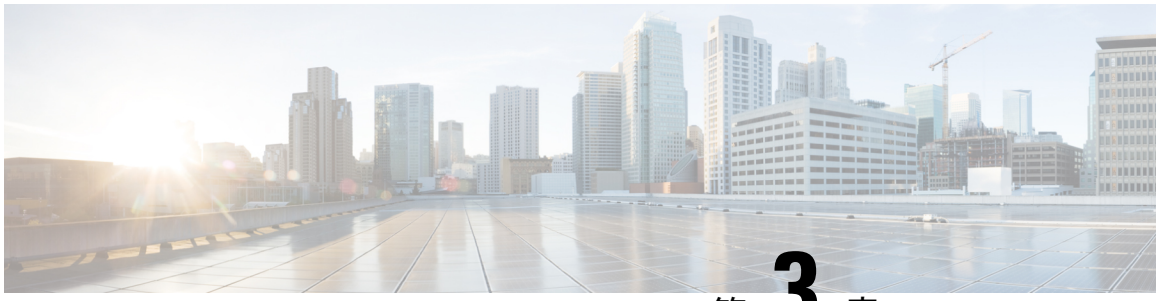
- **アクセスコントロールルール**：高度なプロファイルオプションなしで移行されます（移行後に手動で構成）。
- **サービスグループ**：TCP、UDP、SCTP を含む混合プロトコルグループ（SCTP は削除されます）。
- **オブジェクトグループ**：有効なオブジェクトと無効なオブジェクトが混在（無効なオブジェクトは除去されます）。
- **ダイナミックオブジェクト**：Firewall Migration Manager では、オブジェクトグループはサポートされません。
- **地理位置情報ベースのルール**

### サポートされていない設定

- 時間ベースの ACL とワイルドカード FQDN
- IPv6 NAT
- 変換後の送信元/接続先に FQDN オブジェクトが含まれる NAT ルール（特定のシナリオ）
- OSPF および EIGRP



（注） （サポートされていないものを含む）すべてのポリシーが Firewall Management Center に移行されます。サポートされていないポリシーは、手動で確認して修復できるように**無効化された**状態に設定されます。



第 3 章

# 移行前のタスク


- ダウンロード： Firewall Migration Manager （17 ページ）
- Palo Alto Networks ファイアウォールからの構成のエクスポート （18 ページ）


# ダウンロード： Firewall Migration Manager

**Before you begin**

- ローカルマシンに Firewall Migration Manager をインストールするための管理権限があることを確認します。
- Cisco.com へのインターネット接続が可能な Windows 11 64 ビットマシンか、MacOS バージョン 14 以降のマシンが必要です。

（注） インターネットにアクセスできないエアギャップ環境や隔離された環境で移行を実行する場合は、Cisco TAC に連絡してエアギャップ用の Firewall Migration Manager インストーラを入手してください。

手順

**ステップ 1** Cisco Software Download Center にアクセスし、Firewall Migration Manager をクリックします。

**ステップ 2** Firewall Migration Manager の最新バージョンをダウンロードします。

Windows または MacOS マシン用の Firewall Migration Manager の実行ファイルをダウンロードしたことを確認してください。

# 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 Networks ファイアウォールからの構成ファイルのエクスポート（Panorama の管理対象外）

手順

**ステップ 1** [デバイス（**Device**）> セットアップ（**Setup**）> 操作（**Operations**）] の順に選択し、[命名済みの構成の保存（**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** **[デバイス（Device）] > [セットアップ（Setup）] > [操作（Operations）]** の順に選択し、[命名済みの構成のエクスポート（**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** 実行中の構成を含む XML ファイル <*file_name.xml*> 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 Firewall Migration Manager にアップロードし、構成を移行することができます。

**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。これらの手順を実行しないと、Firewall Migration Manager による移行中に宛先ゾーンがマッピングされず、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 Networks ファイアウォールからの構成ファイルのエクスポート（Panorama の管理対象）

デバイスが Panorama によって管理されている場合は、ゲートウェイから構成を抽出する必要があります。Panorama 構成をゲートウェイと統合し、構成を抽出します。

**Before you begin**

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

手順

**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**）] の順に選択します。

**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。

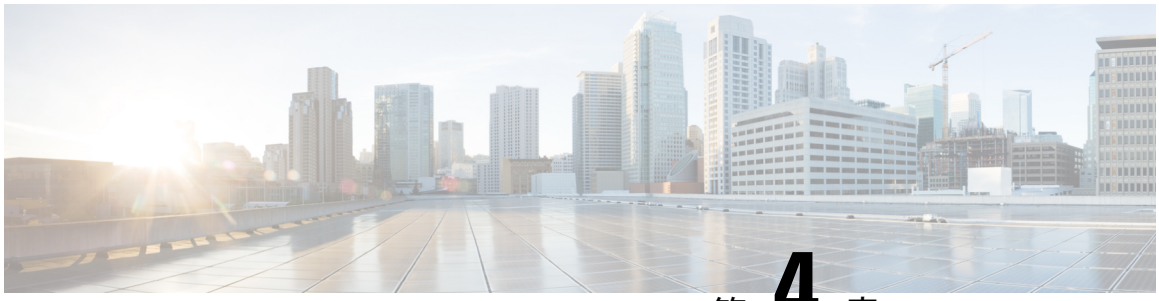
**ステップ 4** ファイルを解凍して展開し、パス *\opt\pancfg\mgmt\saved-configs* に移動して、*merged-running-config.xml* ファイルを取得します。

**ステップ 5** （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。これらの手順を実行しないと、Firewall Migration Manager による移行中に宛先ゾーンがマッピングされず、移行レポートに含まれます。

（注） 階層型ポリシーを持つ Panorama 管理対象の Palo Alto Networks ファイアウォールの場合、Panorama 構成バックアップをエクスポートし、名前を `panorama_running-config.xml` に変更して、ゲートウェイ構成および `route.txt` ファイルとともに zip 圧縮します。



第 4 章

# Palo Alto Networks ファイアウォールから Firewall Threat Defense へのワークフロー


- Firewall Migration Manager による移行の実行 （21 ページ）
- Palo Alto Networks ファイアウォールの構成ファイルのアップロード （22 ページ）
- 接続先パラメータの指定 （23 ページ）
- Palo Alto Networks ファイアウォールの構成と Firewall Threat Defense インターフェイスのマッピング （24 ページ）
- 移行構成の確認と検証 （25 ページ）
- Firewall Migration Manager 移行前レポートの確認 （30 ページ）
- Firewall Migration Manager 移行後レポートの確認 （31 ページ）


## Firewall Migration Manager による移行の実行

移行を実行し、デスクトップ版の Firewall Migration Manager を使用して Palo Alto Networks ファイアウォールの構成をターゲットの Firewall Threat Defense に転送するワークフローを開始します。

この手順は、デスクトップ版の Firewall Migration Manager を使用している場合にのみ適用されます。

**Before you begin**

- Cisco.com から Firewall Migration Manager をダウンロードします。
- 移行のサポート対象となるターゲット Management Center セクションに記載されている要件を確認して検証します。
- 大規模な構成ファイルの移行を計画している場合は、移行の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** Firewall Migration Manager GUI の左側のペインで、[**移行（Migration**）] をクリックします。

**ステップ 2** ウィンドウの右上にある [**新しい移行を開始（Start new migration**）] をクリックします。

移行ワークフローが開始します。

または、ホームページで [**開始しましょう（Lets Begin**）] をクリックして移行ワークフローを開始することもできます。

**ステップ 3** [**移行元を選択（Select source**）] ドロップダウンリストから [**Palo Alto Networks**] を選択します。

### 次のタスク

移行する Palo Alto Networks ファイアウォールの構成をアップロードします。「Palo Alto Networks ファイアウォールからの構成のエクスポート （18 ページ）」を参照してください。

# Palo Alto Networks ファイアウォールの構成ファイルのアップロード

（注） 手動でコード化され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。

移行元の構成ファイルを手動でアップロードするには、次の手順を実行します。

**Before you begin**

移行元の Palo Alto Networks ファイアウォールデバイスから、構成ファイルを .cfg または .txt としてエクスポートします。

手順

**ステップ 1** [**構成の抽出方式の選択（Select configuration extraction method**）] エリアで、[**手動アップロード（Manual Upload**）] オプションボタンを選択します。

**ステップ 2** アップロードを開始するには、次の 2 つのオプションがあります。

- 破線のボックスエリア内をクリックし、アップロードする構成ファイルを参照して選択します。
- 破線で囲まれたエリアにファイルをドラッグアンドドロップします。

**ステップ 3** [続行（Proceed）] をクリックします。

Palo Alto Networks ファイアウォールの構成ファイルがアップロードされ、移行処理の準備ができました。

### 次のタスク

構成の移行先とするターゲットデバイスの詳細を入力します。「接続先パラメータの指定（23 ページ）」を参照してください。

# 接続先パラメータの指定

**Before you begin**

- Firewall Management Center の IP アドレスを取得します。
- （オプション）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、ターゲットデバイスを Firewall 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 Firewall Management Center でポリシーを作成することを強くお勧めします。Firewall Migration Manager は接続されている Firewall 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** [**ターゲット情報（Target information）**] 画面で、次のパラメータを設定します。

a) ドロップダウンリストから [**Firewall Management Center**] を選択します。

b) Firewall Management Center 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。

ターゲット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デバイスにのみ移行できます。

c) [接続（Connect）] をクリックします。

**ステップ 2** [**ターゲットFMCへのログイン（Login to target FMC）**] ダイアログボックスで、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 Migration Manager が Firewall Management Center にログインし、その Firewall Management Center によって管理されている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** [**デバイス選択（Device Selection）**] セクションでは、移行先とするデバイスを選択できます。また、デバイスがない場合は、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 Firewall Management Center に移行できます。

**ステップ 4** [**FTD の選択（Select FTD**）] ドロップダウンリストをクリックし、構成の移行先とするデバイスを選択します。

選択した Firewall Management Center ドメイン内のデバイスは、[**IP アドレス（IP Address**）]、[**デバイスモデル（Device Model**）]、[**名前（Name**）]、[**モード（Mode**）]（ルーテッドまたはトランスペアレント）別に表示されます。

（注） 少なくとも、選択するネイティブデバイスには、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、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。デバイスは、 Palo Alto Networks ファイアウォールの構成と同じファイアウォールモードで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。

**ステップ 5** [次へ（Next）] をクリックします。

# Palo Alto Networks ファイアウォールの構成と Firewall Threat Defense インターフェイスのマッピング

Palo Alto Networks ファイアウォールの構成を Firewall Threat Defense に移行する場合、ターゲットデバイスに Palo Alto Networks ファイアウォールの構成と同じかそれを上回る数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存在していることが不可欠です。インターフェイス名が一致している必要はないため、柔軟にマッピングを行えます。Firewall Migration Manager はインターフェイスのリストを取得し、インターフェイス ID に基づいてデフォルトのマッピングを提供します。たとえば、「管理専用」インターフェイスは自動的にマッピングされ、変更できません。

**Before you begin**

Firewall Management Center に接続し、接続先として Firewall Threat Defense を選択していることを確認します。詳細については、接続先パラメータの指定（23ページ）を参照してください。

手順

**ステップ 1** [**マッピング（Mappings**）] 画面で、両方の Palo Alto Networks ファイアウォール構成とターゲット Firewall Threat Defense デバイスのインターフェイスリストを確認します。

**ステップ 2** インターフェイスのマッピングを変更する場合は、[**FTDインターフェイス（FTD Interface**）] 列のドロップダウンリストをクリックし、その Palo Alto Networks ファイアウォール 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。

（注）
- 管理専用インターフェイスは自動的にマッピングされ、変更できません。
- インターフェイスが割り当てられると、再度選択することはできません。
- 物理インターフェイス、ポートチャネル、およびサブインターフェイスの手動マッピングは、ターゲットデバイスがマルチインスタンスモードで動作している場合にのみ必要です。

**ステップ 3** [**自動マッピング（Auto Map）**] ボタンを使用して、 Palo Alto Networks ファイアウォールのファイアウォール インターフェイスを自動的にマッピングできます。

必要に応じて、マッピングを確認、検証、および編集します。

# 移行構成の確認と検証

移行された Palo Alto Networks ファイアウォールの構成を確認および検証し、精度を確認して競合を解決してから Firewall Management Center にプッシュします。

移行された Palo Alto Networks ファイアウォールの構成を Firewall Management Center にプッシュする前に、構成を慎重に確認し、競合をすべて解決します。Firewall Migration Manager は問題を特定し、それらを直接修正できるようにします。また展開前に、IPS ポリシーやファイルポリシーなどのポリシーをアクセス制御ルールに関連付けたり、オブジェクトに変更を加えたり、構成を最適化したりすることもできます。

（注） [**確認（Review**）] ページで Firewall Migration Manager 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。移行を再開するには、メインメニューで [**移行（Migration**）] をクリックしてから、[**移行プロジェクト（Migration Projects**）] ウィンドウで移行プロジェクト名を選択します。

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。

### 手順

**ステップ 1** Firewall Migration Manager の左側のペインで、[**確認（Review**）] をクリックします。

**ステップ 2** [**移行前レポートのダウンロード（Download Pre-Migration Report**）] をクリックして、移行前レポートを確認します。詳細については、移行前レポートの確認を参照してください。

**ステップ 3** [**共有構成（Shared configurations**）] エリアで [**アクセス制御（Access Control**）] ハイパーリンクをクリックし、次の手順を実行します。

1. 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。
2. 1つまたは複数のアクセス制御リストポリシーを移行しない場合は、各ポリシーの横にあるチェックボックスをオンにして、該当する行を選択します。次に、[**一括アクション（Bulk actions**）] ドロップダウンメニューで [**移行しない（Do not migrate**）] 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。
3. [**ルールの編集（Edit rule**）] ダイアログボックスで、既存のデータを更新するか、新しいデータを追加します。

   オブジェクトを送信元または接続先に追加するには、次の手順を実行します。

   1. 左側のペインでオブジェクトの横にあるチェックボックスをオンにします。
   2. [選択した送信元（Selected Sources）] または [選択した接続先およびアプリケーション（Selected Destination and Applications）] 列で、[送信元を追加（Add Source）] または [接続先を追加（Add Destination）] ボタンをクリックし、オブジェクトをそれぞれの場所に移動します。
   3. [削除（Delete）] アイコンをクリックすると、送信元または接続先から既存のオブジェクトを削除することもできます。

   （注） 該当しないルールは、テーブルでグレーアウトされます。
4. Firewall Management Center ファイルポリシーを 1 つまたは複数のアクセス コントロール ポリシーに適用する場合は、該当する行のチェック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**）] の順に選択します。
5. [**ファイルポリシー（File Policy**）] ダイアログボックスで、該当する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。

6. Firewall Management Center IPS ポリシーを 1 つまたは複数のアクセス コントロール ポリシーに適用する場合は、該当する行のチェックボックスをオンにし、[**アクション（Actions**）] > [**IPSポリシー（IPS Policy**）] の順に選択します。

   [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。

7. ロギングが有効になっているアクセス制御ルールのロギングオプションを変更する場合は、該当する行のチェック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**）] ダイアログボックスでは、接続の開始時、終了時、またはその両方における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（Event Viewer**）]、[**Syslog**]、またはその両方に送信するように選択する必要があります。接続イベントを syslog サーバーに送信するように選択した場合は、Firewall 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。

8. [アクセス制御（Access Control）] テーブル内の移行されたアクセス制御ルールのアクションを変更する場合は、該当する行のチェック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**）] の順に選択します。

   [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。

**ステップ 4** 次のタブをクリックし、構成項目を確認します。

- インターフェイス
- ルート（静的、BGP）
- アクセス コントロール
- NAT
- オブジェクト（ネットワークオブジェクト、ユーザーオブジェクト、ダイナミックオブジェクト、セキュリティ インテリジェンス フィード、ポートオブジェクト、URL オブジェクト、ダイナミック ルート オブジェクト、および VLAN オブジェクト）
- サイト間 VPN
- リモート アクセス 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。

アクセスリストオブジェクトには、BGP およびリモートアクセス VPN で使用される標準 ACL と拡張 ACL が表示されます。

1 つまたは複数の NAT ルールもしくはルートインターフェイスを移行しない場合は、該当する行のチェックボックスをオンにし、[**アクション（Actions**）]>[**移行しない（Do not migrate**）] の順に選択してから、[**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 5** （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 6** [**ダイナミックルートオブジェクト（Dynamic-Route objects**）] セクションで、移行されるすべてのサポート対象オブジェクトを確認します。

**ステップ 7** 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）] エリアからルートを表示し、移行しないルートを選択できます。

**ステップ 8** [サイト間VPNトンネル（Site-to-Site VPN Tunnels）] セクションに、送信元ファイアウォール設定からの VPN トンネルが一覧表示されます。各行の [送信元インターフェイス（Source Interface）]、[VPNタイプ（VPN Type）]、[IKEv1] および [IKEv2] の設定などの VPN トンネルデータを確認し、すべての行に事前共有キーの値を指定していることを確認します。

**ステップ 9** [**リモートアクセスVPN（Remote Access VPN**）] セクションで、 Palo Alto Networks ファイアウォールから Firewall Management Center に移行される、リモートアクセス VPN に対応するすべてのオブジェクトを確認します。

- [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には、対応するエントリを選択し、**[アクション（Actions）]** > **[名前の変更（Rename）]** の順に選択します。
- [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またはSecure Clientパッケージ（AnyConnect or Secure Client packages**）]：AnyConnect または Secure Client パッケージ、および必要なトラストポイント証明書が Firewall Management Center にあることを確認します。
- [**アドレスプール（Address Pool**）]：ここに表示されるすべての IPv4 プールと IPv6 プールを確認します。

- [**グループポリシー（Group-Policy**）]：このエリアから、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します。このエリアには、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を含むグループポリシー、およびプロファイルを含まない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）] 領域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**）]：ここに表示されるすべての接続プロファイル/トンネルグループを確認します。
- [**トラストポイント（Trustpoints**）]： Palo Alto Networks ファイアウォールから Firewall Management Center 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部であり、リモートアクセス VPN の移行を正常に完了させる上で必須です。[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、移行を続行します。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 証明書のアップロードはオプションです。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移行元の Palo Alto Networks ファイアウォールで使用可能な場合は、[**SAMLのオーバーライド（Override SAML**）] で選択できます。

**ステップ 10** （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 11** 移行に関する問題があれば、エラーの説明とともに [**アクション（Actions**）] エリアに表示されます。問題を解決するには [**修復（Remediate**）] をクリックします。

たとえば、既存の Firewall 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求められる場合があります。問題のある行を選択し、[**アクション（Actions**）> **サフィックスの追加（Add suffix**）] をクリックしてデフォルトのサフィックスを追加します。それ以外の場合は、手動で独自のサフィックスに置き換えることができます。

（注） エラーが解決されると、各エラーの横にチェックマークが表示されます。移行を続行する前に、すべての問題が解決されたことを確認してください。

**ステップ 12** 確認が完了したら [**検証（Validate**）] をクリックし、画面下部のチェックボックスをオンにして移行を確認してから、[**移行の開始（Begin Migration**）] をクリックします。

移行の進行中は、このウィンドウを閉じてもかまいません。移行ステータスが変更されると、通知が届きます。メインメニューで [**移行（Migration**）] を選択し、移行プロジェクト名をクリックすると、ワークフローを再開できます。

**ステップ 13** [次へ（Next）] をクリックします。

移行が正常に完了すると、移行後レポートへのリンクを含む概要が画面に表示されます。

**ステップ 14** [**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。

Firewall Migration Manager と同じ場所にある Resources フォルダにも、移行後レポートのコピーが保存されます。

**ステップ 15** 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。

### 次のタスク

移行後レポートの確認。

# Firewall Migration Manager 移行前レポートの確認

このレポートには、特定されたエラー、参照されていないオブジェクト、無視される構成行などの主要な側面を含む、移行プロセスの詳細な概要が表示されます。一部のルールは、完全には移行されない可能性があるため、このレポートをあらかじめ十分に理解することを推奨します。その結果、元の設定に影響が生じたり、許可された通信が制限されたり、意図しない通信が許可されたりする可能性があります。通信管理とシステムパフォーマンスが移行後も最適な状態を保てるように、Firewall Management Center でルールとポリシーを調整することを強く推奨します。

### 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。

（注） Firewall Migration Manager と同じ場所にある `Resources` フォルダにも、**移行前レポート**のコピーが保存されます。

**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、移行を失敗させる可能性があ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。

- [**全体的な概要（Overall Summary**）]： Palo Alto Networks ファイアウォールでサポートされ、Firewall Management Center に正常に移行できる構成要素の概要。

  ライブ Palo Alto Networks ファイアウォールに接続している場合、サマリーには、ヒットカウント情報、 Palo Alto Networks ファイアウォールのルールが検出された回数、およびそのタイムスタンプ情報が含まれます。

- [**サポートされていない構成（Unsupported Configuration**）]：このセクションには、Firewall Migration Manager によって移行されない Palo Alto Networks ファイアウォールの構成要素の詳細が表示されます。各項目を確認し、必要に応じて移行前または移行後に同等の構成を手動で設定します。対処しない場合、サポートされていないルールによって元の構成が変更されたり、承認済みの通信が制限されたり、不要な通信が許可されたりする可能性があります。
- [**無視される構成（Ignored Configuration**）]：このセクションには、Firewall Management Center でサポートされていないか、ターゲットデバイスに無関係なために Firewall Migration Manager で解析されない Palo Alto Networks ファイアウォールの構成要素の詳細が表示されます。これらの行を確認し、各機能が Firewall Management Center でサポートされているかどうかを確かめます。必要に応じて、Firewall Management Center でこれらの機能を手動で構成します。
- [**参照されていない構成（Unreferenced Configuration**）]：移行元の構成で定義されているものの、アクセスグループ、プレフィックスリスト、VPN、またはポリシーで使用されていない Palo Alto Networks ファイアウォールの構成要素の詳細を表示します。これらの項目は移行されません。各項目を確認して、移行元の構成から削除するか、ターゲットデバイスで手動で構成するかを判断します。

Firewall Management Center および Firewall Threat Defense でサポートされている機能の詳細については、『*Cisco Secure Firewall Management Center デバイス構成ガイド*』を参照してください。

# Firewall Migration Manager 移行後レポートの確認

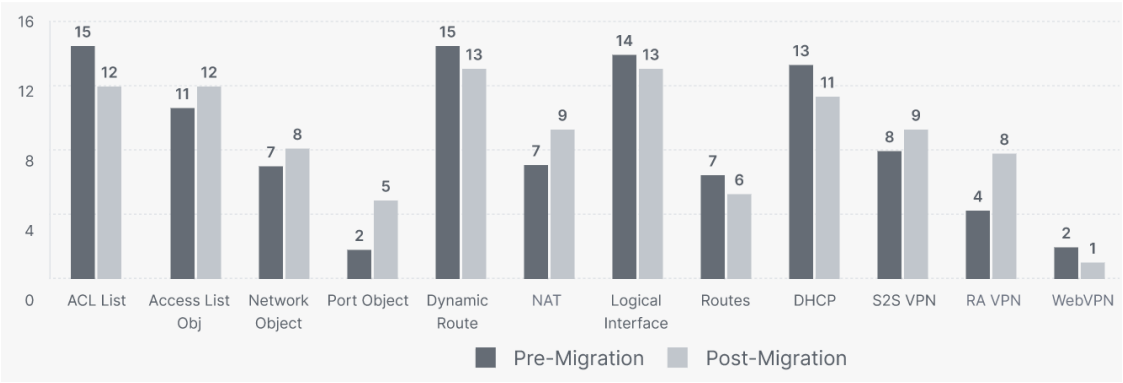
移行後レポートには、移行用に選択された移行元デバイスとターゲットデバイスに関する詳細が記載されています。選択したポリシー、インターフェイスとゾーンのマッピング、さまざまなカテゴリの ACL ルール、ACL の最適化、および構成ファイルに対して実行された最適化の全体像に関する情報が含まれます。また、部分的に移行された構成や、移行中に発生したエラーに関する詳細も記載されています。このレポートは、これらのエラーを解決するためのガイダンスも提供します。

**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、 Palo Alto Networks ファイアウォールの構成がどのように移行されたかを把握します。

- **レポートの概要**
  - [**サマリー概要（Summary Overview**）]：移行前と移行後の状態数の差異を示す比較グラフを表示します。




- [**デバイスの詳細**（**Device Details**）]：移行で使用された移行元デバイスとターゲットデバイスの概要。

- **ネットワーク マッピング**
  - [**移行対象として選択されたポリシー**（**Policies Selected for Migration**）]：移行対象として選択したデバイス構成機能を表示します。このセクションには、機能が正常に移行されたかどうかが表示されます。また、移行しないことを選択した一連の機能も表示されます。このセクションでは、機能を確認し、Management Center で移行されなかった機能を手動で追加するかどうかを決定できます。
  - [**PAN インターフェイス間マッピング**（**PAN Interface to Interface Mapping**）]：正常に移行されたインターフェイスの詳細と、 Palo Alto Networks ファイアウォール構成のインターフェイスを Firewall Threat Defense デバイスのインターフェイスにどのようにマッピングしたかが表示されます。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、接続先の Firewall Threat Defense デバイスがない移行、または移行対象となる**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。

  - [**移行元インターフェイス名とセキュリティ ゾーンおよびインターフェイスグループ**（**Source Interface Names to Security Zones and Interface Groups**）]：正常に移行された Palo Alto Networks ファイアウォール論理インターフェイスとその名前の詳細、およびそれらを Firewall Threat Defense デバイスのセキュリティゾーンとインターフェイスグループにどのようにマッピングしたかが表示されます。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。

- **オブジェクトと ACL の異常**

- [**オブジェクト競合処理（Object Conflict Handling**）]：Management Center での競合を避けるために、分割または名前変更されたオブジェクトの詳細。
- [**ACLカテゴリの競合処理（ACL Category Conflict Handling**）]：Firewall Management Center の命名制限に収まるように切り詰められたカテゴリ名。
- [**最適化（Optimization**）]：競合を避けるために名前変更されたオブジェクト、または同一のオブジェクトがすでに Firewall Management Center に存在する場合に再利用されたオブジェクト。
- [**再利用されたオブジェクト（Reused Objects**）]：Firewall Management Center に同一の構成ですでに存在していたため、Firewall Migration Manager が重複を作成する代わりに再利用したオブジェクト。
- Access Control Rules, NAT, and Routes You Chose Not to Migrate：Firewall Migration Managerで移行しないように選択したルールの詳細。Firewall Migration Manager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。

- 移行の問題
  - [**部分的に移行された構成（Partially Migrated Configuration**）]：一部のみが移行された Palo Alto Networks ファイアウォールのルールの詳細。詳細オプションを使用せずにルールを移行できる、詳細オプション付きのルールが含まれます。これらの行を確認し、詳細オプションが Firewall 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。
  - [**ゾーンルックアップに失敗したポリシールール（Policy Rules Failing Zone Lookup**）]：移行中に送信元または宛先ゾーンを解決できなかったルール。
  - [**展開されたアクセスコントロールルール（Expanded Access Control Rules**）]：移行中に単一の Palo Alto Networks ファイアウォール ポイント ルールから複数の Firewall Threat Defense ルールに展開された Palo Alto Networks ファイアウォール アクセス コントロール ポリシー ルールの詳細。

- 機能に対して実行されたアクション
  - [**変換された機能に対して実行されたアクション（Action Taken on Converted Features**）]：移行中に自動的に調整された VPN ポリシーと非推奨設定。
  - **Actions Taken on Access Control Rules**
    - [**移行しないことを選択したアクセスルール（Access Rules You Chose Not to Migrate**）]：Firewall Migration Manager を使用して移行しないことを選択した Palo Alto Networks ファイアウォール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。
    - [**ルールアクションが変更されたアクセスルール（Access Rules with Rule Action Change**）]：Firewall Migration Manager 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。

- [**IPSポリシーおよび変数セットが適用されているアクセスコントロールルール（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 Palo Alto Networks ファイアウォール 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 Firewall Threat Defense デバイスでサポートされているかどうかを判断します。
- [**ファイルポリシーが適用されているアクセスコントロールルール（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 Palo Alto Networks ファイアウォール 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 Firewall Threat Defense デバイスでサポートされているかどうかを判断します。
- [**ルールの「ログ」設定が変更されたアクセスコントロールルール（Access Control Rules that have Rule 'Log' Setting Change**）]：Firewall Migration Manager を使用して「ログ設定」が変更された Palo Alto Networks ファイアウォール 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 Palo Alto Networks ファイアウォール アクセスコントロールルールの詳細。Firewall Migration Manager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。
- [**トンネル化プロトコルのアクセスコントロールルール（Access Control Rules for Tunneled Protocols**）]：移行中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。

- [**エラーと失敗（Errors & Failures**）]：Firewall Management Center へのプッシュに失敗した項目。各エントリには問題と、その問題を解決する修正方法が一覧表示されます。

  エラーレポートは、移行された構成が正しくないか、既存の構成やサポートされていない機能のために Firewall Management Center 内で競合が発生していることを示しています。これらのエラーを確認し、提供される修復方法を使用して解決します。移行先となる Firewall Management Center への構成のプッシュを続行または再開する前に、修正内容を確認します。



（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。この通信が Firewall Threat Defense デバイスによってブロックされるように、Firewall Management Center でルールを構成することをお勧めします。

（注） [確認と検証（**Review and Validate**）] ページで ACL に IPS またはファイルポリシーを適用する必要がある場合は、移行前に Firewall Management Center でポリシーを作成します。これは強く推奨されます。Firewall Migration Manager は接続されている Firewall 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。新しいポリシーを複数のターゲットに割り当てると、パフォーマンスが低下し、プッシュに失敗する可能性があります。

Firewall Management Center および Firewall Threat Defense でサポートされる機能の詳細については、『Firewall Management Center Configuration Guide』を参照してください。

**ステップ 3** Firewall Management Center で、次の手順を実行します。

a) Firewall 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。

- インターフェイス
- ルート（静的、BGP）
- アクセス コントロール
- NAT
- オブジェクト（ネットワークオブジェクト、ユーザーオブジェクト、ダイナミックオブジェクト、セキュリティ インテリジェンス フィード、ポートオブジェクト、URL オブジェクト、ダイナミック ルート オブジェクト、および VLAN オブジェクト）
- サイト間 VPN
- リモート アクセス VPN

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。

これらの項目およびルールの構成方法については、『Firewall Management Center Configuration Guide』を参照してください。手動設定が必要な構成項目の例を次に示します。

- SSH および HTTPS アクセスを含むプラットフォーム設定（「Platform Settings for Threat Defense」に記載）。
- syslog 設定（「Configure Syslog」に記載）。
- ダイナミックルーティング（「Routing Overview for Threat Defense」に記載）。
- サービスポリシー（「FlexConfig Policies」に記載）。
- VPN 構成（「Threat Defense VPN」に記載）。
- 接続ログ設定（「Connection Logging」に記載）。

**ステップ 4** 確認が完了したら、Firewall Management Center から Firewall 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 Migration Managerでポリシーが Firewall 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容易に識別できるよう、これらのポリシーの説明には Palo Alto Networks ファイアウォールの構成のホスト名が含まれています。

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。