

移行要件

- ライセンス要件 （1 ページ）
- プラットフォーム要件 （1 ページ）
- デバイスの準備状況と要件 （2 ページ）
- サポートされるプラットフォームとバージョン （3 ページ）
- Firewall Management Center 要件 （3 ページ）
- サポートされている構成 （4 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。

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。