# 移行について



## Firewall 移行ツールについて

### 資料

本書『*Firewall* 移行ツールを使用した *Fortinet* から *Threat Defense* への移行』に記載のすべての情報は、Firewall 移行ツールの最新バージョンを参照しています。「Cisco.com から Firewall 移行ツールのダウンロード」の手順に従って、最新バージョンの Firewall 移行ツールをダウンロードします。

2.3 以降では、Firewall 移行ツールは Fortinet ファイアウォール構成の FTD への移行をサポートしています。Firewall 移行ツールは、Fortinet 構成を Firewall Threat Defense（FTD）に移行するためのものです。

### 結果を表示するための ファイアウォール移行ツール

ファイアウォール移行ツール（FMT）は、サポートされている Fortinet 構成をサポートされている Threat Defense プラットフォームに変換します。Firewall 移行ツールを使用すると、サポートされている Fortinet の機能とポリシーの移行を自動化できます。サポートされていない機能は手動で移行する必要がある場合があります。

Firewall 移行ツールは Fortinet 情報を収集して解析し、最終的に Management Center にプッシュします。解析フェーズ中に、Firewall 移行ツールは、以下を特定する**移行前レポート**を生成します。

- 完全に移行された、部分的に移行された、移行がサポートされていない、および移行が無視された Fortinet 構成項目。
- エラーのある Fortinet 構成行には、Firepower 移行ツールが認識できない Fortinet CLI がリストされています。これにより、移行がブロックされています。

解析エラーがある場合は、問題を修正し、新しい構成を再アップロードし、接続先デバイスに接続し、インターフェイスをFTDインターフェイスにマッピングし、アプリケーションをマッピングし、セキュリティゾーンをマッピングして、構成の確認と検証に進むことができます。その後、構成を接続先デバイスに移行できます。

Firewall 移行ツールを使用すると、進行状況が保存され、移行プロセス中の 2 つの段階から移行を再開できます。

- **Fortinet 構成ファイルの解析が正常に完了した後**

（注） 解析エラーが発生した場合、または解析前に終了した場合は、Firewall 移行ツールでアクティビティを最初からやり直す必要があります。

- [最適化、確認および検証（Optimize, Review and Validate）] ページ

（注） この段階で Firewall 移行ツールを終了して再起動すると、[最適化、確認および検証（Optimize, Review and Validate）] ページが表示されます。

### コンソール

Firewall移行ツールを起動すると、コンソールが開きます。コンソールには、Firewall移行ツールの各ステップの進行状況に関する詳細情報が表示されます。コンソールの内容は、Firewall 移行ツールのログファイルにも書き込まれます。

Firewall 移行ツールが開いていて実行中の間は、コンソールを開いたままにする必要があります。

**重要** Firewall 移行ツールを終了するために Web インターフェイスが実行されているブラウザを閉じると、コンソールはバックグラウンドで実行され続けます。Firewall 移行ツールを完全に終了するには、キーボードの Command キー + C を押してコンソールを終了します。

### ログ

Firewall 移行ツールは、各移行のログを作成します。ログには、移行の各ステップで発生した内容の詳細が含まれるため、移行が失敗した場合の原因の特定に役立ちます。

Firewall 移行ツールのログファイルは、`<migration_tool_folder>\logs` にあります。

### リソース

Firewall 移行ツールは、**移行前レポート**、**移行後レポート**、Fortinet 構成、およびログのコピーを `resources` フォルダに保存します。

`resources` フォルダは、`<migration_tool_folder>\resources` にあります。

### 未解析ファイル

未解析ファイルは、`<migration_tool_folder>\resources` にあります。

### Firewall 移行ツールでの検索

[最適化、確認および検証（Optimize, Review and Validate）] ページの項目など、Firewall 移行ツールに表示されるテーブル内の項目を検索できます。

テーブルの任意の列または行の項目を検索するには、テーブルの上の **検索**（🔍）をクリックし、フィールドに検索語を入力します。Firewall 移行ツールはテーブル行をフィルタ処理し、その検索語を含む行のみを表示します。

単一の列で項目を検索するには、列見出しにある [検索（Search）] フィールドに検索語を入力します。Firewall 移行ツールはテーブル行をフィルタ処理し、検索語に一致する行のみを表示します。

### ポート

Firewall 移行ツールは、ポート 8321 ー 8331 およびポート 8888 の 12 ポートのうちいずれかのポートで実行されるテレメトリをサポートします。デフォルトでは、Firewall 移行ツールはポート 8888 を使用します。ポートを変更するには、`app_config` ファイルのポート情報を更新します。更新後、ポートの変更を有効にするために、Firewall 移行ツールを再起動します。`app_config` ファイルは、`<migration_tool_folder>\app_config.txt` にあります。

（注） テレメトリはこれらのポートでのみサポートされているため、ポート 8321 ～ 8331 およびポート 8888 を使用することを推奨します。Cisco Success Network を有効にすると、Firewall 移行ツールに他のポートを使用できなくなります。

# Firewall 移行ツールの履歴

| バージョン | サポートされる機能 |
| --- | --- |
| 2.5.2 | Firewall 移行ツール 2.5.2 は、ネットワーク機能に影響を与えることなく、Fortinet 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。<br>ACL 最適化は、次の ACL タイプをサポートします。<br>• 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。<br>• 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。<br>（注） Fortinet では ACP ルールアクション対してのみ最適化を使用できます<br>Firewall 移行ツール 2.5.2 は、宛先の FMC が 7.1 以降の場合、Border Gateway Protocol （BGP）およびダイナミックルート オブジェクトの移行をサポートします |

| バージョン | サポートされる機能 |
|---|---|
| 2.3 | • Fortinet ファイアウォール OS バージョン 5.0 以降をサポートしています。<br>• Firewall 移行ツールを使用すると、次の ASA VPN 構成要素を Threat Defense に移行できます。<br>  • Interfaces<br>  • ゾーン<br>  • スタティック ルート<br>  • ネットワークオブジェクトおよびグループ<br>  • サービスオブジェクトとグループ<br>  • アクセス コントロール リスト<br>  • NAT 依存オブジェクト（IPプール、仮想 IP）<br>  • NAT ルール<br>  • VDOM<br>  • 時間ベースオブジェクト：Firewall 移行ツールは、アクセスルールで参照される時間ベースオブジェクトを検出すると、その時間ベースオブジェクトを移行し、それぞれのアクセスルールにマッピングします。[構成の確認と検証（Review and Validate Configuration）] ページのルールに対してオブジェクトを確認します。<br>  （注） 時間ベースのオブジェクトは FMC バージョン 6.6 以降でサポートされています。 |

# Firewall 移行ツールのライセンス

Firewall 移行ツールアプリケーションは無料であり、ライセンスは必要ありません。ただし、Threat Defense への正常な登録とポリシーの展開のため、Management Center には関連する Threat Defense 機能に必要なライセンスが必要です。

# 免責事項

Firewall 移行ツール（「ツール」）は、サポート対象のサードパーティ製品の構成を、有効なライセンス対象およびサポート対象である FTD プラットフォーム用の Firewall Threat Defense（「FTD」）構成に容易に変換できるように設計されています。ツールによって作成された

FTDセキュリティポリシーと設定は、変換の完了後に手動で構成する必要があります。お客様は、構成を確認およびテストして、実装前に正確かつ完全であることを確認する責任を負います。ツールは「現状のまま」提供され、シスコは、ツールがお客様のビジネス要件を満たすこと、またはお客様の既存システムで動作することについて、いかなる表明も保証もいたしません。