Firepower 移行ツール リリースノート

初版：2018 年 10 月 4 日

最終更新：2020 年 6 月 26 日

Firepower 移行ツールにようこそ

このドキュメントでは、Cisco Firepower 移行ツールに関する重要かつリリース固有の情報について説明します。Firepower のリリースに精通していて、移行プロセスを以前に経験したことがある場合でも、このドキュメントをよく読んで理解していることを確認してください。

このリリースの新機能

このリリースでは、次の機能が追加されました。

表 *1*: このリリースの新機能

ファイアウォール	新機能

Palo Alto Networks（PAN）ファイアウォール	• PAN OS バージョン 6.1.x 以降のサポート。
	• Firepower 移行ツールを使用すると、次のサポートされている PAN 設定要素を Firepower Threat Defense に移行できます。
	  • インターフェイス
	  • スタティック ルート
	  • ネットワークオブジェクトおよびグループ
	  • ポート オブジェクトおよびグループ
	  • アクセスコントロールリスト（ポリシー）
	  • ゾーン
	  • アプリケーション
	  • NAT ルール
	• [確認と検証（Review and Validate）] ページで使用可能な、コンテンツベースの検索機能
	• UI の機能が強化され、進行状況バーが表示されるようになりました。

Firepower 移行ツールの履歴情報については、次を参照してください。

- ASA の場合：Firepower 移行ツールの履歴
- Check Point ファイアウォールの場合：Firepower 移行ツールの履歴
- Palo Alto Networks ファイアウォールの場合：Firepower 移行ツールの履歴

サポートされている構成

ASA の移行では、次の設定要素がサポートされています。

- ネットワーク オブジェクト
- サービス オブジェクト（Firepower Threat Defense ではポート オブジェクトと呼ばれる）
- アクセス リスト
- NAT ルール
- インターフェイス（例外：冗長、ルーテッドモードBVI、VTI（トンネルインターフェイス））

（注） 送信元 ASA にポート チャネル インターフェイスがある場合は、Firepower Management Center でポート チャネル インターフェイスを作成する必要があります。サブインターフェイスは自動的に作成されます。

- 静的ルート（SLA トラックなし、動的ルーティングはサポートされません）
- ルーテッドおよびトランスペアレント ファイアウォール モード
- ネットワークオブジェクトとグループ、ACL、およびルートでサポートされている name コマンドリファレンス

Check Point ファイアウォールの移行では、次の設定要素がサポートされています。

- インターフェイス（物理インターフェイス、VLANインターフェイス、およびボンドインターフェイス）
- ネットワークオブジェクトおよびグループ
- サービス オブジェクト
- ネットワークアドレス変換（ゲートウェイの背後の自動NATルール、Check Pointのセキュリティゲートウェイを持つ手動 NAT、および IPv6 NAT ルールを除く）
- IPv6 変換のサポート（インターフェイス、静的ルート、オブジェクト）。ACL（IPv6 のゾーンベースを除く）および NAT はサポートされていません

- グローバルに適用されるアクセスルールと、グローバル ACL をゾーンベース ACL に変換するためのサポート
- 静的ルート（値 1 以外のプライオリティ設定で設定されたもの、スコープローカルのもの、論理インターフェイスのものを除く）
- 追加のロギングタイプを持つ ACL

PAN ファイアウォールの移行では、次の設定要素がサポートされています。

- ネットワークオブジェクトおよびグループ
- ゾーン（レイヤ 2、レイヤ 3、仮想ワイヤ）
- サービス オブジェクト
- サービス オブジェクト グループ（ネストされたサービス オブジェクト グループを除く）

（注） Firepower Management Center ではネストはサポートされていないため、Firepower移行ツールは参照されるルールの内容を拡張します。ただし、ルールは完全な機能で移行されます。

- IPv4 および IPv6 FQDN オブジェクトとグループ
- IPv6 変換のサポート（インターフェイス、スタティックルート、オブジェクト、ACL）
- アクセス ルール
- NAT ルール

（注） サービスに「application-default」が設定されているすべてのポリシーは、「any」として移行されます。FTD には同等の機能がないためです。

変換済み送信元と元の宛先には、「any」オブジェクトがFMC で事前定義されていません。したがって、0.0.0.0/0 を持つObj_0.0.0.0 という名前のオブジェクトが作成され、プッシュされます。

- 物理インターフェイス
- サブインターフェイス（サブインターフェイス ID は、移行時に常に VLAN ID と同じ番号に設定されます）
- 集約インターフェイス（ポートチャネル）
- スタティックルート（移行されない Next VR および ECMP ルートとしてネクストホップが設定されているルートを除く）

（注） 送信元ファイアウォール（PAN）にスタティックルートとして設定されたルートが接続されている場合、プッシュ障害が発生します。FMC では、接続済みルートのスタティックルートを作成できません。そのようなルートを削除し、移行を続行します。

移行でサポートされるソフトウェアのバージョン

移行でサポートされている ASA、チェックポイント、PAN および Firepower Threat Defense のバージョンは次のとおりです。

サポートされている ASA のバージョン

Firepower 移行ツールは、ASA ソフトウェアバージョン 8.4 以降を実行しているデバイスからの移行をサポートしています。

サポートされている Check Point のバージョン

移行ツールは、Check Point OS バージョン R75、R76、R77、R77.10、R77.20、および R77.30 を実行している Firepower Threat Defense への移行をサポートしています。

（注） VSX はサポートされていません。

移行ツールは、Check Point プラットフォーム（Windows、Secure Platform、Secure Platform 2.6、Solaris、Linux、および Gaia）を実行している Firepower Threat Defense への移行をサポートしています。

サポートされている Palo Alto Networks のファイアウォールのバージョン

Firepower 移行ツールは、PAN ファイアウォール OS バージョン 6.1.x 以降を実行している Firepower Threat Defense への移行をサポートしています。

ソース ASA 設定でサポートされている Firepower Management Center のバージョン

ASA の場合、Firepower 移行ツールは、バージョン 6.2.3 または 6.2.3+ を実行している Firepower Management Center によって管理される Firepower Threat Defense デバイスへの移行をサポートしています。

（注） 最適な移行時間を実現するには、Firepower Management Center を、software.cisco.com/downloads で提供されている推奨リリースバージョンにアップグレードすることをお勧めします。

ソース Check Point および PAN ファイアウォール設定でサポートされている Firepower Management Center のバージョン

Check Point および PAN ファイアウォールの場合、Firepower 移行ツールは、バージョン 6.2.3.3 以降を実行している Firepower Management Center によって管理される Firepower Threat Defense デバイスへの移行をサポートしています。

サポートされる Firepower Threat Defense のバージョン

Firepower 移行ツールでは、Firepower Threat Defense のバージョン 6.2.3 以降を実行しているデバイスへの移行が推奨されます。

Firepower Threat Defense のオペレーティングシステムとホスティング環境の要件を含めた Cisco Firepower ソフトウェアとハードウェアの互換性の詳細については、『Cisco Firepower Compatibility Guide』を参照してください。

移行ワークフロー

（注） リリース 2.0 以降では、Firepower 移行ツールは Check Point 設定の FTD への移行をサポートしています。移行ワークフローの一部として、次の重要なヒントに注意してください。

（注） リリース 2.1 以降では、Firepower 移行ツールは Palo Alto Networks（PAN）ファイアウォール設定の FTD への移行をサポートしています。移行ワークフローの一部として、次の重要なヒントに注意してください。

ASA の場合

次のいずれかの方式で、移行用の ASA 設定項目を取得できます。

- **手動アップロード方式**：シングルコンテキストモードでは、**show run** コマンドを使用して ASA 設定を取得します。マルチコンテキストモードでは、**show tech** コマンドを使用して ASA 設定を取得します。
- **移行ツールからの ASA への接続**：マルチコンテキスト ASA では、ASA に接続した後に移行するコンテキストを選択し、ターゲット Firepower Threat Defense デバイスを選択します。最初のコンテキストの移行が完了したら、手順を繰り返して他のコンテキストを移行します。つまり、ASA に接続して移行するコンテキストを選択し、ターゲット Firepower Threat Defense デバイスを選択します。

Check Point ファイアウォールの場合

手動アップロード方式でのみ、移行用の Check Point 設定項目を取得できます。手動アップロード方式を使用して Check Point 設定を収集するには、次の手順を実行します。

- **Check Point Web Visualization Tool（WVT）を使用した設定のエクスポート**：コマンドプロンプト ウィンドウを開いて、WVT が保存および展開されたディレクトリに移動し、次のコマンドを実行して Check Point 設定を取得します。

  ```
  C:\Web_Visualisation_Tool> cpdb2web.exe [-s management_server] [-u
  admin_name | -a certificate_file] [-p password] [-o output_file_path]
  [-t table_names] [-c | -m gateway | -l package_names] [-gr] [-go]
  [-w Web_Visualization_Tool_installation_directory]
  ```

- **FMT-CP-Config-Extractor_v2.1.2.4352 ツールを使用したデバイス設定のエクスポート**：Check Point のセキュリティゲートウェイにアクセスできるワークステーションで、Windows の実行ファイル（.exe）である FMT-CP-Config-Extractor_v2.1.2.4352 ツールを開きます。

  この解凍ファイルを実行するには、「FMT-CP-Config-Extractor_v2.1.2.4352 ツール」を参照してください。

- **エクスポートされたファイルの圧縮**：8 つすべてのファイル（Web VisualizationTool（WVT）からの 7 つのファイルと、FMT-CP-Config-Extractor_v2.1.2.4352 ツールからの 1 つの .txt ファイル）を選択し、1 つの zip ファイルに圧縮します。

Firepower 移行ツールを使用して Check Point から情報を抽出する必要がある場合は、「Check Point 設定ファイルのエクスポート」に進みます。

Palo Alto Networks ファイアウォールの場合

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。

詳細については、「Palo Alto Networksファイアウォールからの設定のエクスポート」を参照してください。

Firepower 移行ツールの機能

Firepower 移行ツールは、次の機能を提供します。

- 分析およびプッシュ操作を含む移行全体の検証
- オブジェクト再利用機能
- オブジェクト競合の解決
- インターフェイス マッピング
- インターフェイス オブジェクトの自動作成または再利用（セキュリティ ゾーンとインターフェイス グループ マッピングに対する ASA nameif）
- インターフェイス オブジェクトの自動作成または再利用
- 自動ゾーンマッピング
- ユーザ定義のセキュリティゾーンとインターフェイスグループを作成するためのサポート
- ユーザ定義のセキュリティゾーンを作成するためのサポート

- ターゲット Firepower Threat Defense デバイスのサブインターフェイス制限チェック
- サポートされているプラットフォーム

  ：仮想 ASA から仮想 FTD へ

  ：同じハードウェアでの移行（X から X デバイスへの移行）

  ：X から Y デバイスへの移行（Y に多数のインターフェイスが存在）

移行レポート

Firepower 移行ツールは、次のレポートを移行の詳細とともに HTML 形式で提供します。

- 移行前のレポート
- 移行後のレポート

のプラットフォームの要件 Firepower 移行ツール

Firepower移行ツールには、次のインフラストラクチャとプラットフォームの要件があります。

- Windows 10 64 ビット オペレーティング システムまたは MacOS バージョン 10.13 以降
- Google Chrome がシステムのデフォルト ブラウザ
- システムごとに Firepower 移行ツールのシングルインスタンス
- Firepower Management Center と Firepower Threat Defense がバージョン 6.2.3.3 以降であること

（注） 新しいバージョンをダウンロードする前に、以前のビルドを削除する。

資料

このリリースでは次のドキュメントが提供されます。

- 『*Firepower* 移行ツール リリース ノート』
- 『*Migrating ASA to Firepower Threat Defense with the Firepower Migration Tool*』
- 『*Migrating Check Point Firewall to Firepower Threat Defense with the Firepower Migration Tool*』
- 『*Migrating Palo Alto Networks Firewall to Firepower Threat Defense with the Firepower Migration Tool*』
- 『*Open Source Used in Cisco Firepower Migration Tool*』

未解決のバグおよび解決されたバグ

このリリースで未解決のバグには、Cisco バグ検索ツールを使用してアクセスできます。この Web ベース ツールから、この製品やその他のシスコハードウェアおよびソフトウェア製品でのバグと脆弱性に関する情報を保守するシスコ バグ トラッキング システムにアクセスできます。

（注） Cisco Bug Search Tool にログインしてこのツールを使用するには、Cisco.com アカウントが必要です。アカウントを持っていない場合は、 Cisco.com でアカウントに登録できます。バグ検索ツールの詳細については、「バグ検索ツールのヘルプ（Bug Search Tool Help）」[英語] を参照してください。

Firepower 移行ツールの未解決および解決済みの問題の最新のリストについては、次のダイナミック クエリを使用してください。

- 未解決の警告
- 終了した問題

【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。