Firewall 移行ツールの FAQ

Firewall 移行ツールのよく寄せられる質問

Q. リリース 3.0 の Firewall 移行ツールでサポートされる新機能は何ですか。

A. リリース 3.0 では、次の機能がサポートされています。

- リモートアクセス VPN の移行
- クラウド提供型 Firewall Management Center への移行

Q. リリース 2.5.1 の Firewall 移行ツールでサポートされる新機能は何ですか。

A. リリース 2.5.1 では、次の機能がサポートされています。

- 動的ルートオブジェクト
- Border Gateway Protocol; ボーダー ゲートウェイ プロトコル

Q. リリース 2.5 の Firewall 移行ツールでサポートされる新機能は何ですか。

A. リリース 2.5 では、次の機能がサポートされています。

- ACL の最適化
- ワイルドカードマスク

Q. リリース 2.4 の Firewall 移行ツールでサポートされる新機能は何ですか。

A. 次の ASA VPN 構成を Firewall Threat Defense（FTD）に移行します。

- ASA からのクリプトマップ（静的/動的）ベースの VPN
- ルートベース（VTI）の ASA VPN

- ASA からの証明書ベースの VPN 移行

Q. リリース 2.3.5 の Firewall 移行ツールでサポートされる新機能は何ですか。

A. リリース 2.3.5 では、次の機能がサポートされています。

- 静的ルートでの仮想トンネルインターフェイス（VTI）と関連構成、ACL。
- ルートベース（VTI）の VPN トンネル

Q. リリース 2.3.4 の Firewall 移行ツールでサポートされる新機能は何ですか。

A. リリース 2.3.4 では、次の機能がサポートされています。

- VPN オブジェクト
- サイト間 VPN トンネル

Q. Firewall 移行ツールでポリシーを移行できる送信元プラットフォームとターゲットプラットフォームは何ですか。

A. Firewall 移行ツールは、サポートされている ASA プラットフォームから FTD プラットフォームにポリシーを移行できます。詳細については、「サポートされる送信元 ASA プラットフォーム」を参照してください。

Q. 移行前と移行後のレポートで実行する必要があるタスクは何ですか。

A. ASA から Firewall Threat Defense への移行計画の一環としてタスクを実行するには、ASA から Firewall Threat Defense 2100 への移行：例を参照してください。

Q. サポートされている接続先プラットフォームのバージョンは何ですか。

A. Firewall 移行ツールを使用して、Firewall Management Center 6.2.3 以降の Firewall Threat Defense プラットフォームのスタンドアロンインスタンスまたはコンテナインスタンスに ASA 構成を移行できます。サポートされているデバイスのリストの詳細については、サポートされるターゲット Threat Defense プラットフォームを参照してください。

Q. Firewall 移行ツールが移行に関してサポートする機能は何ですか。

A. Firewall 移行ツールは、FTD への L3/L4 ASA 構成の移行をサポートしています。また、移行プロセス中に、IPS、ファイルポリシーなどの L7 機能を有効にすることもできます。

Firewall 移行ツールは、次の ASA 構成を完全に移行できます。

- ネットワークオブジェクトとグループ（不連続マスクを除く）
- サービスオブジェクト（送信元と接続先に設定されたサービスオブジェクトを除く）

（注） Firewall 移行ツールは拡張サービスオブジェクト（送信元と接続先の構成）は移行しませんが、参照先の ACL と NAT のルールは完全な機能で移行されます。

- 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、VPN オブジェクト、および ASA 暗号マップ VPN の移行を除く）

（注） Firewall Management Center ではネストはサポートされていないため、Firewall移行ツールは参照されるルールの内容を展開します。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 変換サポート（インターフェイス、静的ルート、オブジェクト、ACL、および NAT）
- インバウンド方向とグローバル ACL のインターフェイスに適用されるアクセスルール
- 自動 NAT、手動 NAT、およびオブジェクト NAT（条件付き）
- 静的ルート（部分的に移行されるトラックオプションや移行されないECMPルートで構成されたルートを除く）
- 物理インターフェイス
- サブインターフェイス
- ポート チャネル
- ブリッジグループ（トランスペアレントモードのみ）
- トンネリング プロトコル ベースのアクセス コントロール ポリシー ルール（プレフィルタトンネルルールとして移行）
- CSM 管理対象構成のカテゴリベースのルール
- IP SLA のモニタ
- オブジェクトグループの検索
- 時間ベースのオブジェクト
- VPN オブジェクト
- VTI インターフェイス
- ポリシーベース（暗号マップ）とルートベース（VTI）の VPN トンネル
- ASA から FTD への証明書ベースの VPN の移行

Q. リリース 2.2 の Firewall 移行ツールでサポートされる新機能は何ですか。

A. リリース 2.2 では、次の機能がサポートされています。

- オブジェクトグループの検索
- IP SLA のモニタ

- 時間ベースのオブジェクト

Q. リリース 2.0 の Firewall 移行ツールでサポートされる新機能は何ですか。

A. リリース 2.0 では、次の機能がサポートされています。

- アクセスルールの接続先ゾーンのマッピング
- プレフィルタトンネルルール
- カテゴリベースのルール
- ポリシーの制限とキャパシティの警告
- ASA 5505 と ASA-SM の移行サポート

Q. Firewall 移行ツールで導入された新機能を使用するために Firewall Management Center に依存するものはありますか。

A. はい。次の機能は、ターゲット Firewall Management Center 6.5 以降でサポートされています。

- プレフィルタとしてのトンネルルールの移行
- カテゴリベースのルール
- ASA 5505 の移行

（注） ターゲット FTD FPR-1010 プラットフォームに移行するには、Firewall Management Center バージョン 6.5 以降が必要です。

次の機能は、ターゲット Firewall Management Center 6.6 以降でサポートされています。

- オブジェクトグループの検索
- IP SLA のモニタ
- 時間ベースのオブジェクト
- VPN オブジェクト
- サイト間 VPN トンネル

次の機能は、ターゲット Firewall Management Center 6.7 以降でサポートされています。

- VTI インターフェイスおよび関連するスタティックルート。
- Firepower Management Center へのルートベース（VTI）事前共有キー認証タイプの VPN 構成の移行。

- ルーテッド セキュリティ ゾーンの作成、VTI インターフェイスの追加、VTI トンネルを介して復号化されたトラフィック制御のアクセス制御ルールの定義。

Q. 送信元構成のすべてのアクセスルールをプレフィルタポリシーに移行できますか。

A. いいえ。[トンネルルールをプレフィルタとして移行（Migrate Tunnel rules as Prefilter）] を選択して移行する場合、Firewall 移行ツールはトンネリング プロトコル ベースのアクセス ルールを識別し、それらをトンネルルールとして移行します。

Q. Firewall 移行ツールが現在移行しない機能は何ですか。

A. Firewall 移行ツールは、次の ASA 構成の移行をサポートしていません。これらの構成が Firewall Management Center でサポートされている場合、移行の完了後に手動で構成できます。

- SGT ベースのアクセス コントロール ポリシー ルール
- SGT ベースのオブジェクト
- ユーザベースのアクセス コントロール ポリシー ルール
- ブロック割り当てオプションを使用して構成された NAT ルール
- サポートされていない ICMP タイプとコードを持つオブジェクト
- トンネリング プロトコル ベースのアクセス コントロール ポリシー ルール
- SCTP で構成された NAT ルール
- ホスト ‘0.0.0.0’ で構成された NAT ルール
- トンネリング プロトコルベースのアクセス コントロール ポリシー ルール（ターゲット Firewall Management Center 6.5 以降の Firewall 移行ツール 2.0 以降でサポート）
- 動的暗号マップベースの VPN
- 証明書認証ベースの VPN 構成

詳細については、「ASA 構成の注意事項と制約事項」を参照してください。

Q. サポートされている送信元デバイスとコードバージョンは何ですか。

A. Firewall 移行ツールを使用して、シングルコンテキストまたはマルチコンテキストの ASA プラットフォームから構成を移行できます（ソフトウェアバージョン 8.4 以降）。デバイスのリストの詳細については、「サポートされる送信元 ASA プラットフォーム」を参照してください。

Q. Firewall 移行ツールはマルチコンテキスト ASA の移行をサポートしていますか。

A. はい。Firewall 移行ツールは、マルチコンテキスト ASA の移行を処理できます。任意の時点で、ASA の 1 つのコンテキスト（システムコンテキストを除く）をターゲット Firewall

Management Center の FTD コンテナか、またはネイティブインスタンスのいずれかに移行できます。

Q. 移行エラーが発生した場合のサポートメカニズムは何ですか。

A. Firewall 移行ツールは Cisco Success Network に統合されています。エラーまたは問題がある場合は、Cisco TAC にご連絡ください。トラブルシューティングについては、「移行の問題のトラブルシューティング」を参照してください。

Q. Firewall 移行ツールが構成を正常に移行するには、どのくらいの時間がかかりますか。

A. 移行にかかる時間は、ネットワークの遅延、Firewall Management Center の負荷、構成サイズ、オブジェクトの数、ACL など、さまざまな要因によって異なります。内部テストでは、7000 以上のアクセスコントロールリスト、7000 以上の NAT 変換、および 3000 以上のネットワークオブジェクトを含む 2.0 MB の構成ファイルでは、移行が正常に完了するまでに約 6 分かかっています。