Cisco Secure Firewall 移行ツールのスタートアップガイド

Cisco Secure Firewall 移行ツールについて

このガイドでは、Cisco Secure Firewall 移行ツールをダウンロードして移行を完了する方法について説明します。さらに、発生する可能性のある移行の問題を解決するのに役立つトラブルシューティングのヒントも提供します。

本書に記載されている移行手順の例（移行例： チェックポイント から Threat Defense 2100）は、移行プロセスに関する理解を促進するのに役立ちます。

Cisco Secure Firewall 移行ツールは、サポートされている チェックポイント 構成をサポートされている 脅威に対する防御 プラットフォームに変換します。Cisco Secure Firewall 移行ツールを使用すると、サポートされている チェックポイント の機能とポリシーを自動的に 脅威に対する防御 に移行できます。サポートされていない機能はすべて、手動で移行する必要があります。

Cisco Secure Firewall 移行ツールはチェックポイント の情報を収集して解析し、最終的に Secure Firewall Management Center にプッシュします。解析フェーズ中に、Cisco Secure 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。

- エラーのある Check Point 構成の XML または JSON の行

- Check Point には、Cisco Secure Firewall 移行ツールが認識できない Check Point XML または JSON の行がリストされています。**移行前レポート**とコンソールログのエラーセクションの下には、XML または JSON の構成行が記載されています。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、 チェックポイントインターフェイスを 脅威に対する防御 インターフェイスにマッピングし、セキュリティゾーンとインターフェイスグループをマッピングして、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。

コンソール

Cisco Secure 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、Cisco Secure 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、Cisco Secure Firewall 移行ツールのログファイルにも書き込まれます。

Cisco Secure 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 Cisco Secure 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。Cisco Secure 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

Cisco Secure 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。

Cisco Secure 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

Cisco Secure Firewall 移行ツールは、**移行前レポート**、**移行後レポート**、 チェックポイント 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。

Cisco Secure 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、Cisco Secure 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。Cisco Secure 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。Cisco Secure 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

Cisco Secure 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、Cisco Secure 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、Cisco Secure 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、Cisco Secure Firewall 移行ツールに他のポートを使用できなくなります。

Cisco Success Network

Cisco Success Network はユーザ対応のクラウドサービスです。Cisco Success Network を有効にすると、Cisco Secure Firewall 移行ツールと Cisco Cloud 間にセキュアな接続が確立され、使用状況に関する情報と統計情報がストリーミングされます。テレメトリをストリーミングすることによって、Cisco Secure Firewall 移行ツールからの対象のデータを選択して、それを構造化形式でリモートの管理ステーションに送信するメカニズムが提供されるため、次のメリットが得られます。

- ネットワーク内の製品の有効性を向上させるために、利用可能な未使用の機能について通知します。
- 製品に利用可能な、追加のテクニカルサポートサービスとモニタリングについて通知します。
- シスコ製品の改善に役立ちます。

Cisco Secure Firewall 移行ツールはセキュアな接続を確立および維持し、Cisco Success Network に登録できるようにします。Cisco Success Network を無効にすることで、いつでもこの接続をオフにできます。これにより、デバイスが Cisco Success Network クラウドから接続解除されます。

Cisco Secure Firewall 移行ツールの最新情報

バージョン	サポートされる機能
4.0.1	Cisco Secure Firewall 移行ツール 4.0.1 には、次の新機能と拡張機能が含まれています。 • Check Point R81 構成を Cisco Secure Firewall Threat Defense に移行できるようになりました。 • Check Point Security Gateway に接続するときに、マルチドメイン Virtual System Extension（VSX）デプロイメントから構成をエクスポートするために、仮想システム ID を追加することを選択できるようになりました。 • いくつかのコマンドを手動で実行することで、Check Point VSX バージョン R77 から構成を抽出できます。詳細については、『移行ツールを使用した Check Point ファイアウォールから Threat Defense への移行』ガイドの「FMT-CP-Config-Extractor_v4.0-7965 ツールを使用したデバイス構成のエクスポート」を参照してください。 https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migration-guide-CP/migrating-check-point-firewall-to-threat-defense-with-migration-tool/m-check-point-to-threat-defense-migration-workflow.html#id_119025
3.0.1	• ASA with FirePOWER Services、Check Point、Palo Alto Networks、および Fortinet の場合、Secure Firewall 3100 シリーズは宛先デバイスとしてのみサポートされます。
3.0	Cisco Secure Firewall 移行ツール 3.0 は、移行先の管理センターが 7.2 以降の場合、チェックポイント からクラウド提供型 Firewall Management Center への移行をサポートするようになりました。

バージョン	サポートされる機能
2.5.2	Cisco Secure 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、チェックポイント 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。 ACL 最適化は、次の ACL タイプをサポートします。 • 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。 • 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。 （注） チェックポイントではACP ルールアクション対してのみ最適化を使用できます。 Cisco Secure Firewall 移行ツール 2.5.2 は、移行先の Management Center が 7.1 以降の場合、Border Gateway Protocol （BGP）および動的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
2.2	• r80 Check Point OS バージョンをサポートします。 • Live Connect が Check Point（r80）デバイスから構成を抽出できるようにします。 • r80 では、次のサポートされている Check Point の構成要素を 脅威に対する防御 に移行できます。 • インターフェイス • スタティック ルート • オブジェクト • ネットワーク アドレス変換 • アクセス制御ポリシー • グローバルポリシー：このオプションを選択すると、ルートルックアップがないため、ACL ポリシーの送信元ゾーンと宛先ゾーンが**任意**のものとして移行されます。 • ゾーンベースポリシー：このオプションを選択すると、送信元ゾーンと宛先ゾーンは、送信元と宛先のネットワークオブジェクトまたはグループのルーティングメカニズムによる予測ルートルックアップに基づいて導出されます。 （注） ルートルックアップは静的ルートと動的ルートのみ（PBR と NAT を除く）に限定され、送信元と宛先のネットワーク オブジェクト グループの性質によっては、この操作によりルールが急増する可能性があります。 （注） ゾーンベースポリシーの IPv6 ルートルックアップはサポートされていません。

バージョン	サポートされる機能
2.0	• Cisco Secure Firewall 移行ツールの新しい最適化機能を使用すると、検索フィルタを使用して移行結果を迅速に取得できます。 • Cisco Secure Firewall 移行ツールを使用すると、次のサポートされている Check Point 構成要素を 脅威に対する防御 に移行できます。 • インターフェイス • スタティック ルート • オブジェクト • アクセス コントロール ポリシー • グローバルポリシー：このオプションを選択すると、ACL ポリシーの送信元ゾーンと宛先ゾーンが**任意**のものとして移行されます。 • ゾーンベースポリシー：このオプションを選択すると、送信元ゾーンと宛先ゾーンは、送信元と宛先のネットワークオブジェクトまたはグループのルーティングメカニズムによる予測ルートルックアップに基づいて導出されます。 （注） ルートルックアップは静的ルートと動的ルートのみ（PBR と NAT を除く）に限定され、送信元と宛先のネットワーク オブジェクト グループの性質によっては、この操作によりルールが急増する可能性があります。 • ネットワーク アドレス変換 • Check Point OS バージョン r75、r76、r77、r77.10、r77.20、および r77.30 のサポートを提供します。

Cisco Secure Firewall 移行ツールのライセンス

Cisco Secure 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、脅威に対する防御 デバイス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 脅威に対する防御 機能に必要なライセンスが必要です。

Cisco Secure Firewall 移行ツールのプラットフォーム要件

Cisco Secure Firewall 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。

- Microsoft 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 以降で実行している
- Google Chrome がシステムのデフォルトブラウザである
- （Windows）[Power & Sleep] で [Sleep] 設定が [Never put the PC to Sleep] に設定されているため、大規模な移行プッシュ中にシステムがスリープ状態にならない
- （macOS）大規模な移行プッシュ中にコンピュータとハードディスクがスリープ状態にならないように [Energy Saver] 設定が構成されている

Threat Defense デバイスの要件および前提条件

管理センターに移行する場合、ターゲット Threat Defense デバイスが追加される場合とされない場合があります。Threat Defense デバイスへの今後の展開のために、共有ポリシーを管理センターに移行できます。デバイス固有のポリシーを Threat Defense に移行するには、管理センターに追加する必要があります。チェックポイント 構成を Threat Defense に移行することを計画する場合、次の要件と前提条件を考慮してください。

- ターゲット Threat Defense デバイスは、管理センターに登録されている必要があります。
- Threat Defense デバイスは、スタンドアロンデバイスまたはコンテナインスタンスにすることができます。クラスタまたは高可用性設定の一部であっては**なりません**。
  - ターゲットネイティブ 脅威に対する防御 デバイスには、使用する物理データまたはポート チャネル インターフェイスまたはサブインターフェイスが チェックポイントと同数以上必要です（「管理専用」を除く）。そうでない場合は、ターゲット脅威に対する防御デバイスに必要なタイプのインターフェイスを追加する必要があります。サブインターフェイスは、物理またはポートチャネルのマッピングに基づいて Cisco Secure Firewall 移行ツールによって作成されます。
  - ターゲット Threat Defense デバイスがコンテナインスタンスである場合、使用する物理インターフェイス、物理サブインターフェイス、ポート チャネル インターフェイス、およびポート チャネル サブインターフェイスが チェックポイント と同数以上必要です（「管理専用」を除く）。そうでない場合は、ターゲット Threat Defense デバイスに必要なタイプのインターフェイスを追加する必要があります。

（注）
- サブインターフェイスは、Cisco Secure Firewall 移行ツールでは作成されません。インターフェイスマッピングのみが許可されます。
- 異なるインターフェイスタイプ間のマッピングは許可されます。たとえば、物理インターフェイスをポート チャネル インターフェイスにマップできます。

Check Point 構成のサポート

サポートされているチェックポイントの設定

- 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とグループ：Cisco Secure Firewall 移行ツールは、すべての Check Point ネットワークオブジェクトの Threat Defense への移行をサポートします。
- サービス オブジェクト
- ネットワーク アドレス変換
- 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）と IPv6 によるゾーンベース ACL の除外
- 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（スコープがローカルとして構成され、論理インターフェイスがネクストホップ IP アドレスのない静的ルートの出力インターフェイスとして構成されているルートを除く）
- 追加のロギングタイプを持つ ACL

（注） Check Point 内に対応する NAT ルールを持つ Check Point で構成された ACE の場合、Cisco Secure Firewall 移行ツールは、対応する移行された ACE ルール内の変換された IP アドレスに対して実際の IP アドレスをマッピングしません。Cisco Secure Firewall 移行ツールが IP アドレスをマッピングしないのは、NAT ルールに対する ACE ルールの参照情報が不足しているためです。そのため、Management Center 上の移行された ACE および NAT 構成の検証時に、Threat Defense パケットフローに対応する ACE ルールを検証し、それに手動で変更を加える必要があります。

（注） Cisco Secure Firewall 移行ツールはサービスオブジェクト（送信元および宛先と、オブジェクトグループで呼び出されるものと同じタイプのオブジェクトとのポートの組み合わせで構成される）を移行しませんが、参照される ACL ルールは完全な機能で移行されます。

サポートされていない Check Point 構成の詳細については、「サポートされない Check Point 構成」を参照してください。

部分的にサポートされる Check Point 構成

Cisco Secure Firewall 移行ツールは、次の Check Point 構成の移行を部分的にサポートしています。これらの構成の一部には、詳細オプションを使用するルールが含まれ、それらのオプションなしで移行できます。Management Center がこれらの詳細オプションをサポートしている場合は、移行の完了後に手動で構成できます。

- ランクパラメータと ping パラメータを持つ静的ルートは部分的に移行されます。
- モード、XOR、アクティブバックアップ、ラウンドロビンタイプのボンドインターフェイスは、Cisco Secure Firewall 移行ツールによって Management Center の LACP タイプに部分的に移行されます。
- 物理インターフェイスやボンドインターフェイスといった親インターフェイスの一部であるエイリアスインターフェイス構成、無視される属性および親インターフェイス属性に含まれるエイリアスインターフェイス構成は、そのまま移行されます。
- 除外タイプのネットワークオブジェクトグループは、ACL を介してサポートされ、意味がそのまま維持されます。
- 追加ロギングタイプを持つ ACL と時間範囲を持つ ACL。

サポートされない Check Point 構成

Cisco Secure Firewall 移行ツールは、次の Check Point 構成をサポートしていません。これらの構成が 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。

- エイリアス、ブリッジ、6IN4 トンネル、ループバック、および PPPoE インターフェイス
- ネットワークオブジェクトとグループ：
  - UTM-1 エッジゲートウェイ
  - Check Point ホスト
  - ゲートウェイクラスタ
  - 外部管理ゲートウェイまたはホスト
  - オープンセキュリティ拡張機能（OSE）デバイス
  - 論理サーバ
  - ダイナミックオブジェクト
  - VoIP ドメイン
  - ゾーン
  - CP Security Gateway
  - CP 管理サーバ
  - 除外タイプのネットワーク オブジェクト グループ

- サービスオブジェクト：
  - RPC
  - DCE-RPC
  - 複合 TCP
  - GTP
  - その他の Check Point 固有サービスオブジェクト
- 次を持つ ACL ポリシー：
  - サポートされていない ACE アクションタイプ（クライアント認証、セッション認証、ユーザ認証、およびその他のカスタム認証タイプ）は、許可アクションタイプによって移行されますが、無効な状態になります。
  - アイデンティティベースの ACL ポリシー
  - IPv6 ルートルックアップによるゾーンベースのポリシー
  - ユーザベースのアクセス コントロール ポリシー ルール
  - グローバル マルチドメイン システム ルールは移行できません。

（注） Check Point マルチドメイン展開に含まれるグローバル マルチドメイン システムの設定はエクスポートできません。そのため、特定の CMA に関連する構成は、エクスポートおよび移行のみが可能です。

- サポートされていない ICMP タイプおよび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
- 暗黙の ACL ルール
- 否定パラメータを持つ ACE
- ゾーンベースの ACE が選択されており、それが 100 を超える値の範囲オブジェクトを持つ場合、ACE のゾーンは移行され、ACE 名と適切なコメントに追加されるルックアップなしの「Any」としてマークされます。
- ゾーンベースの ACE が選択されている場合、IPv6 アドレスを持つ ACE のゾーンは、「Any」および適切なコメントによってサポートされない ACE としてマークされます。

サポートされない NAT ルール

Cisco Secure Firewall 移行ツールは、次の NAT ルールをサポートしていません。

- ゲートウェイの背後に隠れている自動 NAT ルール

- Check Point Security Gateway を使用した手動 NAT ルール
- デュアルタイプ IP アドレスを持つネットワークオブジェクトを含む手動 NAT ルール
- 継承されたオブジェクトが IPv6 構成を持つオブジェクトグループを含む手動 NAT ルール
- サービスグループを使用した手動 NAT ルール
- IPv6 NAT ルール

サポートされない静的ルート

- **netstat -rnv** で出力インターフェイスが見つからない場合の静的ルート
- 論理ゲートウェイを出口インターフェイスとして持つ静的ルート
- ECMP タイプの静的ルート
- ローカルスコープ属性を出口インターフェイスとして持つ静的ルート

注意事項と制約事項

変換中に、Cisco Secure Firewall 移行ツールは、ルールまたはポリシーで使用されるかどうかにかかわらず、サポートされているすべてのオブジェクトおよびルールに対して 1 対 1 のマッピングを作成します。ただし、Cisco Secure Firewall 移行ツールには、未使用のオブジェクト（ACL で参照されていないオブジェクト）の移行を除外できる最適化機能があります。

Cisco Secure Firewall 移行ツールは、サポートされていないオブジェクトとルールを指定どおりに処理します。

- サポートされていないオブジェクトとルートは移行されません。
- サポートされていない ACL ルールは、無効なルールとして管理センターに移行されます。

Check Point 構成に関する制約事項

送信元 Check Point 構成の移行には、次の制限があります。

- システム構成は移行されません。
- ライブファイアウォールと VSX はサポートされていません。

（注） VSX は、どのバージョンの Check Point についてもサポートされていません。

Check Point VSX からポリシーを移行する場合は、仮想システムに関連する特定のポリシーパッケージをエクスポートしてから（一度に 1 つの仮想システム）、ポリシーを r77.30 または r80 以降のバージョンから Threat Defense に移行できます。

（注） ファイアウォールの Live Connect は、Check Point（r80）以降のバージョンについてのみサポートされています。

- 明示的なすべてのセキュリティポリシー（r77.30 以前のバージョンの `Security_Policy.xml` および r80 以降のバージョンのセキュリティ ポリシー ファイルで利用可能）が、管理センター上の ACP に移行されます。暗黙のルールはエクスポートされる構成に含まれないため、Check Point Smart ダッシュボード上のルールは移行されません。

（注）

- Check Point（r80）以降のバージョンでは、L4 セキュリティ レイヤポリシーに個別のアプリケーション レイヤ ポリシーが添付されている場合、Cisco Secure Firewall 移行ツールはそれらを「サポートされていない」ものとして移行します。また、そのような場合は、ACE 構成を持つファイルが 2 つ存在します。1 つはセキュリティレイヤに関するファイルで、もう 1 つはアプリケーションレイヤに関するファイルです。Cisco Secure Firewall 移行ツールによる移行は、構成 zip ファイルの *index.json* に含まれている、アクセスレイヤで利用可能な優先順位情報に基づいて行われます。
- マルチドメイン展開がセットアップされており、グローバルポリシーとカスタマー管理アドオン（CMA）固有ポリシーを持つ、Check Point バージョン r80 以降の場合、Cisco Secure Firewall 移行ツールが Check Point 構成を移行する順序は、送信元構成の順序と少し異なります。また、そのような場合は、ACE 構成を持つファイルが 2 つ存在します。 1 つはグローバルポリシーに関するファイルで、もう 1 つは CMA ポリシーに関するファイルです。ドメインレイヤで構成された ACE は、「サポートされていない」ものとして移行されます。
- マルチドメインシステムのドメインレイヤとしてアクションを持つ CMA 用に構成された ACE ルールの順序の定義は、取得された構成では不完全です。そのため、送信元構成の特定の CMA ポリシーにグローバルポリシーが添付されている場合は、取得された構成のルール番号インデックスを検証して、正しい順序になっていることを確認してください。

- 一部の Check Point 構成（Threat Defense へのダイナミックルーティングや VPN など）は、Cisco Secure Firewall 移行ツールで移行できません。これらの構成は手動で移行してください。
- 管理センターへの Check Point ブリッジ、トンネル、およびエイリアスインターフェイスは移行できません。
- 管理センターでは、ネストされたサービス オブジェクト グループまたはポートグループはサポートされていません。変換の一環として、Cisco Secure Firewall 移行ツールは、参照されているネストされたオブジェクトグループまたはポートグループの内容を展開します。
- Cisco Secure Firewall 移行ツールは、同じオブジェクト内で構成されている送信元ポートと宛先ポートを持つサービスのオブジェクトまたはグループを、複数の回線にまたがる異なるオブジェクトに分割します。このようなアクセスコントロールルールの参照は、正確に同じ意味の管理センタールールに変換されます。

Check Point 移行のガイドライン

Check Point ログオプションの移行は、Threat Defense のベストプラクティスに従います。ルールのログオプションは、送信元 Check Point 構成に基づいて有効または無効になります。アクションが **drop** または **reject** のルールの場合、Cisco Secure Firewall 移行ツールは接続の開始時にロギングを構成します。アクションが **permit** の場合、Cisco Secure Firewall 移行ツールは接続の終了時にロギングを構成します。

オブジェクト移行の注意事項

Threat Defense でポートオブジェクトと呼ばれるサービスオブジェクトには、オブジェクトに関するさまざまな構成ガイドラインがあります。たとえば、Check Point では、複数のサービスオブジェクトに大文字か小文字かが異なるだけの同じ名前を付けることができますが、Threat Defense では、大文字か小文字かに関係なく、各オブジェクトに一意の名前を付ける必要があります。Cisco Secure Firewall 移行ツールでは、Check Point のオブジェクトをすべて分析し、次のいずれかの方法で Threat Defense への移行を処理します。

- 各 Check Point オブジェクトに一意の名前と構成がある場合：Cisco Secure Firewall 移行ツールはオブジェクトを変更せずに正常に移行します。
- Check Point サービスオブジェクトの名前に、管理センターでサポートされていない特殊文字が 1 つ以上含まれている場合：Cisco Secure Firewall 移行ツールは、管理センターのオブジェクト命名基準を満たすために、そのオブジェクト名の特殊文字を「_」文字に変更します。
- Check Point サービスオブジェクトの名前と構成が、管理センターの既存のオブジェクトと同じである場合：Cisco Secure Firewall 移行ツールは、Threat Defense 構成に管理センターのオブジェクトを再利用し、Check Point オブジェクトを移行しません。
- Check Point サービスオブジェクトと管理センターの既存のオブジェクトの名前は同じだが構成は異なる場合：Cisco Secure Firewall 移行ツールはオブジェクトの競合を報告します。これにより、ユーザーは、 Check Point サービスオブジェクトの名前に一意のサフィックスを追加して競合を解決することで、移行を実行できます。
- 複数の Check Point サービスオブジェクトに、大文字か小文字かが異なるだけの同じ名前が付けられている場合：Cisco Secure Firewall 移行ツールは、Threat Defense のオブジェクト命名基準を満たすように、そのようなオブジェクトの名前を変更します。

Threat Defense デバイスに関する注意事項と制約事項

チェックポイント 構成を 脅威に対する防御 に移行することを計画する場合は、次の注意事項と制約事項を考慮してください。

- ルート、インターフェイスなど、脅威に対する防御 に既存のデバイス固有の構成がある場合、プッシュ移行中に Cisco Secure Firewall 移行ツールは自動的にデバイスを消去し、チェックポイント 構成から上書きします。

（注） デバイス（ターゲット 脅威に対する防御）構成データの望ましくない損失を防ぐために、移行前にデバイスを手動で消去することを推奨します。

移行中に、Cisco Secure Firewall 移行ツールはインターフェイス構成をリセットします。これらのインターフェイスをポリシーで使用すると、Cisco Secure Firewall 移行ツールはそれらをリセットできず、移行は失敗します。

- Cisco Secure Firewall 移行ツールは、チェックポイント 構成に基づいて 脅威に対する防御 デバイスのネイティブインスタンスにサブインターフェイスを作成できます。移行を開始する前に、ターゲット 脅威に対する防御 デバイスでインターフェイスとポート チャネル インターフェイスを手動で作成します。たとえば、チェックポイント 構成に次のインターフェイスとポートチャネルが割り当てられている場合は、移行前にそれらをターゲット 脅威に対する防御 デバイスで作成する必要があります。
  - 5 つの物理インターフェイス
  - 5 つのポートチャネル
  - 2 つの管理専用インターフェイス

（注） 脅威に対する防御デバイスのコンテナインスタンスの場合、サブインターフェイスは、Cisco Secure Firewall 移行ツールでは作成されません。インターフェイスマッピングのみが許可されます。

移行がサポートされるプラットフォーム

Cisco Secure Firewall 移行ツールによる移行では、以下の チェックポイント 、および 脅威に対する防御 プラットフォームがサポートされています。サポートされる 脅威に対する防御 プラットフォームの詳細については、『Cisco Secure Firewall Compatibility Guide』[英語] を参照してください。

（注） Cisco Secure Firewall 移行ツールは、スタンドアロンモードまたは分散 Check Point 構成からスタンドアロン 脅威に対する防御 デバイスへの移行のみをサポートします。

サポートされるターゲット Threat Defense プラットフォーム

Cisco Secure Firewall 移行ツールを使用して、脅威に対する防御 プラットフォームの次のスタンドアロンまたはコンテナインスタンスに送信元 チェックポイント 構成を移行できます。

- Firepower 1000 シリーズ
- Firepower 2100 シリーズ
- Secure Firewall 3100 シリーズ
- Firepower 4100 シリーズ
- Firepower 9300 シリーズ（次を含む）：
  - SM-24
  - SM-36
  - SM-40
  - SM-44
  - SM-48
  - SM-56

- VMware ESXi、VMware vSphere Web クライアント、または vSphere スタンドアロンクライアントを使用して展開された Threat Defense（VMware 上）
- Microsoft Azure クラウドまたは AWS クラウド上の Threat Defense Virtual

（注）
- Azure における Threat Defense Virtual の前提条件と事前設定については、『Getting Started with Secure Firewall Threat Defense Virtual』[英語] を参照してください。
- AWS クラウドにおける Threat Defense Virtual の前提条件と事前設定については、「Threat Defense Virtual の前提条件」を参照してください。

これらの環境ごとに要件に従って事前設定された Cisco Secure Firewall 移行ツールには、Microsoft Azure または AWS クラウド内の Management Center に接続し、構成をそのクラウド内の Management Center に移行させるためのネットワーク接続が必要です。

（注） 移行を成功させるには、Cisco Secure Firewall 移行ツールを使用する前に、Management Center または Threat Defense Virtual を事前設定するための前提条件が満たされている必要があります。

（注） Cisco Secure Firewall 移行ツールには、クラウドでホストされるデバイスへのネットワーク接続が必要です。それにより、移行元の構成を抽出したり（CP（r80）Live Connect）、手動でアップロードした構成をクラウド内の Management Center に移行させたりします。そのため、前提条件として、Cisco Secure Firewall 移行ツールを使用する前に、IP ネットワーク接続を事前設定する必要があります。

サポートされる移行先の管理センター

Cisco Secure Firewall 移行ツールは、管理センターおよびクラウド提供型 Firewall Management Center によって管理される Threat Defense デバイスへの移行をサポートします。

Management Center

管理センターは強力な Web ベースのマルチデバイスマネージャです。独自のサーバーハードウェア上で、またはハイパーバイザ上の仮想デバイスとして稼働します。移行のためのターゲット管理センターとして、オンプレミス管理センターと仮想管理センターの両方を使用できます。

管理センターは、移行に関する次のガイドラインを満たす必要があります。

- 移行でサポートされる Mangement Center ソフトウェアバージョン（移行でサポートされるソフトウェアのバージョン （19 ページ）を参照）。
- Check Point の移行でサポートされる Management Center ソフトウェアバージョンは 6.2.3.3 以降です。
- チェックポイント インターフェイスから移行する予定のすべての機能を含む 脅威に対する防御 用のスマートライセンスを取得済みおよびインストール済みであること。次を参照してください。
  - Cisco.com の「Cisco Smart Accounts」の「Getting Started」セクション。
  - Register the Firepower Management Center with the Cisco Smart Software Manager [英語]
  - Licensing the Firewall System [英語]

クラウド提供型 Firewall Management Center

クラウド提供型 Firewall Management Center は、Threat Defense デバイスの管理プラットフォームであり、Cisco Defense Orchestrator を介して提供されます。クラウド提供型 Firewall Management Center は、管理センターと同じ機能を多数提供します。

CDO からクラウド提供型 Firewall Management Center にアクセスできます。CDO は、Secure Device Connector（SDC）を介してクラウド提供型 Firewall Management Center に接続します。クラウド提供型 Firewall Management Center の詳細については、「クラウド提供型 Firewall Management Center による Cisco Secure Firewall Threat Defense デバイスの管理」を参照してください。

Cisco Secure Firewall 移行ツールは、移行先の管理センターとしてクラウド提供型 Firewall Management Center をサポートしています。クラウド提供型 Firewall Management Center を移行先の管理センターとして選択するには、CDO リージョンを追加し、CDO ポータルから API トークンを生成する必要があります。

CDO リージョン

CDO は 3 つの異なる地域で利用でき、地域は URL 拡張子で識別できます。

表 *1 : CDO* の地域と *URL*

地域	CDO URL
ヨーロッパ地域	https://defenseorchestrator.eu/
US リージョン	https://defenseorchestrator.com/
APJC リージョン	https://www.apj.cdo.cisco.com/

移行でサポートされるソフトウェアのバージョン

移行のためにサポートされている Cisco Secure Firewall 移行ツール、 チェックポイント 、および 脅威に対する防御 のバージョンは次のとおりです。

サポートされている Cisco Secure Firewall 移行バージョン

software.cisco.com に掲載されているバージョンは、当社のエンジニアリングおよびサポート組織によって正式にサポートされているバージョンです。software.cisco.com から最新バージョンの Cisco Secure Firewall 移行ツールをダウンロードすることを強くお勧めします。現在利用可能なサポートされているバージョンは次のとおりです。

- Cisco Secure Firewall 移行ツール v 3.0.1
- Cisco Secure Firewall 移行ツール v 3.0.2

Cisco Secure Firewall 移行ツールバージョン 3.0.1 は現在サポートが終了しており、software.cisco.com から削除される予定です。

サポートされている Check Point のバージョン

Cisco Secure Firewall 移行ツールは、Check Point OS バージョン r75 ～ r77.30 および r80 ～ r80.40 を実行している 脅威に対する防御 への移行をサポートしています。[Select Source] ページで適切な Check Point バージョンを選択します。

（注） VSX はサポートされていません。

Cisco Secure Firewall 移行ツールは、Check Point Platform Gaia からの移行をサポートしています。

送信元 Check Point ファイアウォール構成でサポートされている Management Center のバージョン

Check Point ファイアウォールの場合、Cisco Secure Firewall 移行ツールは、バージョン 6.2.3.3 以降を実行している Management Center によって管理される 脅威に対する防御 デバイスへの移行をサポートしています。

（注） 6.7 脅威に対する防御 デバイスへの移行は現在サポートされていません。そのため、デバイスに Management Center アクセス用のデータインターフェイスで設定されている場合、移行が失敗する可能性があります。

サポートされる Threat Defense のバージョン

Cisco Secure Firewall 移行ツールでは、脅威に対する防御 のバージョン 6.5 以降を実行しているデバイスへの移行が推奨されます。

脅威に対する防御 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 Firewall の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』[英語] を参照してください。

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。