Firewall 移行ツールを使用した Check Point Firewall から Threat Defense への移行

初版：2019 年 9 月 6 日

最終更新：2022 年 3 月 4 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次

第 1 章 移行について 1

Firewall 移行ツールについて 1

Firewall 移行ツールの履歴 4

Firewall 移行ツールのライセンス 6

Cisco Success Network 6

第 2 章 移行の準備 9

Firewall 移行ツールに関する注意事項と制約事項 9

Threat Defense デバイスに関する注意事項と制約事項 11

Check Point 構成に関する注意事項と制約事項 12

移行がサポートされるプラットフォーム 18

移行でサポートされるソフトウェアのバージョン 20

Firewall 移行ツールのプラットフォーム要件 20

第 3 章 移行の実行 23

Cisco.com から Firewall 移行ツールのダウンロード 23

Firewall 移行ツールの起動 24

Check Point 構成ファイルのエクスポート 26

r77 の Check Point 構成ファイルのエクスポート 26

Check Point Web Visualization Tool（WVT）を使用した構成のエクスポート 27

FMT-CP-Config-Extractor_v2.5.2-6575 ツールを使用したデバイス構成のエクスポート 28

エクスポートされたファイルの圧縮 29

r80 の Check Point 構成ファイルのエクスポート 29

Live Connect を使用した構成抽出のための Check Point（r80）デバイスの事前設定 30

r80 の Check Point 構成ファイルをエクスポートする手順 38
別の構成ファイルの取得 41
Check Point 構成ファイルのアップロード 42
Firewall 移行ツールの接続先パラメータの指定 43
移行前レポートの確認 45
チェックポイント 構成と Threat Defense インターフェイスのマッピング 47
セキュリティゾーン とインターフェイスグループへの チェックポイント インターフェイスのマッピング 49
最適化、 移行する構成の確認と検証 50
ACL 最適化のレポート 55
移行された構成の以下へのプッシュ： Firepower Management Center 57
移行後レポートの確認と移行の完了 58
Firewall 移行ツールのアンインストール 61

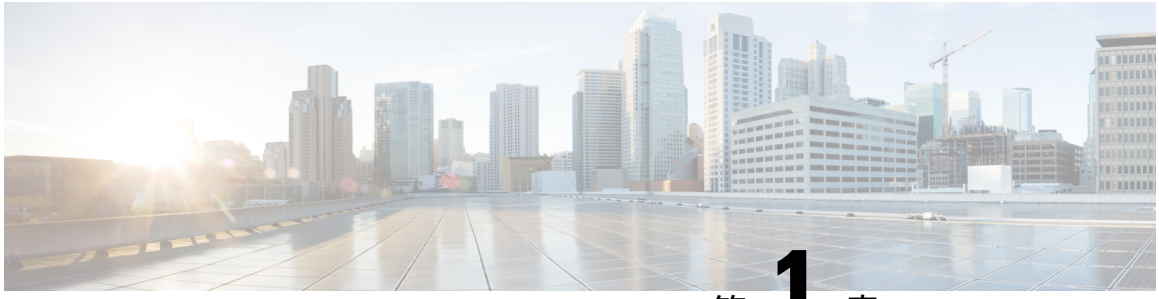
第 4 章 移行の問題のトラブルシューティング 63
Firewall 移行ツールのトラブルシューティングについて 63
トラブルシューティングに使用されるログおよびその他のファイル 64
Check Point ファイルのアップロード失敗のトラブルシューティング 64
Check Point のトラブルシューティング例：オブジェクトグループのメンバーが見つからない（r75 ～ r77.30 のみ） 65
Live Connect の Check Point（r80）に関するトラブルシューティング例 66

第 5 章 Firewall 移行ツールの FAQ 69
Firewall 移行ツールの FAQ 69
Firewall 移行ツールのよく寄せられる質問 69

付録 A： Cisco Success Network：テレメトリデータ 73
Cisco Success Network：テレメトリデータ 73

付録 B： Check Point から Threat Defense 2100 への移行：例 81
チェックポイント から Firewall Threat Defense 2100 への移行：例 81
メンテナンスウィンドウの前に次のタスクを実行する 81

メンテナンスウィンドウ中に次のタスクを実行する 83



第 1 章

移行について

- Firewall 移行ツールについて （1 ページ）
- Firewall 移行ツールの履歴 （4 ページ）
- Firewall 移行ツールのライセンス （6 ページ）
- Cisco Success Network （6 ページ）

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 *Check Point* ファイアウォールから *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。

リリース 2.0 以降では、Firewall 移行ツールは Check Point（CP）構成（r75 ～ r77.30）の FTD への移行をサポートしています。リリース 2.2 以降では、Firewall 移行ツールは Check Point（CP）構成（r80）の FTD への移行をサポートしています。

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チェックポイント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チェックポイント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 チェックポイント 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。

- エラーのある Check Point 構成の XML または JSON の行
- Check Point には、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 FTD 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。

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。

- **チェックポイント 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**、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。

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、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 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
2.2	• 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 構成要素を 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 • 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ダイナミックルートのみ（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	• 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。 • 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 設定要素を 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 • 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ダイナミックルートのみ（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。

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。

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、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

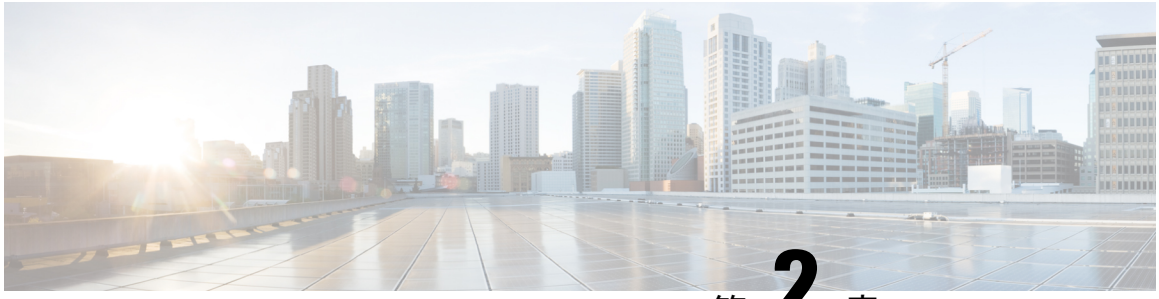
情報と統計情報がストリーミングされます。テレメトリをストリーミングすることによって、Firewall移行ツールからの対象のデータを選択して、それを構造化形式でリモートの管理ステーションに送信するメカニズムが提供されるため、次のメリットが得られます。

- 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。

Firewall 移行ツールは常に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 Success Network の有効化と無効化

Firewall 移行ツールの [エンドユーザーライセンス契約（End User License Agreement）] ページで Cisco Success Network と情報を共有することに同意する場合は、Cisco Success Network を有効にします。詳細については、Firewall移行ツールの起動 （24ページ）を参照してください。移行ごとに、Firewall 移行ツールの [設定（Settings）] ボタンから Cisco Success Network を有効または無効にできます。Cisco Success Network と共有される具体的なテレメトリデータの詳細については、Cisco Success Network：テレメトリデータ （73ページ）を参照してください。



第 2 章

移行の準備

- Firewall 移行ツールに関する注意事項と制約事項 （9 ページ）
- Threat Defense デバイスに関する注意事項と制約事項 （11 ページ）
- Check Point 構成に関する注意事項と制約事項 （12 ページ）
- 移行がサポートされるプラットフォーム （18 ページ）
- 移行でサポートされるソフトウェアのバージョン （20 ページ）
- Firewall 移行ツールのプラットフォーム要件 （20 ページ）

Firewall 移行ツールに関する注意事項と制約事項

チェックポイント 構成

チェックポイント 構成は、次の要件を満たす必要があります。

- 移行でサポートされる チェックポイント 構成であること（移行がサポートされるプラットフォーム （18 ページ）を参照）。
- 移行でサポートされる チェックポイント バージョンであること（移行でサポートされるソフトウェアのバージョン （20 ページ）を参照）。

（オプション）ターゲット Threat Defense デバイス

Management Center 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追加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 Management Center 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、Management Center に追加する必要があります。

- ターゲット Threat Defense デバイスは、次の要件を満たす必要があります。
  - デバイスが、ハードウェアデバイスの注意事項を満たしている。次を参照： Threat Defense デバイスに関する注意事項と制約事項 （11 ページ）

- 移行のターゲットとしてサポートされるデバイス（移行がサポートされるプラットフォーム （18 ページ）を参照）。
- 移行でサポートされる Threat Defense 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 （20 ページ）を参照）。
- Management Center に登録されている Threat Defense デバイス。

Management Center

- 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 （20 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 Threat Defense 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]

ファイアウォール移行ツール

- Firewall 移行ツールの実行に使用するマシンが、要件を満たしていることを確認します（Firewall 移行ツールのプラットフォーム要件 （20 ページ）を参照）。
- Firewall 移行ツールでは、一括プッシュのバッチサイズを次の制限内で構成できます。

構成項目	バッチサイズ制限	デフォルト値
オブジェクト	500	50
ACL	1000	1000
NAT	1000	1000
ルート	1000	1000

> **注** オブジェクトの場合、API バッチサイズは 500 を超えることはできません。Firewall 移行ツールによって値が 50 にリセットされ、一括プッシュが続行されます。
>
> ACL、ルート、およびNATルールの場合、バッチサイズはそれぞれ 1000 を超えることはできません。Firewall 移行ツールによって値が 1000 にリセットされ、一括プッシュが続行されます。

バッチサイズ制限は、*<migration_tool_folder>*\app_config.txt にある app_config ファイルで設定できます。

> **注** 変更を適用するためにアプリケーションを再起動します。

- Firewall 移行ツールから構成のプッシュを開始した後は、移行が完了するまで、Management Center の構成を変更または更新しないでください。

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 Threat Defense に移行することを計画しているときに、次の注意事項と制限事項を考慮してください。

- ルート、インターフェイスなど、FTD に既存のデバイス固有構成がある場合、プッシュ移行中に 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 FTD）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、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、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。

- 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 Threat Defense 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 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。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 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。
  - サブインターフェイスは、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。

- Firewall 移行ツールは、 チェックポイント 構成に基づいて Threat Defense 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 Threat Defense 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 Threat Defense 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 Threat Defense 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、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。

Check Point 構成に関する注意事項と制約事項

変換中に、Firepower 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、Firepower 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。

Firepower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 Firepower Management Center 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 FTD 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、FMC 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、Firepower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。Firepower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、Firepower 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（Firepower Threat Defense へのダイナミックルーティングや VPN など）は、Firepower 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。
- FMC 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。
- Firepower Management Center 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。変換の一部として、Firepower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。

- Firepower 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 Firepower Management Center 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、Firepower 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、Firepower 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、Firepower 移行ツールは接続の終了時にロギングを構成します。

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
- 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、Firepower 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。Firepower 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、FMC 上の移行された ACE および NAT 構成の検証時に、FTD 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） Firepower 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

Firepower 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。Firepower 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、Firepower 移行ツールによって FMC 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

Firepower 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 Firepower 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

Firepower 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

移行がサポートされるプラットフォーム

ファイアウォール移行ツールを使用した移行では、次の チェックポイント および Firepower Threat Defense 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 Firepower Threat Defense プラットフォームの詳細については、『Cisco Firepower Compatibility Guide』を参照してください。

（注） ファイアウォール移行ツールは、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 Firepower Threat Defense 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 Firepower Threat Defense プラットフォーム

ファイアウォール移行ツールを使用して、Firepower Threat Defense 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

- 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
- Firepower Threat Defense Virtual （VMware 上）。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ていること

ファイアウォール移行ツールは、Firepower Threat Defense Virtual for Microsoft Azure Cloud への移行をサポートしています。

Azure における FTDv の前提条件と事前設定については、「Getting Started with Firepower Threat Defense Virtual and Azure」を参照してください。

ファイアウォール移行ツールは、Firepower Threat Defense Virtual for the AWS Cloud への移行をサポートしています。

AWS クラウドにおける FTDv の前提条件と事前設定については、「Firepower Threat Defense Virtual Prerequisites」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ファイアウォール移行ツールには、Microsoft Azure または AWS クラウド内の Firepower Management Center に接続し、構成をそのクラウド内の FMC 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、ファイアウォール移行ツールを使用する前に、FMC または FTD 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） ファイアウォール移行ツールには、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（ASA Live Connect）、手動でアップロードした構成をクラウド内の FMC に移行させたりします。そのため、前提条件として、ファイアウォール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。

移行でサポートされるソフトウェアのバージョン

以下は移行でサポートされている チェックポイント および Firepower Threat Defense バージョンです。

サポートされている Check Point のバージョン

ファイアウォール移行ツールは、Check Point OS バージョン r75 ～ r77.30 および r80 ～ r80.40 を実行している Firepower Threat Defense 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。

ファイアウォール移行ツールは、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 Firepower Management Center のバージョン

Check Point ファイアウォールの場合、ファイアウォール移行ツールは、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。

（注） 6.7 FTD 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 FMC 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 Firepower Threat Defense のバージョン

ファイアウォール移行ツールでは、 Firepower Threat Defense 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。

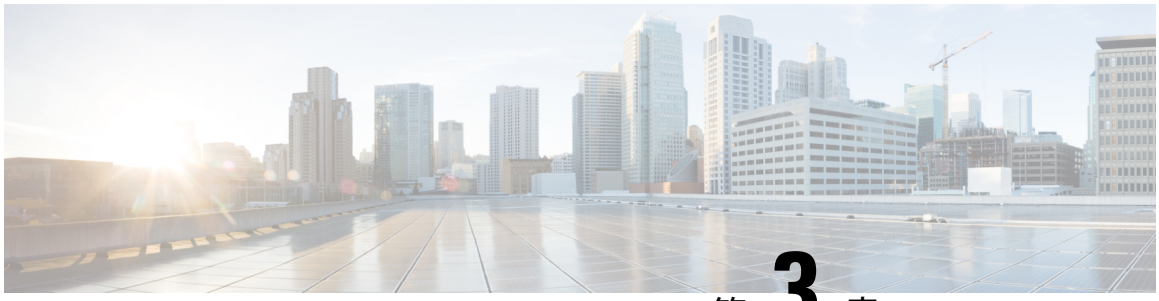
Firepower Threat Defense のオペレーティングシステムとホスティング環境の要件を含めた Cisco Firepower ソフトウェアとハードウェアの互換性の詳細については、『Cisco Firepower Compatibility Guide』を参照してください。

Firewall 移行ツールのプラットフォーム要件

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。

- 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）[パワーおよびスリープ（Power & Sleep）] で [スリープ（Sleep）] 設定が [PC をスリープにしない（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



第 3 章

移行の実行

- Cisco.com から Firewall 移行ツールのダウンロード （23 ページ）
- Firewall 移行ツールの起動 （24 ページ）
- Check Point 構成ファイルのエクスポート （26 ページ）
- Check Point 構成ファイルのアップロード （42 ページ）
- Firewall 移行ツールの接続先パラメータの指定 （43 ページ）
- 移行前レポートの確認 （45 ページ）
- チェックポイント 構成と Threat Defense インターフェイスのマッピング （47 ページ）
- セキュリティゾーン とインターフェイスグループへの チェックポイント インターフェイスのマッピング （49 ページ）
- 最適化、 移行する構成の確認と検証 （50 ページ）
- 移行された構成の以下へのプッシュ： Firepower Management Center （57 ページ）
- 移行後レポートの確認と移行の完了 （58 ページ）
- Firewall 移行ツールのアンインストール （61 ページ）

Cisco.com から Firewall 移行ツールのダウンロード

始める前に

Cisco.com へのインターネット接続が可能な Windows 10 64 ビットまたは macOS バージョン 10.13 以降のマシンが必要です。

ステップ 1 コンピュータで、Firewall 移行ツール用のフォルダを作成します。

このフォルダには、他のファイルを保存しないことをお勧めします。Firewall移行ツールを起動すると、ログ、リソース、およびその他すべてのファイルがこのフォルダに配置されます。

（注） Firewall移行ツールの最新バージョンをダウンロードする場合は、必ず新しいフォルダを作成し、既存のフォルダは使用しないでください。

ステップ 2 https://software.cisco.com/download/home/286306503/type を参照し、[Firewall 移行ツール（Firewall Migration Tool）] をクリックします。

上記のリンクをクリックすると、[Firewall NGFWバーチャル（Firewall NGFW Virtual）] の [Firewall移行ツール（Firewall Migration Tool）] に移動します。Firepower Threat Defense デバイスのダウンロード領域から Firewall 移行ツールをダウンロードすることもできます。

ステップ 3 Firewall 移行ツールの最新バージョンを、作成したフォルダにダウンロードします。

Windows 用または macOS マシン用の適切な Firewall 移行ツール実行可能ファイルをダウンロードします。

次のタスク

r77 の Check Point 構成ファイルのエクスポート

Firewall 移行ツールの起動

（注） Firewall 移行ツールを起動すると、別のウィンドウでコンソールが開きます。移行が進むのに合わせて、Firewall 移行ツールの現在のステップの進行状況がコンソールに表示されます。画面にコンソールが表示されない場合は、Firewall 移行ツールの背後にある可能性があります。

始める前に

- Cisco.com から Firewall 移行ツールのダウンロード
- Firewall 移行ツールに関する注意事項と制約事項 （9 ページ）セクションで要件を確認します。
- Firepower 移行ツールを実行するために、最新バージョンの Google Chrome ブラウザがコンピュータにインストールされていることを確認します。Google Chrome をデフォルトのブラウザとして設定する方法については、「Set Chrome as your default web browser」を参照してください。
- 大規模な構成ファイルを移行する場合は、移行プッシュ中にシステムがスリープ状態にならないようにスリープ設定を構成します。

ステップ 1 コンピュータで、Firewall 移行ツールをダウンロードしたフォルダに移動します。

ステップ 2 次のいずれかを実行します。

- Windows マシンで、Firewall 移行ツールの実行可能ファイルをダブルクリックして、Google Chrome ブラウザで起動します。

  プロンプトが表示されたら、[はい（Yes）] をクリックして、Firewall 移行ツールがシステムに変更を加えることができるようにします。

Firewall 移行ツールは、すべての関連ファイルを作成し、Firepower 移行ツールの存在するフォルダに保存します（ログおよびリソースのフォルダを含む）。

- Mac では、Firewall 移行ツールの `*.command` ファイルを目的のフォルダに移動し、ターミナルアプリケーションを起動して、Firewall 移行ツールがインストールされているフォルダを参照し、次のコマンドを実行します。

```
# chmod 750 Firewall_Migration_Tool-version_number.command
# ./Firewall_Migration_Tool-version_number.command
```

Firewall 移行ツールは、すべての関連ファイルを作成し、Firepower 移行ツールの存在するフォルダに保存します（ログおよびリソースのフォルダを含む）。

ヒント Firewall 移行ツールを開こうとすると、警告ダイアログが表示されます。これは、身元が明らかな開発者によって Firewall 移行ツールが Apple に登録されていないためです。身元不明の開発者によるアプリケーションを開く方法については、「Open an app from an unidentified developer」を参照してください。

（注） MAC のターミナルの zip メソッドを使用します。

ステップ 3 [エンドユーザライセンス契約（End User License Agreement）] ページで、テレメトリ情報をシスコと共有する場合は、[Cisco Success Network と情報を共有することに同意（I agree to share data with Cisco Success Network）] をクリックし、それ以外の場合は [後で行う（I'll do later）] をクリックします。

Cisco Success Network に統計を送信することに同意すると、Cisco.com アカウントを使用してログインするように求められます。Cisco Success Network に統計を送信しないことを選択した場合は、ローカルログイン情報を使用して Firewall 移行ツールにログインします。

ステップ 4 Firewall 移行ツールのログインページで、次のいずれかを実行します。

- Cisco Success Network と統計を共有するには、[CCO でログイン（Login with CCO）] リンクをクリックし、シングルサインオンログイン情報を使用して Cisco.com アカウントにログインします。

  （注） Cisco.com アカウントがない場合は、Cisco.com のログインページで作成します。

- 次のデフォルトログイン情報でログインします。
  - Username：admin
  - Password：Admin123

Cisco.com アカウントを使用してログインしている場合は、ステップ 8 に進みます。

ステップ 5 [パスワードのリセット（Reset Password）] ページで、古いパスワードと新しいパスワードを入力し、新しいパスワードを確認します。

新しいパスワードは 8 文字以上で、大文字と小文字、数字、および特殊文字を含める必要があります。

ステップ 6 [リセット（Reset）] をクリックします。

ステップ 7 新しいパスワードでログインします。

（注） パスワードを忘れた場合は、既存のすべてのデータを <*migration_tool_folder*> から削除し、Firewall 移行ツールを再インストールします。

ステップ 8 移行前チェックリストを確認し、記載されているすべての項目を完了していることを確認します。

チェックリストの項目を 1 つ以上完了していない場合は、完了するまで続行しないでください。

ステップ 9 [新規移行（New Migration）] をクリックします。

ステップ 10 [ソフトウェアアップデートの確認（Software Update Check）] 画面で、Firewall 移行ツールの最新バージョンを実行しているかどうかが不明な場合は、リンクをクリックし、Cisco.com でバージョンを確認します。

ステップ 11 [続行（Proceed）] をクリックします。

次のタスク

次のステップに進むことができます。

- Check Point 構成をコンピュータにエクスポートした場合は、「Check Point 構成ファイルのアップロード」に進みます。
- Firewall 移行ツールを使用して Check Point（r77）から情報を抽出する必要がある場合は、「r77 の Check Point 構成ファイルのエクスポート」に進みます。
- Firewall 移行ツールを使用して Check Point（r80）から情報を抽出する必要がある場合は、「r80 の Check Point 構成ファイルのエクスポート」に進みます。

Check Point 構成ファイルのエクスポート

次の Check Point 構成をエクスポートできます。

- r77 の Check Point 構成ファイルのエクスポート
- r80 の Check Point 構成ファイルのエクスポート

r77 の Check Point 構成ファイルのエクスポート

r77 の Check Point 構成ファイルをエクスポートするには、次の手順を実行します。

- Check Point Web Visualization Tool（WVT）を使用した構成のエクスポート
- FMT-CP-Config-Extractor_v2.5.2-6575 ツールを使用したデバイス構成のエクスポート （28 ページ）
- エクスポートされたファイルの圧縮

Check Point Web Visualization Tool（WVT）を使用した構成のエクスポート

ステップ 1 Check Point Management Server にアクセスできるワークステーションでコマンドプロンプトを開きます。

ステップ 2 Check Point Firewall バージョンに適した Check Point Portal から WVT をダウンロードします。

ステップ 3 WVT zip ファイルを解凍します。

ステップ 4 Check Point WVT ツールが抽出された同じルートフォルダの下に新しいサブフォルダを作成します。

ステップ 5 コマンドプロンプトで、ディレクトリを WVT が保存されているディレクトリに変更し、次のコマンドを実行します。

```
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]
```

次に例を示します。

```
C:\Web_Visualisation_Tool> cpdb2web.exe -s 172.16.0.1  -u admin -p admin123 -o  Outputs
```

次のコマンドを実行すると、合計 7 つのファイルが Outputs ディレクトリに作成されます。

コマンド	説明
C:\Web_Visualisation_Tool	WVT ツールのルートディレクトリ。
172.16.0.1	Check Point Management Server の IP アドレス。
admin	Check Point Management Server のユーザ名。
Admin123	Check Point Management Server のパスワード。
出力	出力ファイルを保存する相対パス。

（注） セキュリティポリシーおよびNATポリシーファイルの名前は、それぞれ `Security_Policy.xml` および `NAT_Policy.xml` である必要があります。ファイル名が異なる場合は、手動で名前を変更します。

複数のセキュリティおよび NAT ポリシーファイルがある場合は、移行する Check Point デバイスの `Security_Policy.xml` および `NAT_Policy.xml` ファイルのみを選択して保持してください。

次のタスク

FMT-CP-Config-Extractor_v2.5.2-6575 ツールを使用したデバイス構成のエクスポート

FMT-CP-Config-Extractor_v2.5.2-6575 ツールを使用したデバイス構成のエクスポート

ステップ 1 Cisco Firepower 移行ツールのソフトウェア ダウンロード ページから FMT-CP-Config-Extractor_v2.5.2-6575.exe をダウンロードします。

ステップ 2 Check Point Security Gateway 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_v2.5.2-6575 ツールを開きます。

ステップ 3 Firepower 移行ツールを使用してポリシーを移行する Check Point Security Gateway に接続します。

接続するには、次の情報が必要です。

a) [IPアドレス（IP Address）]
b) ポート
c) [ユーザ名（Username）]
d) [パスワード（Password）]

ステップ 4 FMT-CP-Config-Extractor_v2.5.2-6575 ツールから取得した出力ファイルの名前を `networking.txt` ファイルに変更します。

次のコマンドが、FMT-CP-Config-Extractor_v2.5.2-6575 ツールによって実行されます。

- **show hostname**
- **show version product**
- **show interfaces**
- **fw vsx stat**
- **show management interface**
- **show configuration bonding**
- **show configuration bridging**
- **show configuration interface**
- **show configuration static-route**
- **show ipv6-state**
- **show configuration ipv6 static-route**
- **netstat -rnv**

すべてのコマンドは FMT-CP-Config-Extractor_v2.5.2-6575 ツールによってバックグラウンドで実行され、出力は .txt ファイルとして保存されます。

たとえば、172.16.0.1 は、ポリシーを移行する Check Point Firewall Gateway の IP アドレスです。

ステップ 5 .txt ファイルを `Outputs` フォルダに移動します。

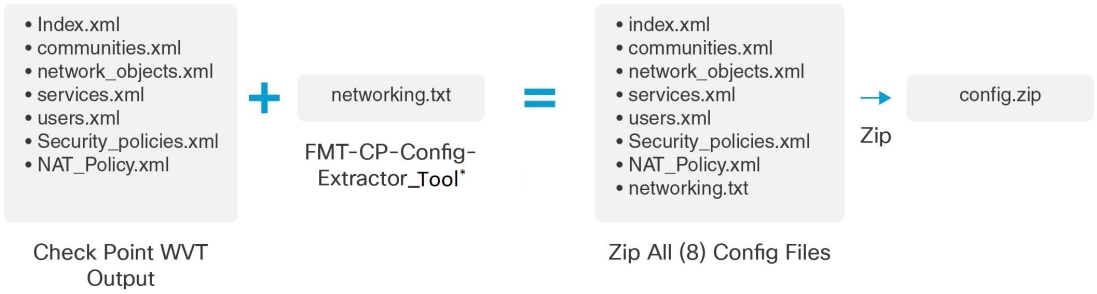
次のタスク

エクスポートされたファイルの圧縮

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 Visualization Tool（WVT）からの 7 つのファイルと、FMT-CP-Config-Extractor_v2.5.2-6575 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。

（注） 移行用のファイルを圧縮する前に、`Security_Policy.xml` および `NAT_Policy.xml` のファイルが FTD に移行する Check Point デバイス用であることを確認します。



*Check Point エクストラクタのバージョン：FMT-CP-Config-Extractor_v2.5.2-6575

（注） .tar またはその他の圧縮ファイルタイプはサポートされていません。

次のタスク

Check Point 構成ファイルのアップロード

r80 の Check Point 構成ファイルのエクスポート

（注） Check Point r80 構成のエクスポートは、Firepower 移行ツールの Live Connect 機能でのみサポートされます。

Check Point デバイスで移行のために必要なログイン情報を構成したり、Check Point 構成ファイルをエクスポートしたりするには、次の手順を実行します。

- Live Connect を使用した構成抽出のための Check Point（r80）デバイスの事前設定
- r80 の Check Point 構成ファイルをエクスポートする手順

Live Connect を使用した構成抽出のための Check Point（r80）デバイスの事前設定

次のいずれかの手順を使用して、移行前に Check Point（r80）デバイスでログイン情報を構成できます。

- 分散 Check Point 展開からのエクスポート：Check Point Security Gateway と Check Point Security Manager が別々にある場合。
- スタンドアロン Check Point 展開からのエクスポート：Check Point Security Gateway と Check Point Security Manager が単一デバイス上にある場合。
- マルチドメイン Check Point 展開からのエクスポート：Check Point Security Gateway と Check Point Security Manager がマルチドメイン設定されている場合。

分散 Check Point 展開からのエクスポート

Check Point 設定を抽出するには、Firepower 移行ツールの Live Connect を使用する前に、Check Point（r80）デバイスでログイン情報を設定する必要があります。

分散 Check Point 展開でのログイン情報事前設定手順には、次のステップが含まれます。

ステップ 1 Gaia Console Check Point Security Gateway で、次を作成します。

a) Web ブラウザで、HTTPS セッション経由で Check Point Gaia Console アプリケーションを開き、Check Point Security Gateway に接続します。

b) [ユーザ管理（User Management）] タブに移動し、**[ユーザ（Users）]** > **[追加（Add）]**を選択します。

c) [ユーザの追加（Add User）] ウィンドウで、次の詳細を使用して新しいユーザ名とパスワードを作成します。

- [シェル（Shell）] ドロップダウンから、*/etc/cli.sh* を選択します。
- [利用可能なロール（Available Roles）] から、*adminRole* を選択します。
- 残りのフィールドはデフォルト値のままにします。
- [OK] をクリックします。

d) Check Point Security Gateway に SSH 接続し、次のコマンドを使用して新しいパスワードを作成します。
set expert-password <password>

（注）
- Check Point デバイスでエキスパートパスワードをすでに設定している場合は、それを再利用します。
- 手順 3 に示すように、[Check Point Security Gateway に接続（Connect to Check Point Security Gateway）] ページでこれらのログイン情報が必要となります。

エキスパートパスワードを構成したら、Check Point r80 Gateway でのログイン情報の事前設定が完了します。

詳細については、図 3 : Check Point Security Gateway への接続 を参照してください。

ステップ 2 r80 の Check Point Security Manager でユーザ名とパスワードを作成します。

a) SmartConsole アプリケーションで、次の手順を実行します。

1. Check Point Security Manager にログインします。
2. **[管理と設定（Manage and Settings）] > [権限と管理者（Permissions and Administrators）] > [管理者（Administrators）]**に移動します。
3. ***** をクリックして新しいユーザ名とパスワードを作成し、次の手順を実行します。
   - [認証方式（Authentication Method）] に [Check Point パスワード（Check Point Password）] を選択します。
   - [新しいパスワードを設定（Set New Password）] をクリックして、新しいパスワードを設定します。

     （注） [ユーザは次回ログイン時にパスワードの変更が必要（User Must Change Password on the Next Login）] チェックボックスはオンにしないでください。

   - [権限プロファイル（Permission Profile）] に [スーパーユーザ（Super User）] を選択します。
   - [有効期限（Expiration）] に [なし（Never）] を選択します。
4. [パブリッシュ（Publish）] をクリックして、Check Point SmartConsole アプリケーションの構成変更を保存します。

b) Check Point Security Manager の Gaia Console で、次の手順を実行します。

（注） ここで作成するユーザ名とパスワードは、ステップ 2a で SmartConsole アプリケーションで作成したものと同じであること確認してください。

1. Web ブラウザで、HTTPS セッション経由で Gaia Console アプリケーションを開き、Check Point Security Manager に接続します。
2. [ユーザ管理（User Management）] タブに移動し、**[ユーザ（Users）] > [追加（Add）]**を選択します。
3. SmartConsole アプリケーションのステップ 2a（3）で作成したものと同じユーザ名とパスワードを作成します。
   - [シェル（Shell）] ドロップダウンから、*/bin/bash* を選択します。
   - [利用可能なロール（Available Roles）] ドロップダウンから、*adminRole* を選択します。
   - 残りのフィールドはデフォルト値のままにします。
   - [OK] をクリックします。
4. Check Point Security Manager に SSH 接続し、次のコマンドを使用してエキスパートパスワードを作成します。

   set expert-password <password>

（注）
- エキスパートパスワードをすでに設定している場合は、そのパスワードを使用できます。
- ステップ 2b（3）とステップ 2a（3） で作成したユーザ名とパスワードは同じである必要があります。

分散展開の Check Point での、Check Point Security Manager のログイン情報の事前設定が完了しました。

手順 4 に示すように、[Check Point Security Manager に接続（Connect to Check Point Security Manager）] ページでこれらのログイン情報が必要となります。

Check Point Smart Manager でカスタム API ポートを使用している場合は、「Check Point（r80）Security Manager にカスタム API ポートを使用しますか。」を参照してください。

次のタスク

r80 の Check Point 構成ファイルをエクスポートする手順

スタンドアロン Check Point 展開からのエクスポート

Check Point 設定を抽出するには、Firepower 移行ツールの Live Connect を使用する前に、Check Point（r80）デバイスでログイン情報を設定する必要があります。

スタンドアロン Check Point 展開でのログイン情報事前設定手順には、次のステップが含まれます。

ステップ 1 Web ブラウザで、Gaia Console アプリケーションを開き、Check Point Security Gateway と Check Point Security Manager の両方を管理するスタンドアロン Check Point デバイスに接続します。

ステップ 2 [ユーザ管理（User Management）] タブに移動し、**[ユーザ（Users）] > [追加（Add）]**を選択します。

a) [ユーザの追加（Add User）] ウィンドウで、次の詳細を使用して新しいユーザ名とパスワードを作成します。
- [シェル（Shell）] ドロップダウンから、*/etc/cli.sh* を選択します。
- [利用可能なロール（Available Roles）] ドロップダウンから、*adminRole* を選択します。
- 残りのフィールドはデフォルト値のままにします。
- [OK] をクリックします。

手順 3 に示すように、[Check Point Security Gateway に接続（Connect to Check Point Security Gateway）] ページでこれらのログイン情報が必要となります。

詳細については、図 3 : Check Point Security Gateway への接続 を参照してください。

b) [ユーザの追加（Add User）] ウィンドウで、次の詳細を使用して別のユーザ名とパスワードを作成します。

- [シェル（Shell）] ドロップダウンから、*/bin/bash* を選択します。
- [利用可能なロール（Available Roles）] ドロップダウンから、*adminRole* を選択します。
- 残りのフィールドはデフォルト値のままにします。
- [OK] をクリックします。

ステップ 3 Check Point デバイス上の r80 用 SmartConsole アプリケーションで、次を作成します。

（注） ここで作成するユーザ名とパスワードは、前のステップで Check Point Gaia Console で作成したものと同じであること確認してください。

a) Check Point デバイスの SmartConsole アプリケーションにログインします。
b) **[管理と設定（Manage and Settings）] > [権限と管理者（Permissions and Administrators）] > [管理者（Administrators）]**に移動します。
c) ***** をクリックして、次の詳細を使用して新しいユーザ名とパスワードを作成します。
   - [認証方式（Authentication Method）] に [Check Point パスワード（Check Point Password）] を選択します。
   - [新しいパスワードを設定（Set New Password）] をクリックして、新しいパスワードを設定します。

     （注） [ユーザは次回ログイン時にパスワードの変更が必要（User Must Change Password on the Next Login）] チェックボックスはオンにしないでください。

   - [権限プロファイル（Permission Profile）] に[スーパーユーザ（Super User）] を選択します。
   - [有効期限（Expiration）] に [なし（Never）] を選択します。

   ステップ 2 のステップ b とステップ 3 のステップ c で作成したユーザ名とパスワードは同じである必要があります。

   手順 4 に示すように、[Check Point Security Manager に接続（Connect to Check Point Security Manager）] ページでこれらのログイン情報が必要となります。
d) [パブリッシュ（Publish）] をクリックして、Check Point SmartConsole アプリケーションの構成変更を保存します。

ステップ 4 Check Point デバイスに SSH 接続し、次のコマンドを使用してエキスパートパスワードを作成します。

set expert-password <password>

（注）
- Check Point デバイスでエキスパートパスワードをすでに設定している場合は、それを再利用します。
- ステップ 2 のステップ b とステップ 3 のステップ c で作成したユーザ名とパスワードは同じである必要があります。

スタンドアロン展開の Check Point デバイスでのログイン情報の事前設定が完了しました。

Check Point Smart Manager でカスタム API ポートを使用している場合は、「Check Point（r80）Security Manager にカスタム API ポートを使用しますか。」を参照してください。

次のタスク

r80 の Check Point 構成ファイルをエクスポートする手順

マルチドメイン Check Point 展開からのエクスポート

Check Point 構成を取得するには、Firepower 移行ツールの Live Connect を使用して、Check Point（r80）デバイスでログイン情報を設定する必要があります。

マルチドメイン Check Point 展開でのログイン情報事前設定手順には、次のステップが含まれます。

ステップ 1 Gaia Console Check Point Security Gateway で、次を作成します。

a) Web ブラウザで、HTTPS セッション経由で Gaia Console アプリケーションを開き、Check Point Security Gateway に接続します。

b) [ユーザ管理（User Management）] タブに移動し、**[ユーザ（Users）]** > **[追加（Add）]**を選択します。

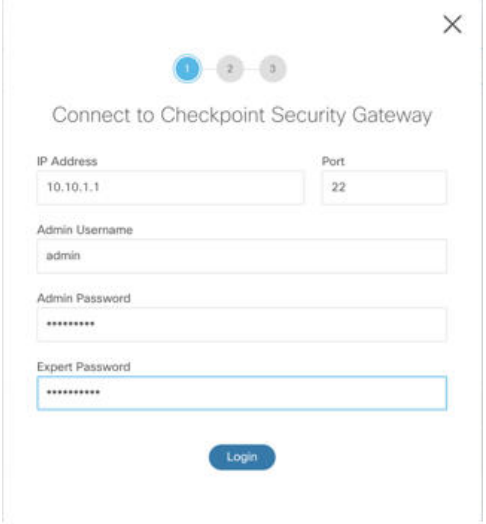
c) [ユーザの追加（Add User）] ウィンドウで、次の詳細を使用して新しいユーザ名とパスワードを作成します。

- [シェル（Shell）] ドロップダウンから、*/etc/cli.sh* を選択します。
- [利用可能なロール（Available Roles）] ドロップダウンから、*adminRole* を選択します。
- 残りのフィールドはデフォルト値のままにします。
- [OK] をクリックします。

d) Check Point Security Gateway に SSH 接続し、次のコマンドを使用して新しいパスワードを作成します。
set expert-password <password>

Check Point Security Gateway でのマルチドメイン展開用のログイン情報の事前設定が完了しました。

図 *1 : Checkpoint Security Gateway* への接続：マルチドメイン展開



ステップ 2 Check Point Security Manager でユーザ名とパスワードを作成します。

a) SmartConsole（mds）アプリケーションで、次の手順を実行します。

1. Check Point Security Manager にログインします。
2. **[管理と設定（Manage and Settings）] > [権限と管理者（Permissions and Administrators）] > [管理者（Administrators）]**に移動します。
3. ***** をクリックして、次の詳細を使用して新しいユーザ名とパスワードを作成します。
   - [認証方式（Authentication Method）] に [Check Point パスワード（Check Point Password）] を選択します。
   - [新しいパスワードを設定（Set New Password）] をクリックして、新しいパスワードを設定します。

     （注） [ユーザは次回ログイン時にパスワードの変更が必要（User Must Change Password on the Next Login）] チェックボックスはオンにしないでください。

   - [権限プロファイル（Permission Profile）] に[マルチドメインスーパーユーザ（Multi-domain Super User）] を選択します。
   - [有効期限（Expiration）] に [なし（Never）] を選択します。
4. [パブリッシュ（Publish）]をクリックして、Check Point SmartConsole アプリケーションの構成変更を保存します。

   Check Point Smart Manager でカスタム API ポートを使用している場合は、「Check Point（r80）Security Manager にカスタム API ポートを使用しますか。」を参照してください。

b) Check Point Security Manager の Gaia Console で、次の手順を実行します。

（注） ここで作成するユーザ名とパスワードは、ステップ 2a（3） で SmartConsole アプリケーションで作成したものと同じであること確認してください。

1. Web ブラウザで、HTTPS セッション経由で Gaia Console アプリケーションを開き、Check Point Security Manager に接続します。
2. [ユーザ管理（User Management）] タブに移動し、**[ユーザ（Users）]** > **[追加（Add）]**を選択します。
3. ステップ 2a（3） で SmartConsole アプリケーションで作成したものと同じユーザ名とパスワードを作成します。
   - [シェル（Shell）] ドロップダウンから、*/bin/bash* を選択します。
   - [利用可能なロール（Available Roles）] ドロップダウンから、*adminRole* を選択します。
   - 残りのフィールドはデフォルト値のままにします。
   - [OK] をクリックします。
4. Check Point Security Manager に SSH 接続し、次のコマンドを使用して新しいパスワードを作成します。

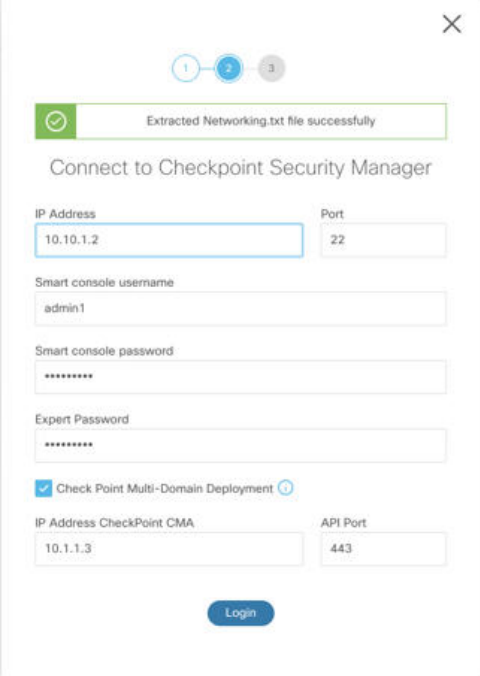
   set expert-password <password>

   （注）
   - Check Point デバイスでエキスパートパスワードをすでに設定している場合は、それを再利用します。
   - ステップ 2a（3） とステップ 2b（3） で作成したユーザ名とパスワードは同じである必要があります。

マルチドメイン展開の Check Point Security Manager でのログイン情報の事前設定が完了しました。

Live Connectに接続するには、図 2 : Checkpoint Security Manager への接続：マルチドメイン展開のようにログイン情報が必要です。

図 *2 : Checkpoint Security Manager* への接続：マルチドメイン展開



（注）
- Check Point Smart Manager でカスタム API ポートを使用している場合は、「Check Point（r80）Security Manager にカスタム API ポートを使用しますか。」を参照してください。
- マルチドメイン展開用のグローバル ポリシー パッケージは取得できません。したがって、Check Point CMA の構成の一部として構成されたオブジェクト、ACE ルール、および NAT ルールは、エクスポートおよび移行のみ行われます。

次のタスク

r80 の Check Point 構成ファイルをエクスポートする手順

Check Point（r80）Security Manager にカスタム API ポートを使用しますか。

（注） Check Point Smart Manager でカスタム API ポートを使用している場合は、次の手順を実行します。

- [Check Point Security Manager] ページの [Check Point マルチドメイン展開（Check Point Multi-domain Deployment）] チェックボックスをオンにします。
- マルチドメイン展開を使用している場合は、Check Point CMA のIP アドレスと API ポートの詳細を追加します。
- 一般的な展開の Check Point Security Manager の場合、Check Point Security Manager の IPアドレスを保持し、カスタム API ポートの詳細を入力します。

r80 の Check Point 構成ファイルをエクスポートする手順

始める前に

Check Point デバイスで以下を事前設定する必要があります。移行前に Check Point（r80）デバイスでログイン情報を構成する詳細については、「Live Connect を使用した構成抽出のための Check Point（r80）デバイスの事前設定」を参照してください。

（注）

- Live Connect を使用して Check Point（r80）構成を抽出することを推奨します。
- Firepower 移行ツールで構成されていない Check Point（r80）構成を使用すると、構成がサポート対象外として移行されたり、部分的に移行されたり、移行が失敗したりします。

  構成のエクスポートの情報が不完全な場合、特定の構成は移行されず、**サポート対象外**としてマークされます。

r80 の Check Point 構成ファイルをエクスポートするには、次の手順を実行します。

ステップ 1 [Select Source Config] ページから [Check Point (r80)] を選択します。

ステップ 2 [接続（Connect）] をクリックします。

（注） Live Connect は、Check Point（r80）でのみ使用できます。

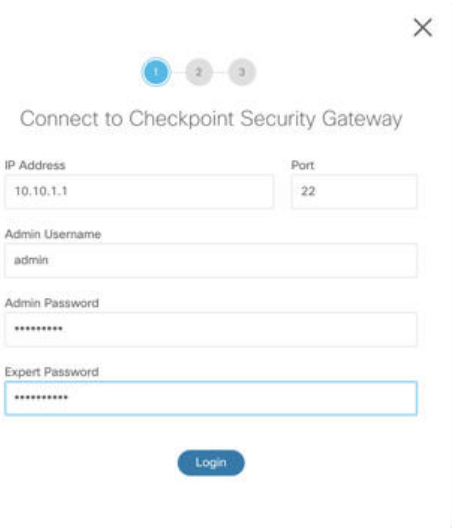
ステップ 3 Check Point Security Gateway に接続します。次の手順を実行します。

a) Check Point r80 Security Gateway に次のように入力します。

- IP アドレス
- SSH ポート
- Admin Username

- Admin Password
- エキスパートパスワード

図 *3 : Check Point Security Gateway* への接続



b) [ログイン（Login）] をクリックします。

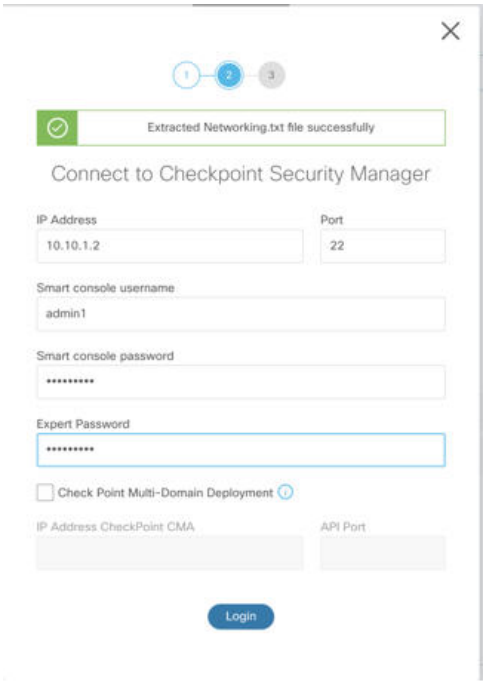
Firepower 移行ツールは、インターフェイス構成やルート構成などのデバイス固有の構成を含む networking.txt ファイルを生成します。Firepower 移行ツールの現在のセッションのローカルディレクトリに networking.txt ファイルを保存します。

ステップ 4 Check Point Security Manager に接続します。次の手順を実行します。

a) Check Point r80 Security Manager に次のように入力します。

- IP アドレス
- SSH ポート
- スマートコンソールのユーザ名
- スマートコンソールのパスワード
- エキスパートパスワード

図 *4 : Check Point Security Manager* への接続



b) [ログイン（Login）] をクリックします。

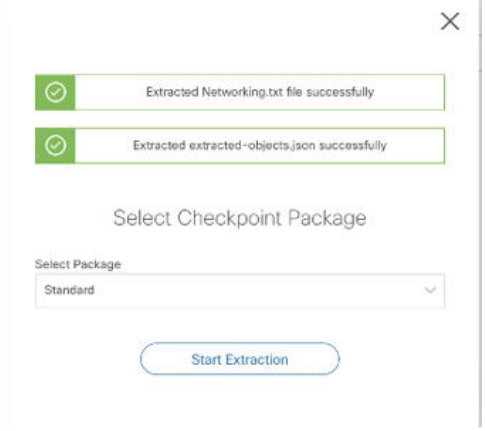
Firepower 移行ツールは、Check Point Security Manager で使用可能な完全なネットワークおよびサービスオブジェクト構成をキャプチャする Extracted-objects.json ファイルを生成します。

Firepower 移行ツールの現在のセッションのローカルディレクトリに Extracted-objects.json ファイルを保存します。

（注） Firepower 移行ツールを Check Point Security Manager に接続している場合は、Check Point Security Manager で使用可能なポリシーパッケージのリストが表示されます。

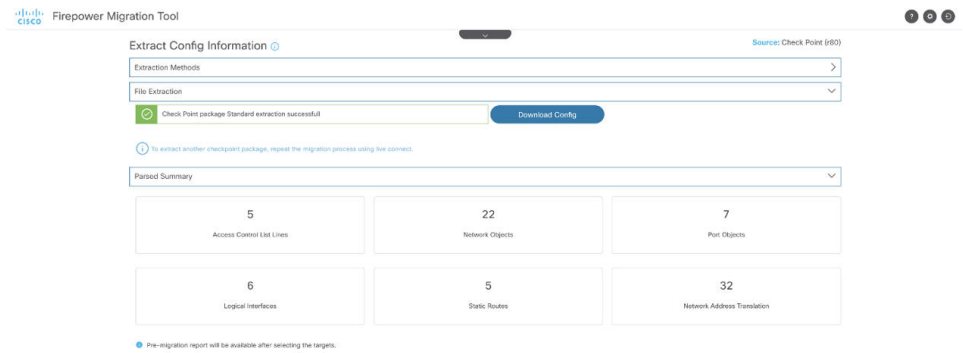
ステップ 5 [Select Check Point Package] リストから移行する Check Point ポリシーパッケージを選択し、[Start Extraction] をクリックします。

図 *5* : *Check Point* ポリシーパッケージの抽出



ステップ 6 構成をダウンロードし、移行を続行します。

図 *6* : 分散展開およびスタンドアロン展開の完全な *Check Point* 構成の抽出



ステップ 7 [Next] をクリックして、Check Point（r80）構成の移行を続行します。

次のタスク

Check Point 構成ファイルのアップロード

別の構成ファイルの取得

別の構成ファイルを取得するには、次の手順を実行します。

- 別のポリシーパッケージの新しい構成を取得するか、別の Check Point（r80）ファイアウォールに接続するには、[送信元の選択に戻る（Back to source selection）] をクリックします。
- 取得した Check Point（r80）構成を後で移行する必要がある場合は、現在の構成をダウンロードします。

注　現在の構成ファイルは、ブラウザで設定されているデフォルトのダウンロード場所にダウンロードされます。

組立てラインアプローチを使用して、r80 構成を取得できます。

- Live Connect を実行して、ファイアウォールの各パッケージまたはさまざまなファイアウォールの Check Point（r80）構成ファイルを取得します。
- 複数の構成のリポジトリを作成します。
- 後で手動アップロードを使用して移行を続行するには、[後で移行を開始（Start Migration later）] オプションを使用します。

Check Point 構成ファイルのアップロード

始める前に

構成ファイルを .zip 形式でエクスポートします。

ステップ 1 [Extract Config Information] 画面の [Manual Upload] セクションで、[Upload] をクリックして Check Point 構成ファイルをアップロードします。

ステップ 2 構成ファイルが保存されている場所を参照します。Check Point（r77）の構成ファイルが抽出され、Check Point（r80）の Live Connect を使用してダウンロードされます。[開く（Open）] をクリックします。

Firepower 移行ツールが構成ファイルをアップロードします。大規模な構成ファイルの場合、この手順には時間がかかります。

これで、解析前プロセスが完了しました。

[Parsed Summary] セクションに解析ステータスが表示されます。

ステップ 3 アップロードされた構成ファイルで、Firepower 移行ツールが検出および解析した要素の概要を確認します。

ステップ 4 [Next] をクリックして、ターゲットパラメータを選択します。

次のタスク

Firewall 移行ツールの接続先パラメータの指定

Firewall 移行ツールの接続先パラメータの指定

始める前に

- IP アドレスの取得： Firepower Management Center
- （任意）インターフェイスやルートなどのデバイス固有の構成を移行する場合は、ターゲット Firepower Threat Defense デバイスを Firepower Management Center に追加します。「Adding Devices to the Firewall Management Center」を参照してください。
- [Review and Validate] ページで IPS またはファイルポリシーを ACL に適用する必要がある場合は、移行前に FMC でポリシーを作成することを強くお勧めします。Firewall 移行ツールは接続された FMC からポリシーを取得するため、同じポリシーを使用します。新しいポリシーを作成して複数のアクセス制御リストに割り当てると、パフォーマンスが低下し、プッシュが失敗する可能性があります。

ステップ 1 [ターゲットの選択（Select Target）] 画面の [Firewall Management Centerに接続（Connect to Firewall Management Center）] セクションで、Firepower Management Center の IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。

ステップ 2 [Domain] ドロップダウンリストで、移行先のドメインを選択します。

Firepower Threat Defense デバイスに移行する場合は、選択したドメインで使用可能な Firepower Threat Defense デバイスにのみ移行できます。

ステップ 3 [接続（Connect）] をクリックします。

ステップ 4 [Firewall Management Centerへのログイン（Firewall Management Center Login）] ダイアログボックスで、Firewall 移行ツール専用アカウントのユーザー名とパスワードを入力し、[ログイン（Login）] をクリックします。

Firewall 移行ツールは Firepower Management Center にログインし、その Firepower Management Center による管理対象 Firepower Threat Defense デバイスのリストを取得します。この手順の進行状況はコンソールで確認できます。

ステップ 5 [続行（Proceed）] をクリックします。

ステップ 6 [Choose FTD] セクションで、次のいずれかを実行します。

- [Firewall Threat Defenseデバイスの選択（Select Firewall Threat Defense Device）] ドロップダウンリストをクリックし、 チェックポイント 構成を移行するデバイスをオンにします。

  選択した Firepower Management Center ドメイン内のデバイスが、**IP アドレス**と**名前**でリストされます。

（注） 少なくとも、選択するネイティブ Firepower Threat Defense デバイスには、移行する チェックポイント 構成と同じ数の物理インターフェイスまたはポート チャネル インターフェイスが必要です。少なくとも、Firepower Threat Defense デバイスのコンテナインスタンスには、同じ数の物理インターフェイスまたはポート チャネル インターフェイスとサブインターフェイスが必要です。チェックポイント 構成と同じファイアウォールモードでデバイスを設定する必要があります。 ただし、これらのインターフェイスは、両方のデバイスで同じ名前である必要はありません。

リモート展開が有効になっている FMC/FTD 6.7 以降への Check Point ファイアウォールの移行は、Firewall 移行ツールでサポートされています。インターフェイスとルートの移行は手動で行う必要があります。

- [FTD を使用せず続行（Proceed without FTD）] をクリックして、構成を Firepower Management Center に移行します。

  FTD なしで続行すると、Firewall 移行ツールは FTD に構成またはポリシーをプッシュしません。したがって、Firewall Threat Defense のデバイス固有の構成であるインターフェイスとルート、およびサイト間 VPN は移行されません。ただし、NAT、ACL、ポートオブジェクトなど、サポートされている他のすべての構成（共有ポリシーとオブジェクト）は移行されます。

ステップ 7 [続行（Proceed）] をクリックします。

移行先に応じて、Firewall 移行ツールを使用して移行する機能を選択できます。

ステップ 8 [機能の選択（Select Features）] セクションをクリックして、移行先に移行する機能を確認して選択します。

- 接続先 Firepower Threat Defense デバイスに移行する場合、Firewall 移行ツールは、[デバイス設定（Device Configuration）] セクションと [共有設定（Shared Configuration）] セクションで、 チェックポイント 構成から移行できる機能を自動的に選択します。要件に応じて、デフォルトの選択をさらに変更できます。
- Firepower Management Center に移行する場合、Firewall 移行ツールは、[共有設定（Shared Configuration）] セクションで、チェックポイント 構成から移行できる機能を自動的に選択します。要件に応じて、デフォルトの選択をさらに変更できます。

  （注） [デバイスの構成（Device Configuration）] セクションは、移行先 Firepower Threat Defense デバイスを選択していない場合は使用できません。

- Check Point の場合は、[Shared Configuration] で、関連する [Access Control] オプションを選択します。
  - 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ダイナミックルート（PBR と NAT は考慮されません）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。

ルーティング情報は、`networking.txt` ファイルから取得されます。このファイルは、**netstat -rnv** コマンドを使用してルーティングテーブルを収集する FMT-CP-Config-Extractor_v2.5.2-6575 ツールの出力です。詳細については、「FMT-CP-Config-Extractor_v2.5.2-6575 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。

このリリースでは、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。グローバルポリシーまたはゾーンベースポリシーのすべてのルールが正常に移行されていることを確認します。

- （任意）[Optimization] セクションで、[Migrate only referenced objects] を選択して、アクセス コントロール ポリシーと NAT ポリシーで参照されているオブジェクトのみを移行します。

  （注） このオプションを選択すると、チェックポイント構成内の参照されていないオブジェクトは移行されません。これにより、移行時間が最適化され、未使用のオブジェクトが構成から消去されます。

ステップ 9 [続行（Proceed）] をクリックします。

ステップ 10 [Rule Conversion/ Process Config] セクションで、[Start Conversion] をクリックして変換を開始します。

ステップ 11 Firewall 移行ツールによって変換された要素の概要を確認します。

構成ファイルが正常にアップロードおよび解析されたかどうかを確認するには、移行を続行する前に**移行前レポート**をダウンロードして確認します。

ステップ 12 [レポートのダウンロード（Download Report）] をクリックし、**移行前レポート**を保存します。

移行前レポートのコピーも、Firewall 移行ツールと同じ場所にある `Resources` フォルダに保存されます。

次のタスク

移行前レポートの確認 （45 ページ）

移行前レポートの確認

（注） ファイアウォール移行ツールによって解析されない構成は、**移行前レポート**で送信元構成ファイルと同じ XML（r75 ～ r77.30）または json（r80）タグで示されます。

移行中に移行前レポートをダウンロードし忘れた場合は、次のリンクを使用してダウンロードしてください。

移行前レポートのダウンロードエンドポイント：http://localhost:8888/api/downloads/pre_migration_summary_html_format

（注） レポートは、ファイアウォール移行ツールの実行中にのみダウンロードできます。

ステップ 1 移行前レポートをダウンロードした場所に移動します。

移行前レポートのコピーも、ファイアウォール移行ツールと同じ場所にある `Resources` フォルダに保存されます。

ステップ 2 移行前レポートを開き、その内容を慎重に確認して、移行が失敗する原因となる問題を特定します。

移行前レポートには、次の情報が含まれています。

- Overall Summary：Check Point 構成情報を抽出するため、または CP に手動アップロードするために使用される方法。

  Firepower Threat Defense に正常に移行できるサポート対象 チェックポイント 構成要素と、移行対象として選択された特定の チェックポイント 機能のサマリー。

- Configuration Lines with Errors：ファイアウォール移行ツールが解析できなかったために正常に移行できない チェックポイント 構成要素の詳細。 チェックポイント 構成でこれらのエラーを修正し、新しい構成ファイルをエクスポートしてから、新しい構成ファイルを ファイアウォール移行ツールにアップロードし、続行してください。

- Partially Supported Configuration：部分的にのみ移行可能な チェックポイント 構成要素の詳細。これらの構成要素には、詳細オプションを含むルールとオブジェクトが含まれているため、詳細オプションを使用せずにルールまたはオブジェクトを移行できます。これらの行を確認し、詳細オプションが Firepower Management Center でサポートされているかどうかを確認します。サポートされている場合は、ファイアウォール移行ツールを使用して移行を完了した後に、これらのオプションを手動で構成することを計画します。

- Unsupported Configuration：ファイアウォール移行ツールがこれらの機能の移行をサポートしていないため、移行できない チェックポイント 構成要素の詳細。これらの行を確認し、各機能が Firepower Management Center でサポートされているかどうかを確認します。サポートされている場合は、ファイアウォール移行ツールを使用して移行を完了した後に、機能を手動で構成することを計画します。

- Ignored Configuration： Firepower Management Center または ファイアウォール移行ツールでサポートされていないために無視される チェックポイント 構成要素の詳細。 ファイアウォール移行ツールはこれらの行を解析しません。これらの行を確認し、各機能が Firepower Management Center でサポートされているかどうかを確認します。サポートされている場合は、機能を手動で構成することを計画します。

Firepower Management Center および Firepower Threat Defense でサポートされる機能の詳細については、『Firepower Management Center Configuration Guide』を参照してください。

ステップ 3 **移行前レポート**で修正措置が推奨されている場合は、チェックポイント インターフェイス で修正を完了し、チェックポイント構成ファイルを再度エクスポートしてから、更新された構成ファイルをアップロードし、続行してください。

ステップ 4 チェックポイント 構成ファイルが正常にアップロードおよび解析されたら、ファイアウォール移行ツールに戻り、[次へ（Next）] をクリックして移行を続行します。

次のタスク

チェックポイント 構成と Threat Defense インターフェイスのマッピング

チェックポイント 構成と Threat Defense インターフェイスのマッピング

Firepower Threat Defense デバイスには、チェックポイント 構成で使用されている数以上の物理インターフェイスとポート チャネル インターフェイスが必要です。これらのインターフェイスは、両方のデバイスで同じ名前である必要はありません。インターフェイスのマッピング方法を選択できます。

[FTDインターフェースのマップ（Map FTD Interface）] 画面で、Firepower Threat Defense デバイス上のインターフェイスのリストを取得します。デフォルトでは、Firewall 移行ツールはチェックポイントのインターフェイスと Firepower Threat Defense デバイスをインターフェイス ID に従ってマッピングします。たとえば、チェックポイント インターフェイスの「管理専用」インターフェイスは、Firepower Threat Defense デバイスの「管理専用」インターフェイスに自動的にマッピングされ、変更できません。

チェックポイント インターフェイスから FTD インターフェイスへのマッピングは、FTD デバイスタイプによって異なります。

- ターゲット FTD がネイティブタイプの場合：
  - FTDには、使用するチェックポイントインターフェイスまたはポートチャネル（PC）データインターフェイスが同数以上必要です（チェックポイント 構成の管理専用とサブインターフェイスを除く）。同数未満の場合は、ターゲット FTD に必要なタイプのインターフェイスを追加します。
  - サブインターフェイスは、物理インターフェイスまたはポートチャネルマッピングに基づいて Firewall 移行ツールによって作成されます。
- ターゲット FTD がコンテナタイプの場合：
  - FTD には、使用する チェックポイント 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、またはポート チャネル サブインターフェイスが同数以上必要

です（チェックポイント 構成の管理専用を除く）。同数未満の場合は、ターゲット FTD に必要なタイプのインターフェイスを追加します。たとえば、ターゲット FTD の物理インターフェイスと物理サブインターフェイスの数が チェックポイント での数より 100 少ない場合、ターゲット FTD に追加の物理または物理サブインターフェイスを作成できます。

- サブインターフェイスは、Firewall移行ツールでは作成されません。物理インターフェイス、ポートチャネル、またはサブインターフェイス間のインターフェイスマッピングのみが許可されます。

始める前に

Firepower Management Center に接続し、接続先として Firepower Threat Defense を選択していることを確認します。詳細については、「Firewall 移行ツールの接続先パラメータの指定 （43 ページ）」を参照してください。

（注） Firepower Threat Defense デバイスなしで Firepower Management Center に移行する場合、この手順は適用されません。

ステップ 1 インターフェイスマッピングを変更する場合は、[Threat Defenseインターフェイス名（Threat Defense Interface Name）]のドロップダウンリストをクリックし、そのチェックポイントインターフェイスにマッピングするインターフェイスを選択します。

管理インターフェイスのマッピングは変更できません。Firepower Threat Defenseインターフェイスがすでにチェックポイント インターフェイスに割り当てられている場合は、ドロップダウンリストからそのインターフェイスを選択できません。割り当て済みのすべてのインターフェイスはグレー表示され、使用できません。

サブインターフェイスをマッピングする必要はありません。Firewall 移行ツールは、 チェックポイント 構成内のすべてのサブインターフェイスについて Firepower Threat Defense デバイスのサブインターフェイスをマッピングします。

ステップ 2 各 チェックポイント インターフェイスを Firepower Threat Defense インターフェイスにマッピングしたら、[次へ（Next）] をクリックします。

次のタスク

チェックポイント インターフェイスを適切な Firepower Threat Defense インターフェイス オブジェクト、セキュリティゾーン、およびインターフェイスグループにマッピングします。詳細については、「セキュリティゾーン とインターフェイスグループへの チェックポイント インターフェイスのマッピング」を参照してください。

セキュリティゾーン とインターフェイスグループへの チェックポイント インターフェイスのマッピング

チェックポイント 構成が正しく移行されるように、 チェックポイント インターフェイスを適切な Firepower Threat Defense インターフェイス オブジェクト、セキュリティゾーン、およびインターフェイスグループにマッピングします。 チェックポイント 構成では、アクセス コントロール ポリシーと NAT ポリシーはインターフェイス名（nameif）を使用します。Firepower Management Center では、これらのポリシーはインターフェイス オブジェクトを使用します。さらに、Firepower Management Center ポリシーはインターフェイス オブジェクトを次のようにグループ化します。

- セキュリティゾーン：インターフェイスは、1 つのセキュリティゾーンにのみ属することができます。
- インターフェイスグループ：インターフェイスは複数のインターフェイスグループに属することができます。

ファイアウォール移行ツールでは、セキュリティゾーンおよびインターフェイスグループとインターフェイスを 1 対 1 でマッピングできます。セキュリティゾーンまたはインターフェイスグループがインターフェイスにマッピングされている場合、他のインターフェイスへのマッピングには使用できませんが、Firepower Management Center では許可されます。Firepower Management Center のセキュリティゾーンとインターフェイスグループの詳細については、「Interface Objects: Interface Groups and Security Zones」を参照してください。

ステップ 1 [セキュリティゾーンとインターフェイスグループへのマッピング（Map Security Zones and Interface Groups）] 画面で、使用可能なインターフェイス、セキュリティゾーン、およびインターフェイスグループを確認します。

ステップ 2 セキュリティゾーンおよびインターフェイスグループが Firepower Management Center に存在する場合、またはセキュリティ ゾーン タイプ オブジェクトとして 構成ファイルに存在し、ドロップダウンリストで使用可能な場合、これらにインターフェイスをマッピングするには、次の手順を実行します。

a) [セキュリティゾーン（Security Zones）] 列で、そのインターフェイスのセキュリティゾーンを選択します。

b) [インターフェイスグループ（Interface Groups）] 列で、そのインターフェイスのインターフェイスグループを選択します。

ステップ 3 セキュリティゾーンおよびインターフェイスグループが Firepower Management Center に存在する場合、またはセキュリティ ゾーン タイプ オブジェクトとして Check Point（r80）構成ファイルに存在し、ドロップダウンリストで使用可能な場合、これらにインターフェイスをマッピングするには、次の手順を実行します。

a) [セキュリティゾーン（Security Zones）] 列で、そのインターフェイスのセキュリティゾーンを選択します。

b) [インターフェイスグループ（Interface Groups）] 列で、そのインターフェイスのインターフェイスグループを選択します。

ステップ 4 セキュリティゾーンとインターフェイスグループは、手動でマッピングすることも自動で作成することもできます。

ステップ 5 セキュリティゾーンとインターフェイスグループを手動でマッピングするには、次の手順を実行します。

a) [セキュリティゾーンとインターフェイスグループの追加（Add SZ & IG）] をクリックします。
b) [セキュリティゾーンとインターフェイスグループの追加（Add SZ & IG）] ダイアログボックスで、[追加（Add）]をクリックして新しいセキュリティゾーンまたはインターフェイスグループを追加します。
c) [セキュリティゾーン（Security Zone）]列にセキュリティゾーン名を入力します。使用できる最大文字数は 48 です。同様に、インターフェイスグループを追加できます。
d) [閉じる（Close）] をクリックします。

セキュリティゾーンとインターフェイスグループを自動作成によってマッピングするには、次の手順を実行します。

a) [自動作成（Auto-Create）] をクリックします。
b) [自動作成（Auto-Create）] ダイアログボックスで、[インターフェイスグループ（Interface Groups）] または [ゾーンマッピング（Zone Mapping）] のいずれかまたは両方をオンにします。
c) [自動作成（Auto-Create）] をクリックします。

ファイアウォール移行ツールは、これらのセキュリティゾーンに Check Point インターフェイスと同じ名前（**outside** や **inside** など）を付け、名前の後に "(A)" を表示して、ファイアウォール移行ツールによって作成されたことを示します。インターフェイスグループには、**outside_ig** や **inside_ig** などの `_ig` サフィックスが追加されます。また、セキュリティゾーンとインターフェイスグループには、Check Point インターフェイスと同じモードがあります。たとえば、Check Point 論理インターフェイスが L3 モードの場合、そのインターフェイス用に作成されたセキュリティゾーンとインターフェイスグループも L3 モードになります。

ステップ 6 すべてのインターフェイスを適切なセキュリティゾーンとインターフェイスグループにマッピングしたら、[Next] をクリックします。

最適化、 移行する構成の確認と検証

移行した チェックポイント 構成を Firepower Management Center にプッシュする前に、構成を慎重に確認し、それが適切で Firepower Threat Defense デバイスの構成内容と一致することを確認します。

これで、ファイアウォール移行ツールは、Firepower Management Center にすでに存在する侵入防御システム（IPS）ポリシーとファイルポリシーを取得し、移行するアクセスコントロールルールにそれらを関連付けることができます。

ファイルポリシーは、システムが全体的なアクセス制御設定の一環として、ネットワークの高度なマルウェア防御とファイル制御を実行するために使用する一連の設定です。この関連付けにより、アクセス コントロール ルールの条件と一致するトラフィック内のファイルを通過させる前に、システムは必ずファイルを検査するようになります。

同様に、トラフィックが接続先に向かうことを許可する前に、システムの最終防御ラインとしてIPSポリシーを使用できます。侵入ポリシーは、セキュリティ違反に関するトラフィックの検査方法を制御し、インライン展開では、悪意のあるトラフィックをブロックまたは変更することができます。システムが侵入ポリシーを使用してトラフィックを評価する場合、システムは関連付けられた変数セットを使用します。セット内の大部分の変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先のIPアドレスとポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にあるIPアドレスを表すこともできます。

タブで特定の構成項目を検索するには、列の上部にあるフィールドに項目名を入力します。テーブルの行はフィルタ処理され、検索語に一致する項目のみが表示されます。

（注） デフォルトでは、[Inline Grouping] オプションが有効になっています。

[構成の最適化、確認および検証（Optimize, Review and Validate Configuration）] 画面で ファイアウォール移行ツールを閉じると、進行状況が保存され、後で移行を再開できます。この画面の前にファイアウォール移行ツールを閉じると、進行状況は保存されません。解析後に障害が発生した場合、[インターフェイスマッピング（Interface Mapping）] 画面から ファイアウォール移行ツールを再起動します。

ファイアウォール移行ツール ACL 最適化の概要

ファイアウォール移行ツール 2.5 は、ネットワーク機能に影響を与えることなく、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。たとえば、2 つのルールが同じネットワーク上で FTP および IP トラフィックを許可し、アクセスを拒否するルールが定義されていない場合、最初のルールを削除できます。
- 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。2 つのルールに同様のトラフィックがある場合、2 番目のルールはアクセスリストの後半に表示されるため、どのトラフィックにも適用されません。2 つのルールがトラフィックに対して異なるアクションを指定している場合、シャドウイングされたルールを移動するか、いずれかのルールを編集して必要なポリシーを実装できます。たとえば、特定の送信元または宛先に対して、基本ルールで IP トラフィックを拒否し、シャドウイングされたルールで FTP トラフィックを許可できます。

ファイアウォール移行ツールは、ACL最適化のルールを比較する際に次のパラメータを使用します。

（注） チェックポイント ではACP ルールアクションに対してのみ最適化を使用できます

- 無効化された ACL は、最適化プロセス中に考慮されません。
- 送信元の ACL は、対応する ACE（インライン値）に展開された後、次のパラメータについて比較されます。
  - 送信元と宛先のゾーン
  - 送信元と宛先のネットワーク
  - [送信元/宛先ポート（Source and Destination Port）]

オブジェクトの最適化

次のオブジェクトは、移行プロセス中にオブジェクトの最適化について考慮されます。

- 未参照のオブジェクト：移行の開始時に、未参照のオブジェクトを移行しないように選択できます。
- 重複したオブジェクト：オブジェクトがすでに FMC に存在する場合、重複したオブジェクトを作成する代わりに、ポリシーが再利用されます。
- 一貫しないオブジェクト：名前が似ていても内容が異なるオブジェクトがある場合、オブジェクト名は移行プッシュの前に ファイアウォール移行ツールで変更されます。

ステップ 1 （オプション）[構成の最適化、確認および検証（Optimize, Review and Validate Configuration）] 画面で、[ACLの最適化（Optimize ACL）] をクリックして最適化コードを実行し、以下の操作を実行します。

a) [はい（Yes）] をクリックして、ACL の最適化を続行します。特定された移行の冗長 ACL ルールとシャドウ ACL ルールが表示されます。

ACL 最適化の分析にかかる時間は、移行元の構成ファイルのサイズによって異なります。予測時間が表示されます。

最適化が考慮された ACL ルールの合計数の概要を示すレポートが表示されます。最適化レポートとそのコンポーネントの詳細については、ACL 最適化のレポート （55 ページ）を参照してください。

[冗長ACL（Redundant ACL）] および [シャドウACL（Shadow ACL）] タブは、ACL 最適化レポートにデータがある場合にのみ表示されます。

ACL は、[冗長ACL（Redundant ACL）] と [シャドウACL（Shadow ACL）] 両方の異なる基本ルールに表示されます。

（注） 冗長またはシャドー ACL の下に表示される ACL エントリは、基本 ACL とは見なされません。

b) 特定された ACL 最適化ルールをダウンロードするには、[ダウンロード（Download）] をクリックします。

c) ルールを選択し、**[アクション（Actions）]** > **[無効として移行（Migrate as disabled）]** または **[移行しない（Do not migrate）]** を選択して、いずれかのアクションを適用します。

d) [保存（Save）] をクリックします。

移行操作が [移行しない（Do not migrate）] から [無効として移行（Migrate as disabled）] またはその逆に変わります。

次のオプションを使用して、ルールの一括選択を実行できます。

- [移行（Migrate）：デフォルトの状態で移行します。
- [移行しない（Do not migrate）]：ACL の移行を無視します。
- [無効として移行（Migrate as disabled）]：[状態（State）] フィールドが [無効（Disable）] に設定されている ACL を移行します。
- [有効として移行（Migrate as enabled）]：[状態（State）] フィールドが [有効（Enable）] に設定されている ACL を移行します。

ステップ 2 [Review and Validate Configuration] 画面で、[Access Control Rules] をクリックし、次の手順を実行します。最適化、

a) テーブル内の各エントリについて、マッピングを確認し、それらが正しいことを確認します。

移行されたアクセスポリシールールは、プレフィックスとして ACL 名を使用し、それに ACL ルール番号を追加することで、チェックポイント 構成ファイルにマッピングしやすくします。たとえば、チェックポイント ACL の名前が "inside_access" の場合、ACL の最初のルール（または ACE）行の名前は "inside_access_#1" になります。TCP または UDP の組み合わせ、拡張サービスオブジェクト、またはその他の理由でルールを拡張する必要がある場合、ファイアウォール移行ツールは名前に番号付きサフィックスを追加します。たとえば、許可ルールが移行のために 2 つのルールへ拡張される場合、それらのルールには "inside_access_#1-1" と "inside_access_#1-2" という名前が付けられます。

サポートされていないオブジェクトを含むルールの場合、ファイアウォール移行ツールは名前に "_UNSUPPORTED" というサフィックスを追加します。

b) 1 つ以上のアクセス制御リストポリシーを移行しない場合は、該当する行のボックスをオンにし、**[アクション（Actions）] > [移行しない（Do not migrate）]** を選択して、[保存（Save）] をクリックします。

移行しないことを選択したすべてのルールは、テーブルでグレー表示されます。

c) Firepower Management Center ファイルポリシーを 1 つ以上のアクセス コントロール ポリシーに適用する場合は、該当する行のボックスをオンにし、**[アクション（Actions）] > [ファイルポリシー（File Policy）]** を選択します。

[ファイルポリシー（File Policy）] ダイアログで、適切なファイルポリシーを選択し、選択したアクセス コントロール ポリシーに適用して、[保存（Save）] をクリックします。

d) Firepower Management Center IPS ポリシーを 1 つ以上のアクセス コントロール ポリシーに適用する場合は、該当する行のボックスをオンにし、**[アクション（Actions）] > [IPS ポリシー（IPS Policy）]** を選択します。

[IPS ポリシー（IPS Policy）] ダイアログで、適切な IPS ポリシーと対応する変数セットを選択し、選択したアクセス コントロール ポリシーに適用して、[保存（Save）] をクリックします。

e) ロギングが有効になっているアクセスコントロールルールのロギングオプションを変更する場合は、該当する行のボックスをオンにし、**[アクション（Actions）] > [ログ（Log）]** を選択します。

[ログ（Log）]ダイアログでは、接続の開始時または終了時、またはその両方でイベントのロギングを有効にできます。ロギングを有効にする場合は、接続イベントを**イベントビューア**または **Syslog** のいずれか、または両方に送信することを選択する必要があります。接続イベントを syslog サーバに送信することを選択した場合、Firepower Management Center ですでに構成されている syslog ポリシーを [Syslog] ドロップダウンメニューから選択できます。

f) [アクセスコントロール（Access Control）] テーブル内の移行されたアクセスコントロールルールのアクションを変更する場合は、該当する行のボックスをオンにし、**[アクション（Actions）] > [ルールアクション（Rule Action）]** を選択します。

ヒント アクセスコントロールルールにアタッチされている IPS およびファイルのポリシーは、[許可（Allow）] オプションを除くすべてのルールアクションに対して自動的に削除されます。

ACEカウントを、昇順、降順、等しい、大なり、および小なりのフィルタリング順序シーケンスでフィルタリングできるようになりました。

フィルタリング条件をクリアするには、[フィルタのクリア（Clear Filter）] をクリックします。

（注） ACE に基づいた ACL のソート順序は、表示のみを目的としています。ACL は、発生した時間順に基づいてプッシュされます。

ステップ 3 次のタブをクリックし、構成項目を確認します。

- **NAT Rules**
- **ネットワーク オブジェクト**
- **ポート オブジェクト**
- **Interfaces**
- **ルート**
- **[動的ルートオブジェクト（Dynamic-Route-Objects）]**

1 つ以上の NAT ルールまたはルートインターフェイスを移行しない場合は、該当する行のボックスをオンにし、**[アクション（Actions）] > [移行しない（Do not migrate）]** を選択して、[保存（Save）] をクリックします。

移行しないことを選択したすべてのルールは、テーブルでグレー表示されます。

ステップ 4 （任意）構成の確認中に、[ネットワークオブジェクト（Network Objects）] タブまたは [ポートオブジェクト（Port Objects）] タブで **[アクション（Actions）] > [名前の変更（Rename）]** を選択して、ネットワークオブジェクトまたはポートオブジェクトの名前を変更することができます。

名前が変更されたオブジェクトを参照するアクセスルールとNATポリシーも、新しいオブジェクト名で更新されます。

ステップ 5 （任意）グリッド内の各構成項目の詳細をダウンロードするには、[ダウンロード（Download）] をクリックします。

ステップ 6 確認が完了したら、[確定（Validate）] をクリックします。

検証中、ファイアウォール移行ツールは Firepower Management Center に接続し、既存のオブジェクトを確認して、それらのオブジェクトを移行対象オブジェクトのリストと比較します。オブジェクトが Firepower Management Center にすでに存在する場合、ファイアウォール移行ツールは次のことを行います。

- オブジェクトの名前と構成が同じ場合、ファイアウォール移行ツールは既存のオブジェクトを再利用し、 Firepower Management Center に新しいオブジェクトを作成しません。
- オブジェクトの名前が同じで構成が異なる場合、ファイアウォール移行ツールはオブジェクトの競合を報告します。

検証の進行状況はコンソールで確認できます。

ステップ 7 検証が完了し、[検証ステータス（Validation Status）] ダイアログボックスに 1 つ以上のオブジェクトの競合が表示された場合は、次の手順を実行します。

a) [競合の解決（Resolve Conflicts）] をクリックします。

ファイアウォール移行ツールは、オブジェクトの競合が報告された場所に応じて、[ネットワークオブジェクト（Network Objects）] タブまたは [ポートオブジェクト（Port Objects）] タブのいずれかまたは両方に警告アイコンを表示します。

b) タブをクリックし、オブジェクトを確認します。

c) 競合がある各オブジェクトのエントリを確認し、**[アクション（Actions）] > [競合の解決（Resolve Conflicts）]** を選択します。

d) [競合の解決（Resolve Conflicts）] ウィンドウで、推奨アクションを実行します。

たとえば、既存の Firepower Management Center オブジェクトとの競合を避けるために、オブジェクト名にサフィックスを追加するように求められる場合があります。デフォルトのサフィックスを受け入れるか、独自のサフィックスに置き換えることができます。

e) [解決（Resolve）] をクリックします。

f) タブ上のすべてのオブジェクトの競合を解決したら、[保存（Save）] をクリックします。

g) [確定（Validate）] をクリックして構成を再検証し、すべてのオブジェクトの競合を解決したことを確認します。

ステップ 8 検証が完了し、[Validation Status] ダイアログボックスに「Successfully Validated」というメッセージが表示されたら、移行された構成の以下へのプッシュ： Firepower Management Center （57 ページ）に進みます。

ACL 最適化のレポート

ACL 最適化レポートには、次の情報が表示されます。

- Summary シート：ACL 最適化のサマリーが表示されます。

Sl.no	ACL name	Redundant ACLs	Shadowed ACLs
1	outsideACL_#1		outsideACL_#2, outsideACL_#3, outsideACL_#4, outsideACL_#5, outsideACL_#6, outsideACL_#7, outsideACL_#8, outsideACL_#9, outsideACL_#10, outsideACL_#11, outsideACL_#12
2	outsideACL_#13		outsideACL_#17, outsideACL_#18
3	outsideACL_#14		outsideACL_#15, outsideACL_#16, outsideACL_#17, outsideACL_#18
4	outsideACL_#19		outsideACL_#20, outsideACL_#21, outsideACL_#22, outsideACL_#23, outsideACL_#24
5	outsideACL_#25		outsideACL_#27, outsideACL_#28, outsideACL_#29, outsideACL_#30
6	outsideACL_#26		
7	outsideACL_#31		outsideACL_#32, outsideACL_#33
8	outsideACL_#34		
9	dmzACL_#1		
10	dmzACL_#2	dmzACL_#5	
11	dmzACL_#3		dmzACL_#5
12	dmzACL_#4		
13	dmzACL_#6		dmzACL_#7, dmzACL_#8, dmzACL_#9, dmzACL_#10
14	dmzACL_#11		dmzACL_#13
15	dmzACL_#12		
16	extACL_#1		
17	extACL_#2		
18	extACL_#3		extACL_#4, extACL_#5, extACL_#6
19	extACL_#7		
20	extACL_#8	extACL_#9, extACL_#10	
21	extACL_#11		
22	extACL_#12	extACL_#13	
23	extACL_#14		
24	extACL_#15		
25	extACL_#16		
26	extACL_#17		extACL_#18, extACL_#19
27	localtoremote_#1		
28	opt_#1		opt_#3
29	opt_#2	opt_#4	opt_#5
30	opt_#6-1	opt_#17-1	opt_#7-1, opt_#8-1
31	opt_#9-1	opt_#10-1	
32	opt_#11-1	opt_#12-1	opt_#13-1
33	opt_#14-1		opt_#15-1, opt_#16-1
34	opt_#18		
35	opt_#19		opt_#20, opt_#21
36	opt_#22-1	opt_#23-1	

Summary | Detailed ACL Information | +

- Detailed ACL Information：ベース ACL の詳細が表示されます。各 ACL には、比較対象の基本の ACL と最適化カテゴリとの関連付けを識別する ACL タイプ（シャドウまたは冗長）のタグが付いています。

Sl.no	ACL name	Source zone	Destination zone	Source network	Destination network	Source port	Destination port	Action	ACL type
1	**outsideACL_#1**	**outside**	**ANY**	**any**	**10.0.0.0/8**	**ANY**	**ANY**	**permit**	
	outsideACL_#2	outside	ANY	any	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#3	outside	ANY	192.168.0.1	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#4	outside	ANY	192.168.0.10	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#5	outside	ANY	any	10.1.1.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#6	outside	ANY	any	10.1.1.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#7	outside	ANY	any	10.1.1.0/24	ANY	tcp:80	permit	Shadowed by outsideACL_#1
	outsideACL_#8	outside	ANY	any	10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#9	outside	ANY	200.200.200.1	10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#10	outside	ANY	10.10.10.10, 10.10.0.0/16	10.10.0.0/19, 10.99.99.99	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#11	outside	ANY	any	10.99.99.90, 10.99.99.99, 10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#12	outside	ANY	any	10.99.99.90, 10.99.99.99, 10.10.10.10, 10.10.0.0/16, 10.99.99.99, 10.10.10.10, 10.10.0.0/16, 10.10.0.0/19	ANY	ANY	permit	Shadowed by outsideACL_#1
2	**outsideACL_#13**	**outside**	**ANY**	**any**	**192.168.0.0/16**	**ANY**	**ANY**	**permit**	
	outsideACL_#17	outside	ANY	10.10.1.1	192.168.0.0/16	ANY	tcp:443	permit	Shadowed by outsideACL_#13
	outsideACL_#18	outside	ANY	10.10.1.1	192.168.0.0/16	ANY	tcp:80	permit	Shadowed by outsideACL_#13

移行された構成の以下へのプッシュ： Firepower Management Center

構成の検証に成功せず、すべてのオブジェクトの競合を解決していない場合は、移行されたチェックポイント 構成を Firepower Management Center にプッシュできません。

移行プロセスのこのステップでは、移行された構成を Firepower Management Center に送信します。Firepower Threat Defense デバイスに構成を展開しません。ただし、Firepower Threat Defense 上の既存の構成はこのステップで消去されます。

（注） ファイアウォール移行ツールが移行された構成を Firepower Management Center に送信している間は、構成を変更したり、デバイスに展開したりしないでください。

ステップ 1 [検証ステータス（Validation Status）] ダイアログボックスで、検証の概要を確認します。

ステップ 2 [構成のプッシュ（Push Configuration）] をクリックして、移行された チェックポイント 構成を Firepower Management Center に送信します。

ファイアウォール移行ツールに、移行の進行状況の概要が表示されます。コンソールに、Firepower Management Center にプッシュされているコンポーネントの詳細な進行状況を行ごとに表示できます。

ステップ 3 移行が完了したら、[レポートのダウンロード（Download Report）] をクリックして、移行後レポートをダウンロードして保存します。

移行前レポートのコピーも、ファイアウォール移行ツールと同じ場所にある `Resources` フォルダに保存されます。

ステップ 4 移行が失敗した場合は、移行後レポート、ログファイル、および未解析ファイルを慎重に確認して、失敗の原因を把握します。

トラブルシューティングについては、サポートチームに問い合わせることもできます。

移行の失敗のサポート

移行に失敗する場合は、サポートにお問い合わせください。

1. [移行完了（Complete Migration）] 画面で、[サポート（Support）] ボタンをクリックします。

   ヘルプサポートページが表示されます。

2. [サポートバンドル（Support Bundle）] チェックボックスをオンにして、ダウンロードする構成ファイルを選択します。

   （注） ログファイルと DB ファイルは、デフォルトでダウンロード用に選択されています。

3. [ダウンロード（Download）] をクリックします。

サポートバンドルファイルは、ローカルパスに.zipとしてダウンロードされます。Zipフォルダを抽出して、ログファイル、DB、および構成ファイルを表示します。

4. [Email us]をクリックして、テクニカルチームに障害の詳細を電子メールで送信します。

   ダウンロードしたサポートファイルを電子メールに添付することもできます。

5. [TACページに移動（Visit TAC page）]をクリックして、シスコのサポートページでTACケースを作成します。

   （注） TACケースは、移行中にいつでもサポートページからオープンできます。

移行後レポートの確認と移行の完了

移行後のレポートには、さまざまなカテゴリのACLカウント、ACL最適化、および構成ファイルで実行された最適化の全体的なビューに関する詳細が表示されます。詳細については、最適化、 移行する構成の確認と検証 （50 ページ）を参照してください。

オブジェクトを確認して検証します。

- **カテゴリ**
  - ACLルール合計数（移行元の構成）
  - 最適化の対象とみなされるACLルールの合計数。冗長、シャドウなどがあります。
- 最適化のACLカウントは、最適化の前後にカウントされたACLルールの合計数を示します。

移行中に移行後レポートをダウンロードし忘れた場合は、次のリンクを使用してダウンロードしてください。

移行後レポートのダウンロードエンドポイント：http://localhost:8888/api/downloads/post_migration_summary_html_format

（注） レポートは、ファイアウォール移行ツールの実行中にのみダウンロードできます。

ステップ1 **移行後レポート**をダウンロードした場所に移動します。

ステップ2 移行後レポートを開き、その内容を慎重に確認して、チェックポイント構成がどのように移行されたかを理解します。

- Migration Summary： チェックポイントからFirepower Threat Defenseへ正常に移行された構成の概要。チェックポイント インターフェイス、 Firepower Management Centerホスト名とドメイン、ターゲット

Firepower Threat Defense デバイス（該当する場合）、および正常に移行された構成要素に関する情報が含まれます。

- Selective Policy Migration：移行用に選択された特定の チェックポイント 機能の詳細は、[デバイス構成機能（Device Configuration Features）]、[共有構成機能（Shared Configuration Features）]、および [最適化（Optimization）] の 3 つのカテゴリ内で使用できます。
- チェックポイント Interface to FTD Interface Mapping：正常に移行されたインターフェイスの詳細と、チェックポイント 構成のインターフェイスを Firepower Threat Defense デバイスのインターフェイスにマッピングした方法。これらのマッピングが期待どおりであることを確認します。

  （注） このセクションは、宛先 Firepower Threat Defense デバイスを使用しない移行、または移行に**インターフェイス**が選択されて**いない**場合には適用されません。

- Source Interface Names to FTD Security Zones and Interface Groups：正常に移行された チェックポイント 論理インターフェイスと名前の詳細、およびそれらを Firepower Threat Defense のセキュリティゾーンとインターフェイスグループにマッピングした方法。これらのマッピングが期待どおりであることを確認します。

  （注） **アクセス制御リスト**と**NAT**が移行に選択されて**いない**場合、このセクションは適用されません。

- Object Conflict Handling：Firepower Management Center の既存のオブジェクトと競合していると識別された チェックポイント オブジェクトの詳細。オブジェクトの名前と設定が同じ場合、ファイアウォール移行ツールは Firepower Management Center オブジェクトを再利用しています。オブジェクトの名前が同じで構成が異なる場合は、管理者がそれらのオブジェクトの名前を変更しています。これらのオブジェクトを慎重に確認し、競合が適切に解決されたことを確認します。
- Access Control Rules, NAT, and Routes You Chose Not to Migrate：ファイアウォール移行ツールで移行しないように選択したルールの詳細。ファイアウォール移行ツールによって無効化され、移行されなかったこれらのルールを確認します。これらの行を確認し、選択したすべてのルールがこのセクションにリストされていることを確認します。必要に応じて、これらのルールを手動で構成できます。
- Partially Migrated Configuration：詳細オプションなしでもルールを移行できる詳細オプション付きルールを含む、一部のみ移行された チェックポイント ルールの詳細。これらの行を確認し、詳細オプションが Firepower Management Center でサポートされているかどうかを確認します。サポートされている場合は、これらのオプションを手動で構成します。
- Unsupported Configuration：ファイアウォール移行ツールがこれらの機能の移行をサポートしていないため、移行されなかった チェックポイント 構成要素の詳細。これらの行を確認し、各機能が Firepower Threat Defense でサポートされているかどうかを確認します。その場合は、Firepower Management Center でこれらの機能を手動で構成します。
- Expanded Access Control Policy Rules：移行時に単一の チェックポイント Point ルールから複数の Firepower Threat Defense ルールに拡張された チェックポイント アクセス コントロール ポリシー ルールの詳細。
- **Actions Taken on Access Control Rules**
  - [移行しないアクセスルール（Access Rules You Chose Not to Migrate）]：ファイアウォール移行ツールで移行しないように選択したチェックポイントアクセスコントロールルールの詳細。これらの

行を確認し、選択したすべてのルールがこのセクションにリストされていることを確認します。必要に応じて、これらのルールを手動で構成できます。

- Access Rules with Rule Action Change：ファイアウォール移行ツールツールを使用して「ルールアクション」が変更されたすべてのアクセスコントロールポリシールールの詳細。ルールアクションの値は、Allow、Trust、Monitor、Block、Block with reset です。これらの行を確認し、選択したすべてのルールがこのセクションにリストされていることを確認します。必要に応じて、これらのルールを手動で構成できます。
- Access Control Rules that have IPS Policy and Variable Set Applied：IPS ポリシーが適用されているすべての チェックポイント アクセス コントロール ポリシー ルールの詳細。これらのルールを慎重に確認し、この機能が Firepower Threat Defense でサポートされているかどうかを確認します。
- Access Control Rules that have File Policy Applied：ファイルポリシーが適用されているすべての チェックポイント アクセス コントロール ポリシー ルールの詳細。これらのルールを慎重に確認し、この機能が Firepower Threat Defense でサポートされているかどうかを確認します。
- Access Control Rules that have Rule 'Log' Setting Change：ファイアウォール移行ツールを使用して「ログ設定」が変更された チェックポイント アクセスコントロールルールの詳細。ログ設定の値は、False、Event Viewer、Syslog です。これらの行を確認し、選択したすべてのルールがこのセクションにリストされていることを確認します。必要に応じて、これらのルールを手動で構成できます。

（注） サポートされていないルールが移行されなかった場合、不要なトラフィックがファイアウォールを通過する問題が発生します。このトラフィックが Firepower Threat Defense によってブロックされるように、Firepower Management Center でルールを構成することを推奨します。

（注） [Review and Validate] ページで IPS またはファイルポリシーを ACL に適用する必要がある場合は、移行前に FMC でポリシーを作成することを強くお勧めします。ファイアウォール移行ツール は接続された FMC からポリシーを取得するため、同じポリシーを使用します。新しいポリシーを作成して複数のポリシーに割り当てると、パフォーマンスが低下し、プッシュが失敗する可能性があります。

Firepower Management Center および Firepower Threat Defense でサポートされる機能の詳細については、『Firepower Management Center Configuration Guide, Version 6.2.3』を参照してください。

ステップ 3 **移行前レポート**を開き、Firepower Threat Defense デバイスで手動で移行する必要がある チェックポイント 構成項目をメモします。

ステップ 4 Firepower Management Center で、次の手順を実行します。

a) Firepower Threat Defense デバイスの移行された構成を確認し、次を含むすべての期待されるルールおよびその他の構成項目が移行されたことを確認します。

- アクセス制御リスト（ACL）
- ネットワークアドレス変換規則
- ポートおよびネットワークオブジェクト
- ルート

- インターフェイス
- [動的ルートオブジェクト（Dynamic-Route-Objects）]

b) 一部がサポートされている、サポートされていない、無視された、無効化された、および移行されなかったすべての構成項目とルールを構成します。

これらの項目とルールを構成する方法の詳細については、『Firepower Management Center Configuration Guide』を参照してください。手動構成が必要な構成項目の例を次に示します。

- プラットフォーム設定（SSH および HTTPS アクセスを含む）（「Platform Settings for Firepower Threat Defense」を参照）
- Syslog 設定（「Configure Syslog」を参照）
- ダイナミックルーティング（「Routing Overview for Firepower Threat Defense」を参照）
- サービスポリシー（「FlexConfig Policies」を参照）
- VPN 構成（「Firepower Threat Defense VPN」を参照）
- 接続ログ設定（「Connection Logging」を参照）

ステップ 5 確認が完了したら、Firepower Management Center から Firepower Threat Defense デバイスに移行された構成を展開します。

サポートされていないルールと一部がサポートされているルールについて、データが**移行後レポート**に正しく反映されていることを確認します。

ファイアウォール移行ツールでポリシーが Firepower Threat Defense デバイスに割り当てられます。変更が実行中の構成に反映されていることを確認します。移行されるポリシーを識別しやすくするために、これらのポリシーの説明には チェックポイント 構成のホスト名が含まれています。

Firewall 移行ツールのアンインストール

すべてのコンポーネントは、Firewall 移行ツールと同じフォルダに保存されます。

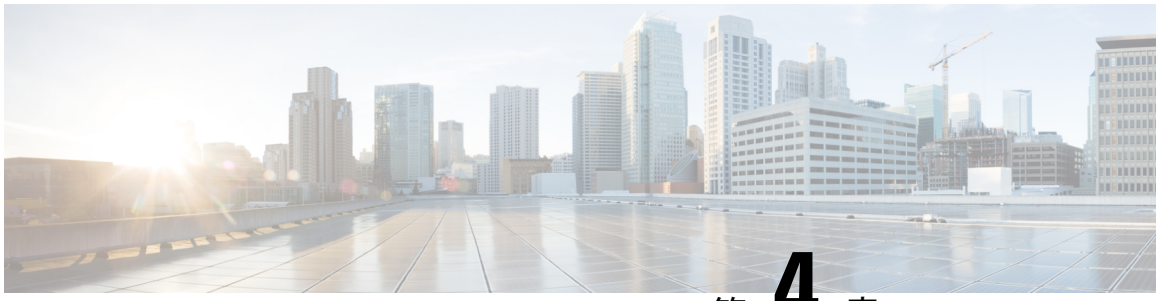
ステップ 1 Firewall 移行ツールを配置したフォルダに移動します。

ステップ 2 ログを保存する場合は、`log` フォルダを切り取りまたはコピーして別の場所に貼り付けます。

ステップ 3 移行前レポートと移行後レポートを保存する場合は、`resources` フォルダを切り取りまたはコピーして別の場所に貼り付けます。

ステップ 4 Firewall 移行ツールを配置したフォルダを削除します。

ヒント　ログファイルはコンソールウィンドウに関連付けられています。Firewall移行ツールのコンソールウィンドウが開いている限り、ログファイルとフォルダは削除できません。



第 4 章

移行の問題のトラブルシューティング

- Firewall 移行ツールのトラブルシューティングについて （63 ページ）
- トラブルシューティングに使用されるログおよびその他のファイル （64 ページ）
- Check Point ファイルのアップロード失敗のトラブルシューティング （64 ページ）

Firewall 移行ツールのトラブルシューティングについて

移行が失敗するのは、通常、 チェックポイント 構成ファイルをアップロードしているとき、または移行された構成を Firepower Management Center にプッシュしているときです。

Check Point 構成の移行プロセスが失敗する一般的なシナリオは次のとおりです。

- Check Point Config.zip からファイルが欠落。
- Check Point Cofig.zip 内の無効なファイルが Firewall 移行ツールで検出された。
- Check Point 構成ファイルが .zip 以外の圧縮ファイルタイプである。

Firewall 移行ツールのサポートバンドル

Firewall 移行ツールには、サポートバンドルをダウンロードして、ログファイル、DB、構成ファイルなどの役立つトラブルシューティング情報を抽出するオプションがあります。次の手順を実行します。

1. [移行完了（Complete Migration）] 画面で、[サポート（Support）] ボタンをクリックします。

   ヘルプサポートページが表示されます。

2. [サポートバンドル（Support Bundle）] チェックボックスをオンにして、ダウンロードする構成ファイルを選択します。

   注 ログファイルと DB ファイルは、デフォルトでダウンロード用に選択されています。

3. [ダウンロード（Download）] をクリックします。

サポートバンドルファイルは、ローカルパスに.zipとしてダウンロードされます。Zipフォルダを抽出して、ログファイル、DB、および構成ファイルを表示します。

4. [Email us] をクリックして、テクニカルチームに障害の詳細を電子メールで送信します。

   ダウンロードしたサポートファイルを電子メールに添付することもできます。

5. [TACページに移動（Visit TAC page）] をクリックして、シスコのサポートページでTACケースを作成します。

注 TACケースは、移行中にいつでもサポートページからオープンできます。

トラブルシューティングに使用されるログおよびその他のファイル

問題の特定とトラブルシューティングに役立つ情報は、次のファイルにあります。

ファイル	ロケーション
ログ ファイル	<migration_tool_folder> \ logs
移行前のレポート	*<migration_tool_folder>*\resources
移行後のレポート	*<migration_tool_folder>*\resources
未解析ファイル	*<migration_tool_folder>*\resources

CheckPointファイルのアップロード失敗のトラブルシューティング

Check Point構成ファイルのアップロードに失敗した場合、通常はFirepower移行ツールがファイル内の1つ以上の行を解析できなかったことが原因です。

アップロードおよび解析の失敗の原因となったエラーに関する情報は、次の場所で確認できます。

- 未解析のファイル：ファイルの末尾を調べて、正常に解析されたCheck Point構成ファイルで最後に無視された行を特定します。
- 予期しないファイル：Check Pointで無効なファイルが検出されました。たとえば、Mac OSを使用してzip圧縮すると、Macシステムファイルが作成されます。Macファイルを削除してください。

- （r75 ～ r77.30 のみ）誤った名前のファイル：Check Point のセキュリティポリシーと NAT ポリシーファイルの名前が正しくない場合。ACL および NAT ファイルの名前を正しく変更します。
- 欠落ファイル：Check Point の config.zip ファイルから一部のファイルが欠落しています。必要なファイルを追加します。

注 r77 の場合は、欠落している構成ファイルを手動で抽出します。詳細については、「r77 の Check Point 構成ファイルのエクスポート」を参照してください。

r80 の場合は、Live Connect を使用して Firepower 移行ツールの正しい構成ファイルを抽出します。詳細については、「r80 の Check Point 構成ファイルのエクスポート」を参照してください。

Check Point のトラブルシューティング例：オブジェクトグループのメンバーが見つからない（r75 ～ r77.30 のみ）

この例では、要素の構成にエラーがあるため、Check Point 構成ファイルのアップロードと解析が失敗します。

ステップ 1 エラーメッセージを確認して問題を特定します。

このエラーにより、次のエラーメッセージが生成されます。

参照先	エラー メッセージ
Firepower 移行ツールのメッセージ	エラーを含む、解析済みの Check Point 構成ファイル。 解析エラーについては移行前レポートの確認のエラーセクション、プッシュステージ中に発生するプッシュエラーについては移行後レポートの確認と移行の完了を参照してください。
ログ ファイル	[ERROR | objectGroupRules] > "ERROR, SERVICE_GROUP_RULE not applied for port-group object [services_epacity_nt_abc] as CheckPoint object [ica] does not exist in <service> table;" [INFO | objectGroupRules] > "Parsing object-group service:[services_gvxs06]" [INFO | objectGroupRules] > "Parsing object-group service:[services_iphigenia]" [INFO | objectGroupRules] > "Parsing object-group service:[Services_KPN_ISP]"

ステップ 2 Check Point `services.xml` ファイルを開きます。

ステップ 3 services_gvxs06 という名前のオブジェクトグループを検索します。

ステップ 4 スマートダッシュボードを使用して、オブジェクトグループの欠落しているメンバーを作成します。

ステップ 5 構成ファイルをもう一度エクスポートします。詳細については、「r77 の Check Point 構成ファイルのエクスポート」を参照してください。

ステップ 6 これ以上エラーがない場合は、新しい Check Point 構成 zip ファイルを Firepower 移行ツールにアップロードし、移行を続行します。

Live Connect の Check Point（r80）に関するトラブルシューティング例

例 1：Check Point Security Manager の詳細を要求する。

この例では、Firepower 移行ツールが Check Point Security Manager の詳細を要求します。

エラーメッセージを確認して問題を特定します。このエラーにより、次のエラーメッセージが生成されます。

参照先	エラー メッセージ
Firepower 移行ツールのメッセージ	Check Point Security Manager の詳細を提供するように要求する画面。
ログファイル	[ERROR | connect_cp] > "Unable to extract the Extracted-objects.json file due to credentials with insufficient privileges, time-out issues and so on. Refer FMT UG for more info." 127.0.0.1 - - [20/Jul/2020 17:20:43] "POST /api/CP/connect HTTP/1.1" 500 -

ログイン情報が正しくありません。以前に説明した手順に従って、ログイン情報を事前設定します。使用するログイン情報には、Check Point Security Manager の Check Point Gaia 上の */bin/bash* シェルプロファイルが必要です。通常の展開では、Check Point Security Manager の Check Point SmartConsole アプリケーションに、同じログイン情報をスーパーユーザ権限で事前設定する必要があります。マルチドメイン展開を使用する場合、権限はスーパーユーザである必要があります。詳細については、「Live Connect を使用した構成抽出のための Check Point（r80）デバイスの事前設定」を参照してください。

例2：不正なファイル形式

この例では、Firepower 移行ツールの移行は、不正なファイル形式が原因でブロックされています。

エラーメッセージを確認して問題を特定します。このエラーにより、次のエラーメッセージが生成されます。

参照先	エラー メッセージ
Firepower 移行ツールのメッセージ	ブロック
ログ ファイル	[ERROR | cp_device_connection] > "Bad file format" 2020-07-20 17:10:57,347 [ERROR | connect_cp] > "Unable to download .tar file." 127.0.0.1 - - [20/Jul/2020 17:10:57] "GET /api/CP/generate_tar_file?package=Standard HTTP/1.1" 500 -

ログイン情報が正しくありません。以前に説明した手順に従って、ログイン情報を事前設定します。使用するログイン情報には、Check Point Security Manager の Check Point Gaia 上の */bin/bash* シェルプロファイルが必要です。Check Point Security Manager の Check Point Smart Console アプリケーションに、同じログイン情報をスーパーユーザ権限で事前設定する必要があります。マルチドメイン展開を使用する場合は、スーパーユーザ権限を付与する必要があります。詳細については、「Live Connect を使用した構成抽出のための Check Point（r80）デバイスの事前設定」を参照してください。

例3：ブロックされた VSX 機能は FTD でサポートされない

この例では、Firepower 移行ツールの移行は、ブロックされた VSX 機能が FTD に存在することが原因で失敗します。

エラーメッセージを確認して問題を特定します。このエラーにより、次のエラーメッセージが生成されます。

参照先	エラー メッセージ
Firepower 移行ツールのメッセージ	ブロックされた VSX 機能は、FTD ではサポートされていません。
ログファイル	[ERROR | config_upload] > "VSX Feature is UNSUPPORTED in FTD" Traceback (most recent call last)

問題の説明：このエラーは、**fw vsx stat** コマンドが Check Point r80.40 以降で廃止されたために発生します。

回避策として、次の手順を実行します。

1. *config.zip* ファイルを解凍します。
2. *networking.txt* ファイルを開きます。

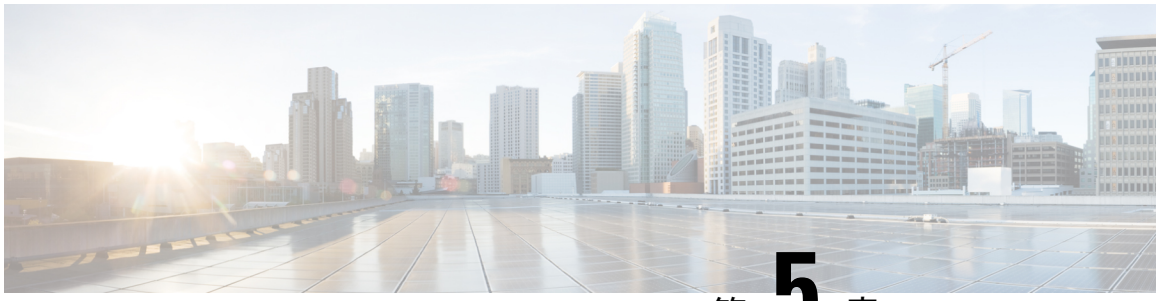
   次に、出力例を示します。

```
firewall> fw vsx stat
Deprecated command, Please see sk144112 for alternative
Deprecated commands: cphaprob cpinfo cplic fw ips raidconfig fwaccel
```

   これを次のように手動で置き換えます。

```
firewall> fw vsx stat
VSX is not supported on this platform
```

3. すべてのファイルを選択し、.zip 拡張子に圧縮します。



第 5 章

Firewall 移行ツールの FAQ

• Firewall 移行ツールの FAQ （69 ページ）

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 2.5.2 の Firewall 移行ツールでサポートされる新機能は何ですか。

A. Check Point の ACL 最適化。

Q. Check Point から FTD への変換におけるハードウェア制限は何ですか。

A. 構成ファイルが Check Point Web Visualization Tool および FMT-CP-Config-Extractor_v2.5.2-6575 ツールと互換性がある場合は、送信元 Check Point を移行できます。

Q. Check Point r76SP からエクスポートされた構成を使用して、それを 4100 および 6100 Firepower プラットフォームに移行できますか。

A. はい。r75 ～ r77.30 は、すべてのプラットフォームでサポートされます。

プラットフォームは、Check Point Web Visualization Tool が利用可能であればサポートされます。

Q. Check Point 上のルールで否定されたオブジェクトを処理する方法を教えてください。

A. オブジェクトが除外タイプのオブジェクト/グループである場合、ACL 変換は「許可」と「ブロック」の組み合わせに従います。この変換は ACL でサポートされていますが、除外タイプのネットワークオブジェクト/グループはサポートされていません。たとえば、Check Point ACE ルールが、参照される除外タイプのオブジェクトグループを持つ場合です。

- Check Point ルールアクションが「許可」の場合は、次のようになります。
  - ACE には、**<exception></exception>** XML タグで参照されている Object-Group を「拒否」するアクションが必要です。ルールに「Rule for Exception Object-Group」コメントを追加してください。

- ACE には、*<base></base>* XML タグで参照されている Object-Group を「許可」するアクションが必要です。ルールに「Rule for Exception Object-Group」コメントを追加してください。

- Check Point ルールアクションが「拒否/リセット」の場合は、次のようになります。
  - ACE には、**<exception></exception>** XML タグで参照されている Object-Group を「許可」するアクションが必要です。ルールに「Rule for Exception Object-Group」コメントを追加してください。
  - ACE には、**<base></base>** XML タグで参照されている Object-Group についての「リセット（拒否）」をともなう「ブロック（拒否）/ブロック」のアクションが必要です。ルールに「Rule for Exception Object-Group」コメントを追加してください。

Q. Firewall 移行ツールは、否定セルをともなう ACE をサポートしていますか。サポートしていない場合、それらのルールは Firewall 移行ツールによってどのように処理されますか。

A. 否定セルをともなう ACE は、Firewall 移行ツールでサポートされておらず、その ACE を通常の ACE として扱うことによって変換されます。これらの問題は今後のリリースで解決される予定です。

Q. 「Failed to bind to the DB. Access denied error.」というメッセージが表示されます。どうすればいいですか。

A. 次の手順を実行します。

- Check Point Gaia Console for Management Server を開きます。
- Gaia Console 上のユーザーおよびロールの設定に移動します。
- 管理者ロールを持つ Check Point Management Server Gaia Console で、ホームディレクトリの `/home` パラメータとシェルの `/etc/cli.sh` パラメータを使用して、新しいユーザー名ログイン情報を作成します。

Q. Firewall 移行ツールを使用して Check Point 構成を解析すると、解析カウントが 0 と表示されます。どうすればいいですか。

A. 次のいずれかの手順を実行します。

FMT-CP-Config-Extractor_v2.5.2-6575 ツールを使用して *networking.txt* ファイルを取得します。手動で作成した *networking.txt* ファイルは使用しないでください。

または

何らかの理由で、*networking.txt* ファイルの出力がエクスポートされた Check Point Security Gateway でロギングが有効になっている可能性があります。ロギングが有効になっているために *networking.txt* ファイルに無関係な情報が追加されており、そのような問題が発生しています。その場合は、次の手順を実行します。

- *networking.txt* ファイルを確認します。
- 追加された余分なログ行を削除してファイルを修正します。

- 新しい zip を Firewall 移行ツールにアップロードします。

Q. VSX を使用して Check Point から構成を移行できますか。

A. 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できます（一度に1つの仮想システム）。たとえば、Web Visualization Tool（r75 ～ r77.30）を使用して構成をエクスポートすると、すべての仮想システムのポリシー要素がエクスポートされます。そのため、*index.xml*、*communities.xml*、*network_objects.xml*、および *networking.txt*（移行されるポリシーの Security Gateway から）とともに移行する仮想システムの NAT ファイルとポリシーファイルのみを保持して、それを完全な構成にします。

r80 の場合、Check Point ポリシーパッケージを選択して構成を取得する際、手順 5 で、移行する Live Connect を介して Check Point Security Manager に接続するときに、特定の仮想システムのポリシーパッケージを選択します。

Check Point Security Gateway にも接続する場合は、Check Point ポリシー パッケージに対応する適切な Check Point Virtual System Check Point Firewall Package の正しい詳細情報を提供してください。

それでも問題が解決しない場合は、Cisco TAC に連絡して、これらの障害の TAC ケースを作成してください。

Q. Check Point（r80）構成を手動で取得できますか。

A. いいえ。Check Point（r80）構成を手動で取得することはできません。完全な r80 構成を取得するには、Firewall 移行ツールで Live Connect を使用します。手動の回避策を使用するか Firewall 移行ツールで構成されていない Check Point（r80）構成を使用して構成を抽出すると、構成が不完全になるだけでなく、サポートされていないものとして移行されるか、部分的に移行されるか、場合によっては移行が失敗します。

詳細については、「r80 の Check Point 構成ファイルをエクスポートする手順」を参照してください。

Q. さまざまな Check Point（r80）展開タイプのログイン情報を事前設定する方法を教えてください。

A. 次のいずれかの方法により、移行前に Check Point（r80）デバイスでログイン情報を構成できます。

- 分散 Check Point 展開からのエクスポート
- スタンドアロン Check Point 展開からのエクスポート
- マルチドメイン Check Point 展開からのエクスポート

Q. Check Point Security Manager 用に Check Point r80 でカスタム API ポートを使用しています。構成を完全に取得する方法を教えてください。

A. Check Point API を使用するために Check Point Smart Manager でカスタム API ポートを使用している場合は、次の手順を実行します。

- [Check Point Security Manager] ページの [Check Point マルチドメイン展開（Check Point Multi-domain Deployment）] チェックボックスをオンにします。

- マルチドメイン展開を使用している場合は、Check Point CMA のIP アドレスと API ポートの詳細を追加します。
- 一般的な展開の Check Point Security Manager の場合、Check Point Security Manager の IPアドレスを保持し、カスタム API ポートの詳細を入力します。

Q. バージョン r80.40 の Check Point Gateway を使用しており、Live Connect を介した取得は問題なく実行できます。ただし、解析時に「Blocked VSX Feature is UNSUPPORTED in FTD」というエラーが表示されます。どうすればいいですか。

A. このエラーは、Check Point r80.40 以降で **fw vsx stat** コマンドが廃止されたために発生します。*networking.txt* ファイルを解析するときに **fw vsx stat** コマンドを実行すると、Firewall 移行ツールは値を解析できません。

回避策として、次の手順を実行します。

1. *config.zip* ファイルを解凍します。
2. *networking.txt* ファイルを開きます。

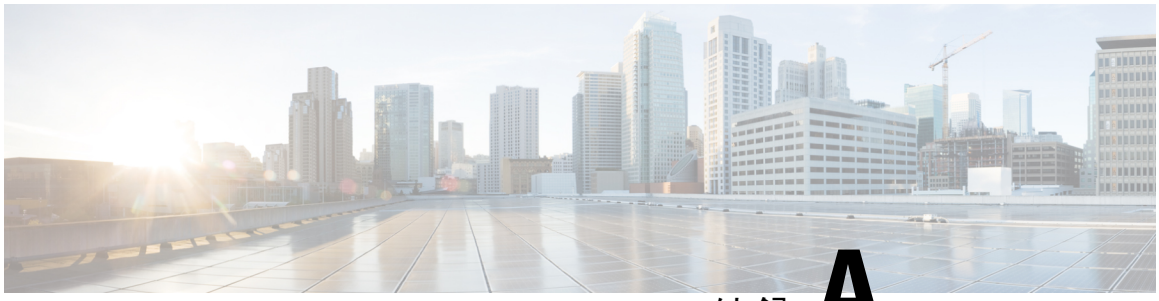
   次に、出力例を示します。

   ```
   firewall> fw vsx stat
   Deprecated command, Please see sk144112 for alternative
   Deprecated commands: cphaprob cpinfo cplic fw ips raidconfig fwaccel
   ```

   これを次のように手動で置き換えます。

   ```
   firewall> fw vsx stat
   VSX is not supported on this platform
   ```

3. すべてのファイルを選択し、.zip 拡張子に圧縮します。



付録 A

Cisco Success Network：テレメトリデータ

• Cisco Success Network：テレメトリデータ （73 ページ）

Cisco Success Network：テレメトリデータ

ファイアウォール移行ツールで移行プロセスを開始するたびに、対応するテレメトリデータファイルが固定の場所に保存されます。Cisco Success Network が有効な場合、移行した チェックポイント 構成を Firepower Management Center にプッシュすると、プッシュサービスはその場所からテレメトリデータファイルを読み取り、データがクラウドに正常にアップロードされた後に削除します。Cisco.com アカウントログイン情報の代わりにローカルログイン情報を使用して ファイアウォール移行ツールにログインする場合、テレメトリデータはクラウドにプッシュされず、データファイルは次の場所にあります。

`<migration_tool_folder>\resources \ telemetry_data`

次の表に、テレメトリデータポイント、その説明、およびサンプル値を示します。

表 *1*：システム情報

データ ポイント	説明	値の例
オペレーティング システム	ファイアウォール移行ツールを実行するオペレーティングシステム。Windows7、Windows10 64-bit、macOS High Sierra を使用できます	Windows 7
ブラウザ	ファイアウォール移行ツールの起動に使用したブラウザ。Mozilla/5.0、Chrome/68.0.3440.106、Safari/537.36 を使用できます	Mozilla/5.0

表 *2*：送信元 *Check Point* 情報

データ ポイント	説明	値の例
ソース タイプ	送信元デバイスタイプ	Check Point

Cisco Success Network：テレメトリデータ

データ ポイント	説明	値の例
Source Device Serial Number	Check Point のシリアル番号	デバイスのシリアル番号（存在する場合）。
Source Device Model Number	Check Point のモデル番号	
Source Device Version	Check Point のバージョン	R77.30
Source Config Counts	送信元構成の行の合計数	504
ファイアウォール モード	Check Point で構成されているファイアウォールモード：ルーテッドまたはトランスペアレント	ROUTED
コンテキスト モード	Check Point のコンテキストモード。これは、シングルコンテキストまたはマルチコンテキストになります。	シングル
Check Point Config Statistics:		
ACL Counts	アクセスグループにアタッチされている ACL の数	46
Access Rules Counts	アクセスルールの合計数	46
NAT Rule Counts	NAT ルールの合計数	17
Network Object Counts	Check Point で構成されたネットワークオブジェクトの数	34
Network Object Group Counts	Check Point のネットワーク オブジェクト グループの数	[6]
Port Object Counts	ポートオブジェクトの数	85
Port Object Group Counts	ポートオブジェクトグループの数	37
Unsupported Access Rules Count	サポートされていないアクセスルールの合計数	3
Unsupported NAT Rule Count	サポートされていない NAT アクセスルールの合計数	0
FQDN Based Access Rule Counts	FQDN ベースのアクセスルールの数	7
Time range Based Access Rule Counts	時間範囲ベースのアクセスルールの数	1
SGT Based Access Rule Counts	SGT ベースのアクセスルールの数	0

Cisco Success Network：テレメトリデータ

データ ポイント	説明	値の例
ツールが解析できない構成行の概要		
Unparsed Config Count	パーサーによって認識されない構成行の数	68
Total Unparsed Access Rule Counts	解析されないアクセスルールの合計数	3

表 *3 :* ターゲット管理デバイス（*Firepower Management Center*）情報

データ ポイント	説明	値の例
Target Management Version	Firepower Management Center のターゲットバージョン	6.2.3.3 (build 76)
Target Management Type	ターゲット管理デバイスのタイプ、つまり Firepower Management Center（FMC）	FMC
Target Device Version	ターゲットデバイスのバージョン	75
Target Device Model	ターゲットデバイスのモデル	Cisco Firepower Threat Defense for VMware
Migration Tool Version	移行ツールのバージョン	1.1.0.1912

表 *4 :* 移行の概要

データ ポイント	説明	値の例
アクセス コントロール ポリシー		
名前	アクセス コントロール ポリシーの名前	存在しない
Access Rule Counts	移行された ACL ルールの合計数	0
Partially Migrated ACL Rule Counts	部分的に移行された ACL ルールの合計数	3
Expanded ACP Rule Counts	拡張 ACP ルールの数	0
NAT ポリシー		
名前	NAT ポリシーの名前	存在しない
NAT Rule Counts	移行された NAT ルールの合計数	0
Partially Migrated NAT Rule Counts	部分的に移行された NAT ルールの合計数	0
その他の移行詳細		
Interface Counts	更新されたインターフェイスの数	0

Cisco Success Network：テレメトリデータ

データ ポイント	説明	値の例
Sub Interface Counts	更新されたサブインターフェイスの数	0
Static Routes Counts	静的ルートの数	0
Objects Counts	作成されたオブジェクトの数	34
Object Group Counts	作成されたオブジェクトグループの数	[6]
Interface Group Counts	作成されたインターフェイスグループの数	0
Security Zone Counts	作成されたセキュリティゾーンの数	3
Network Object Reused Counts	再利用されたオブジェクトの数	21
Network Object Rename Counts	名前が変更されたオブジェクトの数	1
Port Object Reused Counts	再利用されたポートオブジェクトの数	0
Port Object Rename Counts	名前が変更されたポートオブジェクトの数	0

表 *5:* ファイアウォール移行ツール パフォーマンスデータ

データ ポイント	説明	値の例
Conversion Time	チェックポイント 構成行の解析にかかった時間（分）	14
Migration Time	エンドツーエンドの移行にかかった合計時間（分）	592
Config Push Time	最終構成のプッシュにかかった時間（分）	7
Migration Status	Firepower Management Center への チェックポイント 構成移行のステータス	SUCCESS
エラー メッセージ	ファイアウォール移行ツールによって表示されるエラーメッセージ	null
エラーの説明	エラーが発生した段階および考えられる根本原因に関する説明	null

r77 のテレメトリ Check Point ファイルの例

次に、Firepower Threat Defense に Check Point 構成を移行する場合のテレメトリデータファイルの例を示します。

```
{
  "metadata": {
    "contentType": "application/json",
    "topic": "migrationtool.telemetry"
  },
  "payload": {
    "Check Point_config_stats": {
      "Ipv6_access_rule_counts": 0,
```

Cisco Success Network：テレメトリデータ


```
  "Ipv6_bgp_count": 0,
  "Ipv6_nat_rule_count": 0,
  "Ipv6_network_counts": 24,
  "Ipv6_static_route_counts": 6,
  "access_rules_counts": 63,
  "acl_counts": 63,
  "fqdn_based_access_rule_counts": 0,
  "nat_rule_counts": 0,
  "network_object_counts": 143,
  "network_object_group_counts": 31,
  "no_of_fqdn_based_objects": 0,
  "ospfv3_count": 0,
  "port_object_counts": 370,
  "port_object_group_counts": 55,
  "sgt_based_access_rules_count": 0,
  "timerange_based_access_rule_counts": 0,
  "total_unparsed_access_rule_counts": 0,
  "tunneling_protocol_based_access_rule_counts": 0,
  "unparsed_config_count": 15,
  "unsupported_access_rules_count": 0,
  "unsupported_nat_rule_count": 0
},
"context_mode": "SINGLE",
"error_description": null,
"error_message": null,
"firewall_mode": "ROUTED",
"log_info_acl_count": 0,
"migration_status": "SUCCESS",
"migration_summary": {
  "access_control_policy": [
    [
      {
        "access_rule_counts": 63,
        "apply_file_policy_rule_counts": 0,
        "apply_ips_policy_rule_counts": 0,
        "apply_log_rule_counts": 0,
        "do_not_migrate_rule_counts": 0,
        "enable_Global-ACL-Policy": true,
        "enable_Zone-Specific-ACL-Policy": false,
        "enable_hit_count": false,
        "expanded_acp_rule_counts": 1,
        "name": "FTD-Mig-1566804327",
        "partially_migrated_acl_rule_counts": 0,
        "update_rule_action_counts": 0
      }
    ]
  ],
  "interface_counts": 12,
  "interface_group_counts": 0,
  "interface_group_manually_created_counts": 0,
  "nat_Policy": [
    [
      {
        "NAT_rule_counts": 0,
        "do_not_migrate_rule_counts": 0,
        "name": "Doesn't Exist",
        "partially_migrated_nat_rule_counts": 0
      }
    ]
  ],
  "network_object_rename_counts": 0,
  "network_object_reused_counts": 0,
  "object_group_counts": 15,
  "objects_counts": 54,
```

Cisco Success Network：テレメトリデータ


```
      "port_object_rename_counts": 0,
      "port_object_reused_counts": 5,
      "security_zone_counts": 13,
      "security_zone_manually_created_counts": 0,
      "static_routes_counts": 22,
      "sub_interface_counts": 11
    },
    "migration_tool_version": "2.0.3169",
    "rule_change_acl_count": 0,
    "source_config_counts": 0,
    "source_device_model_number": "Check Point Model Not Exists",
    "source_device_serial_number": null,
    "source_device_version": "R77.30",
    "source_type": "Check Point",
    "system_information": {
      "browser": "Chrome/76.0.3809.100",
      "operating_system": "Windows NT 10.0; Win64; x64"
    },
    "target_device_model": "Cisco Firepower 9000 Series SM-24 Threat Defense",
    "target_device_version": "76",
    "target_management_type": "6.4.0.4 (build 31)",
    "target_management_version": "6.4.0.4 (build 31)",
    "template_version": "1.1",
    "time": "2019-08-26 12:55:40",
    "tool_analytics_data": {
      "objectsplit_100_count": 0
    },
    "tool_performance": {
      "config_push_time": 725,
      "conversion_time": 29,
      "migration_time": 1020
    }
  },
  "version": "1.0"
}
```


r80 のテレメトリ Check Point ファイルの例

次に、Firepower Threat Defense に Check Point 構成を移行する場合のテレメトリデータファイルの例を示します。

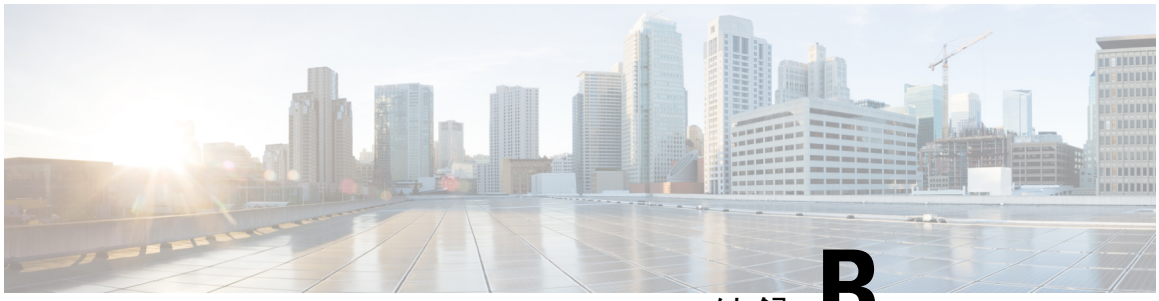

```
{
"Check Point_config_stats":{
        "Ipv6_access_rule_counts":0,
        "Ipv6_bgp_count":0,
        "Ipv6_nat_rule_count":0,
        "Ipv6_network_counts":3,
        "Ipv6_static_route_counts":0,
        "access_rules_counts":726,
        "acl_category_count":0,
        "acl_counts":726,
        "fqdn_based_access_rule_counts":0,
        "nat_rule_counts":335,
        "network_object_counts":7645,
        "network_object_group_counts":268,
        "no_of_fqdn_based_objects":0,
        "port_object_counts":1051,
        "port_object_group_counts":66,
        "s2s_vpn_tunnel_counts":0,
        "sgt_based_access_rules_count":0,
        "timerange_based_access_rule_counts":0,
        "total_unparsed_access_rule_counts":0,
        "tunneling_protocol_based_access_rule_counts":0,
```

Cisco Success Network：テレメトリデータ


```
"unparsed_config_count":234,
"unsupported_access_rules_count":0,
"unsupported_nat_rule_count":0},
"context_mode":"SINGLE",
"error_description":"No data.",
"error_message":"push failed for object network",
"firewall_mode":"ROUTED",
"log_info_acl_count":0,
"migration_status":"FAIL",
"migration_summary":{
  "access_control_policy":[
   [
   {
       "access_rule_counts":0,
       "apply_file_policy_rule_counts":0,
       "apply_ips_policy_rule_counts":0,
       "apply_log_rule_counts":0,
       "do_not_migrate_rule_counts":0,
       "enable_Global-ACL-Policy":true,
       "enable_Zone-Specific-ACL-Policy":false,
       "enable_hit_count":false,
       "expanded_acp_rule_counts":1,
       "name":"Doesn't Exist",
       "partially_migrated_acl_rule_counts":0,
       "total_acl_element_counts":389416,
       "update_rule_action_counts":0
    }
]
],
"interface_counts":11,
"interface_group_counts":0,
"interface_group_manually_created_counts":0,
"nat_Policy":[
[
    {
        "NAT_rule_counts":0,
        "do_not_migrate_rule_counts":0,
        "name":"Doesn't Exist",
        "partially_migrated_nat_rule_counts":0
    }
]
],
"network_object_rename_counts":0,
"network_object_reused_counts":0,
"object_group_counts":222,"objects_counts":7148,
"port_object_rename_counts":2,
"port_object_reused_counts":30,
"prefilter_control_policy":[
   [
     {
        "do_not_migrate_rule_counts":0,
        "name":null,
        "partially_migrated_acl_rule_counts":0,
        "prefilter_rule_counts":0
      }
    ]
    ],
"security_zone_counts":11,
"security_zone_manually_created_counts":0,
"static_routes_counts":0,
"sub_interface_counts":8,
"time_out":false},
"migration_tool_version":"2.1.4283",
"mtu_info":{"interface_name":null,
```

Cisco Success Network：テレメトリデータ


```
"mtu_value":null},
"rule_change_acl_count":0,
"selective_policy":
        {
        "acl":true,
        "acl_policy":true,
        "application":false,
        "csm":false,
"interface":true,
"interface_groups":true,
"migrate_tunneled_routes":false,
"nat":true,
"network_object":true,
"policy_assignment":true,
"populate_sz":false,
"port_object":true,
"routes":true,
"security_zones":true,
"unreferenced":true},
"source_config_counts":0,
"source_device_model_number":"Check Point Model Not Exists",
"source_device_serial_number":null,
"source_device_version":"R77.30",
"source_type":"Check Point",
"system_information":
{
"browser":"Chrome/80.0.3987.163","operating_system":
"Macintosh; Intel Mac OS X 10_15_4"},
"target_device_model":"Cisco Firepower 4110 Threat Defense",
"target_device_version":"76",
"target_management_type":"6.5.0 (build 63)",
"target_management_version":"6.5.0 (build 63)",
"template_version":"1.1",
"time":"2020-04-16 04:50:05",
"tool_analytics_data":{"objectsplit_100_count":6},
"tool_performance":
        {
                "config_push_time":1457,
                "conversion_time":279,
                "migration_time":2637
        }
}
```



付録 B

Check Point から Threat Defense 2100 への移行：例

• チェックポイント から Firewall Threat Defense 2100 への移行：例 （81 ページ）

チェックポイントから Firewall Threat Defense 2100 への移行：例

（注） 移行の完了後にターゲットデバイスで実行できるテスト計画を作成します。

• メンテナンスウィンドウの前に次のタスクを実行する （81 ページ）
• メンテナンスウィンドウ中に次のタスクを実行する （83 ページ）

メンテナンスウィンドウの前に次のタスクを実行する

始める前に

Firepower Management Center をインストールして展開していることを確認します。詳細については、適切な『Management Center Hardware Installation Guide』および適切な『Management Center Getting Started Guide』を参照してください。

ステップ 1 Check Point Web Visualization Tool および FMT-CP-Config-Extractor_v2.5.2-6575 ツールを使用して、移行しようとしている Check Point デバイス構成を収集し、Check Point 構成ファイルのコピーを保存します。

ステップ 2 Check Point 構成 zip ファイルを確認します。

ステップ 3 ネットワークに Firepower 2100 シリーズ デバイスを展開し、インターフェイスを接続してアプライアンスの電源をオンにします。

Check Point から Threat Defense 2100 への移行：例

詳細については、『Cisco Threat Defense for the 2100 Series Using Management Center Quick Start Guide』を参照してください。

ステップ 4 Firepower Management Center によって管理される Firepower 2100 シリーズ デバイスを登録します。

詳細については、「Add Devices to the Management Center」を参照してください。

ステップ 5 （任意）送信元チェックポイント構成に結合インターフェイスがある場合は、ターゲット Firepower 2100 シリーズ デバイスでポートチャネル（EtherChannel）を作成します。

詳細については、「Configure EtherChannels and Redundant Interfaces」を参照してください。

ステップ 6 ファイアウォール移行ツールの最新バージョンを https://software.cisco.com/download/home/286306503/type からダウンロードして実行します。

詳細については、Cisco.com から Firewall 移行ツールのダウンロード （23 ページ）を参照してください。

ステップ 7 ファイアウォール移行ツールを起動し、接続先パラメータを指定する場合は、Firepower Management Center に登録した Firepower 2100 シリーズ デバイスを選択します。

詳細については、Firewall 移行ツールの接続先パラメータの指定 （43 ページ）を参照してください。

ステップ 8 チェックポイント 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ます。

（注） ファイアウォール移行ツールでは、チェックポイントインターフェイスタイプを FTD インターフェイスタイプにマッピングできます。

たとえば、Check Point の結合インターフェイスを FTD の物理インターフェイスにマッピングできます。

詳細については、「チェックポイント 構成と Threat Defense インターフェイスのマッピング」を参照してください。

ステップ 9 論理インターフェイスをセキュリティゾーンにマッピングするときに、[自動作成（Auto-Create）] をクリックして、ファイアウォール移行ツールで新しいセキュリティゾーンを作成できるようにします。既存のセキュリティゾーンを使用するには、手動で チェックポイント 論理インターフェイスをセキュリティゾーンにマッピングします。

詳細については、「セキュリティゾーン とインターフェイスグループへの チェックポイント インターフェイスのマッピング」を参照してください。

ステップ 10 このガイドの手順に従って、移行する構成を順に確認および検証し、構成を Firepower Management Center にプッシュします。

ステップ 11 移行後レポートを確認し、手動で他の構成をセットアップして FTD に展開し、移行を完了します。

詳細については、「移行後レポートの確認と移行の完了 （58 ページ）」を参照してください。

ステップ 12 移行の計画時に作成したテスト計画を使用して、Firepower 2100 シリーズ デバイスをテストします。

メンテナンスウィンドウ中に次のタスクを実行する

始める前に

メンテナンスウィンドウの前に実行する必要があるすべてのタスクが完了していることを確認します。メンテナンスウィンドウの前に次のタスクを実行する （81 ページ）を参照してください。

ステップ 1 Gaia Console を介して Check Point Security Gateway に接続します。

ステップ 2 Gaia Console を介して目的の Security Gateway の Check Point インターフェイスをシャットダウンします。

ステップ 3 （任意）Firepower Management Center にアクセスし、Firepower 移行ツールによって移行されないダイナミックルーティング、プラットフォーム設定、およびその他の機能を、手動で Firepower 2100 シリーズ デバイス用に構成します。

ステップ 4 周辺スイッチング インフラストラクチャの Address Resolution Protocol（ARP）キャッシュをクリアします。

ステップ 5 周辺スイッチング インフラストラクチャから Firepower 2100 シリーズ デバイスインターフェイスの IP アドレスに対して基本的な ping テストを実行し、アクセス可能であることを確認します。

ステップ 6 Firepower 2100 シリーズ デバイスインターフェイスの IP アドレスに対するレイヤ 3 ルーティングが必要なデバイスから基本的な ping テストを実行します。

ステップ 7 Firepower 2100 シリーズ デバイスに新しい IP アドレスを割り当て、 チェックポイント デバイスに割り当てられた IP アドレスを再利用しない場合は、次の手順を実行します。

1. IP アドレスを参照する静的ルートを更新し、Firepower 2100 シリーズ デバイスの IP アドレスを指すようにします。
2. ルーティングプロトコルを使用している場合は、ネイバーが Firepower 2100 シリーズ デバイスの IP アドレスを予期される接続先のネクストホップとして認識していることを確認します。

ステップ 8 包括的なテスト計画を実行し、Firepower 2100 デバイスの管理 Firepower Management Center 内でログをモニタします。

メンテナンスウィンドウ中に次のタスクを実行する