Firepower 移行ツールを使用した Palo Alto Networks ファイアウォールから Firepower Threat Defense への移行

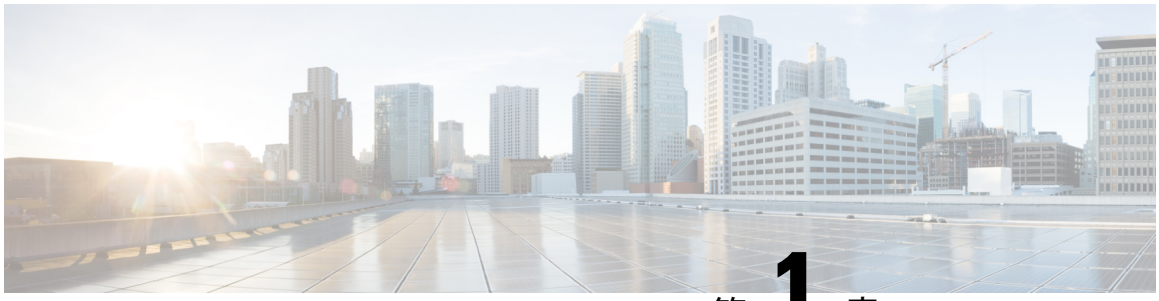
初版：2020 年 7 月 1 日

最終更新：2021 年 1 月 27 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

Firepower 移行ツールについて

FirePOWER 移行ツール について

資料

本書『*Firepower* 移行ツールを使用した *Palo Alto Networks*（*PAN*）ファイアウォールから *Firepower Threat Defense* への移行』に記載のすべての情報は、FirePOWER 移行ツール の最新バージョンを参照しています。「Cisco.com からの FirePOWER 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 Firepower 移行ツールをダウンロードします。

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

Firepower 移行ツール

FirePOWER 移行ツール（FMT）は、サポートされている PAN 構成をサポートされている Firepower Threat Defense（FTD）プラットフォームに変換します。Firepower 移行ツールを使用すると、サポートされている PAN 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。

Firepower 移行ツールは PAN 情報を収集して解析し、最終的に Firepower Management Center にプッシュします。解析フェーズ中に、Firepower 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 PAN 構成の XML 行

- PAN には、Firepower 移行ツールが認識できない PAN XML 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 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、インターフェイスをFTDインターフェイスにマッピングし、アプリケーションをマッピングし、セキュリティゾーンをマッピングして、構成の確認と検証に進むことができます。その後、構成を接続先デバイスに移行できます。

Firepower 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。

- **PAN 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、Firepower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。

- [Review and Validate] ページ

（注） この段階でFirepower移行ツールを終了して再起動すると、[Review and Validate] ページが表示されます。

コンソール

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

Firepower 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 Firepower 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。Firepower 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

Firepower 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。

Firepower 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

Firepower 移行ツールは、**移行前レポート**、**移行後レポート**、 PAN 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

Firepower移行ツールは、未解析ファイルで無視した構成行に関する情報をログに記録します。この Firepower 移行ツールは、 PAN 構成ファイルを解析するときにこのファイルを作成します。

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

Firepower 移行ツールでの検索

[Review and Validate] ページの項目など、Firepower 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。Firepower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 [Search] フィールドに検索語を入力します。Firepower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

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

Firepower 移行ツールの履歴

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

Firepower 移行ツールのライセンス

Firepower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、Firepower Threat Defense への正常な登録とポリシーの展開のため、Firepower Management Center には関連する Firepower 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、Firepower 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、Firepower 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。

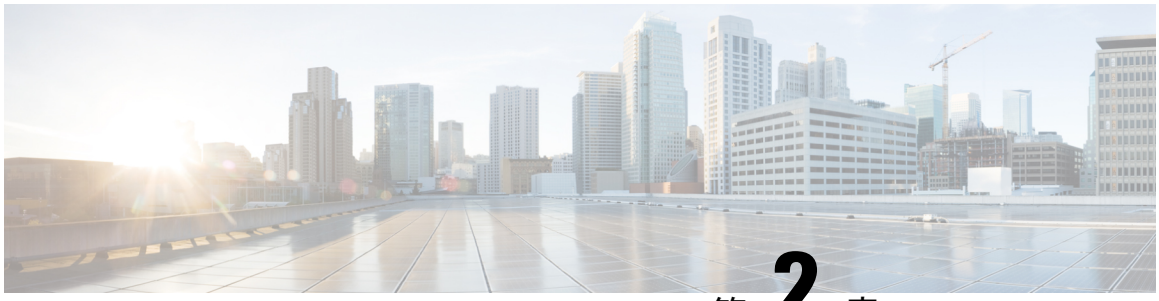
Firepower 移行ツールは常にセキュアな接続を確立および維持し、Cisco Success Network に登録できるようにします。Cisco Success Network を無効にすることで、いつでもこの接続をオフにできます。これにより、デバイスが Cisco Success Network クラウドから接続解除されます。

Cisco Success Network の有効化と無効化

Firepower 移行ツールの [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、「Firepower 移行ツールの起動 （18 ページ）」を参照してください。移行ごとに、Firepower 移行ツールの [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 （47 ページ）を参照してください。

免責事項

Firepower 移行ツール（「ツール」）は、サポート対象のサードパーティ製品の構成を、有効なライセンス対象およびサポート対象である FTD プラットフォーム用の Firepower Threat Defense（「FTD」）構成に容易に変換できるように設計されています。ツールによって作成された FTD セキュリティポリシーと設定は、変換の完了後に手動で構成する必要があります。お客様は、構成を確認およびテストして、実装前に正確かつ完全であることを確認する責任を負います。ツールは「現状のまま」提供され、シスコは、ツールがお客様のビジネス要件を満たすこと、またはお客様の既存システムで動作することについて、いかなる表明も保証もいたしません。



第 2 章

移行の準備

Firepower 移行ツールに関する注意事項と制約事項

PAN 構成を移行する前に、 PAN 構成、Firepower Threat Defense デバイス、および FirePOWER 移行ツール に関する次の注意事項と制約事項を考慮してください。

PAN 構成

PAN 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 PAN 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 （13 ページ）を参照）。
- 移行でサポートされる PAN 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 （14 ページ）を参照）。

（任意）ターゲット Firepower Threat Defense デバイス

Firepower Management Center に移行すると、ターゲット Firepower Threat Defense デバイスが追加される場合とされない場合があります。

Firepower Threat Defense デバイスへの今後の展開のために、共有ポリシーを Firepower Management Center に移行できます。デバイス固有のポリシーを Firepower Threat Defense に移行するには、Firepower Management Center に追加する必要があります。

- ターゲット Firepower 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：Firepower Threat Defense デバイスに関する注意事項と制約事項 （9 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 （13 ページ）を参照）。
- 移行でサポートされる Firepower 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 （14 ページ）を参照）。
- Firepower Management Center に登録されている Firepower Threat Defense デバイス。

Firepower Management Center

- 移行でサポートされる Firepower Management 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 （14 ページ）を参照）。
- PAN の移行でサポートされる Firepower Management Center ソフトウェアバージョンは 6.1.x 以降です。
- PAN 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 Firepower 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。
  - Firepower システムのライセンス

FirePOWER 移行ツール

- Firepower 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（のプラットフォームの要件 FirePOWER 移行ツール （15 ページ）を参照）。
- Firepower 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。Firepower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。Firepower 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。

- Firepower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、Firepower Management Center の構成を変更または更新しないでください。

Firepower Threat Defense デバイスに関する注意事項と制約事項

構成を Firepower Threat Defense に移行することを計画する場合は、次の注意事項と制約事項を考慮してください。

- ルート、インターフェイスなど、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 Firepower 移行ツールは自動的にデバイスを消去し、 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、Firepower 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、Firepower 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。

- Firepower 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 Firepower 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 Firepower 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、Firepower 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。

PAN 構成に関する注意事項と制約事項

Firepower移行ツールは、変換中に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。 Firepower 移行ツールには、未使用のオブジェクト（ACL および NAT 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、NAT ルール、およびルートを移行しません。

PAN 構成の制約事項

送信元 PAN 構成の移行には、次の制限があります。

- Firepower 移行ツールを使用すると、マルチ VSYS を移行できます。
- システム構成は移行されません。
- ダイナミックルーティングやVPNなどの一部のPAN構成は、Firepower移行ツールによって移行されないため、手動で移行する必要があります。
- 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、1つの回線にある送信元ポートと宛先ポートを持つ拡張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、同じ意味の Firepower Management Center ルールに変換されます。

PAN 移行の注意事項

Firepower 移行ツールは、次のような Firepower Threat Defense 構成のベストプラクティスを使用します。

- ACL 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PAN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 **deny** 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。

サポートされる PAN 構成

Firepower 移行ツールは、次の PAN 構成を完全に移行できます。

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

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

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

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

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

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

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

（注） 仮想ワイヤインターフェイスは移行されませんが、仮想ワイヤゾーンは移行されます。移行後、FTD で BVI インターフェイスを手動で作成する必要があります。

部分的にサポートされる PAN 構成

Firepower 移行ツールは、次の PAN 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されます。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。

- プロファイルを使用したアクセス コントロール ポリシー ルール
- TCP、UDP、SCTP を含むプロトコルを使用するサービスオブジェクトを含むサービスグループ。

（注） SCTP タイプが削除され、サービスグループが部分的に移行されます。

- サポートされているオブジェクトとサポートされていないオブジェクトを含むオブジェクトグループは、サポートされていないオブジェクトを削除することによって移行されます。

サポートされない PAN 構成

Firepower 移行ツールは、次の PAN 構成の移行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、移行の完了後に構成を手動で構成できます。

- 時間ベースのアクセス コントロール ポリシー ルール
- ユーザベースのアクセス コントロール ポリシー ルール
- プロトコル SCTP を使用するサービスオブジェクト
- 特殊文字で始まる、または特殊文字を含む FQDN オブジェクト
- ワイルドカード FQDN

- SCTP で構成された NAT ルール
- 送信元または接続先に FQDN オブジェクトを含む NAT ルール
- IPv6 NAT
- URL フィルタリングを使用するポリシー
- アプリケーションが "any" で、サービスが "application-default" であるポリシー

FTD でサポートされていない機能を構成するには、『FTD Configuration Guide』を参照してください。

（注） サポートされているポリシーもサポートされていないポリシーもすべてFMCに移行されます。サポートされていないポリシーは、無効として移行されます。これらのポリシーは、回避策の後、または FMC に従って構成した後に、有効にすることができます。

プロファイル URL フィルタリング、ユーザ ID、送信元、または宛先ネゲートを含むポリシーは**サポートされていません**。

移行がサポートされるプラットフォーム

次の PAN および Firepower Threat Defense プラットフォームは、FirePOWER 移行ツール を使用した移行で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。

サポートされるターゲット Firepower Threat Defense プラットフォーム

Firepower 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 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 仮想 （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

Firepower 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。

Firepower 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 Firepower 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、Firepower 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） Firepower 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、手動でアップロードした構成をクラウド内の FMC に移行させます。そのため、前提条件として、Firepower 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

移行でサポートされている PAN および Firepower Threat Defense のバージョンは次のとおりです。

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

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

送信元 PAN 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

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

（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

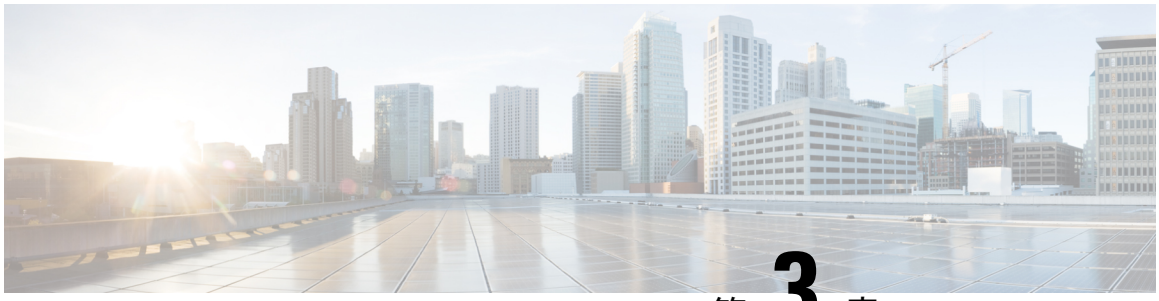
Firepower 移行ツールでは、Firepower Threat Defense のバージョン 6.2.3 以降を実行しているデバイスへの移行が推奨されます。

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

のプラットフォームの要件 FirePOWER 移行ツール

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

- Windows 10 64 ビット オペレーティング システムまたは macOS バージョン 10.13 以降で実行している
- Google Chrome がシステムのデフォルトブラウザである
- （Windows）[Power & Sleep] で [Sleep] 設定が [Never put the PC to Sleep] に設定されているため、大規模な移行プッシュ中にシステムがスリープ状態にならない
- （macOS）大規模な移行プッシュ中にコンピュータとハードディスクがスリープ状態にならないように [Energy Saver] 設定が構成されている



第 3 章

移行の実行

Cisco.com からの FirePOWER 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、Firepower 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。Firepower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） Firepower 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、[Firepower Migration Tool] をクリックします。

上記のリンクをクリックすると、[Firepower NGFW Virtual] の [Firepower 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 Firepower 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 Firepower 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 Firepower 移行ツール実行可能ファイルをダウンロードします。

Firepower 移行ツールの起動

（注） Firepower 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、Firepower 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、Firepower 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 からの FirePOWER 移行ツール のダウンロード
- Firepower 移行ツールに関する注意事項と制約事項 （7 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、Firepower 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、Firepower 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、[Yes] をクリックして、Firepower 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。

Firepower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、Firepower 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、Firepower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 Firepower_Migration_Tool-version_number.command
```

```
# ./Firepower_Migration_Tool-version_number.command
```

Firepower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 Firepower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Firepower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 [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、[I agree to share data with Cisco Success Network] をクリックし、それ以外の場合は [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 Firepower 移行ツールにログインします。

ステップ 4 Firepower 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、[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 [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、Firepower 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 [New Migration] をクリックします。

ステップ 10 [Software Update Check] 画面で、Firepower 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 [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。

- Firepower 移行ツールを使用して PAN ファイアウォールから情報を抽出する必要がある場合は、「Palo Alto Networks ファイアウォールからの構成のエクスポート」に進みます。

Palo Alto Networks ファイアウォールからの構成のエクスポート

デバイスが Panorama で管理されている場合は、ゲートウェイから設定を抽出する必要があります。Panorama 設定をゲートウェイと統合し、設定を抽出します。ゲートウェイから構成を抽出するには、次の手順を実行します。

ステップ 1 [Device] > [Setup] > [Operations] に移動し、[Save Named Configuration <file_name.xml>] を選択します。

ステップ 2 [OK] をクリックします。

ステップ 3 [Device] > [Setup] > [Operations] に移動し、[Export Named Configuration] をクリックします。

ステップ 4 <file_name.xml> ファイルを選択します。

ステップ 5 [OK] をクリックします。

ステップ 6 実行構成 <file_name.xml> を含む XML ファイルを選択し、[Ok] をクリックして構成ファイルをエクスポートします。

ステップ 7 エクスポートしたファイルをファイアウォールの外部の場所に保存します。このバックアップを使用してファイアウォール移行ツールにアップロードし、構成を Firepower Threat Defense に移行できます。

ステップ 8 （任意）接続先 NAT に同じ送信元ゾーンと接続先ゾーンがある NAT ポリシーがある場合は、次の手順を実行します。

a) ファイアウォールで CLI から **show routing route** コマンドを実行します。

b) ルーティングテーブルを .txt ファイルにコピーします。

c) この .txt ファイルをフォルダに追加します。このフォルダで .txt ファイルと .xml ファイル（panconfig.xml を含む）を圧縮します。

これらのステップは、移行に必須ではありません。これらのステップを実行しない場合、接続先ゾーンは Firepower 移行ツールでの移行中にマッピングされず、移行レポートに含まれます。

（注） **show routing route** コマンドを使用して、ルーティングテーブルの詳細を抽出します。抽出した出力をメモ帳に貼り付けます。

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

Palo Alto Gateway ファイアウォールの panconfig.xml、および route.txt をエクスポートします（同じ送信元ゾーンと宛先ゾーンを持つ NAT ルールがある場合）。

Firepower 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 Firepower 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。Firepower 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 [Select Target] 画面の [Connect to Firepower 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 [Firepower Management Center Login] ダイアログボックスで、Firepower 移行ツール専用アカウントのユーザ名とパスワードを入力し、[Login] をクリックします。

Firepower 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 [Proceed] をクリックします。

[FTD の選択（Choose FTD）] セクションでは、移行先の Firepower Threat Defense デバイスを選択できます。また、Firepower Threat Defense デバイスがない場合は、構成の共有ポリシー（アクセス制御リスト、NAT、およびオブジェクト）を Firepower Management Center に移行できます。

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。

- [Firepower Threat Defense デバイスの選択（Select Firepower Threat Defense Device）] ドロップダウンリストをクリックし、 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 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。 構成と同じファイアウォールモードでデバイスを構成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 Palo Alto Networks ファイアウォールの移行は、Firepower 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。

- [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、Firepower 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、Firepower 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 [Proceed] をクリックします。

移行先に応じて、Firepower 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 [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、Firepower 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、 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、Firepower 移行ツールは、[共有設定（Shared Configuration）] セクションで、 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。

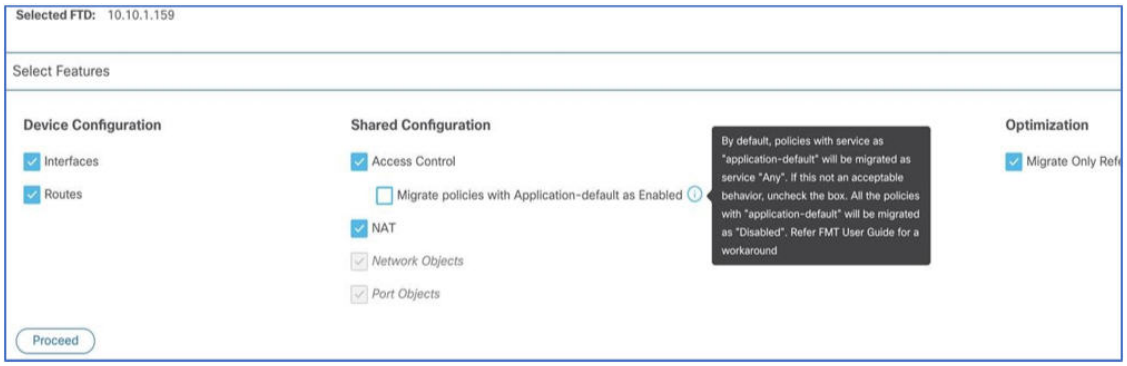
（注） [Device Configuration] セクションは、移行先 Firepower Threat Defense デバイスを選択していない場合は使用できません。

- PAN の場合は、[Shared Configuration] で、関連する [Access Control] オプションを選択します。

  Migrate policies with Application-Default as Enabled：このオプションを選択すると、PAN アプリケーションが移行されます。

  このチェックボックスをオンにした場合にのみ、[Migrate policies with Application-Default as Enabled] オプションが表示されます。

  （注） [Application Mapping] は、ポリシーが移行対象として選択されている場合にのみ有効になります。



サービスが "Application-Default" であるポリシー

サービスが "**application-default**" であり、アプリケーションが参照されているメンバーまたはグループを持つポリシーは、[Feature Selection] ページでの選択に従って移行されます。FMC には **application-default** に相当するものがないため、このようなポリシーはサービス "any" でプッシュされます。**application-default** と同様の機能を複製する場合は、アプリケーションが使用するポートを Palo Alto Networks ファイアウォールから見つけ、FMC の [ポリシー（Policy）] のポートセクションでそのポートを構成します。

たとえば、"**web-browsing**" を持ち、サービスが"**application-default**" であるポリシーは、アプリケーション HTTP（web-browsing と同等）と "**any**" ポートとして移行されます。"**application-default**" と同じ機能を複製するには、ポートを TCP/80 および TCP/8080 として構成します。web-browsing は、ポート TCP 80 および TCP 8080 を使用します。ポリシーに複数のアプリケーションがある場合は、各アプリケーションで使用されるポートを構成します。

ポリシーに複数のアプリケーションがある場合は、ポートを構成する前にポリシーを分割することを推奨します。これにより、他のアプリケーションへの追加アクセスが許可される可能性があるためです。

"**any**" として構成されたアプリケーションと "**application-default**" として構成されたサービスが設定されているポリシーは、[Feature Selection] ページで選択できる項目（アプリケーションは "**any**"、サービスは"**any**"）に関係なく、無効として移行されます。これが許容可能な動作である場合は、アプリケーションを有効にして変更をコミットします。それ以外の場合は、必要なアプリケーションまたはサービスを選択し、ポリシーを有効にします。

- （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、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 [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 Firepower 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 [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、Firepower 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 （24 ページ）

移行前レポートの確認

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、Firepower 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、Firepower 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。

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

- Configuration Lines with Errors：Firepower 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 構成要素の詳細。 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 Firepower 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 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、Firepower 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：Firepower 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 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、Firepower 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 Firepower 移行ツールでサポートされていないために無視される 構成要素の詳細。Firepower 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、 インターフェイス で修正を完了し、 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 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、Firepower 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

PAN ファイアウォール 構成と Firepower Threat Defense インターフェイスのマッピング

PAN ファイアウォール 構成と Firepower 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、 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。

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 PAN 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またはサブインターフェイスが同数以上必要です（PAN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。
- 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 Firepower 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 PAN 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（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 PAN 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。

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、「Firepower 移行ツールの接続先パラメータの指定 （21 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、[Firepower Threat Defense インターフェイス名（Firepower Threat Defense Interface Name）] のドロップダウンリストをクリックし、その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。Firepower 移行ツールは、Firepower Threat Defense 構成内のすべてのサブインターフェイスについて デバイスのサブインターフェイスをマッピングします。

（注） 送信元ファイアウォールのインターフェイスの数がターゲットファイアウォールのインターフェイスの数よりも多い場合は、ターゲットファイアウォールにサブインターフェイスを作成し、移行を再試行します。

ステップ 2 各 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

PAN インターフェイスを適切な Firepower Threat Defense インターフェイス オブジェクトと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への PAN 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への PAN インターフェイスのマッピング

構成が正しく移行されるように、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にマッピングします。 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。

Firepower 移行ツールでは、セキュリティゾーン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の詳細については、「Security Zones」を参照してください。

ステップ 1 [Map Security Zones] 画面で、使用可能なインターフェイスとセキュリティゾーンを確認します。

ステップ 2 Firepower Management Center に存在するセキュリティゾーンにインターフェイスをマッピングするには、[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。

ステップ 3 セキュリティゾーンは、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。

セキュリティゾーンを手動でマッピングするには、次の手順を実行します。

a) [Add SZ & IG] をクリックします。
b) [Add SZ & IG] ダイアログボックスで、[Add] をクリックして新しいセキュリティゾーンを追加します。
c) [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。
d) [Close] をクリックします。

セキュリティゾーン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) [Auto-Create] をクリックします。
b) [Auto-Create] ダイアログボックスで、[Zone Mapping] をオンにします。
c) [Auto-Create] をクリックします。

[Auto-Create] をクリックすると、送信元ファイアウォールゾーンが自動的にマッピングされます。同じ名前のゾーンがFMCにすでに存在する場合、そのゾーンは再利用されます。マッピングページには、再利用ゾーンに対して "(A)" が表示されます。たとえば、**inside** "(A)" となります。

ステップ 4 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にマッピングしたら、[Next] をクリックします。

構成とアプリケーションのマッピング

アプリケーションを対応するターゲットアプリケーションにマッピングできます。アプリケーションに基づくルールを移行できます。

Firepower Management Center（FMC）の定義済みアプリケーションと、構成ファイルに含まれる一部のアプリケーションのリストが、このタブにはリストされます。FMC に存在する定義済みマッピングの一部がマップされます。

（注） 定義済みマッピングを編集することはできません。

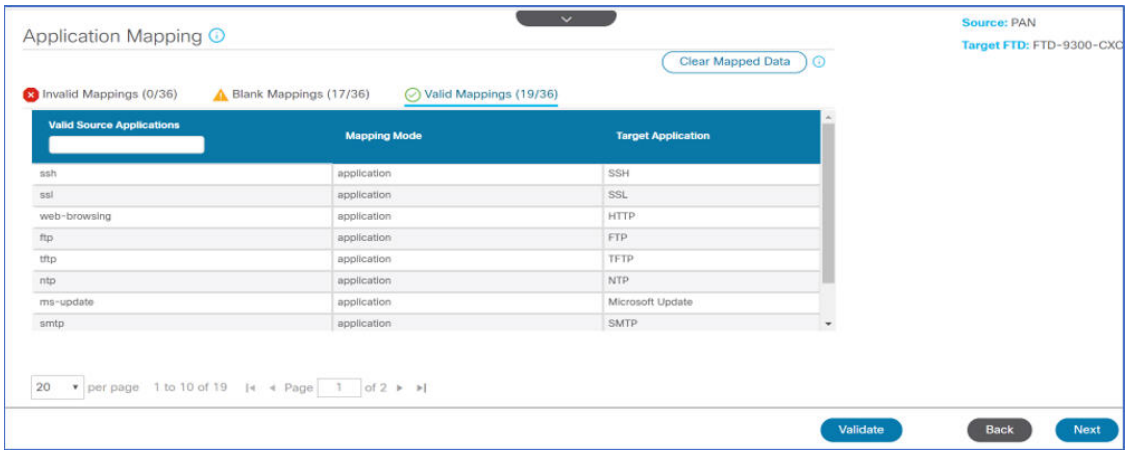
[Application Mapping] ページには、次のタブが表示されます。

- Invalid Mappings：その移行で無効なマッピングのリストを表示します。

  マッピングは、次のシナリオで **Invalid** と呼ばれます。

  - [Mapping Mode] に [Application] または [Port] が選択されているが、[Target] が空の場合。
  - [Mapping Mode] が [Port] で、ポートの構文が正しくない場合。移行を続行するには、[Invalid Mapping] をゼロにする必要があります。

（注） 正しい検証が行われるまで、[Next] ボタンは無効になります。



送信元からマッピングの定義済みリストを取得すると、自動的にマップされる定義済みアプリケーションがあります。マップされていないアプリケーションがある場合は、ポートまたはアプリケーションに手動でマップする必要があります。

- Blank Mappings：マッピングされていないアプリケーションを表示し、ユーザアクションを要求します。**アプリケーション**は、**アプリケーション**または**ポート**にマッピングされている必要があります。

（注） すべての**アプリケーション**をマッピングすることを推奨しますが、必須ではありません。

マッピングモードが選択され、ターゲットアプリケーションに有効なデータがある場合、それは有効なマッピングです。

（注） デフォルトでは、すべての定義済みマッピングを [Valid Mappings] タブで使用できます。

- Valid Mappings：正しいマッピングを表示します。Firepower 移行ツールには、一般的に使用されるアプリケーション用に PAN および FTD のアプリケーションとの定義済みマッピングのデータベースが独自に用意されています。PAN アプリケーションが定義済みマッピング DB と一致する場合、それらのアプリケーションは自動的にマッピングされ、有効なマッピングの下に表示されます。

  アプリケーションが [Blank Mapping] で**アプリケーション**または**ポート**にマッピングされると、検証後に [Valid Mapping] に移動されます。

（注） 定義済みマッピングは編集できません。

無効、有効、およびブランクのマッピング数は、移行に基づいて変化し続けます。

次の表に、アプリケーションマッピングのプロパティを示します。

表 *1:* アプリケーション マッピング テーブル プロパティ

フィールド	説明
送信元アプリケーション（Source Application）	PAN で使用されるアプリケーションのリストを表示します。
Mapping Mode	[Application] または [Port(s)] のいずれかのマッピングモードを選択します。 • Application：マッピングに使用可能なターゲットアプリケーションのリストから選択します。マッピングできるアプリケーションは 1 つだけです。 • Port(s)：マッピングに使用できるポートのリストから選択します。[Ports] を選択する場合は、指定された形式で関連するポート情報を入力します。たとえば、tcp/80 や udp/80 です。 （注） 文字間のスペースは使用できません。
対象のアプリケーション（Target Application）	マッピングモードに基づくターゲットアプリケーションまたはポートのリストを表示します。

ICMP および Ping のアプリケーションは、**ICMP** および **ping** のサービスとして移行されます。これは Firepower 移行ツールによって自動的に実行されるため、[Application Mapping] ページには表示されません。

ステップ 1 [Invalid Mappings] タブをクリックして、無効なマッピングのリストを表示します。次の手順を実行します。

a) Invalid Application：移行中に無効なマッピングが表示されます。
b) Mapping Mode：[Application] または [Port] のいずれかのマッピングモードを選択します。
c) Target Application：アプリケーションマッピングのターゲットアプリケーションを選択します。

たとえば、マッピングモードを選択したが、別のターゲット接続先にマップした場合、他のタブに進むことはできません。[Invalid Mappings] タブを確認し、正しいターゲットアプリケーションを入力して、アプリケーションマッピングを実行します。

ステップ 2 [Valid Mappings] タブをクリックして、その移行に有効なマッピング数を表示します。**有効な送信元アプリケーション**と、有効な**マッピングモード**および**ターゲットアプリケーション**をマッピングします。

マッピングが有効になると、有効なマッピング数の増加を確認できます。

ステップ 3 [Blank Mappings] をクリックして、その移行のブランクマッピングのリストを表示します。**ブランク送信元アプリケーション**と、有効な**マッピングモード**および**ターゲットアプリケーション**をマッピングします。

たとえば、マッピングモードを選択し、ターゲット接続先を入力せずに保存すると、ブランクマッピング数が増加します。タブを確認して正しくマッピングし、移行を続行します。

（注） ブランクマッピングがある場合でも、移行を続行できます。

ステップ 4 各タブで [Validate] をクリックして、その移行の無効なマッピング、ブランクマッピング、または有効なマッピングを検証します。

ステップ 5 [Next] をクリックして続行します。

ステップ 6 [Clear Mapped Data] をクリックして、アプリケーションマッピングを最後に保存したバージョンにリセットします。

次のタスク

移行する構成の確認と検証

移行する構成の確認と検証

移行した 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、Firepower 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。

[Review and Validate Configuration] 画面で Firepower 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 Firepower 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、[Interface Mapping] 画面から Firepower 移行ツールを再起動します。

ステップ 1 [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。

a) 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。

b) 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。

[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、[Save] をクリックします。

c) 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 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、[Save] をクリックします。

d) 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。

[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。

e) アクセスコントロール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、[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 2 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**
- スタティック ルート

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、**[Actions]** > **[Do not migrate]** を選択して、[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 3 （任意）構成の確認中に、[Network Objects] タブまたは [Port Objects] タブで **[Actions]** > **[Rename]** を選択して、1 つ以上の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 4 （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、[Download] をクリックします。

ステップ 5 確認が完了したら、[Validate] をクリックします。

検証中、Firepower 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、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。オブジェクトがすでに Firepower Management Center に存在する場合、Firepower 移行ツールは次の処理を実行します。

- オブジェクトの名前と構成が同じ場合、Firepower 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、Firepower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 6 検証が完了し、[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) [Resolve Conflicts] をクリックします。

Firepower 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、[Network Objects] タブまたは [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、**[Actions]** > **[Resolve Conflicts]** を選択します。
d) [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) [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、[Save] をクリックします。
g) [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 7 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 （34 ページ）に進みます。

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） Firepower 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 [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 構成を Firepower Management Center に送信します。

Firepower 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、[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、Firepower 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. [Complete Migration] 画面で、[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. [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. [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. [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、Firepower 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、 構成がどのように移行されたかを理解します。

- Migration Summary： Firepower Threat Defense へ正常に移行された構成の概要。 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 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。
- 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、 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：正常に移行された PAN 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 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、Firepower 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：Firepower 移行ツールで移行しないように選択したルールの詳細。Firepower 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 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：Firepower 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に移行されなかった 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 Point ルールから複数の Firepower Threat Defense ルールに拡張された 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**
  - Access Rules You Chose Not to Migrate：Firepower 移行ツールで移行しないように選択した 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：Firepower 移行ツールを使用して「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 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 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：Firepower 移行ツールを使用して「ログ設定」が変更された 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。Firepower 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、デバイスで手動で移行する必要がある Firepower Threat Defense 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
- スタティック ルート
- インターフェイス
- 時間ベースのオブジェクト

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。

Firepower 移行ツールは、ポリシーを Firepower Threat Defense デバイスに割り当てます。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 構成のホスト名が含まれています。

解析のサマリー

解析のサマリーには、オブジェクト、インターフェイス、NAT、ポリシー、およびアプリケーションの数が表示されます。サマリーには、[Pre-parse Summary]、[Parse Summary]、および [Pre-push Summary] の 3 つのコンポーネントがあります。

- Pre-parse Summary：構成のアップロード後に、解析前サマリーが表示されます。この段階で、Firepower 移行ツールはさまざまなコンポーネントの数を表示します。カスタムアプリケーション、またはグループで使用されているアプリケーションのみが表示されます。構成がマルチ VSYS の場合、完全な VSYS のインターフェイス数が表示されます。ポリシーで直接呼び出されるアプリケーションはカウントされないため、解析前サマリーには一部のアプリケーションが表示されません。したがって、アプリケーション数は解析のサマリーと異なります。同様の動作が NAT にも適用されます。解析前サマリーの一部のコンポーネントにはゼロカウントが表示される場合がありますが、これはこれらの構成の構成要素が 0 であることを意味しません。
- Parse Summary：変換の開始をクリックすると、解析のサマリーが表示されます。この段階で、Firepower 移行ツールは構成に対してアクションを実行し、サポートされていないすべての構成がサマリーカウントから削除されます。サポートされていないポリシーは無効として FMC に移行されるため、サポートされていないポリシーはカウントの一部になります。構成の各コンポーネントが解析されます。解析のサマリーで表示されるカウントは、移行される正確な構成カウントです。
- Pre-push Summary：構成を FMC にプッシュするよう求めるプロンプトが表示される前に、プッシュ前サマリーが表示されます。解析前サマリーのカウントは、Firepower 移行ツールによって実行されるアクションによって、解析のサマリーと異なる場合があります。NAT で直接参照される IP は、オブジェクトとしてプッシュされます。アプリケーションがポートにマッピングされると、サービスカウントが増加し、アプリケーションがダウンします。アプリケーションマッピングを空白のままにすると、アプリケーション数は減少します。静的ルートに重複するエントリがある場合、そのエントリは削除され、カウントは減少します。

移行の失敗

移行中の解析エラーは次のとおりです。

- **解析の失敗**：構成が Firepower 移行ツールにアップロードされた後に解析が失敗します。インターフェイスの不良構成が原因です。複数の IP が構成されているか、/32 または /128 の IP がインターフェイスに割り当てられている場合、解析に失敗します。

  インターフェイスに複数の IP が割り当てられている場合、またはトンネリング、ループバック、VLANインターフェイスがルーティングの一部である場合は、プッシュの失敗が発生します。

  回避策：**移行前レポート**をダウンロードし、移行レポートの [Configuration lines with errors] セクションを参照します。このセクションには、問題の原因となっている構成の詳細が表示されます。問題を修正し、Firepower 移行ツールに構成を再アップロードする必要があります。

  ルート内のトンネル、ループバック、または VLAN インターフェイスによってプッシュの失敗が発生した場合は、そのようなルートを削除して移行を再試行する必要があります。このようなインターフェイスは FMC でサポートされていないためです。

- **プッシュの失敗**：Firepower 移行ツールが構成を移行し、FMC にプッシュされているときに、プッシュの失敗が発生します。プッシュの失敗は、**移行後レポート**でキャプチャされます。

  回避策：**移行後レポート**をダウンロードし、移行レポートの [Error Reporting] セクションを参照します。このセクションには、問題の原因となっている構成の詳細が表示されます。[確認と検証（Review and Validation）] ページで問題を修正する必要があります。これには、失敗が表示されているセクションで [移行しない（do not migrate）] オプションを選択するか、または送信元構成で問題を修正し、Firepower移行ツールに構成を再アップロードします。

アンインストール： FirePOWER 移行ツール

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

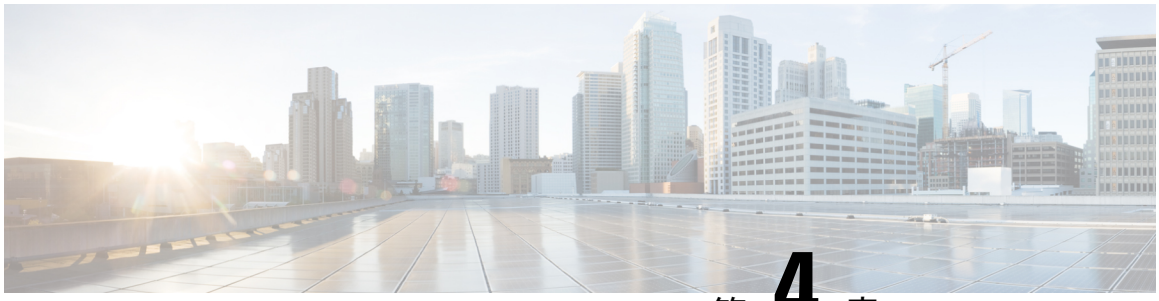
ステップ 1 Firepower 移行ツールを配置したフォルダに移動します。

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 Firepower 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。Firepower移行ツールのコンソールウィンドウが開いている限り、ログの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

Firepower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、 PAN 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。

予期しないファイル：PAN 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。

Firepower 移行ツールのサポートバンドル

Firepower 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. [Complete Migration] 画面で、[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. [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. [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。

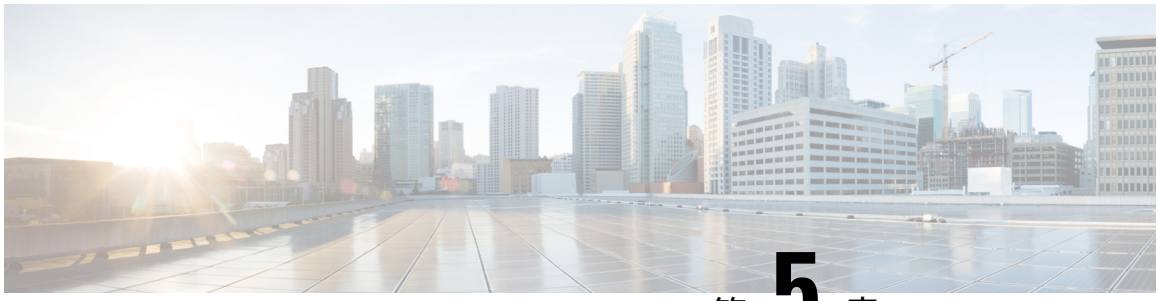
5. [Visit TAC page] をクリックして、シスコのサポートページで TAC ケースを作成します。

（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
telemetry_sessionid_timestamp.json	*<migration_tool_folder>*\resources\telemetry_data



第 5 章

Firepower 移行ツールの FAQ

Firepower 移行ツールのよく寄せられる質問

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

A. Firepower 移行ツールは、サポートされている PAN ファイアウォール プラットフォームから FTD プラットフォームにポリシーを移行できます。詳細については、「移行がサポートされるプラットフォーム」を参照してください。

Q. PAN 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. Firepower 移行ツールは、PAN OS バージョンが 6.1.x 以降の場合に構成を移行します。

Q. PAN ファイアウォールはインターフェイスグループをサポートしますか。

A. いいえ。PAN ファイアウォールは、FTD への変換でインターフェイスグループをサポートしていません。

Q. NAT で FMC でサポートされていない FQDN を使用しています。何をすればよいですか。

A. NAT の FQDN は FMC でサポートされていませんが、同様に Firepower 移行ツールでも FQDN はサポートされていません。送信元と同じ構成を複製するには、FQDN にマッピングされた IP アドレスのセット全体を移行後に手動で構成する必要があります。

Q. 送信元ファイアウォールにターゲットよりも多くのインターフェイスがある場合はどうしたらいいですか。

A. 送信元ファイアウォールにターゲットよりも多くのインターフェイスがある場合は、移行を開始する前に、FTD にサブインターフェイスを作成します。

Q. Firepower 移行ツールは集約インターフェイス（ポートチャネル）を移行しますか。

A. Firepower 移行ツールは集約インターフェイス（ポートチャネル）を移行しません。移行を開始する前に、FMC でポート チャネル インターフェイスを構成する必要があります。

Q. VR 間ルーティングは FMC でサポートされていますか。

A. ネクストホップがネクスト VR であるルートはサポートされません。

Q. PAN からルートテーブルを抽出するためのコマンドは何ですか。

A. **Show routing route** コマンドを使用します。ルートを txt ファイルに貼り付けたら、形式が正しいことを確認します。マルチ VSYS の場合は、関連する VSYS のルートのみを貼り付けます。これらのインターフェイスは FMC でサポートされていないため、ルーティングテーブルからトンネル、ループバック、および VLAN ルートを削除することを推奨します。

Q. [Ignored Configuration] のファイルはどうすればよいですか。

A. [Ignored Configuration] には、PAN 専用の XML タグが含まれていますが、これらは FMC とは無関係です。したがって、それらは無視されます。[Ignored Configuration] は慎重に確

認する必要があります。無視セクションに反映される予期しない項目は、FMC で手動で設定する必要があります。

Q. 移行前レポートにエラーが表示されます。インターフェイスを無視して続行できますか。

A. インターフェイスなしで続行することを選択した場合は、ルートの移行もありません。

Q. 解析の失敗の一般的な原因は何ですか。

A. 解析の失敗は、インターフェイスに複数の IP アドレスが設定されている場合や、IP アドレスにサブネット（/32 または /128 など）が割り当てられている場合に失敗します。続行するには、IP アドレスを修正して、移行を再試行する必要があります。

Q. [Pre-Parsing Summary] で NAT がゼロとして表示されるのはなぜですか。

A. 詳細については、「解析のサマリー」を参照してください。

Q. PAN 構成をエクスポートするにはどうすればよいですか。

A. デバイスが Panorama で管理されている場合は、ゲートウェイから設定を抽出する必要があります。Panorama 設定をゲートウェイと統合し、設定を抽出します。

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

Q. アプリケーションマッピングとはどのような機能ですか。

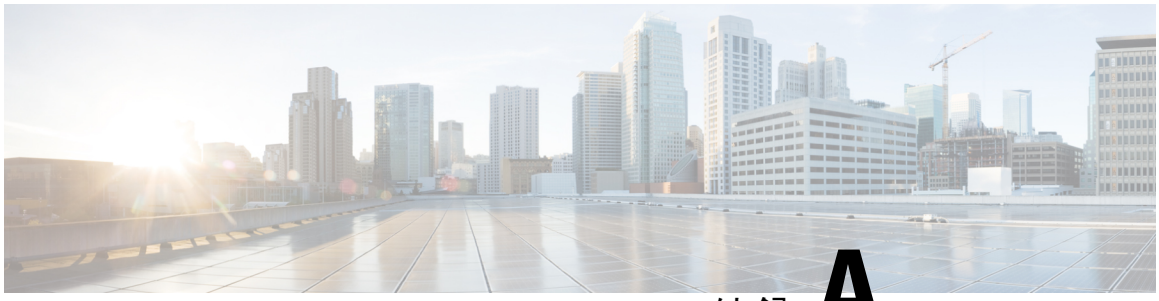
A. アプリケーションマッピングを使用すると、アプリケーションを HTTP、SSH などの対応するターゲットアプリケーションにマップできます。アプリケーションに基づくルールを移行することもできます。

詳細については、「Map Configurations with Applications」を参照してください。

Q. "application-default" のポリシーはどうなりますか。

A. 次の手順を実行します。

- アプリケーションに "any" が選択され、ポートが "application-default" に設定されている場合、ポリシーはサポートされず、無効として移行されます。
- アプリケーションに "xyz" が選択され、ポートが "application-default" に設定されている場合、ポリシーはサービスが "any" に設定されて、アプリケーション "xyz" で移行されます。



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

Firepower 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 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 Firepower 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 *2*：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	Firepower 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	Firepower 移行ツールの起動に使用されるブラウザ。Mozilla/5.0、Chrome/68.0.3440.106、Safari/537.36 を使用できます	Mozilla/5.0

表 *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)

Cisco Success Network：テレメトリデータ

データ ポイント	説明	値の例
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
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]
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

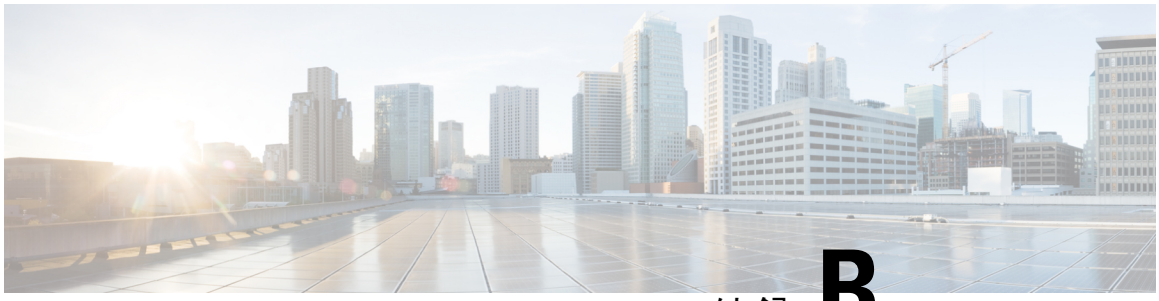
Cisco Success Network：テレメトリデータ

データ ポイント	説明	値の例
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 : Firepower* 移行ツールのパフォーマンスデータ

データ ポイント	説明	値の例
Conversion Time	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 構成移行のステータス	SUCCESS
エラー メッセージ	Firepower 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

Cisco Success Network：テレメトリデータ



付録 B

PAN から Firepower Threat Defense 2100 への移行：例

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『Firepower Management Center Hardware Installation Guide』および適切な『Firepower Management Center Getting Started Guide』を参照してください。

ステップ 1 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。

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

ステップ 2 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 Firepower Management Center」を参照してください。

ステップ 3 Firepower 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 からの FirePOWER 移行ツール のダウンロード （17 ページ）」を参照してください。

ステップ 4 Firepower 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、「Firepower 移行ツールの接続先パラメータの指定 （21 ページ）」を参照してください。

ステップ 5 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） Firepower 移行ツールでは、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。

詳細については、「PAN ファイアウォール 構成と Firepower 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 6 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、[Auto-Create] をクリックして、Firepower 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 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への PAN 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 7 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 8 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 （35 ページ）」を参照してください。

ステップ 9 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 （51 ページ）を参照してください。

ステップ 1 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 2 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 3 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 4 Firepower 2100 シリーズ デバイスに新しい IP アドレスを割り当て、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 5 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。