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 （7 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 （8 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 （3 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 （7 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 （8 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 （8 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 （9 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