移行の準備

Firewall 移行ツールに関する注意事項と制約事項

Fortinet 構成

Fortinet 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 Fortinet 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 （8 ページ）を参照）。
- 移行でサポートされる Fortinet 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 （9 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 （7 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 （8 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 （9 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 （9 ページ）を参照）。
- Fortinet 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 （10 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。

Fortinetファイアウォール構成に関する注意事項と制限事項

変換中に、Firewall移行ツールは、ルールまたはポリシーで使用されるかどうかにかかわらず、サポートされているすべてのオブジェクトおよびルールに対して 1 対 1 のマッピングを作成します。Firewall 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。

Firewall移行ツールは、サポートされていないオブジェクトとルールを次のように処理します。

- サポートされていないインターフェイス、オブジェクト、NAT ルール、および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 Management Center に移行されます。

Fortinet ファイアウォール構成ファイル

Fortinet ファイアウォールの構成ファイルは手動で取得できます。

Firewall移行ツールに手動でインポートする Fortinet ファイアウォール構成ファイルは、次の要件を満たしている必要があります。

- Fortinetデバイスからエクスポートされた実行構成が含まれている。Firewall移行ツールでは、グローバルと VDOM ごとのエクスポートの両方からの構成バックアップがサポートされています。詳細については、「Fortinet 構成ファイルのエクスポート」を参照してください。
- 有効な Fortinet ファイアウォール CLI 構成のみが含まれます。
- 構文エラーは含まれません。
- 拡張子が .conf または .txt のファイルタイプである。
- UTF-8 ファイルエンコーディングを使用している。

- コードの手入力または手動変更をしていない。Fortinet のファイアウォール構成を変更する場合は、変更した構成ファイルを Fortinet ファイアウォールデバイスでテストして、有効な設定であることを確認することが推奨されます。

Fortinet ファイアウォール構成の制限事項

送信元 Fortinet 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。
- Firewall 移行ツールは、50 以上のインターフェイスに適用される単一の ACL ポリシーの移行をサポートしていません。50以上のインターフェイスに適用されるACLポリシーは、手動で移行する必要があります。
- ダイナミックルーティングや VPN などの Fortinet ファイアウォール構成を Threat Defense に移行することはできません。これらの構成は手動で移行してください。
- タイプが仮想ワイヤ、冗長インターフェイス、トンネルインターフェイス、VDOM リンク、および SD-WAN インターフェイスまたはゾーンの Fortinet ファイアウォールインターフェイスはサポートされておらず、移行されません。

  FortiNet のハードウェアまたはソフトウェアスイッチの論理インターフェイスは、FTD L3 インターフェイスとして移行されます。Firewall 移行ツールでは、ハードウェアまたはソフトウェアスイッチ メンバー インターフェイスは移行されません。
- ワイルドカードFQDN、ワイルドカードIP、ダイナミックオブジェクト、除外グループなどのオブジェクトの移行はサポートされていません。
- トランスペアレントモードまたはトランスペアレントVDOMのFortinetファイアウォールデバイスは移行できません。
- Management Center では、ネストされたサービス オブジェクト グループおよび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、Firewall 移行ツールは、参照されているネストされたオブジェクトグループまたはポートグループの内容を展開します。
- Firewall 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、正確に同じ意味の Management Center ルールに変換されます。

Fortinet ファイアウォールの移行ガイドライン

Firewall 移行ツールは、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、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 Fortinet 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、Firewall 移行ツールは接続の開始時にロギングを構成します。アクションが **permit** の場合、Firewall 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 Fortinet ファイアウォール構成

Firewall 移行ツールは、次の Fortinet ファイアウォール構成を完全に移行できます。

- ネットワークオブジェクトとグループ（ワイルドカードFQDN、ワイルドカードマスク、FortiNet ダイナミックオブジェクトを除く）
- 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） Management Center ではネストはサポートされていないため、Firewall 移行ツールは参照されるルールの内容を展開します。ただし、ルールは完全な機能で移行されます。

- IPv4 および IPv6 FQDN オブジェクトとグループ
- IPv6変換サポート（インターフェイス、静的ルート、オブジェクト、ACL、およびNAT）
- アクセス ルール
- NAT ルール
- 静的ルート、移行されない ECMP ルート
- 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 は移行時の VLAN ID と同じ番号に常に設定されます）
- 集約インターフェイス（ポートチャネル）
- Firewall 移行ツールは、個別の Threat Defense デバイスとしての Fortinet ファイアウォールからの個々の VDOM の移行をサポートします。
- 時間ベースオブジェクト：Firewall 移行ツールは、アクセスルールで参照される時間ベースオブジェクトを検出すると、その時間ベースオブジェクトを移行し、それぞれのアクセスルールにマッピングします。[構成の最適化、確認および検証（Optimize, Review and Validate Configuration）] ページのルールに対してオブジェクトを確認します。

  時間ベースのオブジェクトは、期間に基づいてネットワークアクセスを許可するアクセスリストタイプです。このようなオブジェクトは、特定の時刻または特定の曜日に基づいてアウトバウンドトラフィックまたはインバウンドトラフィックを制限する必要がある場合に便利です。

（注）
- 送信元の FortiNet からターゲットの FTD にタイムゾーン設定を手動で移行する必要があります。
- 時間ベースのオブジェクトは非 FTD フローではサポートされていないため、無効になります。
- 時間ベースのオブジェクトは FMC バージョン 6.6 以降でサポートされています。

部分的にサポートされる Fortinet ファイアウォール構成

Firewall 移行ツールは、次の Fortinet ファイアウォール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。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。

- サポートされていないアドレスオブジェクトを含むアドレスグループ。
- 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 プロトコルが削除され、サービスグループが部分的に移行されます。

サポートされていない Fortinet ファイアウォール構成

Firewall 移行ツールは、次の Fortinet ファイアウォール構成の移行をサポートしません。これらの構成が Management Center でサポートされている場合、移行の完了後に手動で構成できます。

- ユーザーベース、デバイスベース、およびインターネットサービス ID ベースのアクセス コントロール ポリシー ルール
- サポートされていない ICMP タイプとコードを持つサービスオブジェクト
- 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
- ブロック割り当てオプションを使用して構成された NAT ルール
- SCTP で構成された NAT ルール
- ホスト ‘0.0.0.0’ で構成された NAT ルール
- 送信元または接続先に FQDN オブジェクトを含む NAT ルール
- 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
- Fortinet では、IPv4 と IPv6 を組み合わせたポリシー（統合されたポリシー）を構成できます。

（注） このポリシーは、Firewall 移行ツールではサポートされていません。

Threat Defense デバイスに関する注意事項と制約事項

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、 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。

FortiNet のハードウェアまたはソフトウェアスイッチの論理インターフェイスは、FTD L3 インターフェイスとして移行されます。Firewall 移行ツールでは、ハードウェアまたはソフトウェアスイッチ メンバー インターフェイスは移行されません。

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 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 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。

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 Fortinet 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。

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 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、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、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 Fortinet および Firepower Threat Defense バージョンです。

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

ファイアウォール移行ツールは、Fortinet ファイアウォール OS バージョン 5.0 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 Fortinet 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

Fortinet 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）[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