移行の準備

- Firewall 移行ツールに関する注意事項と制約事項 （1 ページ）
- ASA with FPS 構成の注意事項と制約事項 （3 ページ）
- Threat Defense デバイスに関する注意事項と制約事項 （13 ページ）
- 移行がサポートされるプラットフォーム （15 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 （17 ページ）
- Firewall 移行ツールのプラットフォーム要件 （18 ページ）

Firewall 移行ツールに関する注意事項と制約事項

ASA with FPS 構成

ASA with FPS 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 ASA with FPS 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 （15 ページ）」を参照）。
- 移行でサポートされる ASA with FPS 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 （17 ページ）」を参照）。

（任意）ターゲット Threat Defense デバイス

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

脅威に対する防御 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 脅威に対する防御 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 脅威に対する防御 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 （13 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 （15 ページ）を参照）。
- 移行でサポートされる 脅威に対する防御 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 （17 ページ）を参照）。
- Management Center に登録されている 脅威に対する防御 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 （17 ページ）を参照）。
- ASA with FPS インターフェイスから移行する予定のすべての機能を含む 脅威に対する防御 用のスマートライセンスを取得済みおよびインストール済みであること。次を参照してください。
- Cisco.com の「Cisco Smart Accounts」の「Getting Started」セクション。
- Register the Firepower Management Center with the Cisco Smart Software Manager [英語]
- Licensing the Firewall System [英語]
- REST API の Management Center が有効になっています。

ヒント Management Center Web インターフェイスで、次に移動します。**[システム（System）] > [設定（Configuration）] > [Rest API設定（Rest API Preferences）] > [Rest APIを有効にする（Enable Rest API）]**。その後 [Rest APIを有効にする（Enable Rest API）] チェックボックスをオンにします。

- Firewall 移行ツール用に Management Center で REST API 権限を持つ専用ユーザーを作成しました（「管理アクセス用のユーザーアカウント」を参照）。

Firewall 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 （18 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

構成項目	バッチサイズ制限	デフォルト値
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。

ASA with FirePOWER Services

Firewall 移行ツール 2.4 以降では、ASA with FirePOWER Services モジュールの Firewall サービスモジュール構成を移行できます。

ASA with FPS 構成の注意事項と制約事項

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。

Firewall 移行ツールは、サポートされていないコンポーネントを次のように処理します。

- サポートされていないオブジェクトと NAT ルールは移行されません。
- 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。
- アウトバウンド ACL は**サポートされていない構成（Unsupported Configuration）**であり、Management Center に移行されません。送信元ファイアウォールにアウトバウンド ACL が

ある場合、**移行前レポート**の**無視される構成（Ignored Configration）**セクションで報告されます。

- サポートされるすべての ASA with FPS 暗号マップ VPN は、Management Center ポイントツーポイント トポロジとして移行されます。
- サポートされていない、または不完全なスタティック暗号マップ VPN トポロジは移行されません。
- Firewall 移行ツール 2.4 以降では、動的暗号マップと証明書ベースの VPN の移行がサポートされています。
- Firewall 移行ツール 2.5.1 以降、BGP と動的ルートオブジェクトの移行がサポートされています。
- Firewall 移行ツール 3.0 以降、リモートアクセス VPN の移行がサポートされています。
- ユーザベースの FPS ACL は移行ではサポートされず、無効として移行されます。

ASA with FPS 構成ファイル

ASA with FPS 構成ファイルは、手動で、または Firewall 移行ツールからライブ ASA with FPS に接続して取得できます。

Firewall 移行ツールへの ASA with FPS 構成ファイルの移行は、次の 2 段階のプロセスです。

- 手動方式またはライブ接続方式を使用して ASA with FPS 構成ファイルをインポートできます。
- FPS を管理する Management Center に接続し、移行する必要がある送信元 ACL ポリシーを選択して、FPS 構成ファイルをインポートする必要があります。

Firewall 移行ツールに手動でインポートする ASA with FPS 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。

- シングルモード構成またはマルチコンテキストモード構成の特定のコンテキストで ASA with FPS デバイスからエクスポートされる実行構成を含んでいる。ASA with FPS 構成ファイルのエクスポートを参照してください。
- バージョン番号を含んでいる。
- 有効な ASA with FPS CLI 構成のみを含んでいる。
- 構文エラーは含まれません。
- ファイル拡張子が `.cfg` または `.txt` 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。ASA with FPS 構成を変更する場合は、変更した構成ファイルを ASA with FPS デバイスでテストして、有効な構成であることを確認することが推奨されます。

- 「--More--」キーワードをテキストとして含んでいない。

ASA with FPS 設定の制限

送信元 ASA with FPS 構成の移行には、次の制限があります。

- Firewall 移行ツールは、個別の Threat Defense デバイスとして、ASA with FPS からの個々のセキュリティコンテキストの移行をサポートします。
- 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、手動で移行してください。
- 動的ルーティングなど、ASA with FPS 構成の一部は Threat Defense に移行できません。これらの構成は手動で移行してください。
- ブリッジ仮想インターフェイス（BVI）、冗長インターフェイス、またはトンネルインターフェイスを使用するルーテッドモードの ASA with FPS デバイスは移行できません。ただし、BVI を使用するトランスペアレントモードの ASA with FPS デバイスを移行することはできます。
- 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。変換の一環として、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。
- 特定のトンネリングプロトコル（GRE、IP-in-IP、IPv6-in-IP など）を参照しないアクセス制御ルールが送信元 ASA with FPS 構成にあり、これらのルールが ASA with FPS 上の暗号化されていないトンネルトラフィックに一致する場合、Threat Defense に移行すると、対応するルールは ASA with FPS 上と同じようには動作しません。Threat Defense のプレフィルタポリシーで、これらの特定のトンネルルールを作成することを推奨します。
- サポートされるすべての ASA with FPS 暗号マップは、ポイントツーポイント トポロジとして移行されます。
- Firewall 移行ツール 2.4 以降では、動的暗号マップと証明書ベースの VPN の移行がサポートされています。
- Firewall 移行ツール 2.5.1 以降、BGP および動的ルートオブジェクトの移行がサポートされています。
- Management Center に同じ名前の AS-Path オブジェクトが表示された場合、移行は次のエラーメッセージで停止します。

「Management Center で競合する AS-Path オブジェクト名が検出されました。続行するには、Management Center の競合を解決してください。（Conflicting AS-Path object name detected in , please resolve conflict in to proceed further）」

（注） 標準のアクセスリストのみがサポートされています。

- ルートマップオブジェクトは、 Firewall 移行ツール を使用して部分的に移行されます。API の制限により、match 句と set 句はサポートされていません。
- **RA VPN の移行の制限事項**

  Firewall 移行ツール 3.0 以降、リモートアクセス VPN の移行が次の制限付きでサポートされています。

  - API の制限により、カスタム属性、SSL 設定、および VPN 負荷分散の移行はサポートされていません。
  - LDAP サーバーは、暗号化タイプが「なし（none）」として移行されます。
  - ポリシーは Management Center 全体に適用されるため、DfltGrpPolicy は移行されません。Management Center で必要な変更を直接行うことができます。
  - Radius サーバーでは、動的認証が有効になっている場合は、AAA サーバー接続は動的ルーティングではなくインターフェイスを介して行う必要があります。インターフェイスなしで動的認証が有効になっている AAA サーバーで ASA with FirePOWER Services 構成が見つかった場合、Firewall 移行ツールは動的認証を無視します。管理センターでインターフェイスを選択した後に、動的認証を手動で有効にする必要があります。
  - トンネルグループの下でアドレスプールを呼び出している間は ASA with FirePOWER Services 構成にインターフェイスを含めることができます。ただし、管理センターではこれはサポートされていません。 ASA with FirePOWER Services 構成でインターフェイスが検出された場合、そのインターフェイスは Firewall 移行ツールで無視され、アドレスプールがインターフェイスなしで移行されます。
  - ASA with FirePOWER Services 構成には、トンネルグループの下の DHCP サーバーにキーワード **link-selection/subnet-selection** を含めることができます。ただし、管理センターではこれはサポートされていません。これらのキーワードを使用して ASA with FirePOWER Services 構成で検出された DHCP サーバーがある場合、それらのサーバーは Firewall 移行ツールで無視され、DHCP サーバーはキーワードなしでプッシュされます。
  - ASA with FirePOWER Services 構成は、トンネルグループの下の認証サーバーグループ、セカンダリ認証サーバーグループ、承認サーバーグループを呼び出す間はインターフェイスを持つことができます。ただし、管理センターではこれはサポートされていません。 ASA with FirePOWER Services 構成でインターフェイスが検出された場合、そのインターフェイスは Firewall 移行ツールで無視され、コマンドはインターフェイスなしでプッシュされます。

- ASA with FirePOWER Services 構成は、リダイレクト ACL を Radius サーバーにマッピングしません。したがって、Firewall 移行ツールから取得する方法はありません。リダイレクト ACL が ASA with FirePOWER Services で使用される場合、その ACL は空のままになり、管理センターで手動で追加してマッピングする必要があります。
- ASA with FirePOWER Services は vpn-addr-assign のローカル再利用遅延値 0 ～ 720 をサポートします。ただし、管理センターは 0 ～ 480 の値をサポートします。 ASA with FirePOWER Services 構成に 480 を超える値が見つかった場合、管理センターでサポートされている最大値の 480 に設定されます。
- 接続プロファイルへの IPv4 プールと DHCP useSecondaryUsernameforSession の設定の構成は、API の問題によりサポートされていません。
- バイパスアクセス制御 sysopt permit-vpn オプションは、RA VPN ポリシーで有効になっていません。ただし、必要に応じて、管理センターから有効にすることができます。
- Anyconnect クライアントモジュールとプロファイルの値は、プロファイルが Firewall 移行ツールから管理センターにアップロードされた場合にのみ、グループポリシーに従って更新できます。
- 証明書を管理センターに直接マッピングする必要があります。
- IKEv2 パラメータは、デフォルトでは移行されません。それらのパラメータは管理センターを使用して追加する必要があります。

Firewall サービス（FPS）移行の注意事項

Firewall 移行ツールは、次のような 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 ASA with FPS 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。
- FPS のルールを使用した ASA は、次のように移行されます。

  ASA with FPS のリダイレクションの ACL は、プレフィルタのルール（条件付き）として移行されます。

（注） FPS モジュールが Management Center で管理されている場合にのみ、Firewall 移行ツールを使用して FPS のルールを移行できます。

  - ソースリダイレクションの ACL に **Action=DENY** がある場合：**Action=Fastpath** を使用して Management Center プレフィルタのルールとして移行されます。また、この特定の ACL は DISABLED 状態の最初の ACL のルールとして配置されます。

- ソースリダイレクションの ACL に **Action=Permit** がある場合、Firewall 移行ツールでは移行されません。

サポートされている ASA with FPS 構成

Firewall 移行ツールは、次の ASA with FPS 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
- サービスオブジェクト（送信元と接続先に設定されたサービスオブジェクトを除く）

（注） Firewall 移行ツールは拡張サービスオブジェクト（送信元と接続先の構成）は移行しませんが、参照先の ACL と NAT のルールは完全な機能で移行されます。

- 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）
- インバウンド方向とグローバル ACL のインターフェイスに適用されるアクセスルール
- 自動 NAT、手動 NAT、およびオブジェクト NAT（条件付き）
- 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
- ASA with FPS インターフェイス上のセカンダリ VLAN は Threat Defense に移行されません。
- 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）
- ポート チャネル
- 仮想トンネルインターフェイス（VTI）
- ブリッジグループ（トランスペアレントモードのみ）
- IP SLA のモニタ

Firewall 移行ツールは IP SLA オブジェクトを作成し、オブジェクトを特定の静的ルートにマッピングし、オブジェクトを Management Center に移行します。

IP SLA モニタでは、モニタリング対象のアドレスへの接続ポリシーを定義し、そのアドレスへのルートの可用性をトラッキングします。静的ルートの可用性は、ICMP エコー要求を送信し、応答を待機することによって、定期的にチェックされます。エコー要求がタイムアウトすると、その静的ルートはルーティングテーブルから削除され、バックアップルートに置き換えられます。SLA モニタリングジョブは、デバイス構成から SLA モニタを削除していない限り、展開後すぐに開始して実行し続けます（つまり、ジョブはエージングアウトしません）。SLA モニタオブジェクトは、IPv4 静的ルートポリシーの [ルートトラッキング（Route Tracking）] フィールドで使用されます。IPv6 ルートでは、ルートトラッキングによって SLA モニタを使用することはできません.

（注） IP SLA モニターは、Threat Defense 以外のフローではサポートされていません。

- オブジェクトグループの検索

  オブジェクトグループ検索を有効にすると、ネットワークオブジェクトを含むアクセスコントロールポリシーのメモリ要件が軽減されます。オブジェクトグループ検索を有効にして、Threat Defense でアクセスポリシーによる最適なメモリの使用を実現することをお勧めします。

（注）
- オブジェクトグループ検索は、6.6 より前の Management Center または Threat Defense のバージョンでは使用できません。
- オブジェクトグループ検索は Threat Defense 以外の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

  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。[構成の確認と検証（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。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 ASA with FPS からターゲットの FTD にタイムゾーン構成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 Threat Defense 以外の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 Management Center バージョン 6.6 以降でサポートされています。

- [サイト間 VPN トンネル（Site-to-Site VPN Tunnels）]
  - サイト間 VPN：Firewall 移行ツールは、送信元 ASA with FPS で暗号マップ構成を検出すると、暗号マップを Management Center VPN にポイントツーポイント トポロジとして移行します。
  - ASA からのクリプトマップ（静的/動的）ベースの VPN
  - ルートベース（VTI）の ASA VPN
  - ASA からの証明書ベースの VPN 移行
  - ASA トラストポイントまたは証明書の Management Center への移行は手動で実行する必要があり、また、移行前のアクティビティに含まれている必要があります。
- 動的ルートオブジェクトと BGP
  - ポリシーリスト
  - プレフィックスリスト
  - コミュニティ リスト
  - 自律システム（AS）パス
- リモートアクセス VPN
  - SSL と IKEv2 プロトコル
  - 認証方式：[AAA のみ（AAA only）]、[クライアント証明書のみ（Client Certificate only）]、および [AAA とクライアント証明書（AAA + Client Certificate）]
  - AAA：Radius、ローカル、LDAP、および AD
  - 接続プロファイル、グループポリシー、動的アクセス ポリシー、LDAP 属性マップ、および証明書マップ
  - 標準的な ACL と拡張 ACL
  - 移行前のアクティビティの一環として、次の手順を実行します。

- ASA トラストポイントを PKI オブジェクトとして手動で Management Center に移行します。
- AnyConnect パッケージ、Hostscan ファイル（Dap.xml、Data.xml、Hostscan Package）、外部ブラウザパッケージ、および AnyConnect プロファイルを送信元 ASA から取得します。
- すべての AnyConnect パッケージを Management Center にアップロードします。
- AnyConnect プロファイルを Management Center に直接アップロードするか、または Firewall 移行ツールからアップロードします。
- Live Connect ASA からプロファイルを取得できるようにするには、ASA で **ssh scopy enable** コマンドを有効にします。

部分的にサポートされる ASA with FPS 構成

Firewall 移行ツールは、次の ASA with FPS 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。

- 重大度や時間間隔など、高度なロギング設定を使用して設定されたアクセス コントロール ポリシー ルール
- トラックオプションを使用して設定された静的ルート
- 証明書ベースの VPN 移行
- 動的ルートオブジェクトと BGP
  - 標準的なアクセスリストのみ
  - ルートマップ

未サポートの ASA with FPS 構成

Firewall 移行ツールは、次の ASA with FPS 構成の移行をサポートしていません。これらの構成が Management Center でサポートされている場合、移行の完了後に手動で構成できます。

- SGT ベースのアクセス コントロール ポリシー ルール
- SGT ベースのオブジェクト
- ユーザベースのアクセス 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
- 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

（注） Firewall 移行ツール 2.0 と Management Center 6.5 でのプレフィルタのサポート。

- 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
- SLA トラッキングを使用した DHCP または PPPoE によって取得されたデフォルトルート
- sla monitor schedule
- トランスポートモードの IPsec のトランスフォームセット
- Management Center への ASA トラストポイントの移行
- ユーザベースの FPS ACL は移行ではサポートされず、無効として移行されます。
- BGP のトランスペアレント ファイアウォール モード

ASA with FPS のオブジェクトと Threat Defense

ASA with FPS の構成ファイルには、Threat Defense に移行できる次のオブジェクトが含まれています。

- ネットワーク オブジェクト
- サービスオブジェクト（Threat Defense ではポートオブジェクトと呼ばれる）
- IP SLA オブジェクト
- 時間ベースのオブジェクト
- VPN オブジェクト（IKEv1/IKEv2 ポリシー、IKEv1/IKEv2 IPsec-Proposal）
- 動的ルートオブジェクト（ポリシーリスト、プレフィックスリスト、コミュニティリスト、AS パス、アクセスリスト、およびルートマップ）
- BGP は、ルーテッドモードでサポートされています。
- RA VPN オブジェクト：
  - グループ ポリシー
  - AAA オブジェクト（Radius、SAML、ローカルレルム、AD/LDAP/LDAPS レルム）
  - アドレスプール（IPv4 と IPv6）
  - 接続プロファイル
  - LDAP Attribute Map
  - IKEv2 ポリシー

- IKEv2 IPsec プロポーザル
- 証明書マップ
- DAP

ASA with FPS と Threat Defense では、オブジェクトの構成ガイドラインが異なります。たとえば、ASA with FPS では、複数のオブジェクトに大文字か小文字かが異なるだけの同じ名前を付けることができますが、Threat Defense では、大文字か小文字かに関係なく、各オブジェクトに一意の名前を付ける必要があります。このような違いに対応するために、Firewall 移行ツールでは、ASA with FPS のオブジェクトをすべて分析し、次のいずれかの方法でその移行を処理します。

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

（注） Firewall 移行ツール 2.5 は、接続先の Firewall Management Center が 7.1 以降の場合は、不連続ネットワークマスク（ワイルドカードマスク）オブジェクトの移行をサポートします。

```
ASA example:
object network wildcard2
subnet 2.0.0.2 255.0.0.255
```

Threat Defense デバイスに関する注意事項と制約事項

ASA with FPS 構成を 脅威に対する防御 に移行する計画を立てている場合は、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、脅威に対する防御 に既存のデバイス固有の構成がある場合、プッシュ移行中に Firewall 移行ツールは自動的にデバイスを消去し、 ASA with FPS 構成から上書きします。

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

移行中に、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。

- 脅威に対する防御デバイスは、スタンドアロンデバイスまたはコンテナインスタンスにすることができます。クラスタまたは高可用性設定の一部であっては**なりません**。
  - ターゲットネイティブ 脅威に対する防御 デバイスには、使用する物理データとポート チャネル インターフェイスが ASA with FPS と同数以上必要です（「管理専用」とサブインターフェイスを除く）。そうでない場合は、ターゲット 脅威に対する防御 デバイスに必要なタイプのインターフェイスを追加する必要があります。サブインターフェイスは、物理またはポートチャネルのマッピングに基づいて Firewall 移行ツールによって作成されます。
  - ターゲット 脅威に対する防御 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 脅威に対する防御 デバイスに必要なタイプのインターフェイスを追加する必要があります。
    - サブインターフェイスは、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、 構成に基づいて 脅威に対する防御 デバイスのネイティブインスタンスにサブインターフェイスを作成できます。移行を開始する前に、ターゲット 脅威に対する防御 デバイスでインターフェイスとポート チャネル インターフェイスを手動で作成します。たとえば、 ASA with FPS 構成に次のインターフェイスとポートチャネルが割り当てられている場合は、移行前にそれらをターゲット 脅威に対する防御 デバイス上に作成する必要があります。
  - 5 つの物理インターフェイス
  - 5 つのポートチャネル
  - 2 つの管理専用インターフェイス

（注） 脅威に対する防御デバイスのコンテナインスタンスの場合、サブインターフェイスは、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。

- Firewall 移行ツールは、 ASA with FPS 構成に基づいて 脅威に対する防御 デバイスのネイティブインスタンスに、サブインターフェイスとブリッジグループ仮想インターフェイス（トランスペアレントモード）を作成できます。移行を開始する前に、ターゲット 脅威に対する防御 デバイスでインターフェイスとポート チャネル インターフェイスを手動で作成します。たとえば、 ASA with FPS 構成に次のインターフェイスとポートチャネルが割り当てられている場合は、移行前にそれらをターゲット 脅威に対する防御 デバイス上に作成する必要があります。
  - 5 つの物理インターフェイス
  - 5 つのポートチャネル
  - 2 つの管理専用インターフェイス

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

移行がサポートされるプラットフォーム

Firewall 移行ツールを使用した移行では、次の ASA with FPS および 脅威に対する防御 プラットフォームがサポートされています。サポートされる 脅威に対する防御 プラットフォームの詳細については、『Cisco Secure Firewall Compatibility Guide』[英語] を参照してください。

（注） Firewall 移行ツールは、スタンドアロン ASA with FPS デバイスからスタンドアロン Secure Firewall Threat Defense デバイスへの移行のみをサポートします。

ASA with FPS の移行でサポートされる送信元 ASA モデル

Cisco ASA FirePOWER モジュールは、次のデバイスに展開されます。

- ASA5506-X
- ASA5506H-X
- ASA5506W-X
- ASA5508-X

- ASA5512-X
- ASA5515-X
- ASA5516-X
- ASA5525-X
- ASA5545-X
- ASA5555-X
- ASA5585-X-SSP-10
- ASA5585-X-SSP-20
- ASA5585-X-SSP-40
- ASA5585-X-SSP-60

サポートされるターゲット Threat Defense プラットフォーム

Firewall 移行ツールを使用して、脅威に対する防御 プラットフォームの次のスタンドアロンまたはコンテナインスタンスに送信元 ASA with FPS 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
- VMware ESXi、VMware vSphere Web クライアント、または vSphere スタンドアロンクライアントを使用して展開された Threat Defense（VMware 上）

Firewall 移行ツール は、Microsoft Azure Cloud での Threat Defense Virtual への移行をサポートしています。

Azure における Threat Defense Virtual の前提条件と事前設定については、『Getting Started with Secure Firewall Threat Defense Virtual』[英語] を参照してください。

Firewall 移行ツール は AWS Cloud での Threat Defense Virtual の移行をサポートしています。

AWS クラウドにおける Threat Defense Virtual の前提条件と事前設定については、「Threat Defense Virtual の前提条件」を参照してください。

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

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

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

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 ASA with FPS および 脅威に対する防御 バージョンです。

サポートされている ASA with FPS のバージョン

Firewall 移行ツールは、ASA with FPS ソフトウェアバージョン 9.2.2 以降を実行しているデバイスからの移行をサポートしています。

詳細については、Cisco ASA 互換性ガイドの「ASA FirePOWER Module Compatibility」セクションを参照してください。

送信元 ASA with FPS 構成でサポートされている Management Center のバージョン

ASA with FPS の場合、 Firewall 移行ツールは、バージョン 6.5 以降を実行している Management Center によって管理される Threat Defense デバイスへの移行をサポートしています。

サポートされる Threat Defense のバージョン

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

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

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