Cisco Secure Firewall 移行ツールのスタートアップガイド

Cisco Secure Firewall 移行ツールについて

このガイドでは、Cisco Secure Firewall 移行ツールをダウンロードして移行を完了する方法について説明します。さらに、発生する可能性のある移行の問題を解決するのに役立つトラブルシューティングのヒントも提供します。

本書に記載されている移行手順の例（移行例： ASA with FPS から Threat Defense 2100）は、移行プロセスに関する理解を促進するのに役立ちます。

Cisco Secure Firewall 移行ツールは、サポートされている ASA with FPS 構成をサポートされている 脅威に対する防御 プラットフォームに変換します。Cisco Secure Firewall 移行ツールを使用すると、サポートされている ASA with FPS の機能とポリシーを自動的に 脅威に対する防御 に移行できます。サポートされていない機能はすべて、手動で移行する必要があります。

Cisco Secure Firewall 移行ツールは ASA with FPS の情報を収集して解析し、最終的に Secure Firewall Management Center にプッシュします。解析フェーズ中に、Cisco Secure 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。

- 完全に移行された、部分的に移行された、移行がサポートされていない、および移行が無視された ASA with FPS（Firewall Services）構成項目。
- エラーのある ASA with FPS 構成行には、Cisco Secure Firewall 移行ツールが認識できない ASA with FPS CLI がリストされています。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、ASA with FPS インターフェイスを 脅威に対する防御 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。

コンソール

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

Cisco Secure 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 Cisco Secure 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。Cisco Secure 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

Cisco Secure 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。

Cisco Secure 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

Cisco Secure Firewall 移行ツールは、**移行前レポート**、**移行後レポート**、 ASA with FPS 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

Cisco Secure Firewall 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 Cisco Secure Firewall 移行ツールは、 ASA with FPS 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。

Cisco Secure 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、Cisco Secure 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。Cisco Secure 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。Cisco Secure 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

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

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、Cisco Secure 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、Cisco Secure 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。

Cisco Secure Firewall 移行ツールは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 Secure Firewall 移行ツールの最新情報

バージョン	サポートされる機能
4.0.1	Cisco Secure Firewall 移行ツール 4.0.1 には、次の新機能と拡張機能が含まれています。 Cisco Secure Firewall 移行ツールは、名前と構成の両方に基づいてすべてのオブジェクトとオブジェクトグループを分析し、同じ名前と構成を持つオブジェクトを再利用するようになりました。以前は、ネットワークオブジェクトとネットワーク オブジェクト グループのみが、名前と構成に基づいて分析されていました。リモートアクセス VPN の XML プロファイルは名前のみを使用して検証されることに注意してください。
3.0.1	• ASA with FirePOWER Services、Check Point、Palo Alto Networks、および Fortinet の場合、Secure Firewall 3100 シリーズは宛先デバイスとしてのみサポートされます。

バージョン	サポートされる機能

3.0	Cisco Secure Firewall 移行ツール 3.0 は、以下をサポートします。
	• 移行先の管理センターが 7.2 以降の場合の ASA with FirePOWER Services からのリモートアクセス VPN の移行。Secure Firewall Threat Defense の有無にかかわらず、RA VPN の移行を実行できます。Threat Defense での移行を選択する場合、Threat Defense のバージョンは 7.0 以降である必要があります。
	• ASA with FirePOWER Services からのサイト間 VPN 事前共有キーの自動化。
	• 移行前のアクティビティの一環として、次の手順を実行する必要があります。
	  • ASA with FirePOWER Services トラストポイントは、PKI オブジェクトとして管理センターに手動で移行する必要があります。
	  • 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 プロファイルは、送信元 ASA から取得する必要があります。
	  • AnyConnect パッケージを管理センターにアップロードする必要があります。
	  • AnyConnect プロファイルは、管理センターに直接アップロードするか、または Cisco Secure Firewall 移行ツールからアップロードする必要があります。
	  • 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 with FirePOWER Services で **ssh scopy enable** コマンドを有効にする必要があります。

バージョン	サポートされる機能
2.4	

バージョン	サポートされる機能
	Cisco Secure Firewall 移行ツールは、ターゲットの Management Center と脅威に対する防御 が 6.5 以降の場合に、脅威に対する防御 への Cisco Firewall Services（FPS）構成の移行をサポートしています。 • Management Center プレフィルタルールとしての ASA with FPS アクセスルールの移行：Firewall による詳細なインスペクションに合わせた Management Center への ASA with FPS アクセスルールのマッピング。アクセスポリシーには、IP とポートを含むルールが含まれています。 （注） プレフィルタとアクセス制御のポリシーを使用して、トラフィックをブロックまたは許可できます。 ASA からのアクセスルールは、Management Center プレフィルタルールとして移行されます。FPS からのアクセスルールは、アクセス コントロール ポリシーとして Management Center に移行されます。 • ASA with FPS ルールは、次のように移行されます。 ASA から FPS へ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、Cisco Secure 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、Cisco Secure Firewall 移行ツールでは移行されません。 • Cisco Secure Firewall 移行ツールは、ASDM 管理対象の FPS ルールの Cisco Secure Firewall 移行ツールへの移行をサポートしていません。したがって、送信元の設定（FPS を備えた ASA）の選択時には、移行前の設定情報を把握しておく必要があります。 次の ASA VPN 構成を 脅威に対する防御 に移行します。 • 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 （注） • ASA トラストポイントまたは証明書は手動で移行され、移行前のアクティビティに含まれています。

バージョン	サポートされる機能
	• ASA トラストポイントは、Management Center PKI オブジェクトとして移行する必要があります。PKI オブジェクトは、証明書ベースの VPN トポロジの作成時に Cisco Secure Firewall 移行ツールで使用されます。

Cisco Secure Firewall 移行ツールのライセンス

Cisco Secure 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、脅威に対する防御 デバイス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 脅威に対する防御 機能に必要なライセンスが必要です。

Cisco Secure Firewall 移行ツールのプラットフォーム要件

Cisco Secure 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。

- Microsoft 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

ASA with FPS 構成ファイルの要件と前提条件

ASA with FPS 構成ファイルは、手動で、または Cisco Secure 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。

Cisco Secure 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。

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

- 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 構成のみが含まれている。
- 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、有効な設定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。

Threat Defense デバイスの要件および前提条件

管理センターに移行する場合、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、共有ポリシーを管理センターに移行できます。デバイス固有のポリシーを Threat Defense に移行するには、管理センターに追加する必要があります。ASA with FPS 構成を Threat Defense に移行することを計画する場合、次の要件と前提条件を考慮してください。

- ターゲット Threat Defense デバイスは、管理センターに登録されている必要があります。
- 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およびポート 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」および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 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 Cisco Secure 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 ASA with FPS 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。

（注）
- サブインターフェイスは、Cisco Secure 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。

ASA with FPS 構成のサポート

サポートされている ASA with FPS 構成

Cisco Secure 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） Cisco Secure 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とともに移行されます。

- 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、Cisco Secure 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とともに移行されます。

- 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 脅威に対する防御 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、移行時に常に VLAN ID と同じ番号に設定されます）
- 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

  Cisco Secure 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、デバイス設定から 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、脅威に対する防御 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、脅威に対する防御 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 脅威に対する防御 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 脅威に対する防御 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

  Cisco Secure 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脅威に対する防御 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：Cisco Secure 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、BGP、および EIGRP
  - 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 ACL および拡張 ACL
- RA VPN カスタム属性と VPN ロードバランシング
- 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 Cisco Secure 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

Cisco Secure 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。

- シビラティ（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、BGP、および EIGRP
  - ルートマップ

未サポートの ASA with FPS 構成

Cisco Secure 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） Cisco Secure Firewall 移行ツールと 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

注意事項と制約事項

変換中に、Cisco Secure 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。Cisco Secure 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。

Cisco Secure 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。
- 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 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。

- Cisco Secure Firewall 移行ツールは、個別の 脅威に対する防御 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。
- Cisco Secure 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 脅威に対する防御 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、Cisco Secure 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。
- Cisco Secure 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、脅威に対する防御 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。脅威に対する防御 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。
- 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）」

- OSPF および Routing Information Protocol（RIP）から EIGRP への再配布はサポートされていません。

RA VPN の移行の制限事項

リモートアクセス VPN の移行は、次の制限付きでサポートされています。

- API の制限により、SSL 設定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、Cisco Secure 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 Cisco Secure 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 Cisco Secure 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 Cisco Secure 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、Cisco Secure 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 Cisco Secure 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

Cisco Secure Firewall 移行ツールは、次のような 脅威に対する防御 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、脅威に対する防御 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、Cisco Secure 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、Cisco Secure 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、Cisco Secure 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、Cisco Secure Firewall 移行ツールでは移行されません。

オブジェクト移行の注意事項

ASA with FPS と Threat Defense では、オブジェクトに関する構成上の注意事項が異なります。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、Cisco Secure 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：Cisco Secure 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、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：Cisco Secure 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 Management Center の既存オブジェクトと同じ場合：Cisco Secure 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：Cisco Secure 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：Cisco Secure 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。

重要 Cisco Secure Firewall 移行ツールは、すべてのオブジェクトとオブジェクトグループの名前と構成の両方を分析します。ただし、リモートアクセス VPN 構成の XML プロファイルは、名前のみを使用して分析されます。

（注） Cisco Secure Firewall 移行ツールは、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 Cisco Secure 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、Cisco Secure 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、Cisco Secure 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。

- Cisco Secure 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、Cisco Secure 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。

- Cisco Secure 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、Cisco Secure 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

Cisco Secure Firewall 移行ツールによる移行では、以下の 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） Cisco Secure 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 脅威に対する防御 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

Cisco Secure 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
- Secure Firewall 3100 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）
- Microsoft Azure クラウドまたは AWS クラウド上の Threat Defense Virtual

（注）
- 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。
- 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 Cisco Secure 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、Cisco Secure 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）Cisco Secure 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、Cisco Secure 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。

サポートされる移行先の管理センター

Cisco Secure Firewall 移行ツールは、管理センターおよびクラウド提供型 Firewall 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ます。

Management Center

管理センターは強力な Web ベースのマルチデバイスマネージャです。独自のサーバーハードウェア上で、またはハイパーバイザ上の仮想デバイスとして稼働します。移行のためのターゲット管理センターとして、オンプレミス管理センターと仮想管理センターの両方を使用できます。

管理センターは、移行に関する次のガイドラインを満たす必要があります。

- 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 （22 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。

- Cisco Secure 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）。

移行でサポートされるソフトウェアのバージョン

移行のためにサポートされている Cisco Secure Firewall 移行ツール、ASA with FPS 、および 脅威に対する防御 のバージョンは次のとおりです。

サポートされている Cisco Secure Firewall 移行バージョン

software.cisco.com に掲載されているバージョンは、当社のエンジニアリングおよびサポート組織によって正式にサポートされているバージョンです。software.cisco.com から最新バージョンの Cisco Secure Firewall 移行ツールをダウンロードすることを強くお勧めします。現在利用可能なサポートされているバージョンは次のとおりです。

- Cisco Secure Firewall 移行ツール v 3.0.1
- Cisco Secure Firewall 移行ツール v 3.0.2

Cisco Secure Firewall 移行ツールバージョン 3.0.1 は現在サポートが終了しており、software.cisco.com から削除される予定です。

サポートされている ASA with FPS のバージョン

Cisco Secure 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、ファイアウォール移行ツールは、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 脅威に対する防御 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

Cisco Secure 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。

翻訳について
このドキュメントは、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。