Cisco Secure Firewall 移行ツールを使用した Cisco Secure Firewall Threat Defense への ASA with FirePOWER Services（FPS）ファイアウォールの移行

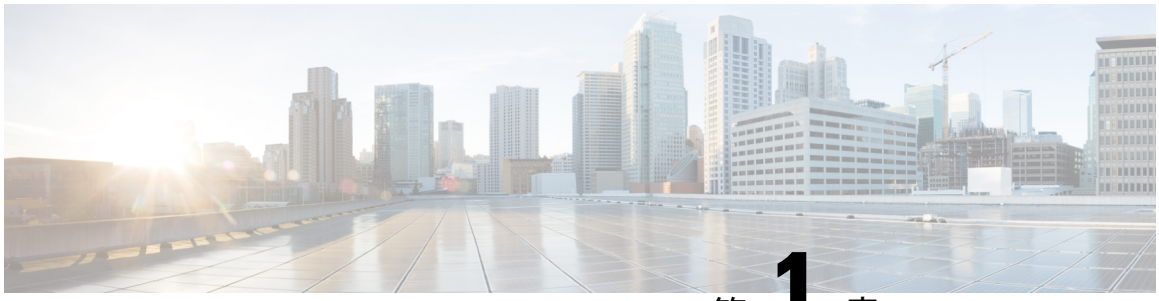
初版：2021 年 7 月 30 日

最終更新：2022 年 6 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

Firewall 移行ツールについて

Firewall 移行ツールについて

資料

本書『*Cisco Secure Firewall* 移行ツールを使用した *ASA with Firewall Services*（*FPS*）から *Cisco Secure Firewall Threat Defense* への移行』に記載されているすべての情報については、最新バージョンの Secure Firewall を参照しています。「Cisco.com から Firewall 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 Firewall 移行ツールをダウンロードします。

2.4 以降では、Firewall 移行ツールは ASA with Firewall Services（FPS）ファイアウォール構成の脅威に対する防御 への移行をサポートしています。Firewall 移行ツールは、ASA with FPS 構成を 脅威に対する防御 に移行するためのものです。

結果を表示するための Firewall 移行ツール

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。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。

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 Management Center にプッシュします。解析フェーズ中に、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、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。

Firewall 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。

- **ASA with FPS 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、Firewall 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。

- [最適化、確認および検証（Optimize, Review and Validate）] ページ

（注） この段階で Firewall 移行ツールを終了して再起動すると、[最適化、確認および検証（Optimize, Review and Validate）] ページが表示されます。

コンソール

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、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、Firewall移行ツールのログファイルにも書き込まれます。

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 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。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

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。

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

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

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 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。

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、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。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。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

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、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、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、Firewall 移行ツールに他のポートを使用できなくなります。

Firewall 移行ツールの履歴

バージョン	サポートされる機能

3.0	Firewall 移行ツール 3.0 は、以下をサポートするようになりました。
	• 移行先の Secure Firewall Management Center 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 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
	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、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。 • Firewall 移行ツールは、ASDM 管理対象の FPS ルールの 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 Firewall 移行ツールで使用されます。

Firewall 移行ツールのライセンス

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 へ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 Success Network

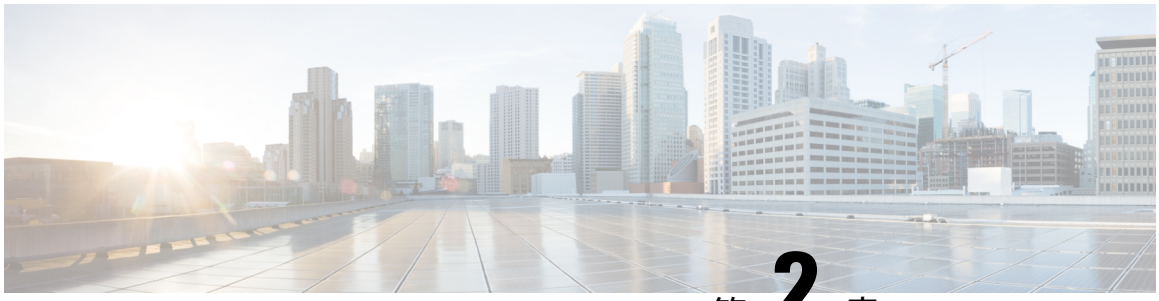
Cisco Success Network はユーザ対応のクラウドサービスです。Cisco Success Network を有効にすると、Firewall 移行ツールと Cisco Cloud 間にセキュアな接続が確立され、使用状況に関する情報と統計情報がストリーミングされます。テレメトリをストリーミングすることによって、Firewall 移行ツールからの対象のデータを選択して、それを構造化形式でリモートの管理ステーションに送信するメカニズムが提供されるため、次のメリットが得られます。

- 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。

Firewall 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

Firewall 移行ツールの [エンドユーザーライセンス契約（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、「Firewall 移行ツールの起動 （29 ページ）」を参照してください。移行ごとに、Firewall 移行ツールの [設定（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 （65 ページ）を参照してください。



第 2 章

移行の準備

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 （23 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 （25 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 （21 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 （23 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 （25 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 （25 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 （26 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 （28 ページ）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

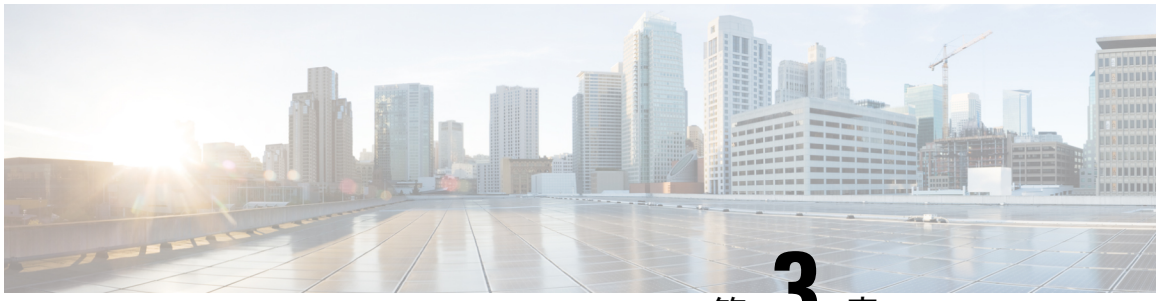
Firewall 移行ツールでは、 脅威に対する防御 のバージョン 6.5 以降を実行しているデバイスへの移行が推奨されます。

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



第 3 章

Firewall 移行ツールの実行

Cisco.com から Firewall 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。

手順

ステップ 1 コンピュータで、Firewall 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。Firewall 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） Firewall 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、[Firewall移行ツール（Firewall Migration Tool）] をクリックします。

上記のリンクをクリックすると、[Firewall NGFWバーチャル（Firewall NGFW Virtual）] の [Firewall移行ツール（Firewall Migration Tool）] に移動します。脅威に対する防御デバイスのダウンロード領域から Firewall 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 Firewall 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 Firewall 移行ツール実行可能ファイルをダウンロードします。

ASA with FPS 構成ファイルの取得

ASA with FPS 構成ファイルを取得するには、次のいずれかの方法を使用できます。

- ASA with FPS 構成ファイルのエクスポート （28 ページ）
- Firewall 移行ツールから ASA への接続 （33 ページ）

ASA with FPS 構成ファイルのエクスポート

このタスクは、ASA with FPS 構成ファイルを手動でアップロードする場合にのみ必要です。ASA with FPSから Firewall 移行ツール に接続する場合は、Firewall 移行ツールから ASA への接続 （33 ページ）に進みます。

（注） ファイルをエクスポートした後、ASA with FPS 構成を手動でコーディングしたり、変更を加えたりしないでください。これらの変更は Secure Firewall Threat Defense に移行されず、移行でエラーが発生するか、移行が失敗します。たとえば、端末で構成ファイルを開いて保存すると、Firewall 移行ツールで解析できない空白または空白行が追加されることがあります。

エクスポートされた ASA with FPS 構成ファイルに "--More--" キーワードがテキストとして含まれていないことを確認します。含まれていると、移行が失敗する可能性があります。

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 構成ファイルをインポートできます。
- FPS を管理する Firewall 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。

手順

ステップ 1 移行する ASA デバイスまたはコンテキストに対して **show running-config** コマンドを使用し、そこから構成をコピーします。「View the Running Configuration」[英語] を参照してください。

または、移行する ASA デバイスまたはコンテキストに対して Adaptive Security Device Manager（ASDM）を使用し、**[ファイル（File）] > [新しいウインドウに実行コンフィギュレーションを表示（Show Running Configuration in New Window）]** を選択して、構成ファイルを取得します。

（注） マルチコンテキスト ASA with FPS の場合は、**show tech-support** コマンドを使用して、単一ファイル内のすべてのコンテキストの構成を取得できます。

ステップ 2 構成を `.cfg` または `.txt` として保存します。

異なる拡張子の Firewall 移行ツール 構成を ASA with FPSにアップロードすることはできません。

ステップ 3 ASA with FPSをダウンロードしたコンピュータに Firewall 移行ツール 構成ファイルを転送します。

次のタスク

Firewall 移行ツールの起動 （29 ページ）

Firewall 移行ツールの起動

（注） Firewall 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、Firewall 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、Firewall 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 Firewall 移行ツールのダウンロード
- Firewall 移行ツールに関する注意事項と制約事項 （9 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。

手順

ステップ 1 コンピュータで、Firewall 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、Firewall 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、[はい（Yes）] をクリックして、Firewall 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。

  Firewall 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、Firewall 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、Firewall 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 Firewall_Migration_Tool-version_number.command
  ```

  ```
  # ./Firewall_Migration_Tool-version_number.command
  ```

  Firewall 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 Firewall 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 Firewall 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 [エンドユーザライセンス契約（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、[Cisco Success Network と情報を共有することに同意（I agree to share data with Cisco Success Network）] をクリックし、それ以外の場合は [後で行う（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 Firewall 移行ツールにログインします。

ステップ 4 Firewall 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、[CCO でログイン（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。
  - ユーザー名：admin
  - パスワード：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 [パスワードのリセット（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、Firewall 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 [新規移行（New Migration）] をクリックします。

ステップ 10 [ソフトウェアアップデートの確認（Software Update Check）] 画面で、Firewall 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 [続行（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。

- ASA with FPS 構成をコンピュータにエクスポートした場合は、「ASA with FPS 構成ファイルのアップロード」に進みます。
- Firewall 移行ツールを使用して ASA with FPS から情報を抽出する場合は、Firewall 移行ツールから ASA への接続 （33 ページ）に進みます。

ASA with FPS 構成ファイルのアップロード

始める前に

送信元 ASA with FPS デバイスから構成ファイルを `.cfg` または `.txt` としてエクスポートします。

（注） ハードコーディングした構成ファイルや手動で変更した構成ファイルはアップロードしないでください。テキストエディタは、移行に失敗する原因となる空白行やその他の問題をファイルに追加します。

手順

ステップ 1 [Cisco ASA（9.2.2 以降）with FPS情報の抽出（Extract Cisco ASA (9.2.2+) with FPS Information）] 画面の [手動アップロード（Manual Upload）] セクションで、[アップロード（Upload）] をクリックして ASA with FPS 構成ファイルをアップロードします。

ステップ 2 ASA with FPS 構成ファイルの場所を参照し、[開く（Open）] をクリックします。

Firewall 移行ツールは構成ファイルをアップロードします。大規模な構成ファイルの場合、この手順には時間がかかります。コンソールには、解析中の ASA with FPS 構成行など、行ごとに進行状況のログが表示されます。コンソールが表示されない場合は、 Firewall 移行ツールの背後にある別のウィンドウで確認できます。[コンテキストの選択（Context Selection）] セクションで、アップロードされた構成がマルチコンテキスト に対応するかが識別されます。

ステップ 3 [Firewall Management Center IP アドレス/ホスト名（Firewall Management Center IP Address/Hostname）] フィールドに、次の関連する詳細情報を入力します。

- シングルコンテキスト ASA with FPS：管理 IP アドレスまたはホスト名
- マルチコンテキスト ASA with FPS：管理コンテキストの IP アドレスまたはホスト名

ステップ 4 [接続（Connect）] をクリックします。

[Firewall Management Center へのログイン（Firewall Management Center Login）] 画面で次の詳細情報を入力します。

- ユーザ名
- パスワード
- [ログイン（Login）] をクリックして Firewall Management Center に接続します。

ステップ 5 [FPS デバイスの選択（Select FPS Device）] ドロップダウンには、特定の管理センター接続されている FPS デバイスのリストが表示されます。デバイスごとに、デバイス名と、関連付けられた ACL ポリシーが表示されます。

ステップ 6 [コンテキストの選択（Context Selection）] セクションを確認し、移行する ASA with FPS を選択します。

ステップ 7 [続行（Proceed）] をクリックします。

アクセスルールがデバイスから取得されます。

ステップ 8 [解析サマリー（Parsed Summary）] セクションに解析ステータスが表示されます。

ステップ 9 アップロードされた構成ファイルで、 Firewall 移行ツールが検出および解析した要素の概要を確認します。

ステップ 10 [次へ（Next）] をクリックして、ターゲットパラメータを選択します。

次のタスク

Firewall 移行ツールの接続先パラメータの指定 （35 ページ）

Firewall 移行ツールから ASA への接続

Firewall 移行ツールは、移行する デバイスに接続し、必要な構成情報を抽出できます。

始める前に

- Firewall 移行ツールをダウンロードして起動します。
- シングルコンテキスト ASA の場合、管理 IP アドレス、管理者ログイン情報、およびイネーブルパスワードを取得します。
- マルチコンテキストモード ASA の場合は、**管理**コンテキストの IP アドレス、管理者ログイン情報、およびイネーブルパスワードを取得します。

（注） ASA に**イネーブルパスワード**が構成されていない場合は、Firewall 移行ツールでこのフィールドを空白のままにしておくことができます。

手順

ステップ 1 [Cisco ASA (9.2.2+) with FPS情報の抽出（Extract Cisco ASA (9.2.2+) with FPS Information）] 画面の [ASAへの接続（Connect to ASA）] セクションで、[接続（Connect）] をクリックして、移行する ASA デバイスに接続します。

ステップ 2 [ASA ログイン（ASA Login）] 画面で、次の情報を入力します。

1. [ASA IP アドレス/ホスト名（ASA IP Address/Hostname）] フィールドに、管理 IP アドレスまたはホスト名（シングルコンテキスト ASA の場合）か、管理コンテキストの IP アドレスまたはホスト名（マルチコンテキスト ASA の場合）を入力します。
2. [ユーザ名（Username）]、[パスワード（Password）]、および[イネーブルパスワード（Enable Password）] フィールドに、適切な管理者用のログイン資格情報を入力します。

   （注） ASA に**イネーブルパスワード**が構成されていない場合は、Firewall 移行ツールでこのフィールドを空白のままにしておくことができます。
3. [ログイン（Login）] をクリックします。

Firewall 移行ツールが ASA に接続すると、ASA に正常に接続されたというメッセージが表示されます。マルチコンテキスト ASA の場合、Firewall 移行ツールはコンテキストを識別してリストします。

ステップ 3 [コンテキスト（Context）] ドロップダウンリストから、移行するコンテキストを選択します。

ステップ 4 （任意）[ヒットカウントの収集（Collect Hitcounts）] を選択します。

オンにすると、このツールは ASA ルールが使用された回数と、ASA 稼働時間以降または最後の ASA 再起動以降にルールが使用された最後の時刻を計算し、[確認と検証（Review and Validate）] ページにこの情報を表示します。これにより、移行前にルールの有効性と関連性を評価できます。

ステップ 5 [抽出を開始（Start Extraction）] をクリックします。

Firewall 移行ツールが ASA に接続し、構成情報の抽出を開始します。抽出が正常に完了すると、[コンテキストを選択（Context Selection）] セクションで、アップロードされた構成がシングルコンテキストまたはマルチコンテキスト ASA のどちらに対応するかが識別されます。

ステップ 6 [コンテキストを選択（Context Selection）] セクションを確認し、移行する ASA コンテキストを選択します。

ステップ 7 [Firewall Management Center IP アドレス/ホスト名（Firewall Management Center IP Address/Hostname）] フィールドに、次の関連する詳細情報を入力します。

- シングルコンテキスト ASA with FPS：管理 IP アドレスまたはホスト名
- マルチコンテキスト ASA with FPS：管理コンテキストの IP アドレスまたはホスト名

ステップ 8 [接続（Connect）] をクリックします。

[Firewall Management Center へのログイン（Firewall Management Center Login）] 画面で次の詳細情報を入力します。

- ユーザ名
- パスワード
- [ログイン（Login）] をクリックして Firewall Management Center に接続します。

ステップ 9 [FPS デバイスの選択（Select FPS Device）] ドロップダウンには、特定の管理センターアタッチされている FPS デバイスのリストが表示されます。デバイスごとに、デバイス名と、関連付けられた ACL ポリシーが表示されます。

ステップ 10 [続行（Proceed）] をクリックします。

アクセスルールがデバイスから取得されます。

ステップ 11 [解析サマリー（Parsed Summary）] セクションに解析ステータスが表示されます。Firewall 移行ツールは構成ファイルを解析し、ASA から切断します。

ステップ 12 アップロードされた構成ファイルで、Firewall 移行ツールが検出および解析した要素の概要を確認します。

ステップ 13 [次へ（Next）] をクリックして、ターゲットパラメータを選択します。

次のタスク

Firewall 移行ツールの接続先パラメータの指定 （35 ページ）

Firewall 移行ツールの接続先パラメータの指定

始める前に

- オンプレミス Firewall Management Center の Management Center の IP アドレスを取得します。
- 「User Accounts for Management Access」の説明に従って、REST API にアクセスするための十分な権限で、Management Center に Firewall 管理ツールの専用アカウントを作成します。
- （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 脅威に対する防御 デバイスを Management Center に追加します。「Adding Devices to the Firewall Management Center」を参照してください。
- [確認と検証（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 Management Center でポリシーを作成することを強くお勧めします。Firewall 移行ツールは接続された Management Center 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。

手順

ステップ 1 [ターゲットの選択（Select Target）] 画面の [ファイアウォール管理（Firewall Management）] セクションで、次の手順を実行します。

a) [オンプレミス FMC（On-Prem FMC）] オプションボタンをクリックします。

b) 管理センターの IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。
c) [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。

脅威に対する防御 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 脅威に対する防御 デバイスにのみ移行できます。

d) [接続（Connect）] をクリックして、**手順 2** に進みます。

ステップ 2 [Firewall Management Centerへのログイン（Firewall Management Center Login）] ダイアログボックスで、Firewall 移行ツール専用アカウントのユーザー名とパスワードを入力し、[ログイン（Login）] をクリックします。

Firewall 移行ツールは Management Center にログインし、その Management Center による管理対象 脅威に対する防御 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 3 [ターゲットの選択（Select Target）] 画面の [Threat Defense の選択（Choose Threat Defense）] セクションでは、移行先の 脅威に対する防御 デバイスを選択できます。また、脅威に対する防御 デバイスがない場合は、ASA with FPS 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 Management Center に移行できます。

ステップ 4 [Threat Defense の選択（Choose Threat Defense）] セクションで、次のいずれかを実行します。

- [Firewall Threat Defenseデバイスの選択（Select Firewall Threat Defense Device）] ドロップダウンリストをクリックし、 ASA with FPS 構成を移行するデバイスをオンにします。

  選択した 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 脅威に対する防御デバイスには、移行する ASA with FPS 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、脅威に対する防御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。 ASA with FPS 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。

表 *1 : ASA with FPS* ファイアウォール機能とサポートされている *Management Center* または *Threat Defense* のバージョン

ファイアウォール機能	サポートされている管理センターまたは Threat Defense のバージョン
ASA with FPS とリモート展開	6.7 以降
暗号マップサイト間 VPN	6.6 以降
仮想トンネルインターフェイス（VTI）とルートベース（VTI）	6.7 以降
ASA with FPS 展開	6.5 以降

ファイアウォール機能	サポートされている管理センターまたは Threat Defense のバージョン
動的ルートオブジェクトと BGP	7.1 以降
リモート アクセス VPN	Management Center 7.2 以降と Threat Defense 7.0 以降。

（注） サイト間 VPN、VTI、およびルートベース（VTI）インターフェイスを移行するには、Management Center で 脅威に対する防御 を構成する必要があります。

- ASA 5505 の場合、デバイス固有の構成（インターフェイスおよびルータ）と共有ポリシー（NAT、ACL、オブジェクト）は、サポートされているターゲット 脅威に対する防御 プラットフォームが Management Center バージョン 6.5 以降を備えた Firewall 1010 の場合にのみ移行できます。

  （注） ターゲット 脅威に対する防御 が FPR-1010 でない場合、またはターゲット Management Center が 6.5 よりも前の場合は、ASA 5505 の移行サポートは共有ポリシーにのみ適用されます。デバイス固有の設定は移行されません。

  （注） 送信元構成は ASA 5505 であるため、[Select Device] ドロップダウンリストから FPR-1010 のみを選択できます。

  （注） ASA-SM 移行のサポートは、共有ポリシーのみを対象としています。デバイス固有の設定は移行されません。

- [Threat Defense を使用せず続行（Proceed without Threat Defense）] をクリックして、構成を Management Center に移行します。

  脅威に対する防御 なしで続行すると、Firewall 移行ツールは 脅威に対する防御 に構成またはポリシーをプッシュしません。したがって、脅威に対する防御 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、およびサイト間 VPN 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。リモートアクセス VPN は共有ポリシーであり、Threat Defense なしでも移行できます。

ステップ 5 [続行（Proceed）] をクリックします。

移行先に応じて、Firewall 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 6 [機能の選択（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 脅威に対する防御 デバイスに移行する場合、Firewall 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、 ASA with FPS 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。
- Management Center に移行する場合、Firewall 移行ツールは、[共有設定（Shared Configuration）] セクションで、 ASA with FPS 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） [デバイスの構成（Device Configuration）] セクションは、移行先 脅威に対する防御 デバイスを選択していない場合は使用できません。

- Firewall 移行ツールでは、移行中に次のアクセス制御がサポートされています。
  - 宛先セキュリティゾーンの指定：移行中の ACL の宛先ゾーンのマッピングを有効にします。

    ルートルックアップロジックは静的ルートと接続ルートに限定され、PBR、動的ルート、および NAT は考慮されません。インターフェイス ネットワーク構成は、接続ルート情報を取得するために使用されます。

    送信元および接続先のネットワーク オブジェクト グループの性質によっては、この操作によりルールが急増することがあります。

  - 非暗号化トンネルルール（ASA）のプレフィルタポリシーとしての移行：ASA カプセル化トンネルプロトコルルールをプレフィルタトンネルルールにマッピングすると、次のような利点があります。
    - ディープインスペクションの調整：カプセル化トラフィックの場合に、ファストパス処理でのパフォーマンスを向上させます。
    - パフォーマンスの向上：早期処理のメリットがあるその他の接続についても、ファストパスやブロックをすることができます。

    Firewall 移行ツールは、送信元構成でカプセル化されたトンネルトラフィックルールを識別し、プレフィルタトンネルルールとして移行します。プレフィルタポリシーで移行されたトンネルルールを確認できます。プレフィルタポリシーは、Management Center で移行されたアクセス コントロール ポリシーに関連付けられます。

    プレフィルタトンネルルールとして移行されるプロトコルは次のとおりです。
    - GRE（47）
    - IPv4 カプセル化（4）
    - IPv6 カプセル化（41）
    - Teredo トンネリング（UDP:3544）

    （注） プレフィルタオプションを選択しない場合、すべてのトンネルトラフィックルールがサポートされていないルールとして移行されます。

    ASA with FPS 構成の ACL トンネルルール（GRE および IPnIP）は、現在、デフォルトで双方向として移行されます。アクセスコントロールの状態オプションで、接続先のルール方向を双方向または単方向に指定できるようになりました。

- Firewall 移行ツールは、VPN トンネル移行用に次のインターフェイスとオブジェクトをサポートしています。
  - ポリシーベース（暗号マップ）：ターゲット Management Center と 脅威に対する防御がバージョン 6.6 以降の場合

- ルートベース（VTI）：ターゲット Management Center と 脅威に対する防御 がバージョン 6.7 以降の場合

- ファイアウォール移行ツールは、ターゲットの管理センターが 7.2 以降の場合はリモートアクセス VPN の移行をサポートします。リモートアクセス VPN は、Threat Defense なしで移行できる共有ポリシーです。Threat Defense を使用する移行を選択した場合、Threat Defense のバージョンは 7.0 以降である必要があります。
- （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、ASA with FPS 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。

- （任意）[最適化（Optimization）] セクションで、脅威に対する防御 のアクセスポリシーによる最適なメモリ使用率を実現する場合は、[オブジェクトグループの検索（Object group search）] を選択します。
- （任意）[インライングループ化（Inline Grouping）] セクションでは、Firewall 移行ツールを使用して、CSM または DM で始まる定義済みのネットワークおよびサービスオブジェクト名のアクセスルールをクリアできます。このオプションをオフにすると、定義済みのオブジェクト名が移行時に保持されます。詳細については、「インライングループ化」を参照してください。

  （注） デフォルトでは、インライングループ化のオプションが有効になっています。

ステップ 7 [続行（Proceed）] をクリックします。

ステップ 8 [変換の開始（Start Conversion）] をクリックし、変換を開始します。

ステップ 9 [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 10 Firewall 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 11 [レポートのダウンロード（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、Firewall 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 （41 ページ）

インライングループ化

ASDM および CSM マネージド ASA によるオブジェクトグループ化

送信元または接続先のアドレス、あるいは送信元または接続先のサービスに複数の項目（オブジェクトまたはインラインの値）を入力すると、CSM または ASDM でオブジェクトグループが自動的に作成されます。各 ASA デバイスに構成を展開する際に、CSM および ASDM で使用されるこれらのオブジェクトグループの命名規則は、それぞれ CSM_INLINE および DM_INLINE です。

（注） オブジェクトグループ化の動作を変更するには、**[ツール（Tools）]** > **[設定（Preferences）]** から、[指定したプレフィックスを持つネットワークおよびサービスオブジェクトを自動展開する（Auto-expand network and service objects with specified prefix）] ルールテーブル設定を選択します。

次に、ASDM によって管理される ASA で **show run** コマンドを使用して抽出された構成スニペットを示します。

```
object network host1
 host 10.1.1.100
object network fqdn_obj1
 fqdn abc.cisco.com
object-group network DM_INLINE_NETWORK_1
 network-object 10.21.44.189 255.255.255.255
 network-object 10.21.44.190 255.255.255.255
object-group network DM_INLINE_NETWORK_2
 network-object 10.21.44.191 255.255.255.255
 network-object object host1
 network-object object fqdn_obj1


access-list CSM_DM_ACL extended permit tcp object-group DM_INLINE_NETWORK_1 object-group
 DM_INLINE_NETWORK_2
```

上記の例では、ASDM UI の access-list CSM_DM_ACL は、ルールの送信元および接続先のネットワークとして DM_INLINE グループを表示せず、代わりに DM_INLINE グループの内容を表示します。

インライングループ化：ASDM/CSM

Firewall 移行ツールのインライングループ化機能を使用すると、ASDM または CSM のマネージド ASA デバイスの **show running-configuration** を解析できます。ASDM または CSM と同じアクセスリストルールの UI 表現を保持するオプションがあります。オプトアウトした場合、移行されたルールは、ASA **show running-configuration** で記録されている DM_INLINE グループを参照します。

（注） 引き続き Firewall 移行ツールへの送信元 ASA 構成ファイル入力は、ASA からまたは ASA デバイス（SSH）へのライブ接続を介して収集された **show run** または **show tech** になります。Firewall 移行ツールは、他形式の構成のファイルまたは方式をサポートしていません。

次の図は、ACE または RULE の [送信元ネットワーク（Source Network）] フィールドと [接続先ネットワーク（Destination Network）] フィールドが、それぞれインライングループ化オプションの有効化または無効化に基づいてどのように変化するかを示しています。

図 *1*：インライングループ化あり：*ASDM/CSM* が有効

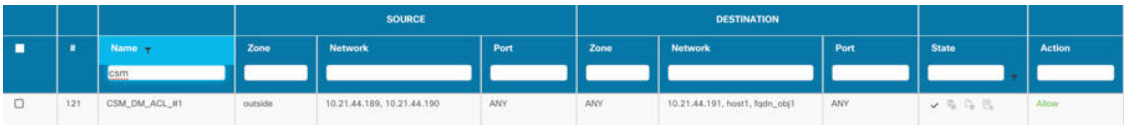


図 *2*：インライングループ化あり：*ASDM/CSM* が無効

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、 Firewall 移行ツールの実行中にのみダウンロードできます。

手順

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、 Firewall 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。

- [全体のサマリー（Overall Summary）]：ASA with FPS 構成情報を抽出するため、または ASA with FPS に手動アップロードするために使用される方法。

  ライブ ASA に接続している場合は、 ASA with FPS で検出されたファイアウォールモード。マルチコンテキストモードの場合は、移行用に選択したコンテキスト。

  脅威に対する防御 に正常に移行できるサポート対象 ASA with FPS 構成要素と、移行対象として選択された特定の ASA with FPS 機能のサマリー。

  ライブ ASA に接続している場合、サマリーにはヒットカウント情報（ASA ルールが検出された回数とそのタイムスタンプ情報）が含まれます。

- [エラーのある構成行（Configuration Lines with Errors）]： Firewall 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 ASA with FPS の構成要素の詳細。 ASA with FPS 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 Firewall 移行ツールにアップロードし、続行してください。

- [部分的なサポート構成（Partially Supported Configuration）]：部分的にのみ移行可能な ASA with FPS 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 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、 Firewall 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。

- [未サポートの構成（Unsupported Configuration）]： Firewall 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 ASA with FPS 構成要素の詳細。これらの行を確認し、各機能が 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、 Firewall 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。

- [無視される構成（Ignored Configuration）]： Management Center または Firewall 移行ツールでサポートされていないために無視される ASA with FPS 構成要素の詳細。 Firewall 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 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。

Management Center と 脅威に対する防御 でサポートされる機能の詳細については、『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、 ASA with FPS インターフェイス で修正を完了し、 ASA with FPS 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 ASA with FPS 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、 Firewall 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

ASA with FPS 構成と Secure Firewall Device Manager Threat Defense インターフェイスのマッピング

ASA with FPS 構成と Secure Firewall Device Manager Threat Defense インターフェイスのマッピング

脅威に対する防御 デバイスには、 ASA with FPS 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。

[Threat Defense インターフェイスのマップ（Map Threat Defense Interface）] 画面で、脅威に対する防御 デバイス上のインターフェイスのリストを取得します。デフォルトでは、Firewall 移行ツールは ASA with FPS のインターフェイスと 脅威に対する防御 デバイスをインターフェイス ID に従ってマッピングします。たとえば、 インターフェイスの「管理専用」インターフェイスは、脅威に対する防御デバイスの「管理専用」インターフェイスに自動的にマッピングされ、変更できません。

ASA with FPS インターフェイスから 脅威に対する防御 インターフェイスへのマッピングは、脅威に対する防御 デバイスタイプによって異なります。

- ターゲット 脅威に対する防御 がネイティブタイプの場合は次のようになります。
  - 脅威に対する防御 には、使用する ASA with FPS 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が同数以上必要です（ ASA with FPS 構成の管理専用とサブインターフェイスを除く）。同数未満の場合は、ターゲット 脅威に対する防御 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 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 がコンテナタイプの場合は次のようになります。
  - 脅威に対する防御 には、使用する ASA with FPS 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（ ASA with FPS 構成の管理専用を除く）。同数未満の場合は、ターゲット 脅威に対する防御 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 脅威に対する防御 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 ASA with FPS での数より 100 少ない場合、ターゲット 脅威に対する防御 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。
  - 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。物理インターフェイス、ポートチャネル、またはサブインターフェイス間のインターフェイスマッピングのみが許可されます。

始める前に

Management Center に接続し、接続先として 脅威に対する防御 を選択していることを確認します。詳細については、「Firewall 移行ツールの接続先パラメータの指定 （35 ページ）」を参照してください。

（注） 脅威に対する防御 デバイスなしで Management Center に移行する場合、この手順は適用されません。

手順

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、[Threat Defenseインターフェイス名（Threat Defense Interface Name）] のドロップダウンリストをクリックし、その ASA with FPS 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。脅威に対する防御インターフェイスがすでに ASA with FPS 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。Firewall 移行ツールは、 ASA with FPS 構成内のすべてのサブインターフェイスについて 脅威に対する防御 デバイスのサブインターフェイスをマッピングします。

ステップ 2 各 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たら、[次へ（Next）] をクリックします。

次のタスク

ASA with FPS インターフェイスを適切な 脅威に対する防御 インターフェイス オブジェクト、セキュリティゾーン、およびインターフェイスグループ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 とインターフェイスグループへの ASA with FPS 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 とインターフェイスグループへの ASA with FPS インターフェイスのマッピング

（注） ASA with FPS 構成にアクセスリストと NAT ルールが含まれていない場合、またはこれらのポリシーを移行しない場合は、この手順をスキップして「最適化、 移行する構成の確認と検証（47 ページ）」に進むことができます。

ASA with FPS 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 脅威に対する防御 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。 ASA with FPS 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。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、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。
- インターフェイスグループ：インターフェイスは複数のインターフェイスグループに属することができます。

Firewall 移行ツールでは、セキュリティゾーンおよびインターフェイスグループ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またはインターフェイスグループ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、Management Center では許可されます。Management Center のセキュリティゾーンとインターフェイスグループの詳細については、「Interface Objects: Interface Groups and Security Zones」[英語] を参照してください。

手順

ステップ 1 [セキュリティゾーンとインターフェイスグループへのマッピング（Map Security Zones and Interface Groups）] 画面で、使用可能なインターフェイス、セキュリティゾーン、およびインターフェイスグループを確認します。

ステップ 2 セキュリティゾーンおよびインターフェイスグループが Management Center に存在する場合、またはセキュリティ ゾーン タイプ オブジェクトとして ASA with FPS 構成ファイルに存在し、ドロップダウンリストで使用可能な場合、これらにインターフェイスをマッピングするには、次の手順を実行します。

a) [セキュリティゾーン（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。

b) [インターフェイスグループ（Interface Groups）] 列で、そのインターフェイスのインターフェイスグループを選択します。

ステップ 3 セキュリティゾーンとインターフェイスグループは、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。

ステップ 4 セキュリティゾーンとインターフェイスグループを手動でマッピングするには、次の手順を実行します。

a) [セキュリティゾーンとインターフェイスグループの追加（Add SZ & IG）] をクリックします。

b) [セキュリティゾーンとインターフェイスグループの追加（Add SZ & IG）] ダイアログボックスで、[追加（Add）] をクリックして新しいセキュリティゾーンまたはインターフェイスグループを追加します。

c) [セキュリティゾーン（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。同様に、インターフェイスグループを追加できます。

d) [閉じる（Close）] をクリックします。

ASA with FPS の移行の場合：

- セキュリティゾーンタイプ「ASA」からセキュリティゾーンタイプ「ルーテッド/スイッチド」（Threat Defense でサポート）への移行がサポートされています。
- Management Center は一意のセキュリティゾーン名しか受け入れないため、Threat Defense でサポートされる新しいセキュリティゾーンを送信元 ASA with FPS のゾーンと同じ名前にすることはできません。
- 送信元 Management Center に存在する、選択した ASA with FPS のすべての ASA タイプゾーンについて、新しい Threat Defense （ルーテッド/スイッチド）ゾーンが [ゾーンマッピング（Zone Mapping）] ページの Firewall 移行ツールに作成されます。ASA から Management Center への移行とは異なり、ASA with FPS のシナリオでは、セキュリティゾーンは FPS ポリシーから取得されます。Threat Defense 論理名（ASA nameif）に基づいて作成されることはありません。
- インターフェイスグループは Threat Defense 論理名を使用して移行されるため、NAT には影響しません。

[FPSゾーン（FPS Zones）] カラムには、ASA 論理インターフェイスにマッピングされているセキュリティゾーンが表示されます。

（注） このカラムでは、選択した ASA with FPS デバイスゾーンのみが表示され、それぞれのインターフェイスに対してリストされます。

1 つの ASA with FPS ゾーンが、同じ ASA with FPS デバイスの複数のインターフェイスに関連付けられている場合、そのゾーンは、Threat Defense でサポートされる 2 つのゾーンに分割されます。

セキュリティゾーンとインターフェイスグループ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) [自動作成（Auto-Create）] をクリックします。

b) [自動作成（Auto-Create）] ダイアログボックスで、[インターフェイスグループ（Interface Groups）] または [ゾーンマッピング（Zone Mapping）] のいずれかまたは両方をオンにします。

c) [自動作成（Auto-Create）] をクリックします。

Firewall 移行ツールは、これらのセキュリティゾーンに ASA with FPS インターフェイスと同じ名前（**outside** や **inside** など）を付け、名前の後に "(A)" を表示して、 Firewall 移行ツールによって作成されたことを示します。インターフェイスグループには、**outside_ig** や **inside_ig** などの _igサフィックスが追加されます。また、セキュリティゾーンとインターフェイスグループには、 ASA with FPS インターフェイスと同じモードがあります。たとえば、 ASA with FPS 論理インターフェイスがL3モードの場合、そのインターフェイス用に作成されたセキュリティゾーンとインターフェイスグループも L3 モードになります。

ステップ 5 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とインターフェイスグループにマッピングしたら、[次へ（Next）] をクリックします。

最適化、 移行する構成の確認と検証

移行した ASA with FPS 構成を 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 脅威に対する防御 デバイスの構成内容と一致することを確認します。点滅しているタブは、次の一連のアクションを実行する必要があることを示しています。

これで、 Firewall 移行ツールは、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。

（注） デフォルトでは、[インライングループ化（Inline Grouping）] オプションが有効になっています。

[構成の最適化、確認および検証（Optimize, Review and Validate Configuration）] 画面で Firewall 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 Firewall 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、[インターフェイスマッピング（Interface Mapping）] 画面から Firewall 移行ツールを再起動します。

Firewall 移行ツール ACL 最適化の概要

は、ネットワーク機能に影響を与えることなく、ファイアウォール ルール ベースから最適化（無効化または削除）できる ACL を識別および分離するサポートを提供します。

ACL 最適化は、次の ACL タイプをサポートします。

- 冗長 ACL：2 つの ACL の構成とルールのセットが同じ場合、基本以外の ACL を削除してもネットワークに影響はありません。たとえば、2 つのルールが同じネットワーク上で FTP および IP トラフィックを許可し、アクセスを拒否するルールが定義されていない場合、最初のルールを削除できます。
- シャドウ ACL：最初の ACL は、2 番目の ACL の設定を完全にシャドウイングします。2 つのルールに同様のトラフィックがある場合、2 番目のルールはアクセスリストの後半に表示されるため、どのトラフィックにも適用されません。2 つのルールがトラフィックに対して異なるアクションを指定している場合、シャドウイングされたルールを移動するか、いずれかのルールを編集して必要なポリシーを実装できます。たとえば、特定の送信元または宛先に対して、基本ルールで IP トラフィックを拒否し、シャドウイングされたルールで FTP トラフィックを許可できます。

は、ACL 最適化のルールを比較する際に次のパラメータを使用します。

（注） ではACP ルールアクションに対してのみ最適化を使用できます

- 無効化された ACL は、最適化プロセス中に考慮されません。
- 送信元の ACL は、対応する ACE（インライン値）に展開された後、次のパラメータについて比較されます。
  - 送信元と宛先のゾーン
  - 送信元と宛先のネットワーク
  - 送信元/宛先ポート

オブジェクトの最適化

次のオブジェクトは、移行プロセス中にオブジェクトの最適化について考慮されます。

- 未参照のオブジェクト：移行の開始時に、未参照のオブジェクトを移行しないように選択できます。
- 重複したオブジェクト：オブジェクトがすでに Management Center に存在する場合、重複したオブジェクトを作成する代わりに、ポリシーが再利用されます。

アクセス制御には次の 2 つのセクションがあります。

- プレフィルタ：Management Center に移行される ASA ACL が表示されます。
- ACP：FPS アクセス コントロール ポリシーおよび関連する詳細が表示されます。

  ユーザ、SI など、サポートされていない機能の場合、対応する ACL はサポート対象外としてマークされます。

手順

ステップ 1 （オプション）[構成の最適化、確認および検証（Optimize, Review and Validate Configuration）] 画面で、[ACLの最適化（Optimize ACL）] をクリックして最適化コードを実行し、以下の操作を実行します。

a) 特定された ACL 最適化ルールをダウンロードするには、[ダウンロード（Download）] をクリックします。

b) ルールを選択し、**[アクション（Actions）] > [無効として移行（Migrate as disabled）]** または **[移行しない（Do not migrate）]** を選択して、いずれかのアクションを適用します。

c) **[保存（Save）]** をクリックします。
移行操作が [移行しない（Do not migrate）] から [無効として移行（Migrate as disabled）] またはその逆に変わります。

次のオプションを使用して、ルールの一括選択を実行できます。

- [移行（Migrate）]：デフォルトの状態で移行します。
- [移行しない（Do not migrate）]：ACL の移行を無視します。
- [無効として移行（Migrate as disabled）]：[状態（State）] フィールドが [無効（Disable）] に設定されている ACL を移行します。
- [有効として移行（Migrate as enabled）]：[状態（State）] フィールドが [有効（Enable）] に設定されている ACL を移行します。

ステップ 2 最適化、 [構成の確認と検証（Review and Validate Configuration）] 画面で、[アクセス制御ルール（Access Control Rules）] をクリックし、次の手順を実行します。

a) テーブル内の各エントリについて、マッピングを確認し、それらが正しいことを確認します。

移行されたアクセスポリシールールは、プレフィックスとして ACL 名を使用し、それに ACL ルール番号を追加することで、 ASA with FPS 構成ファイルにマッピングしやすくします。たとえば、 ASA with FPS ACL の名前が "inside_access" の場合、ACL の最初のルール（または ACE）行の名前は "inside_access_#1" になります。TCP または UDP の組み合わせ、拡張サービスオブジェクト、またはその他の理由でルールを拡張する必要がある場合、Firewall移行ツールは名前に番号付きサフィックスを追加します。たとえば、許可ルールが移行のために2つのルールへ拡張される場合、それらのルールには "inside_access_#1-1" と "inside_access_#1-2" という名前が付けられます。

サポートされていないオブジェクトを含むルールの場合、 Firewall 移行ツールは名前に "_UNSUPPORTED" というサフィックスを追加します。

b) 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。

c) 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。

[ファイルポリシー（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、[保存（Save）] をクリックします。

d) 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 ポリシー（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、[保存（Save）] をクリックします。

e) 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。

[ログ（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、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。

f) [アクセスコントロール（Access Control）] 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。

[ルールアクション（Rule Action）] ダイアログの [アクション（Actions）] ドロップダウンで、[ACP] タブまたは [プレフィルタ（Prefilter）] タブを選択できます。

- ACP：アクセスコントロールルールには、システムが一致するトラフィックをどのように処理し、ログに記録するのかを指定するアクションがあります。アクセスコントロールルールに対して許可、信頼、モニタ、ブロック、またはリセット付きブロックのいずれかのアクションを実行できます。
- Prefilter：ルールのアクションによって、一致したトラフィックの処理とログ記録の方法が決まります。ファストパスとブロックを実行できます。

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、[許可（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。

[ACLルールカテゴリ（ACL Rule Category）]： Firewall 移行ツールは、CSM マネージド ASA 構成の [ルール（Rule）] セクションを保持し、Management Center の ACL カテゴリとして移行します。

ポリシーのキャパシティと制限の警告： Firewall 移行ツールは、移行したルールの合計 ACE カウントを、ターゲットプラットフォームでサポートされている ACE 制限と比較します。

Firewall 移行ツールは比較の結果に基づいて、移行された ACE の総数がしきい値を超えた場合や、ターゲットデバイスのサポートされている制限のしきい値に近づいている場合は、視覚インジケータと警告メッセージを表示します。

ルールが [ACE カウント（ACE Count）] 列を超える場合は、最適化することも、移行しないことを決定することもできます。移行を完了してからこの情報を使用して、Management Center でプッシュしてから展開するまでの間に、ルールを最適化することもできます。

（注） Firewall 移行ツールは、警告にもかかわらず移行をブロックしません。

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 3 次のタブをクリックし、構成項目を確認します。

- [NAT ルール（NAT Rules）]
- [オブジェクト（Objects）]（[アクセスリストオブジェクト（Acess List Objects）]、[ネットワークオブジェクト（Network Objects）]、[ポートオブジェクト（Port Objects）]、[VPN オブジェクト（VPN Objects）]、および[動的ルートオブジェクト（Dynamic-Route-Objects）]）
- [インターフェイス（Interfaces）]
- [ルート（Routes）]
- [サイト間 VPN トンネル（Site-to-Site VPN Tunnels）]
- [リモートアクセス VPN（Remote Access VPN）]

アクセスリストオブジェクトには、BGP と RA VPN で使用される標準 ACL と拡張 ACL が表示されます。

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、**[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。

ステップ 4 （任意）構成の確認中に、[ネットワークオブジェクト（Network Objects）] タブ、[ポートオブジェクト（Port Objects）] タブ、または [VPNオブジェクト（VPN Objects）] タブで **[アクション（Actions）]** > **[名前の変更（Rename）]** を選択して、ネットワークオブジェクト、ポートオブジェクト、または VPN 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 5 [動的ルートオブジェクト（Dynamic-Route-Objects）] セクションには、移行されるすべてのサポートされているオブジェクトが表示されます。

- ポリシーリスト
- プレフィックスリスト
- ルートマップ
- コミュニティ リスト
- AS パス
- アクセス リスト

ステップ 6 [ルート（Routes）] セクションには、次のルートが表示されます。

- [スタティック（Static）]：すべての IPv4 および IPv6 スタティックルートを表示します。
- [BGP]：すべての BGP ルートを表示します。

ステップ 7 [リモートアクセス VPN（Remote Access VPN）] セクションでは、リモートアクセス VPN に対応するすべてのオブジェクトがASAから管理センターに移行され、次のように表示されます。

- **Anyconnect ファイル**：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 デバイスから取得する必要があり、また、移行に使用できる必要があります。

  移行前のアクティビティの一環として、すべての AnyConnect パッケージを管理センターにアップロードします。AnyConnect プロファイルは、管理センターに直接アップロードしたり、Firewall 移行ツールからアップロードしたりできます。

  管理センターから取得した既存の Anyconnect、Hostscan、または外部ブラウザパッケージを選択します。1 つ以上の AnyConnect パッケージを選択する必要があります。送信元の構成で使用可能な場合は、Hostscan、dap.xml、data.xml、または外部ブラウザを選択する必要があります。AnyConnect プロファイルはオプションです。

  dap.xml は、ASA から取得した正しいファイルである必要があります。検証は、構成ファイルで使用可能な dap.xml で実行されます。検証に必要なすべてのファイルをアップロー

ドして選択する必要があります。更新に失敗すると不完全とマークされ、Firewall移行ツールは検証に進みません。

- [AAA]：Radius、LDAP、AD、LDAP、SAML、およびローカルレルムタイプの認証サーバーが表示されます。すべての AAA サーバーのキーを更新します。Firewall 移行ツール 3.0 以降、Live Connect ASA の事前共有キーは自動的に取得されます。**more system: running-config** ファイルを使用して、隠しキーを含む送信元の構成をアップロードすることもできます。ASAからクリアテキスト形式でキーを取得する方法については、「リモートアクセス VPN の移行」を参照してください。
- LDAPS では、管理センターにドメインが必要です。暗号化タイプ LDAPS のドメインを更新する必要があります。
- AD サーバーの Management Center には、一意の AD プライマリドメインが必要です。一意のドメインが識別されると、Firewall移行ツールに表示されます。競合が見つかった場合、オブジェクトを正常にプッシュするには、一意の AD プライマリドメインを入力する必要があります。ドメインと AD プライマリドメインの取得については、「リモートアクセス VPN の移行」を参照してください。
- [アドレスプール（Address Pool）]：すべての IPv4 プールと IPv6 プールがここに表示されます。
- [グループポリシー（Group-Policy）]：このセクションには、クライアントプロファイル、管理プロファイル、クライアントモジュール、およびプロファイルのないグループポリシーを含むグループポリシーが表示されます。プロファイルが [AnyConnect ファイル（AnyConnect file）]セクションに追加されている場合は、事前に選択された状態で表示されます。ユーザープロファイル、管理プロファイル、およびクライアント モジュール プロファイルを選択または削除できます。
- [接続プロファイル（Connection Profile）]：すべての接続プロファイル/トンネルグループがここに表示されます。
- [トラストポイント（Trustpoint）]：ASA から管理センターへのトラストポイントまたは PKI オブジェクトの移行は、移行前アクティビティの一環であり、RA VPN の移行を正常に実行するために不可欠です。[リモート アクセス インターフェイス（Remote Access Interface）] セクションでグローバル SSL、IKEv2、およびインターフェイスのトラストポイントをマッピングして、移行の次の手順に進みます。LDAPS プロトコルが有効になっている場合、グローバル SSL と IKEv2 トラストポイントは必須です。SAML オブジェクトが存在する場合、SAML IDP と SP のトラストポイントを SAML セクションでマッピングできます。SP 証明書はオプションです。特定のトンネルグループについては、トラストポイントをオーバーライドすることもできます。オーバーライドされた SAML トラストポイント構成が送信元 ASA で使用可能な場合は、[SAML のオーバーライド（Override SAML）] オプションで選択できます。

  ASA からの PKI 証明書のエクスポートについては、「リモートアクセス VPN の移行」を参照してください。
- [証明書マップ（Certificate Maps）]：ここに証明書マップが表示されます。

ステップ 8 （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、[ダウンロード（Download）] をクリックします。

ステップ 9 確認が完了したら、[検証（Validate）] をクリックします。

検証中、 Firewall 移行ツールは Management Center に接続し、既存のオブジェクトを確認して、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 Management Center にすでに存在する場合、 Firewall 移行ツールは次のことを行います。

- オブジェクトの名前と構成が同じ場合、 Firewall 移行ツールは既存のオブジェクトを再利用し、 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、 Firewall 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 10 検証が完了し、[検証ステータス（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) [競合の解決（Resolve Conflicts）] をクリックします。

Firewall 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、[ネットワークオブジェクト（Network Objects）] タブまたは [ポートオブジェクト（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、**[アクション（Actions）] > [競合の解決（Resolve Conflicts）]** を選択します。

d) [競合の解決（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 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) [解決（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、[保存（Save）] をクリックします。

g) [検証（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 11 検証が完了し、[検証ステータス（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 Management Center へのプッシュ （54 ページ）に進みます。

移行された構成の Management Center へのプッシュ

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 ASA with FPS 構成を Secure Firewall 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 Secure Firewall Management Center に送信します。Secure Firewall Threat Defense デバイスに構成を展開しません。ただし、Secure Firewall Threat Defense 上の既存の構成はこのステップで消去されます。

（注） Firewall 移行ツールが移行された構成を Secure Firewall 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。

手順

ステップ 1 [検証ステータス（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 ASA with FPS 構成を Secure Firewall Management Center に送信します。

Firewall 移行ツールの新しい最適化機能を使用すると、検索フィルタを使用して移行結果を迅速に取得できます。

Firewall 移行ツールは、CSV ダウンロードを最適化し、ページビューごとにまたはすべてのルールにアクションを適用することもできます。

Firewall 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、Secure Firewall 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、[レポートのダウンロード（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、 Firewall 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. [移行完了（Complete Migration）] 画面で、[サポート（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. [サポートバンドル（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. [ダウンロード（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. [電子メールでのお問い合わせ（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. [TAC ページに移動（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

移行後のレポートには、さまざまなカテゴリの ACL カウント、ACL 最適化、および構成ファイルで実行された最適化の全体的なビューに関する詳細が表示されます。詳細については、最適化、 移行する構成の確認と検証 （47 ページ）を参照してください。

オブジェクトを確認して検証します。

- **カテゴリ**
  - ACL ルール合計数（移行元の構成）
  - 最適化の対象とみなされる ACL ルールの合計数。冗長、シャドウなどがあります。
- 最適化の ACL カウントは、最適化の前後にカウントされた ACL ルールの合計数を示します。

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、 Firewall 移行ツールの実行中にのみダウンロードできます。

手順

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、 ASA with FPS 構成がどのように移行されたかを理解します。

- [移行の概要（Migration Summary）]： ASA with FPS から Threat Defense へ正常に移行された構成の概要。 インターフェイス、 Management Center ホスト名とドメイン、ターゲット 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。
- [選択的ポリシーの移行（Selective Policy Migration）]：移行用に選択された特定の ASA with FPS 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。
- [ASA with FPSインターフェイスからThreat Defenseへのマッピング（ASA with FPS Interface to Threat Defense Interface Mapping）]：正常に移行されたインターフェイスの詳細と、 ASA with FPS 構成のインターフェイスを 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 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。

- [Threat Defenseセキュリティゾーンおよびインターフェイスグループへのソースインターフェイス名（Source Interface Names to Threat Defense Security Zones and Interface Groups）]：正常に移行された ASA with FPS 論理インターフェイスと名前の詳細、およびそれらを Threat Defense のセキュリティゾーンとインターフェイスグループ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。

- [オブジェクト競合の処理（Object Conflict Handling）]：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 ASA with FPS 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、 Firewall 移行ツールは 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。
- [移行しないアクセスコントロールルール、NAT、ルート（Access Control Rules, NAT, and Routes You Chose Not to Migrate）]： Firewall 移行ツールで移行しないように選択したルールの詳細。 Firewall 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。
- [部分的に移行された構成（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 ASA with FPS ルールの詳細。これらの行を確認し、詳細オプションが 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。
- [未サポートの構成（Unsupported Configuration）]： Firewall 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、移行されなかった ASA with FPS 構成要素の詳細。これ

らの行を確認し、各機能が 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、Management Center でこれらの機能を手動で構成します。

- [拡張アクセス コントロール ポリシー ルール（Expanded Access Control Policy Rules）]：移行時に単一の Point ルールから複数の Threat Defense ルールに拡張された ASA with FPS アクセス コントロール ポリシー ルールの詳細。
- [アクセスコントロールルールに適用されるアクション（Actions Taken on Access Control Rules）]
  - [移行しないアクセスルール（Access Rules You Chose Not to Migrate）]： Firewall 移行ツールで移行しないように選択した ASA with FPS 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。
  - [ルールアクション変更によるアクセスルール（Access Rules with Rule Action Change）]：Firewall 移行ツールツールを使用して「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、[許可（Allow）]、[信頼（Trust）]、[モニタ（Monitor）]、[ブロック（Block）]、[リセット付きブロック（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。
  - [IPSポリシーと変数セットが適用されているアクセスコントロールルール（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 ASA with FPS 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 Threat Defense でサポートされているかどうかを確認します。
  - [ファイルポリシーが適用されているアクセスコントロールルール（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 ASA with FPS 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 Threat Defense でサポートされているかどうかを確認します。
  - [ログのルール設定が変更されたアクセスコントロールルール（Access Control Rules that have Rule ‘Log’ Setting Change）]： Firewall 移行ツールを使用して「ログ設定」が変更された ASA with FPS 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。
  - [ゾーンのルックアップに失敗したアクセスコントロールルール（Access Control Rules that have failed Zone-lookup）]：ルートルックアップ操作に失敗し、**移行後レポート**に入力される ASA with FPS アクセスコントロールルールの詳細。 Firewall 移行ツールは、送信元構成のルート（静的および接続）情報に基づいてルートルックアップ操作を実行し、アクセスルールに宛先セキュリティゾーンを設定します。

- [トンネルプロトコルに対するアクセスコントロールルール（Access Control Rules for Tunneled Protocols）]：移行時にプレフィルタトンネルルールとして移行されるトンネルルールの詳細。

（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 Threat Defense によってブロックされるように、Management Center でルールを構成することを推奨します。

（注） [確認と検証（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、移行前に管理センターでポリシーを作成することを強くお勧めします。 Firewall 移行ツールは接続された管理センター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。

Management Center と Threat Defense でサポートされる機能の詳細については、『Management Center Configuration Guide, Version 6.2.3』[英語] を参照してください。

ステップ 3 **移行前レポート**を開き、Threat Defense デバイスで手動で移行する必要がある ASA with FPS 構成項目をメモします。

ステップ 4 Management Center で、次の手順を実行します。

a) 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
- ルート
- インターフェイス
- IP SLA オブジェクト
- オブジェクトグループの検索
- 時間ベースのオブジェクト
- VPN オブジェクト
- サイト間 VPN トンネル
- 動的ルートオブジェクト

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、『Management Center Configuration Guide』[英語] 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 アクセスと HTTPS アクセスを含む）（「Platform Settings for Threat Defense」[英語] を参照）
- Syslog 設定（「Configure Syslog」[英語] を参照）
- 動的ルーティング（「Routing Overview for Threat Defense」[英語] を参照）
- サービスポリシー（「FlexConfig Policies」[英語] を参照）
- VPN 構成（「Threat Defense VPN」[英語] を参照）
- 接続ログ設定（「Connection Logging」[英語] を参照）

ステップ 5 確認が完了したら、Management Center から 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。

Firewall 移行ツールでポリシーが Threat Defense デバイスに割り当てられます。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 ASA with FPS 構成のホスト名が含まれています。

Firewall 移行ツールのアンインストール

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

手順

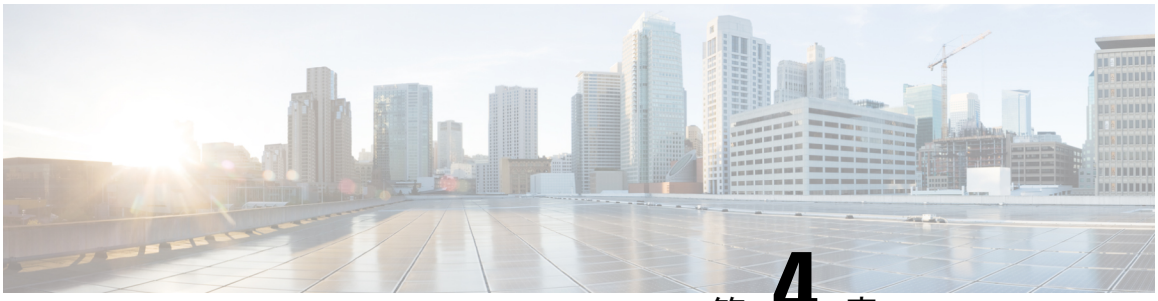
ステップ 1 Firewall 移行ツールを配置したフォルダに移動します。

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 Firewall 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。Firewall 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

Firewall 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、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 Management Center にプッシュしているときです。

Firewall 移行ツールのサポートバンドル

Firewall 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. [移行完了（Complete Migration）] 画面で、[サポート（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. [サポートバンドル（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. [ダウンロード（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. [TAC ページに移動（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

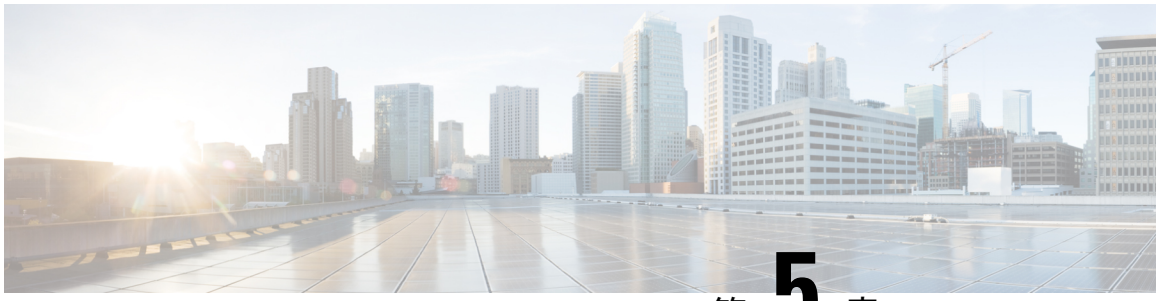
問題の特定とトラブルシューティングに役立つ情報は、次のファイルにあります。

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

ASA with FPS ファイルのアップロード失敗のトラブルシューティング

ASA with FPS 構成ファイルの抽出エラー

Firewall 移行ツールは、ASDM 管理対象の FPS ルールの 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、送信元の構成（ASA または ASA with FPS）の選択時には、移行前の構成情報を把握しておく必要があります。このような場合は、移行の開始時に送信元を **Cisco ASA** として使用する必要があります。



第 5 章

Firewall 移行ツールの FAQ

Firewall 移行ツールの FAQ

Firewall 移行ツールのよくある質問

Q. リリース 3.0 では、 Firewall 移行ツール でサポートされている新機能は何ですか。

A. リリース 3.0 では、次の機能がサポートされています。

- リモートアクセス VPN
- サイト間 VPN 事前共有キーの自動化

Q. リリース 2.5.1 では、 Firewall 移行ツール でサポートされている新機能は何ですか。

A. リリース 2.5.1 では、次の機能がサポートされています。

- 動的ルートオブジェクト
- Border Gateway Protocol; ボーダー ゲートウェイ プロトコル

Q. リリース 2.4 では、 Firewall 移行ツール でサポートされている新機能は何ですか。

A. リリース 2.4 では、次の機能がサポートされています。

- FTD への ASA with FPS の移行
- 証明書ベースの VPN の Firewall Management Center への移行

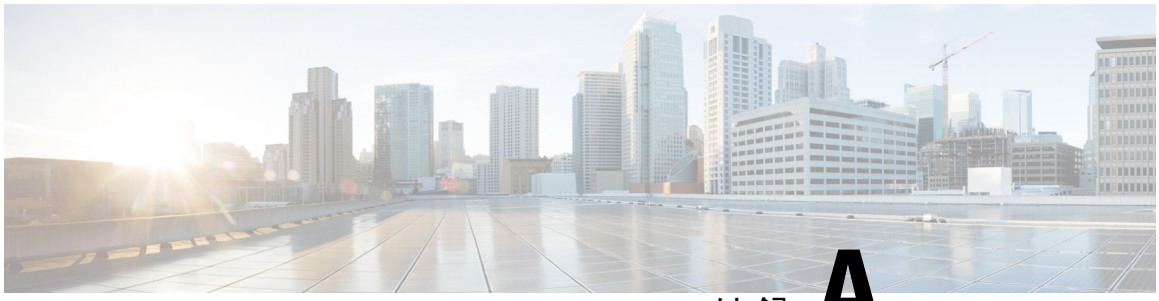
Q. Firewall Management Center に 8 つの FPS セキュリティゾーンがあり、FPS1 に 5 つのゾーン、FPS2 に 3 つのゾーンがあります。FPS1 に関連付けられている ACL ポリシーは、ア

クセスルールで FPS1 ゾーンと FPS2 ゾーンの組み合わせを使用しています。FPS1 ゾーンと FPS2 ゾーンの両方が FTD に移行されますか。

A. Firewall 移行ツール は FPS1 ゾーンを FTD ゾーンに移行します。FPS2 ゾーンは移行されません。ただし、FPS2 を使用する送信元 ACL は部分的に移行されます。

Q. FPS ユーザベース ACL はどのように移行されますか。

A. Firewall 移行ツール は、FPS ユーザーベースの ACL の Firewall Management Center への移行をサポートしていません。ユーザフィールドが削除され、無効な状態で ACL が移行されます。Firewall Management Center で移行後アクティビティの一環として、ユーザーフィールドを手動で追加し、ACL を有効にする必要があります。



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

Firewall 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 ASA with FPS 構成を 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 Firewall 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	Firewall 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	Firewall 移行ツールの起動に使用したブラウザ。Mozilla/5.0、Chrome/68.0.3440.106、Safari/537.36 を使用できます	Mozilla/5.0

表 *3*：送信元 *ASA with FPS* 情報

データ ポイント	説明	値の例
Source Type	送信元デバイスタイプ	ASA with FPS
Source Device Serial Number	ASA のシリアル番号	JAF1528ACAD

Cisco Success Network：テレメトリデータ

データ ポイント	説明	値の例
Source Device Model Number	ASA のモデル番号	ASA 5505-X
Source Device Version	ASA with FPS のバージョン	9.2(2)
Source Config Counts	送信元構成の行の合計数	504
Firewall Mode	ASA で構成されているファイアウォールモード：ルーテッドまたはトランスペアレント	ROUTED
Context Mode	ASA のコンテキストモード。これは、シングルコンテキストまたはマルチコンテキストになります。	シングル
ASA 構成の統計情報:		
ACL Counts	アクセスグループにアタッチされている ACL の数	46
Access Rules Counts	アクセスルールの合計数	46
NAT Rule Counts	NAT ルールの合計数	17
Network Object Counts	ASA で構成されたネットワークオブジェクトの数	34
Network Object Group Counts	ASA のネットワーク オブジェクト グループの数	6
Port Object Counts	ポートオブジェクトの数	85
Port Object Group Counts	ポートオブジェクトグループの数	37
Unsupported Access Rules Count	サポートされていないアクセスルールの合計数	3
Unsupported NAT Rule Count	サポートされていない NAT アクセスルールの合計数	0
FQDN Based Access Rule Counts	FQDN ベースのアクセスルールの数	7
Time range Based Access Rule Counts	時間範囲ベースのアクセスルールの数	1
SGT Based Access Rule Counts	SGT ベースのアクセスルールの数	0
ツールが解析できない構成行の概要		
Unparsed Config Count	パーサーによって認識されない構成行の数	68
Total Unparsed Access Rule Counts	解析されないアクセスルールの合計数	3

Cisco Success Network：テレメトリデータ

データ ポイント	説明	値の例
その他の ASA 構成詳細		
Is RA VPN Configured	RA VPN が ASA で構成されているかどうか	false
Is S2S VPN Configured	サイト間 VPN が ASA で構成されているかどうか	false
Is BGP Configured	BGP が ASA で構成されているかどうか	false
Is OSPF Configured	OSPF が ASA で構成されているかどうか	false
Local Users Counts	構成されているローカルユーザの数	0

表 *4*：ターゲット管理デバイス（*Management Center*）情報

データ ポイント	説明	値の例
Target Management Version	Management Center のターゲットバージョン	6.5 以降
Target Management Type	ターゲット管理デバイスのタイプ（Management Center）	Management Center
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	VMware 向け Cisco Secure Firewall Threat Defense
Migration Tool Version	移行ツールのバージョン	2.3.4

表 *5*：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		
Name	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（FPS）	移行された FPS ACL ルールの合計数	10
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		
Name	NAT ポリシーの名前	存在しない

Cisco Success Network：テレメトリデータ

データ ポイント	説明	値の例
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
Interface Group Counts	作成されたインターフェイスグループの数	0
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
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
Prefilter rule counts	ASA から送信されたプレフィルタルールの数	44

表 *6*：*Firewall* 移行ツール パフォーマンスデータ

データ ポイント	説明	値の例
Conversion Time	ASA with FPS 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	ASA with FPS 構成の Management Center への移行のステータス	SUCCESS
Error Message	Firewall 移行ツールによって表示されるエラーメッセージ	null
Error Description	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

テレメトリ ASA with FPS ファイルの例

次に、脅威に対する防御 に ASA with FPS 構成を移行する場合のテレメトリデータファイルの例を示します。


```
"Verbatim_Comments": "Very good!",
"asa_config_stats": {
"Ipv6_access_rule_counts": 0,
"Ipv6_bgp_count": 0,
"Ipv6_nat_rule_count": 0,
"Ipv6_network_counts": 10,
"Ipv6_static_route_counts": 3,
"access_rules_counts": 39,
"acl_category_count": 0,
"acl_counts": 60,
"cert_based_auth": false,
"dm_inline_applied": 0,
"dm_inline_present": 0,
"dynamic_crypto_map": false,
"fqdn_based_access_rule_counts": 0,
"ikev1_count": 0,
"ikev2_count": 0,
"is_aaa_configured": false,
"is_anyconnect_configured": false,
"is_bgp_configured": false,
"is_eigrp_configured": false,
"is_ipv6_configured": true,
"is_multicast_configured": false,
"is_ospf_configured": false,
"is_pbr_configured": false,
"is_ra_vpn_configured": false,
"is_s2s_vpn_configured": false,
"is_snmp_configured": false,
"is_ssl_server_version_configured": false,
"is_webvpn_configured": false,
"local_users_counts": 1,
"nat_rule_counts": 38,
"network_object_counts": 76,
"network_object_group_counts": 10,
"no_of_fqdn_based_objects": 6,
"ospfv3_count": 0,
"port_object_counts": 10,
"port_object_group_counts": 26,
"s2s_vpn_tunnel_counts": 0,
"s2s_vpn_vti": false,
"sgt_based_access_rules_count": 0,
"timerange_based_access_rule_counts": 0,
"total_unparsed_access_rule_counts": 3,
"tunneling_protocol_based_access_rule_counts": 0,
"unparsed_config_count": 115,
"unsupported_access_rules_count": 9,
"unsupported_nat_rule_count": 2,
"vpn_object_count": 0
},
"context_mode": "SINGLE",
"error_description": null,
"error_message": null,
"feedback_score": "5",
"firewall_mode": "ROUTED",
"log_info_acl_count": 0,
"migration_status": "SUCCESS",
"migration_summary": {
"access_control_policy": [
[{
```

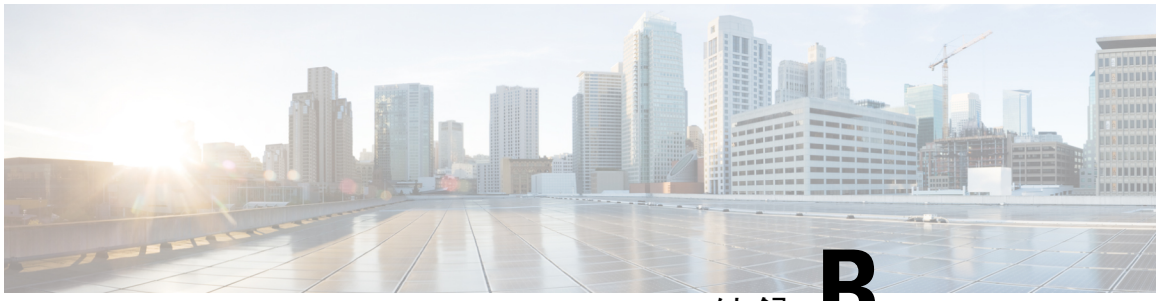
Cisco Success Network：テレメトリデータ


```
"access_rule_counts": 16,
"apply_file_policy_rule_counts": 1,
"apply_ips_policy_rule_counts": 2,
"apply_log_rule_counts": 0,
"do_not_migrate_rule_counts": 0,
"enable_hit_count": false,
"expanded_acp_rule_counts": 0,
"name": "Doesn't Exist",
"partially_migrated_acl_rule_counts": 9,
"time_based_acl_count": 0,
"total_acl_element_counts": 98,
"update_rule_action_counts": 0
}]
],
"interface_counts": 0,
"interface_group_counts": 0,
"interface_group_manually_created_counts": 0,
"ip_sla_monitor_count": 0,
"nat_Policy": [
[{
"NAT_rule_counts": 0,
"do_not_migrate_rule_counts": 0,
"name": "Doesn't Exist",
"partially_migrated_nat_rule_counts": 1
}]
],
"network_object_rename_counts": 0,
"network_object_reused_counts": 83,
"object_group_counts": 10,
"objects_counts": 90,
"port_object_rename_counts": 0,
"port_object_reused_counts": 0,
"prefilter_control_policy": [
[{
"do_not_migrate_rule_counts": 0,
"name": "Doesn't Exist",
"partially_migrated_acl_rule_counts": 0,
"prefilter_rule_counts": 44
}]
],
"security_zone_counts": 8,
"security_zone_manually_created_counts": 0,
"static_routes_counts": 0,
"sub_interface_counts": 0,
"time_out": false
},
"migration_tool_version": "2.4",
"mtu_info": {
"interface_name": null,
"mtu_value": null
},
"rule_change_acl_count": 0,
"selective_policy": {
"acl": false,
"acl_policy": false,
"application": false,
"csm": true,
"fps_acl": true,
"interface": false,
"interface_groups": true,
"migrate_tunneled_routes": false,
"nat": false,
"network_object": true,
"policy_assignment": true,
```

Cisco Success Network：テレメトリデータ


```
"policy_based_crypto_map": false,
"populate_sz": false,
"port_object": false,
"remote_deployment_enabled": false,
"route_based_vti": false,
"routes": false,
"s2s_vpn_flag": false,
"security_zones": true,
"unreferenced": false
},
"source_config_counts": 813,
"source_device_model_number": " ASAv, 8192 MB RAM, CPU Xeon E5 series 2600 MHz, 1 CPU
(4 cores)",
"source_device_serial_number": "9A2EPUNLD80",
"source_device_version": "9.6(3)1",
"source_type": "ASAFPS",
"system_information": {
"browser": "Chrome/91.0.4472.124",
"operating_system": "Windows NT 10.0; Win64; x64"
},
"target_device_model": "Not Exists",
"target_device_version": "Not Exists",
"target_management_type": "6.6.1 (build 91)",
"target_management_version": "6.6.1 (build 91)",
"template_version": "1.1",
"time": "2021-07-14 19:10:59",
"tool_analytics_data": {
"objectsplit_100_count": 0
},
"tool_performance": {
"config_push_time": 6,
"conversion_time": 34,
"migration_time": 334
}
```

Cisco Success Network：テレメトリデータ



付録 B

Threat Defense 2100 への の移行：例

から Firewall Threat Defense 2100 への移行：例

（注） 移行の完了後にターゲットデバイスで実行できるテスト計画を作成します。

メンテナンスウィンドウの前に次のタスクを実行する

始める前に

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

手順

ステップ 1 移行する ASA with FPS デバイスまたはコンテキストに対して **show running-config** コマンドを使用し、ASA with FPS 構成のコピーを保存します。「View the Running Configuration」[英語] を参照してください。

または、移行する ASA with FPS デバイスまたはコンテキストに対して Adaptive Security Device Manager（ASDM）を使用し、[ファイル（File）] > [新しいウィンドウに実行構成を表示する（Show Running Configuration in New Window）] を選択して、構成ファイルを取得します。

（注） マルチコンテキスト ASA with FPS の場合は、**show tech-support** コマンドを使用して、すべてのコンテキストの構成を単一ファイルに取得できます。

Threat Defense 2100 への の移行：例

ステップ 2 ASA with FPS 構成ファイルを確認します。

ステップ 3 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 Threat Defense for the 2100 Series Using Management Center Quick Start Guide』[英語] を参照してください。

ステップ 4 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 Management Center」[英語] を参照してください。

ステップ 5 （任意）送信元 ASA with FPS 構成にポートチャネルがある場合は、ターゲット Firepower 2100 シリーズ デバイスでポートチャネル（EtherChannel）を作成します。

詳細については、「Configure EtherChannels and Redundant Interfaces」[英語] を参照してください。

ステップ 6 Firewall 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 Firewall 移行ツールのダウンロード （27 ページ）」を参照してください。

ステップ 7 Firewall 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、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、「Firewall 移行ツールの接続先パラメータの指定 （35 ページ）」を参照してください。

ステップ 8 ASA with FPS インターフェイスを Threat Defense インターフェイスにマッピングします。

（注） Firewall 移行ツールでは、 ASA with FPS インターフェイスタイプを Threat Defense インターフェイスタイプにマッピングできます。

たとえば、ASA with FPS のポートチャネルを Threat Defense の物理インターフェイスにマッピングできます。

詳細については、「ASA with FPS 構成と Secure Firewall Device Manager 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 9 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、[自動作成（Auto-Create）] をクリックして、 Firewall 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 ASA with FPS 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 とインターフェイスグループへの ASA with FPS 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 10 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 Management Center にプッシュします。

ステップ 11 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 Threat Defense 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 （56ページ）」を参照してください。

ステップ 12 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 （73 ページ）を参照してください。

手順

ステップ 1 SSH コンソールを介して ASA with FPS に接続し、インターフェイス構成モードに切り替えます。

ステップ 2 **shutdown** コマンドを使用して、ASA with FPS インターフェイスをシャットダウンします。

ステップ 3 （任意）Management Center にアクセスし、Firepower 2100 シリーズ デバイスの動的ルーティングを構成します。

詳細については、「Dynamic Routing」[英語] を参照してください。

ステップ 4 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 5 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。

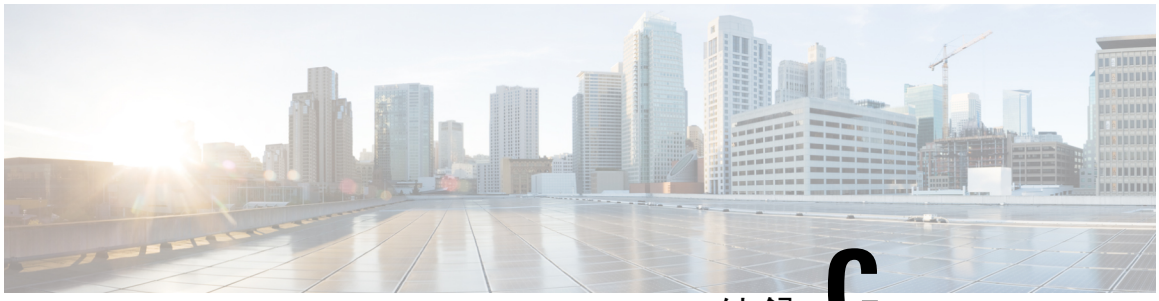
ステップ 6 Firepower 2100 シリーズ デバイスインターフェイスの IP アドレスに対するレイヤ 3 ルーティングが必要なデバイスから基本的な ping テストを実行します。

ステップ 7 Firepower 2100 シリーズ デバイスに新しい IP アドレスを割り当て、 ASA with FPS 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 8 包括的なテスト計画を実行し、 Firepower 2100 デバイスの管理 Management Center 内でログをモニタリングします。

メンテナンスウィンドウ中に次のタスクを実行する



付録 C

サイト間 VPN トンネル構成認証

サイト間 VPN トンネル構成認証

ASA with FirePOWER Services 構成ファイルからのクリアテキスト形式での事前共有キーの取得

ASA with FirePOWER Services では、設定した事前共有キーは暗号化されたハッシュとして保存されます。したがって、*show run* コマンドを使用したときに、実行構成で、事前共有キーがクリアテキストで表示されることはありません。

事前共有キーをクリアテキスト形式で取得するには、次の手順を実行します。

手順

ステップ 1 SSH コンソールから ASA with FirePOWER Services に接続し、*more system:running-config* コマンドを入力します。

このコマンドにより、事前共有キーがクリアテキスト形式で表示されます。

ステップ 2 **tunnel-group** セクションに移動して、すべてのトンネルピアとクリアテキスト形式の各事前共有キー値を確認します。

```
ciscoASA# more system:running-config
!
tunnel-group 1.1.1.1 type ipsec-l2l
tunnel-group 1.1.1.1 ipsec-attributes
pre-shared-key <PSK-in-plaintext> <-----The pre-shared-key is now displayed in clear
text format.
```

ASA with FirePOWER Services 構成ファイルまたは Live Connect ASA からの事前共有キーの自動取得

Firepower 移行ツール 3.0 は、送信元が Live Connect ASA である場合、または **More System: Running Configuration** のファイルがアップロードされている場合は、サイト間 VPN に使用されている事前共有キーの取得を自動化します。

IKEv2 ベースの VPN では、ローカル認証キーとリモート認証キーが同じでない場合はリモート認証キーが取得されます。

ASAwithFirePOWERServicesからのPKI証明書のエクスポートとFirewall Management Center へのインポート

Firewall 移行ツール 2.4 では、証明書ベースの VPN の Firewall Management Center への移行がサポートされるようになりました。

ASA with FirePOWER Services では、トラストポイントモデルを使用して、証明書を構成に保存します。トラストポイントは、証明書が保存されるコンテナです。ASA with FirePOWER Services トラストポイントは最大 2 つの証明書を保存できます。

ASA with FirePOWER Services 構成ファイルの ASA with FirePOWER Services トラストポイントまたは証明書にはハッシュ値が含まれています。したがって、Firewall Management Center に直接インポートすることはできません。

インポート先の Firewall Management Center で、移行前アクティビティの一環として、ASA with FirePOWER Services トラストポイントまたは VPN 証明書を PKI オブジェクトとして手動で移行します。このアクティビティは、Firewall 移行ツールを使用した移行を開始する前に実行する必要があります。

手順

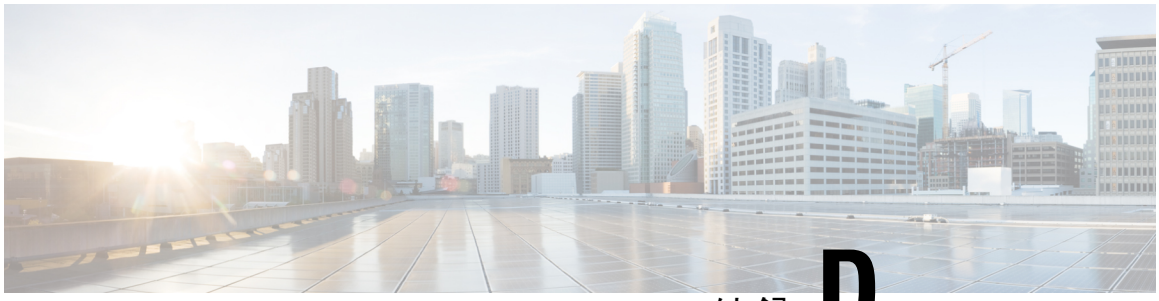
ステップ 1 次のコマンドを使用し、CLI を介してインポート元の ASA with FirePOWER Services から PKI 証明書をキーとともに PKCS12 ファイルにエクスポートします。

```
ASA(config)#crypto ca export <trust-point-name> pkcs12 <passphrase>
```

ステップ 2 PKI 証明書を Firewall Management Center にインポートします（**[オブジェクト管理（Object Management）] > [PKI オブジェクト（PKI Objects）]**）。

詳細については、『Firewall Management Center Configuration Guide』[英語] を参照してください。

手動で作成した PKI オブジェクトは、 Firewall 移行ツール の [VPNトンネル（VPN Tunnels）] セクションの [確認と検証（Review and Validate）] ページで使用できます。



付録 D

リモートアクセス VPN の移行

AAA サーバーキーの取得の自動化

Firewall 移行ツール 3.0 は、ローカルユーザー、Radius、および Live Connect ASA の LDAP/LDAPS/AD サーバーに使用されるキーの取得を自動化するか、または **more system: running-config** コマンドをアップロードする場合。また、すべてのキーを手動で取得し、**[確認と検証（Review and Validate）] > [リモートアクセス （Remote Access VPN）]** の下の [AAA] セクションに入力することもできます。

ASA with FirePOWER Services 構成からのクリアテキスト形式での AAA サーバーキーの取得

始める前に

ASA with FirePOWER Services では、構成したキーは暗号化されたハッシュとして保存されます。ただし、*showrun* コマンドを使用すると、実行構成でキーがクリアテキストで表示されることはありません。キーは、ローカルユーザー、Radius と LDAP、LDAPS、または AD サーバーに使用されます。クリアテキスト形式でキーを取得するには、次の手順を実行します。

手順

ステップ 1 SSH コンソールを介して ASA に接続します。

ステップ 2 *more system:running-config* コマンドを入力します。

ステップ 3 **aaa-server and local user** セクションに移動してクリアテキスト形式のすべての AAA 構成と対応するキー値を見つけます。

```
ciscoASA#more system:running-config

!

aaa-server Test-RADIUS (inside) host 2.2.2.2

 key <key in clear text>     <-----The radius key is now displayed in clear text format.

aaa-server Test-LDAP (inside) host 3.3.3.3

ldap-login-password <クリアテキストのパスワード> <-----LDAP/AD/LDAPS パスワードがクリアテキスト形式で表示されるようになりました。

username Test_User password <Password in clear text> <-----The Local user
        password is shown in clear text.
```

（注） ローカルユーザーのパスワードが暗号化されている場合は、パスワードを内部で確認するか、または Firewall 移行ツールで新しいパスワードを構成できます。

ASA with FirePOWER Services からの PKI 証明書のエクスポートと管理センターへのインポート

始める前に

リモートアクセス VPN には、次の証明書が必要です。

- グローバル SSL プロトコル
- IKEv2 プロトコル
- インターフェイス証明書
- SAML

ASAASA with FirePOWER Services では、トラストポイントモデルを使用して、証明書を構成に保存します。トラストポイントは、証明書が保存されるコンテナです。ASAASA with FirePOWER Services トラストポイントは最大 2 つの証明書を保存できます。

ASAASA with FirePOWER Services 構成ファイルの ASAASA with FirePOWER Services トラストポイントまたは証明書にはハッシュ値が含まれています。したがって、それらを管理センターに直接インポートすることはできません。

インポート先の管理センターで、移行前アクティビティの一環として、ASAASA with FirePOWER Services トラストポイントまたは VPN 証明書を PKI オブジェクトとして手動で移行します。

手順

ステップ 1 次のコマンドを使用し、CLI を介してインポート元の ASAASA with FirePOWER Services 構成から PKI 証明書をキーとともに PKCS12 ファイルにエクスポートします。

```
ASA(config)#crypto ca export <trust-point-name> pkcs12 <passphrase>
```

ステップ 2 PKI 証明書を管理センターにインポートします（[オブジェクト管理（Object Management）] [PKI オブジェクト（PKI Objects）]。

詳細については、『Firewall Management Center Configuration Guide』[英語] を参照してください。

手動で作成した PKI オブジェクトは、[リモートアクセス VPN（Remote Access VPN）] の [トラストポイント（Trustpoint ）] セクションにある [確認と検証（Review and Validate ）] ページの Firewall 移行ツールで使用できるようになりました。

AnyConnect パッケージとプロファイルの取得

AnyConnectプロファイルはオプションであり、管理センターまたはFirewall移行ツールを介してアップロードできます。

始める前に

- 管理センターのリモートアクセス VPN には、1 つ以上の AnyConnect パッケージが必要です。
- 構成が Hostscan と外部ブラウザパッケージで構成されている場合は、これらのパッケージをアップロードする必要があります。
- 移行前のアクティビティの一環として、すべてのパッケージを管理センターに追加する必要があります。
- Dap.xml と Data.xml は、Firewall 移行ツールを介して追加する必要があります。

手順

ステップ 1 次のコマンドを使用して、必要なパッケージを送信元 ASA から FTP または TFTP サーバーにコピーします。

```
Copy <source file location:/source file name> <destination>
ASA# copy disk0:/anyconnect-win-4.10.02086-webdeploy-k9.pkg tftp://1.1.1.1 <----- Example
 of copying Anyconnect Package.
ASA# copy disk0:/ external-sso- 4.10.04071-webdeploy-k9.zip tftp://1.1.1.1 <----- Example
```

```
 of copying External Browser Package.
ASA# copy disk0:/ hostscan_4.10.04071-k9.pkg tftp://1.1.1.1 <----- Example of copying
Hostscan Package.
ASA# copy disk0:/ dap.xml tftp://1.1.1.1. <----- Example of copying Dap.xml
ASA# copy disk0:/ sdesktop/data.xml tftp://1.1.1.1 <----- Example of copying Data.xml
ASA# copy disk0:/ VPN_Profile.xml tftp://1.1.1.1 <----- Example of copying Anyconnect
Profile.
```

ステップ 2 ダウンロードしたパッケージを管理センターにインポートします（**[オブジェクト管理（Object Management）] > [VPN] > [AnyConnect ファイル（AnyConnect File）]**）。

1. Dap.xml と Data.xml は、**[確認と検証（Review and Validate）] > [リモートアクセス VPN（Remote Access VPN）] > [AnyConnect ファイル（AnyConnect File）]** セクションの Firewall 移行ツールから管理センターにアップロードする必要があります。
2. 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 **[確認と検証（Review and Validate）] > [リモートアクセス VPN（Remote Access VPN）] > [AnyConnect ファイル（AnyConnect File）]** セクションの Firewall 移行ツールを介してアップロードできます。

手動でアップロードされたファイルが Firewall 移行ツールで使用できるようになりました。

ドメインと AD プライマリドメインの取得

暗号化が LDAPS に設定されている AAA サーバーの場合、ASA は IP とホスト名またはドメインをサポートしますが、管理センターはホスト名またはドメインのみをサポートします。ASA 構成にホスト名またはドメインが含まれている場合、それらが取得されて表示されます。ASA 構成に LDAPS の IP アドレスが含まれている場合は、[リモートアクセス VPN（Remote Access VPN）] の下の [AAA] セクションにドメインを入力します。AAA サーバーの IP アドレスに解決できるドメインを入力する必要があります。

タイプが AD の AAA サーバー（サーバータイプは ASA 構成で Microsoft）の場合、[AD プライマリドメイン（AD Primary Domain）] は管理センターで構成する必須フィールドです。このフィールドは ASA では個別に構成されず、ASA の LDAP-base-dn 構成から抽出されます。

```
If the ldap-base-dn is: ou=Test-Ou,dc=gcevpn,dc=com
```

[AD プライマリドメイン（AD Primary Domain）] は、プライマリドメインを形成する dc、dc=gcevpn、dc=com で始まるフィールドです。AD プライマリドメインは gcevpn.com になります。

LDAP-base-dn のサンプルファイル：

```
cn=asa,OU=ServiceAccounts,OU=abc,dc=abc,dc=com:
```

ここで、dc=abc と dc=com が abc.com として結合され、AD プライマリドメインが形成されます。

```
cn=admin, cn=users, dc=fwsecurity, dc=cisco, dc=com:
```

AD プライマリドメインは fwsecurity.cisco.com です。

AD プライマリドメインは自動的に取得され、Firewall 移行ツールに表示されます。

（注） AD プライマリドメインの値は、レルムオブジェクトごとに一意である必要があります。競合が検出された場合か、または Firewall 移行ツールが ASA 構成で値を見つけられない場合は、特定のサーバーの AD プライマリドメインを入力するように求められます。AD プライマリドメインを入力して構成を検証します。

リモートアクセス VPN の移行