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」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：テレメトリデータを参照してください。