Firewall 移行ツールについて

- Firewall 移行ツールについて （1 ページ）
- Firewall 移行ツールの履歴 （4 ページ）
- Firewall 移行ツールのライセンス （12 ページ）
- Cisco Success Network （12 ページ）
- 関連資料 （12 ページ）

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 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。

本書では、Firewall 移行ツールのダウンロードから移行の完了まで、 Firewall 移行ツールについて説明します。また、移行の問題を解決するためのトラブルシューティングのヒントも示します。エンドツーエンドの移行プロセスの理解を深めるために、本書では、ターゲットデバイスの例として Firewall 2100 シリーズを使用した移行手順の例を示します。付録 B「移行ワークフロー：例」を参照してください。

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 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 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 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 Cisco 適応型セキュリティアプライアンス（ASA）構成項目。
- エラーのある ASA 構成行には、Firewall 移行ツールが認識できない ASA 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 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

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 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 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 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 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
2.5.2	Firewall 移行ツール 2.5.2 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。 • 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。 （注） ASA では ACP ルールアクション対してのみ最適化を使用できます。 Firewall 移行ツール 2.5.2 は、移行先の Management Center が 7.1 以降の場合、Border Gateway Protocol （BGP）および動的ルートオブジェクトの移行をサポートします。
2.5.1	Firewall 移行ツール 2.5.1 は、移行先の Management Center が 7.1 以降の場合、Border Gateway Protocol （BGP）および動的ルートオブジェクトの移行をサポートします。
2.5	Firewall 移行ツール 2.5 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するようになりました。 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。 • 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。 （注） ソース ASA では ACP ルールアクション対してのみ最適化を使用できます。 移行先の Management Center が 7.1 以降の場合、連続していないネットワークマスク（ワイルドカードマスク）オブジェクトのサポート。

バージョン	サポートされる機能
2.4	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。 • 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。
2.3.5	Firewall 移行ツールは、ターゲットの Management Center および 脅威に対する防御 が 6.7 以降の場合、次の仮想トンネルインターフェイス（VTI）構成の 脅威に対する防御 への移行をサポートします。 • VTI インターフェイスおよび関連する静的ルート • Management Center と 脅威に対する防御 へのルートベース（VTI）事前共有キー認証タイプの VPN 構成の移行。 • ルーテッド セキュリティ ゾーンの作成、VTI インターフェイスの追加、VTI トンネルを介して復号化されたトラフィック制御のアクセス制御ルールの定義。

バージョン	サポートされる機能
2.3.4	Firewall 移行ツールを使用すると、次の ASA VPN の構成要素を 脅威に対する防御 に移行できます。 • ポリシーベース（暗号マップ）の事前共有キー認証タイプの VPN 構成の Management Center への移行をサポートします。 • VPN オブジェクト：VPN オブジェクト（IKEv1/IKEv2 ポリシー、IKEv1/IKEv2 IPsec プロポーザル）を作成し、VPN オブジェクトを特定のサイト間 VPN トポロジにマッピングし、オブジェクトを Management Center に移行します。 [構成の確認と検証（Review and Validate Configuration）] ページのルールに対して VPN オブジェクトを確認します。 • サイト間 VPN トポロジ：送信元 ASA 設定の暗号マップ関連の設定は、それぞれの VPN オブジェクトとともに移行されます。ポリシーベース（暗号マップ）VPN トポロジは、Management Center バージョン 6.6 以降でサポートされます。 （注） このリリースの Firewall 移行ツールでは、スタティック暗号マップの移行のみサポートされます。 サポートされるすべての ASA 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。

バージョン	サポートされる機能
1.3	

バージョン	サポートされる機能
	• Firewall移行ツールでは、管理者ログイン情報とASAで構成されている**イネーブルパスワード**を使用して ASA に接続することができます。 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。 • app_configファイル内の一括プッシュのバッチ サイズ制限を次のように設定できるようになりました。 • オブジェクトの場合、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 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。 • Firewall 移行ツールを使用すると、CSM または ASDM の管理型設定を解析できます。 インライングループ化または ASDM 管理型設定をクリアすることを選択すると、事前に定義されたオブジェクトが実際のオブジェクトまたはメンバー名に置き換えられます。 CSM または ASDM 管理型設定をクリアしない場合、事前に定義されたオブジェクト名は移行のために保持されます。 • 移行の失敗時にログファイル、DB、および構成ファイルをダウンロードするためのカスタマーサポートを提供します。また、テクニカル チームに電子メールでサポート ケースを上げることもできます。 • オブジェクト、インターフェイス、ACL、NAT、およびルートでの IPv6 構成の移行をサポートします。 • Firewall移行ツールでは、物理インターフェイス、ポートチャネル、およびサブインターフェイスの 脅威に対する防御 オブジェクトタイプの物理インターフェイスに ASA インターフェイス名をマッピングすることができます。たとえば、ASA のポートチャネルを Management Center の物理インターフェイスにマッピングできます。 • Firewall移行ツールは、選択したNATルールとルートインターフェイスの移行をスキップするサポートを提供します。Firewall移行ツールの以前のバージョンでは、このオプションはアクセスコントロールルールのみに提供されていました。 • [構成の最適化、確認および検証（Optimize, Review and Validate

バージョン	サポートされる機能
	Configuration）] 画面から、解析されたアクセス制御、NAT、ネットワークオブジェクト、ポートオブジェクト、インターフェイス、およびルートの設定項目を Excel または CSV 形式でダウンロードできます。 （注） CSV ファイルをインポートすることはできません。
1.2	• Management Center 6.3 への移行をサポート • IPv4 FQDN オブジェクトとグループの移行をサポート • マルチコンテキスト ASA の手動アップロード方式で **show tech-support** コマンドをサポート • Management Center に登録されているコンテナタイプ 脅威に対する防御（MI）への移行をサポートします。 • アクセス コントロール テーブルの移行されたアクセスコントロールルールに対するルール アクション マッピング サポート（[許可（Allow）]、[信頼（Trust）]、[モニタ（Monitor）]、[ブロック（Block）]、または [リセット付きブロック（Block with Reset）]）。 • Firewall 移行ツールのバージョンチェック。Firewall 移行ツールの最新バージョンを使用していることを確認します。

バージョン	サポートされる機能
1.1	• オブジェクト、NAT、静的ルートの一括プッシュにより、Management Center に構成をプッシュするのにかかる時間が大幅に短縮されます。 • 実稼働 ASA からの構成の抽出 • 選択的機能移行（共有ポリシーおよびデバイス固有のポリシー） • ルールの最適化 • 移行する ASA アクセスコントロールルールを、Management Center で構成されている侵入防御システムとファイルポリシーのリストにマッピングします。 • 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。これにより、移行時間が最適化され、構成中に未使用のオブジェクトが消去されます。 • マルチコンテキストモードで実行されている ASA のデータコンテキストの 1 つから、**running-config** または **sh run** の移行サポート。 • macOS バージョン 10.13 以降でのサポート • 移行されたアクセスコントロールルールのロギングアクション（有効化、無効化、開始時または終了時のロギング）の変更をサポートします。 • Management Center のドメイン内で構成された 脅威に対する防御 デバイスへの移行 • オブジェクト名の一括編集機能。 • Cisco Success Network によるテレメトリサポート
1.0	• 解析およびプッシュ操作を含む、移行全体の検証 • オブジェクト再利用機能 • オブジェクト競合の解決 • インターフェイス マッピング • インターフェイス オブジェクトの自動作成または再利用（セキュリティゾーンとインターフェイス グループ マッピングに対する場合の ASA 名） • ACL の一括移行のサポート

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。

関連資料

このセクションでは、 Firewall 移行ツールに関連するドキュメントの概要を示します。

- 『Migrating Certificates from ASA to Firepower Threat Defense』：Cisco ASA から Secure Firewall Threat Defense デバイスにアイデンティティ（ID）および認証局（CA）証明書を移行する手順について説明します。
- 『Migrating ASA to Firepower Threat Defense Site-to-Site VPN Using IKEv1 with Certificates』：既存の Cisco ASA から Management Center 管理下の Threat Defense に、証明書（rsa-sig）を

認証方式として使用して、サイト間 IKEv1 VPN トンネルを移行する手順について説明します。

- 『Migrating ASA to Firepower Threat Defense Site-to-Site VPN Using IKEv2 with Certificates』：既存の ASA から Management Center 管理下の Threat Defense に、証明書（rsa-sig）を認証方式として使用して、サイト間 IKEv2 VPN トンネルを移行する手順について説明します。
- 『Migrating ASA to Firepower Threat Defense Dynamic Crypto Map Based Site-to-Site Tunnel on FTD』：既存の ASA から Management Center 管理下の Threat Defense に、事前共有キーと証明書を認証方式として使用して、動的暗号マップベースのサイト間 VPN トンネル（IKEv1 または IKEv2 を使用）を移行する手順について説明します。
- 『Migrating ASA to Firepower Threat Defense Site-to-Site VPN Using IKEv1 with Pre-Shared Key Authentication』：既存の ASA から Management Center 管理下の Threat Defense に、事前共有キー（PSK）を認証方式として使用して、サイト間 IKEv1 VPN トンネルを移行する手順について説明します。
- 『Migrating ASA to Firepower Threat Defense Site-to-Site VPN Using IKEv2 with Pre-Shared Key Authentication』：既存の ASA から Management Center 管理下の Threat Defense に、事前共有キー（PSK）を認証方式として使用して、サイト間 IKEv2 VPN トンネルを移行する手順について説明します。
- 『Migrating ASA to Firepower Threat Defense Platform Settings』：ASA のプラットフォーム設定の構成を Threat Defense デバイスに移行する手順について説明します。
- 『Cisco ASA FirePOWER Module Quick Start Guide』：ASA FirePOWER モジュールと ASA がどのように連携するかについて説明します。