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

Cisco Secure Firewall 移行ツールについて

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

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

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

一般的に使用される ASA 機能とそれに相当する Threat Defense 機能の詳細については、『Cisco Secure Firewall ASA to Threat Defense Feature Mapping』ガイドを参照してください。

Cisco Secure Firewall 移行ツールは ASA の情報を収集して解析し、最終的に Secure Firewall Management Center にプッシュします。解析フェーズ中に、Cisco Secure Firewall 移行ツールは、以下を特定する**移行前レポート**を生成します。

- 完全に移行された、部分的に移行された、移行がサポートされていない、および移行が無視された 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、Cisco Secure 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。

コンソール

Cisco Secure Firewall 移行ツールを起動すると、コンソールが開きます。コンソールには、Cisco Secure Firewall 移行ツールの各ステップの進行状況に関する詳細情報が表示されます。コンソールの内容は、Cisco Secure Firewall 移行ツールのログファイルにも書き込まれます。

Cisco Secure Firewall 移行ツールが開いていて実行中の間は、コンソールを開いたままにする必要があります。

重要 Cisco Secure Firewall 移行ツールを終了するために Web インターフェイスが実行されているブラウザを閉じると、コンソールはバックグラウンドで実行され続けます。Cisco Secure Firewall 移行ツールを完全に終了するには、キーボードの Command キー + C を押してコンソールを終了します。

ログ

Cisco Secure Firewall 移行ツールは、各移行のログを作成します。ログには、移行の各ステップで発生した内容の詳細が含まれるため、移行が失敗した場合の原因の特定に役立ちます。

Cisco Secure Firewall 移行ツールのログファイルは、*<migration_tool_folder>*\logs にあります。

リソース

Cisco Secure Firewall 移行ツールは、**移行前レポート**、**移行後レポート**、ASA 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、次の場所にあります。

<migration_tool_folder>\resources

Cisco Secure Firewall 移行ツールでの検索

[最適化、確認および検証（Optimize, Review and Validate）] ページの項目など、Cisco Secure Firewall 移行ツールに表示されるテーブル内の項目を検索できます。

テーブルの任意の列または行の項目を検索するには、テーブルの上の **検索**（🔍） をクリックし、フィールドに検索語を入力します。Cisco Secure Firewall 移行ツールはテーブル行をフィルタ処理し、その検索語を含む行のみを表示します。

単一の列で項目を検索するには、列見出しにある [検索（Search）] フィールドに検索語を入力します。Cisco Secure Firewall 移行ツールはテーブル行をフィルタ処理し、検索語に一致する行のみを表示します。

ポート

Cisco Secure Firewall 移行ツールは、ポート 8321 ー 8331 およびポート 8888 の 12 ポートのうちいずれかのポートで実行されるテレメトリをサポートします。デフォルトでは、Cisco Secure Firewall 移行ツールはポート 8888 を使用します。ポートを変更するには、*app_config* ファイルのポート情報を更新します。更新後、ポートの変更を有効にするために、Cisco Secure Firewall 移行ツールを再起動します。app_config ファイルは、<migration_tool_folder>\app_config.txt にあります。

（注） テレメトリはこれらのポートでのみサポートされているため、ポート 8321 ～ 8331 およびポート 8888 を使用することを推奨します。Cisco Success Network を有効にすると、Cisco Secure Firewall 移行ツールに他のポートを使用できなくなります。

Cisco Success Network

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

- ネットワーク内の製品の有効性を向上させるために、利用可能な未使用の機能について通知します。
- 製品に利用可能な、追加のテクニカルサポートサービスとモニタリングについて通知します。
- シスコ製品の改善に役立ちます。

Cisco Secure Firewall 移行ツールはセキュアな接続を確立および維持し、Cisco Success Network に登録できるようにします。Cisco Success Network を無効にすることで、いつでもこの接続をオフにできます。これにより、デバイスが Cisco Success Network クラウドから接続解除されます。

Cisco Secure Firewall 移行ツールの最新情報

バージョン	サポートされる機能
6.0	

バージョン	サポートされる機能
	このリリースには、次の新機能と機能拡張が含まれています **Cisco Secure Firewall Threat Defense への Cisco Secure Firewall ASA の移行** • Secure Firewall ASA の WebVPN 設定を、Threat Defense デバイスの Zero Trust Access Policy 設定に移行できるようになりました。[機能の選択（Select Features）] ページで [WebVPN] チェックボックスがオンになっていることを確認し、[設定の最適化、確認、検証（Optimize, Review and Validate Configuration）] ページで新しい [WebVPN] タブを確認します。Threat Defense デバイスとターゲット管理センターは、バージョン 7.4 以降で実行され、検出エンジンとして Snort3 を実行している必要があります。 • Simple Network Management Protocol（SNMP）および Dynamic Host Configuration Protocol（DHCP）の設定を Threat Defense デバイスに移行できるようになりました。[機能の選択（Select Features）] ページで、[SNMP] および [DHCP] チェックボックスがオンになっていることを確認します。Secure Firewall ASA で DHCP を設定している場合は、DHCP サーバーまたはリレーエージェントと DDNS の設定も移行対象として選択できることに注意してください。 • マルチコンテキスト ASA デバイスを実行するときに、等コストマルチパス（ECMP）ルーティング設定を単一インスタンスの脅威防御のマージされたコンテキスト移行に移行できるようになりました。解析されたサマリーの [ルート（Routes）] タイルに ECMP ゾーンも含まれるようになりました。[設定の最適化、レビュー、検証（Optimize, Review and Validate Configuration）] ページの [ルート（Routes）] タブで同じことを検証できます。 • ダイナミック仮想トンネルインターフェイス（DVTI）設定のダイナミックトンネルを Secure Firewall ASA から Threat Defense デバイスに移行できるようになりました。これらは、[セキュリティゾーン、インターフェイスグループ、およびVRFへのASAインターフェイスのマッピング（Map ASA Interfaces to Security Zones, Interface Groups, and VRFs）] ページでマッピングできます。この機能を適用するには、ASA のバージョンが 9.19(x) 以降であることを確認します。 **Cisco Secure Firewall Threat Defense への FDM 管理対象デバイスの移行** • SNMP や HTTP を含むレイヤ 7 セキュリティポリシー、マルウェアおよびファイルポリシー設定を FDM 管理対象デバイスから Threat Defense デバイスに移行できるようになりました。ターゲット管理センターのバージョンが 7.4 以降であること、および [機能の選択（Select Features）] ページの [プラットフォーム設定（Platform

バージョン	サポートされる機能
	Settings）]および[ファイルとマルウェアポリシー（File and Malware Policy）]チェックボックスがオンになっていることを確認します。 **Cisco Secure Firewall Threat Defense への Check Point ファイアウォールの移行** • Check Point ファイアウォールのサイト間 VPN（ポリシーベース）設定を Threat Defense デバイスに移行できるようになりました。この機能は、Check Point R80 以降のバージョン、および Management Center および Threat Defense バージョン 6.7 以降に適用されることに注意してください。[機能の選択（Select Features）]ページで、[サイト間VPNトンネル（Site-to-Site VPN Tunnels）]チェックボックスがオンになっていることを確認します。これはデバイス固有の設定であるため、[FTDなしで続行（Proceed without FTD）]を選択した場合、移行ツールにこれらの設定は表示されないことに注意してください。 **Cisco Secure Firewall Threat Defense への Fortinet ファイアウォールの移行** • Fortinet ファイアウォールから Threat Defense デバイスに設定を移行するときに、アプリケーション アクセス コントロール リスト（ACL）を最適化できるようになりました。[設定の最適化、レビュー、検証（Optimize、Review and Validate Configuration）]ページの[ACLの最適化（Optimize ACL）]ボタンを使用して、冗長 ACL とシャドウ ACL のリストを表示し、最適化レポートをダウンロードして詳細な ACL 情報を表示します。

バージョン	サポートされる機能
5.0.1	このリリースには、次の新機能と機能拡張が含まれています。 • Cisco Secure Firewall 移行ツールは、Cisco Secure Firewall ASA デバイスから Threat Defense デバイスへの複数のトランスペアレント ファイアウォール モードのセキュリティコンテキストの移行をサポートするようになりました。Cisco Secure Firewall ASA デバイス内の 2 つ以上のトランスペアレント ファイアウォール モードのコンテキストをトランスペアレントモードのインスタンスにマージし、それらを移行できます。 1 つ以上のコンテキストに VPN 設定がある場合の VPN 設定の ASA 展開では、VPN 設定をターゲットの Threat Defense デバイスに移行するコンテキストを 1 つのみ選択できます。選択しなかったコンテキストからは、VPN 設定以外のすべての設定が移行されます。 詳細については、「ASA セキュリティコンテキストの選択 」を参照してください。 • Cisco Secure Firewall 移行ツールを使用して、サイト間およびリモートアクセス VPN 設定を Fortinet および Palo Alto Networks ファイアウォールから Threat Defense に移行できるようになりました。[機能の選択（Select Features）]ペインから、移行する VPN 機能を選択します。『Migrating Palo Alto Networks Firewall to Secure Firewall Threat Defense with the Migration Tool』および『Migrating Fortinet Firewall to Secure Firewall Threat Defense with the Migration Tool』の「Specify Destination Parameters for the Secure Firewall Migration Tool」セクションを参照してください。 • Cisco Secure Firewall ASA デバイスから 1 つ以上のルーテッドまたはトランスペアレント ファイアウォール モードのセキュリティコンテキストを選択し、Cisco Secure Firewall 移行ツールを使用してシングルコンテキストまたはマルチコンテキストを移行できるようになりました。

バージョン	サポートされる機能
5.0	• Cisco Secure Firewall 移行ツールは、Cisco Secure Firewall ASA から Threat Defense デバイスへの複数のセキュリティコンテキストの移行をサポートするようになりました。いずれかのコンテキストから設定を移行するか、すべてのルーテッド ファイアウォール モードのコンテキストから設定をマージして移行するかを選択できます。複数のトランスペアレント ファイアウォール モード コンテキストからの設定のマージのサポートは、まもなく利用可能になります。詳細については、「ASA プライマリ セキュリティ コンテキストの選択」を参照してください。 • 移行ツールは、仮想ルーティングおよび転送（VRF）機能を活用して、マルチコンテキストの ASA 環境で観察される分離されたトラフィックフローを複製します。これは、新たにマージされた設定の一部になります。移行ツールが検出したコンテキストの数は、新しい **[コンテキスト（Contexts）]** タイルで確認でき、解析後は **[解析の概要（Parsed Summary）]** ページの新しい **[VRF]** タイルで確認できます。また移行ツールは、**[セキュリティゾーンとインターフェイスグループへのインターフェイスのマッピング（Map Interfaces to Security Zones and Interface Groups）]** ページに、これらの VRF がマッピングされているインターフェイスを表示します。 • Cisco Secure Firewall 移行ツールの新しいデモモードを使用して移行ワークフロー全体を試し、実際の移行がどのようになるかを可視化できるようになりました。詳細については、「ファイアウォール移行ツールでのデモモードの使用」を参照してください。 • 新しい機能拡張とバグの修正により、Cisco Secure Firewall 移行ツールは、Palo Alto Networks ファイアウォールの Threat Defense への移行に関して、改善された迅速な移行エクスペリエンスをご提供します。
4.0.3	Cisco Secure Firewall 移行ツール 4.0.3 には、バグの修正と、次の新たな拡張機能が含まれています。 • 移行ツールで、PAN 設定を Threat Defense に移行するための強化された **[アプリケーションマッピング（Application Mapping）]** 画面が提供されるようになりました。詳細については、『移行ツールを使用した *Palo Alto Networks* ファイアウォールから *Cisco Secure Firewall Threat Defense* への移行』ガイドの「構成とアプリケーションのマッピング」を参照してください。

バージョン	サポートされる機能
4.0.2	Cisco Secure Firewall 移行ツール 4.0.2 には、次の新機能と拡張機能が含まれています。 • Secure Firewall 移行ツールは、接続先管理センターと Threat Defense のバージョンが 7.1 以降の場合に、サイト間 VPN フィルタ設定とそれらの設定に関連する拡張アクセスリストオブジェクトの移行をサポートするようになっています。これまでは、サイト間VPNフィルタ設定は移行されず、移行後に手動で設定する必要がありました。 • 移行ツールに常時接続のテレメトリが追加されました。ただし、限定的なテレメトリデータまたは広範なテレメトリデータの送信を選択できるようになっています。限定的なテレメトリデータにデータポイントはほとんど含まれませんが、広範なテレメトリデータは、より詳細なテレメトリデータのリストを送信します。この設定は、**[設定（Settings）]** > **[テレメトリデータをシスコに送信しますか（Send Telemetry Data to Cisco?）]** から変更できます。.
4.0.1	Cisco Secure Firewall 移行ツール 4.0.1 には、次の新機能と拡張機能が含まれています。 Cisco Secure Firewall 移行ツールは、名前と構成の両方に基づいてすべてのオブジェクトとオブジェクトグループを分析し、同じ名前と構成を持つオブジェクトを再利用するようになりました。以前は、ネットワークオブジェクトとネットワーク オブジェクト グループのみが、名前と構成に基づいて分析されていました。リモートアクセス VPN の XML プロファイルは名前のみを使用して検証されることに注意してください。

バージョン	サポートされる機能
4.0	Cisco Secure Firewall 移行ツール 4.0 は、以下をサポートします。 • ASA からのポリシーベースルーティング（PBR）の移行（移行先の管理センターと Threat Defense のバージョンが 7.3 以降の場合）。 （注） PBR の移行の場合、移行を続行する前に、既存のフレックス構成を管理センターから削除する必要があります。 • ASA からのリモートアクセス VPN のカスタム属性および VPN ロードバランシングの移行（移行先管理センターが 7.3 以降の場合）。 リモートアクセス VPN の移行は、ファイアウォールの有無にかかわらず実行できます。ただし、ファイアウォールありで移行を実行することを選択した場合、Threat Defense のバージョンは 7.0 以降である必要があります。 （注） 対象のファイアウォールを使用してリモートアクセス VPN を移行するには、対象のファイアウォールを選択し、次のいずれかのライセンスを対象のファイアウォールに追加する必要があります。 • AnyConnect Plus • AnyConnect Apex • AnyConnect VPN Only • ASA からの等コストマルチパス（ECMP）ルートの移行（移行先の管理センターが 7.1 以降で、Threat Defense バージョンが 6.5 以降の場合）。
3.0.2	Cisco Secure Firewall 移行ツール 3.0.2 には、 ASA から Management Center バージョン 7.2 以降へのリモートアクセス VPN 設定の移行に関するバグ修正が含まれています。
3.0.1	Cisco Secure Firewall 移行ツール 3.0.1 は、以下をサポートします。 • 宛先の Management Center がバージョン 7.2 以降で、Threat Defense のバージョンが 7.0 以降の場合における ASA からの Enhanced Interior Gateway Routing Protocol（EIGRP）の移行。 （注） Threat Defense デバイスなしでは、ASA および ASA with FirePOWER Services から EIGRP を移行することはできません。 • Cisco Secure Firewall 3100 シリーズは、ASA からの移行の送信元デバイスまたは宛先デバイスとしてサポートされています。

バージョン	サポートされる機能

3.0	Cisco Secure Firewall 移行ツール 3.0 は、以下をサポートします。
	• 移行先の管理センターが 7.2 以降の場合の ASA 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 Cisco Secure Firewall 移行ツールからアップロードする必要があります。
	  • Live Connect ASA からプロファイルを取得できるようにするには、ASA で **ssh scopy enable** コマンドを有効にする必要があります。
	• クラウド提供型 Firewall Management Center への移行（移行先の管理センターが 7.2 以降の場合）。

バージョン	サポートされる機能
2.5.2	Cisco Secure 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 ルールアクションに対してのみ最適化を使用できます。 Cisco Secure 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	Cisco Secure 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	Cisco Secure 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） ソース ASA 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。 移行先の Management Center のバージョンが 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）オブジェクトはサポートされます。

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 Cisco Secure Firewall 移行ツールで使用されます。
2.3.5	Cisco Secure 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	Cisco Secure 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 構成の暗号マップ関連の構成は、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 Cisco Secure 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
	• Cisco Secure 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、Cisco Secure 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。Cisco Secure 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。Cisco Secure 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。 • Cisco Secure 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。 • Cisco Secure 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。 • Cisco Secure 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。Cisco Secure Firewall 移行ツールの以前のバージョンでは、このオプ

バージョン	サポートされる機能
	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 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）]）。 • Cisco Secure Firewall 移行ツールのバージョンチェック。Cisco Secure 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

Cisco Secure Firewall 移行ツールのライセンス

Cisco Secure Firewall 移行ツールアプリケーションは無料であり、ライセンスは必要ありません。ただし、脅威に対する防御 デバイスの正常な登録とポリシーの展開のため、Management Center には関連する 脅威に対する防御 機能に必要なライセンスが必要です。

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

Cisco Secure Firewall 移行ツールには、次のインフラストラクチャとプラットフォームの要件があります。

- Microsoft Windows 10 64 ビット オペレーティング システムまたは macOS バージョン 10.13 以降で実行している
- Google Chrome がシステムのデフォルトブラウザである
- （Windows）[Power & Sleep] で [Sleep] 設定が [Never put the PC to Sleep] に設定されているため、大規模な移行プッシュ中にシステムがスリープ状態にならない
- （macOS）大規模な移行プッシュ中にコンピュータとハードディスクがスリープ状態にならないように [Energy Saver] 設定が構成されている

ASA構成ファイルの要件と前提条件

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

Cisco Secure Firewall 移行ツールに手動でインポートする ASA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 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 構成ファイルのエクスポートを参照してください。
- バージョン番号を含んでいる。
- 有効な ASA CLI 構成のみが含まれている。
- 構文エラーは含まれません。
- ファイル拡張子が `.cfg` または `.txt` である。
- UTF-8 ファイルエンコーディングを使用している。
- コードの手入力または手動変更をしていない。ASA構成を変更する場合は、変更した構成ファイルをASAデバイスでテストして、有効な設定であることを確認することが推奨されます。

- 「--More--」キーワードをテキストとして含んでいない。

Threat Defense デバイスの要件および前提条件

管理センターに移行する場合、ターゲット Threat Defense デバイスが追加される場合とされない場合があります。Threat Defense デバイスへの今後の展開のために、共有ポリシーを管理センターに移行できます。デバイス固有のポリシーを Threat Defense に移行するには、管理センターに追加する必要があります。ASAの設定の Threat Defense への移行を計画する場合は、次の要件と前提条件を考慮してください。

- ターゲット Threat Defense デバイスは、管理センターに登録されている必要があります。
- Threat Defense デバイスは、スタンドアロンデバイスまたはコンテナインスタンスにすることができます。クラスタまたは高可用性設定の一部であっては**なりません**。
  - ターゲットネイティブ Threat Defense デバイスには、使用する物理データおよびポート チャネル インターフェイスが ASAと同数以上必要です（「管理専用」およびサブインターフェイスを除く）。そうでない場合は、ターゲット Threat Defense デバイスに必要なタイプのインターフェイスを追加する必要があります。サブインターフェイスは、物理またはポートチャネルのマッピングに基づいて Cisco Secure Firewall 移行ツールによって作成されます。
  - ターゲット Threat Defense デバイスがコンテナインスタンスである場合、使用する物理インターフェイス、物理サブインターフェイス、ポート チャネル インターフェイス、およびポート チャネル サブインターフェイス（「管理専用」を除く）が、ASA の使用しているものと同数以上必要です。そうでない場合は、ターゲット Threat Defense デバイスに必要なタイプのインターフェイスを追加する必要があります。

（注）
- サブインターフェイスは、Cisco Secure Firewall 移行ツールでは作成されません。インターフェイスマッピングのみが許可されます。
- 異なるインターフェイスタイプ間のマッピングは許可されます。たとえば、物理インターフェイスをポート チャネル インターフェイスにマップできます。

ASA 構成のサポート

サポートされている ASA 構成

Cisco Secure Firewall 移行ツールは、次の ASA 構成を完全に移行できます。

- ネットワークオブジェクトおよびグループ

- サービスオブジェクト（送信元と接続先に設定されたサービスオブジェクトを除く）

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

- サービス オブジェクト グループ（ネストされたサービス オブジェクト グループを除く）

（注） Management Center ではネストはサポートされていないため、Cisco Secure Firewall 移行ツールは参照されるルールの内容を拡張します。ただし、ルールは完全な機能とともに移行されます。

- IPv4 および IPv6 FQDN オブジェクトとグループ
- IPv6 変換サポート（インターフェイス、静的ルート、オブジェクト、ACL、および NAT）
- インバウンド方向とグローバル ACL のインターフェイスに適用されるアクセスルール
- 自動 NAT、手動 NAT、およびオブジェクト NAT（条件付き）
- 静的ルート、ECMP ルート、および PBR
- DHCP 設定（サーバー、リレー、および DDNS を含む）
- SNMP
- 物理インターフェイス
- ASA インターフェイス上のセカンダリ VLAN は 脅威に対する防御 に移行されません。
- サブインターフェイス（サブインターフェイス ID は、移行時に常に VLAN ID と同じ番号に設定されます）
- ポート チャネル
- 仮想トンネルインターフェイス（VTI）
- ダイナミック VTI および IPv6
- ブリッジグループ（トランスペアレントモードのみ）
- IP SLA のモニタ

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

  IP SLA モニタでは、モニタリング対象のアドレスへの接続ポリシーを定義し、そのアドレスへのルートの可用性をトラッキングします。静的ルートの可用性は、ICMP エコー要求を送信し、応答を待機することによって、定期的にチェックされます。エコー要求がタイムアウトすると、その静的ルートはルーティングテーブルから削除され、バックアップ

ルートに置き換えられます。SLA モニタリングジョブは、デバイス設定から SLA モニタを削除していない限り、展開後すぐに開始して実行し続けます（つまり、ジョブはエージングアウトしません）。SLA モニタオブジェクトは、IPv4 静的ルートポリシーの [ルートトラッキング（Route Tracking）] フィールドで使用されます。IPv6 ルートでは、ルートトラッキングによって SLA モニタを使用することはできません.

（注） IP SLA モニターは、脅威に対する防御 以外のフローではサポートされていません。

- オブジェクトグループの検索

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

（注）
- オブジェクトグループ検索は、6.6 より前の Management Center または 脅威に対する防御 のバージョンでは使用できません。
- オブジェクトグループ検索は 脅威に対する防御 以外のフローではサポートされていないため、無効になります。

- 時間ベースのオブジェクト

  Cisco Secure Firewall 移行ツールは、アクセスルールで参照される時間ベースオブジェクトを検出すると、その時間ベースオブジェクトを移行し、それぞれのアクセスルールにマッピングします。[構成の確認と検証（Review and Validate Configuration）] ページのルールに対してオブジェクトを確認します。

  時間ベースのオブジェクトは、期間に基づいてネットワークアクセスを許可するアクセスリストタイプです。特定の時刻または特定の曜日に基づいてアウトバウンドトラフィックまたはインバウンドトラフィックを制限する必要がある場合に便利です。

（注）
- 送信元の ASA からターゲットの FTD にタイムゾーン構成を手動で移行する必要があります。
- 時間ベースのオブジェクトは 脅威に対する防御 以外のフローではサポートされていないため、無効になります。
- 時間ベースのオブジェクトは Management Center バージョン 6.6 以降でサポートされています。

- [サイト間 VPN トンネル（Site-to-Site VPN Tunnels）]

- サイト間 VPN：Cisco Secure Firewall 移行ツールは、送信元 ASA で暗号マップ構成を検出すると、暗号マップを Management Center VPN にポイントツーポイント トポロジとして移行します。
- ASA からのクリプトマップ（静的/動的）ベースの VPN
- ルートベース（VTI）の ASA VPN
- ASA からの証明書ベースの VPN 移行
- ASA トラストポイントまたは証明書の Management Center への移行は手動で実行する必要があり、また、移行前のアクティビティに含まれている必要があります。

- 動的ルートオブジェクト、BGP、および EIGRP
  - ポリシーリスト
  - プレフィックスリスト
  - コミュニティ リスト
  - 自律システム（AS）パス

- リモートアクセス VPN
  - SSL と IKEv2 プロトコル
  - 認証方式：[AAAのみ（AAA only）]、[クライアント証明書のみ（Client Certificate only）]、および [AAAとクライアント証明書（AAA + Client Certificate）]
  - AAA：Radius、ローカル、LDAP、および AD
  - 接続プロファイル、グループポリシー、動的アクセス ポリシー、LDAP 属性マップ、および証明書マップ
  - 標準 ACL および拡張 ACL
  - RA VPN カスタム属性と VPN ロードバランシング
  - 移行前のアクティビティの一環として、次の手順を実行します。
    - ASA トラストポイントを PKI オブジェクトとして手動で Management Center に移行します。
    - AnyConnect パッケージ、Hostscan ファイル（Dap.xml、Data.xml、Hostscan Package）、外部ブラウザパッケージ、および AnyConnect プロファイルを送信元 ASA から取得します。
    - すべての AnyConnect パッケージを Management Center にアップロードします。
    - AnyConnect プロファイルを Management Center に直接アップロードするか、または Cisco Secure Firewall 移行ツールからアップロードします。

- Live Connect ASA からプロファイルを取得できるようにするには、ASA で **ssh scopy enable** コマンドを有効にします。

- WebVPN
  - グループ セキュリティ ポリシー SSL クライアントレス VPN トンネルプロトコル
  - 認証方式としてセキュリティアサーションマークアップ言語（SAML）を使用する、グループポリシーに関連するトンネルグループ
  - HTTPS ベースのアプリケーション URL を含むトンネルグループ

（注） 前述の基準が満たされていると、SAML 設定とアプリケーション URL が移行されます。

部分的にサポートされる ASA 構成

Cisco Secure Firewall 移行ツールは、次の ASA 構成の移行を部分的にサポートしています。これらの構成の一部には、詳細オプションを使用するルールが含まれ、それらのオプションなしで移行されます。Management Center がこれらの詳細オプションをサポートしている場合は、移行の完了後に手動で構成できます。

- シビラティ（重大度）や時間間隔など、高度なロギング設定を使用して設定されたアクセス コントロール ポリシー ルール
- トラックオプションを使用して設定された静的ルート
- 証明書ベースの VPN 移行
- 動的ルートオブジェクト、BGP、および EIGRP
  - ルートマップ

未サポートの ASA 構成

Cisco Secure Firewall 移行ツールは、次の ASA 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
- トンネリング プロトコルベースのアクセス コントロール ポリシー ルール

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

- SCTP で構成された NAT ルール
- ホスト '0.0.0.0' で構成された NAT ルール
- SLA トラッキングを使用した DHCP または PPPoE によって取得されたデフォルトルート
- sla monitor schedule
- トランスポートモードの IPsec のトランスフォームセット
- Management Center への ASA トラストポイントの移行
- BGP のトランスペアレント ファイアウォール モード
- ASA WebVPN から Zero Trust アプリケーション（ZTA）ポリシーへの移行では、以下はサポートされません。
  - WebVPN ブックマークのインポート
  - ローカル、RADIUS、および LDAP の認証方式

注意事項と制約事項

変換中に、Cisco Secure Firewall 移行ツールは、ルールまたはポリシーで使用されるかどうかにかかわらず、サポートされているすべてのオブジェクトおよびルールに対して 1 対 1 のマッピングを作成します。Cisco Secure Firewall 移行ツールには、未使用のオブジェクト（ACL および NAT で参照されていないオブジェクト）の移行を除外できる最適化機能があります。

Cisco Secure Firewall 移行ツールは、サポートされていないオブジェクトとルールを次のように処理します。

- サポートされていないオブジェクトと NAT ルールは移行されません。
- サポートされていない ACL ルールは、無効なルールとして Management Center に移行されます。
- アウトバウンド ACL は**サポートされていない構成（Unsupported Configuration）**であり、Management Center に移行されません。送信元ファイアウォールにアウトバウンド ACL がある場合、**移行前レポート**の**無視される構成（Ignored Configration）**セクションで報告されます。
- サポートされるすべての ASA 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。
- ASA マルチコンテキストから単一インスタンスの Threat Defense への移行では、等コストマルチパス（ECMP）ルーティング設定が、対応する Virtual Routing and Forwarding（VRF）設定に移行されます。
  - 同じ名前を持つ2つの異なるセキュリティコンテキスト内のインターフェイスは、アンダースコアとコンテキスト名を追加することで名前が変更されます。
  - 同じ名前を持つ2つの異なるセキュリティコンテキスト内のセキュリティゾーンは、アンダースコアとコンテキスト名を追加することで名前が変更されます。
  - ECMP ルーティング設定が VPN 設定とともに存在する場合は、それらの設定がグローバルルータ（グローバル VRF）に移行されます。

ASA 設定の制限

送信元 ASA 構成の移行には、次の制限があります。

- Cisco Secure Firewall 移行ツールは、個別の 脅威に対する防御 デバイスとして、ASA からの個々のセキュリティコンテキストの移行をサポートします。
- システム構成は移行されません。
- Cisco Secure Firewall 移行ツールは、50 **以上**のインターフェイスに適用される単一の ACL ポリシーの移行をサポートしていません。50 以上のインターフェイスに適用される ACL ポリシーは、手動で移行してください。
- 動的ルーティングなど、ASA 構成の一部は 脅威に対する防御 に移行できません。これらの構成は手動で移行してください。
- ブリッジ仮想インターフェイス（BVI）、冗長インターフェイス、またはトンネルインターフェイスを使用するルーテッドモードの ASA 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 デバイスを移行することはできます。
- Management Center では、ネストされたサービス オブジェクト グループまたはポートグループはサポートされていません。変換の一環として、Cisco Secure Firewall 移行ツールは、参照されているネストされたオブジェクトグループまたはポートグループの内容を展開します。
- Cisco Secure Firewall 移行ツールは、1 つの回線にある送信元ポートと宛先ポートを持つ拡張サービスのオブジェクトまたはグループを、複数の回線にまたがる異なるオブジェクトに分割します。このようなアクセスコントロールルールの参照は、正確に同じ意味の Management Center ルールに変換されます。
- 特定のトンネリングプロトコル（GRE、IP-in-IP、IPv6-in-IP など）を参照しないアクセス制御ルールが送信元 ASA 構成にあり、これらのルールが ASA 上の暗号化されていないトンネルトラフィックに一致する場合、脅威に対する防御 に移行すると、対応するルールは

ASA 上と同じようには動作しません。脅威に対する防御 のプレフィルタポリシーで、これらの特定のトンネルルールを作成することを推奨します。

- サポートされるすべての ASA 暗号マップは、ポイントツーポイント トポロジとして移行されます。
- Management Center に同じ名前の AS-Path オブジェクトが表示された場合、移行は次のエラーメッセージで停止します。

  「Management Center で競合する AS-Path オブジェクト名が検出されました。続行するには、Management Center の競合を解決してください。（Conflicting AS-Path object name detected in , please resolve conflict in to proceed further）」
- OSPF および Routing Information Protocol（RIP）から EIGRP への再配布はサポートされていません。
- PBR の場合、ASA の設定にはルートマップがありますが、管理センターはルートマップを使用しません。Cisco Secure Firewall 移行ツールは、インターフェイスに適用されたルートマップ内の構成を移行します。
- 複数のシーケンス番号を持つルートマップの場合、最初のシーケンス番号だけが移行されます。他のすべてのシーケンス番号は無視され、移行前レポートに表示されます。

RA VPN の移行の制限事項

リモートアクセス VPN の移行は、次の制限付きでサポートされています。

- API の制限により、SSL 設定の移行はサポートされていません。
- LDAP サーバーは、暗号化タイプが「なし（none）」として移行されます。
- ポリシーは Management Center 全体に適用されるため、DfltGrpPolicy は移行されません。Management Center で必要な変更を直接行うことができます。
- Radius サーバーでは、動的認証が有効になっている場合は、AAA サーバー接続は動的ルーティングではなくインターフェイスを介して行う必要があります。インターフェイスなしで動的認証が有効になっている AAA サーバーで ASA 構成が見つかった場合、Cisco Secure Firewall 移行ツールは動的認証を無視します。管理センターでインターフェイスを選択した後に、動的認証を手動で有効にする必要があります。
- トンネルグループの下でアドレスプールを呼び出している間は ASA 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 構成でインターフェイスが検出された場合、そのインターフェイスは Cisco Secure Firewall 移行ツールで無視され、アドレスプールがインターフェイスなしで移行されます。
- ASA 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 構成で検出された DHCP サーバーがある場合、それらのサーバーは Cisco Secure Firewall 移行ツールで無視され、DHCP サーバーはキーワードなしでプッシュされます。

- ASA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構成でインターフェイスが検出された場合、そのインターフェイスはCisco Secure Firewall移行ツールで無視され、コマンドはインターフェイスなしでプッシュされます。
- ASA 構成は、リダイレクト ACL を Radius サーバーにマッピングしません。したがって、Cisco Secure Firewall 移行ツールから取得する方法はありません。リダイレクト ACL が ASA 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 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 構成に 480 を超える値が見つかった場合、管理センターでサポートされている最大値の 480 に設定されます。
- 接続プロファイルへの IPv4 プールと DHCP useSecondaryUsernameforSession の設定の構成は、API の問題によりサポートされていません。
- バイパスアクセス制御 sysopt permit-vpn オプションは、RA VPN ポリシーで有効になっていません。ただし、必要に応じて、管理センターから有効にすることができます。
- AnyConnect クライアントモジュールとプロファイルの値は、プロファイルが Cisco Secure Firewall移行ツールから管理センターにアップロードされた場合にのみ、グループポリシーに従って更新できます。
- 証明書を管理センターに直接マッピングする必要があります。
- IKEv2 パラメータは、デフォルトでは移行されません。それらのパラメータは管理センターを使用して追加する必要があります。

ASA 移行の注意事項

ACL ログオプションの移行は、脅威に対する防御 のベストプラクティスに従います。ルールのログオプションは、送信元 ASA 構成に基づいて有効または無効になります。アクションが **deny** のルールの場合、Cisco Secure Firewall 移行ツールは接続の開始時にロギングを構成します。アクションが **permit** の場合、Cisco Secure Firewall 移行ツールは接続の終了時にロギングを構成します。

オブジェクト移行の注意事項

ASA と Threat Defense では、オブジェクトに関する構成上の注意事項が異なります。たとえば、ASAでは、複数のオブジェクトに大文字か小文字かが異なるだけの同じ名前を付けることができますが、Threat Defense では、大文字か小文字かに関係なく、各オブジェクトに一意の名前を付ける必要があります。このような違いに対応するために、Cisco Secure Firewall 移行ツールでは、ASA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 オブジェクトに一意の名前と構成がある場合：Cisco Secure Firewall 移行ツールはオブジェクトを変更せずに正常に移行します。

- ASA オブジェクトの名前に、Management Center でサポートされていない特殊文字が 1 つ以上含まれている場合：Cisco Secure Firewall 移行ツールは、管理センターのオブジェクト命名基準を満たすために、そのオブジェクト名の特殊文字を「_」文字に変更します。
- ASA オブジェクトの名前と構成が Management Center の既存オブジェクトと同じ場合：Cisco Secure Firewall 移行ツールは Secure Firewall Threat Defense 構成に Secure Firewall Management Center オブジェクトを再利用し、ASA オブジェクトを移行しません。
- ASA オブジェクトと Secure Firewall Management Center の既存オブジェクトの名前は同じだが構成は異なる場合：Cisco Secure Firewall 移行ツールはオブジェクトの競合を報告します。これにより、ユーザーは、ASA 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 オブジェクトに、大文字か小文字かが異なるだけの同じ名前が付けられている場合：Cisco Secure Firewall 移行ツールは、Secure Firewall Threat Defense のオブジェクト命名基準を満たすように、そのようなオブジェクトの名前を変更します。

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

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

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

ASA WebVPN から ZTA への移行に関する注意事項と制約事項

ASA WebVPN から ZTA への移行を試みる前に、次の点をよくお読みください。

- ターゲットの管理センターと Threat Defense デバイスは、バージョン 7.4 以降を実行している必要があります。
- ターゲットの Threat Defense デバイスは、検出エンジンとして Snort3 を使用している必要があります。
- 移行前に、ASA トラストポイント証明書（IdP および事前認証）をターゲット管理センターに手動でアップロードする必要があります。
- 移行前に、アプリケーション SSL 証明書とその秘密キーをターゲット管理センターにアップロードする必要があります。
- ローカル、RADIUS、および LDAP の認証方式はサポートされていません。
- Threat Defense デバイスに割り当てることができる ZTA ポリシーは 1 つだけです。

Threat Defense デバイスに関する注意事項と制約事項

ASA 構成を 脅威に対する防御 に移行する計画を立てている場合は、次の注意事項と制限事項を考慮してください。

- ルート、インターフェイスなど、脅威に対する防御 に既存のデバイス固有の構成がある場合、プッシュ移行中にCisco Secure Firewall移行ツールは自動的にデバイスを消去し、ASA構成から上書きします。

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

移行中に、Cisco Secure Firewall移行ツールはインターフェイス構成をリセットします。これらのインターフェイスをポリシーで使用すると、Cisco Secure Firewall移行ツールはそれらをリセットできず、移行は失敗します。

- Cisco Secure Firewall 移行ツールは、ASA 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構成に次のインターフェイスとポートチャネルが割り当てられている場合は、移行前にそれらをターゲット 脅威に対する防御 デバイス上に作成する必要があります。
  - 5 つの物理インターフェイス
  - 5 つのポートチャネル
  - 2 つの管理専用インターフェイス

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

- Cisco Secure Firewall 移行ツールは、ASA 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構成に次のインターフェイスとポートチャネルが割り当てられている場合は、移行前にそれらをターゲット 脅威に対する防御 デバイス上に作成する必要があります。
  - 5 つの物理インターフェイス
  - 5 つのポートチャネル

- 2 つの管理専用インターフェイス

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

移行がサポートされるプラットフォーム

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

（注） Cisco Secure Firewall 移行ツールは、スタンドアロン ASA デバイスからスタンドアロン 脅威に対する防御 デバイスへの移行のみをサポートします。

サポートされる送信元 ASA プラットフォーム

Cisco Secure Firewall 移行ツールを使用して、次のシングルコンテキスト/マルチコンテキスト ASA プラットフォームから構成を移行できます。

- ASA 5510
- ASA 5520
- ASA 5540
- ASA 5550
- ASA 5580
- ASA 5506
- ASA 5506W-X
- ASA 5506H-X
- ASA 5508-X
- ASA 5512-X
- ASA 5515-X
- ASA 5516-X
- ASA 5525-X
- ASA 5545-X
- ASA 5555-X

- ASA 5585-X（ASA のみ。Cisco Secure Firewall 移行ツールは ASA FirePOWER moduleから構成を移行しません）
- Firepower 1000 シリーズ
- Firepower 2100 シリーズ
- Secure Firewall 3100 シリーズ
- Firepower 4100 シリーズ
- Cisco Secure Firewall 4200 シリーズ
- Firepower 9300 シリーズ
  - 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 VMware 上の ASA Virtual

サポートされるターゲット Threat Defense プラットフォーム

Cisco Secure Firewall 移行ツールを使用して、脅威に対する防御 プラットフォームの次のスタンドアロンまたはコンテナインスタンスに送信元 ASA 構成を移行できます。

- ASA 5506
- ASA 5506W-X
- ASA 5506H-X
- ASA 5508-X
- ASA 5512-X
- ASA 5515-X
- ASA 5516-X
- ASA 5525-X
- ASA 5545-X
- ASA 5555-X
- Firepower 1000 シリーズ
- Firepower 2100 シリーズ

- Secure Firewall 3100 シリーズ
- Firepower 4100 シリーズ
- Cisco Secure Firewall 4200 シリーズ
- Firepower 9300 シリーズ（次を含む）：
  - SM-24
  - SM-36
  - SM-40
  - SM-44
  - SM-48
  - SM-56
- VMware ESXi、VMware vSphere Web クライアント、または vSphere スタンドアロンクライアントを使用して展開された Threat Defense（VMware 上）
- Microsoft Azure クラウドまたは AWS クラウド上の Threat Defense Virtual

（注）
- Azure における Threat Defense Virtual の前提条件と事前設定については、『Getting Started with Secure Firewall Threat Defense Virtual』[英語] を参照してください。
- AWS クラウドにおける Threat Defense Virtual の前提条件と事前設定については、「Threat Defense Virtual の前提条件」を参照してください。

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

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

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

サポートされる移行先の管理センター

Cisco Secure Firewall 移行ツールは、管理センターおよびクラウド提供型 Firewall Management Center によって管理される Threat Defense デバイスへの移行をサポートします。

Management Center

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

管理センターは、移行に関する次のガイドラインを満たす必要があります。

- 移行でサポートされる Management 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 （35 ページ）を参照）。
- ASA 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。

    Management Center Web インターフェイスで、**[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）]**に移動し、**[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。

重要 REST API を有効にするには、 Management Center の管理者ユーザーロールが必要です。管理センターのユーザーロールの詳細については、「ユーザーロール」を参照してください。

クラウド提供型 Firewall Management Center

クラウド提供型 Firewall Management Center は、Threat Defense デバイスの管理プラットフォームであり、Cisco Defense Orchestrator を介して提供されます。クラウド提供型 Firewall Management Center は、管理センターと同じ機能を多数提供します。

CDO からクラウド提供型 Firewall Management Center にアクセスできます。CDO は、Secure Device Connector（SDC）を介してクラウド提供型 Firewall Management Center に接続します。クラウド提供型 Firewall Management Center の詳細については、「クラウド提供型 Firewall Management Center による Cisco Secure Firewall Threat Defense デバイスの管理」を参照してください。

Cisco Secure Firewall 移行ツールは、移行先の管理センターとしてクラウド提供型 Firewall Management Center をサポートしています。クラウド提供型 Firewall Management Center を移行先の管理センターとして選択するには、CDO リージョンを追加し、CDO ポータルから API トークンを生成する必要があります。

CDO リージョン

CDO は 3 つの異なる地域で利用でき、地域は URL 拡張子で識別できます。

表 *1 : CDO* の地域と *URL*

地域	CDO URL
ヨーロッパ地域	https://defenseorchestrator.eu/
US リージョン	https://defenseorchestrator.com/
APJC リージョン	https://www.apj.cdo.cisco.com/

移行でサポートされるソフトウェアのバージョン

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

サポートされている Cisco Secure Firewall 移行ツールのバージョン

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

サポートされている ASA のバージョン

Cisco Secure Firewall 移行ツールは、ASA ソフトウェアバージョン 8.4 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。

ソース ASA 設定でサポートされている Management Center のバージョン

ASA の場合、Cisco Secure Firewall 移行ツールは、バージョン 6.2.3 または 6.2.3+ を実行している Management Center によって管理される 脅威に対する防御 デバイスへの移行をサポートしています。

（注） 一部の機能は、以降のバージョンの Management Center および 脅威に対する防御 でのみサポートされています。

（注） 最適な移行時間を実現するには、Management Center を、software.cisco.com/downloads で提供されている推奨リリースバージョンにアップグレードすることをお勧めします。

サポートされる Threat Defense のバージョン

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

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

関連資料

この項では、ASA から 脅威に対する防御 への移行に関連するドキュメントの概要を示します。

- 『Cisco Secure Firewall ASA to Threat Defense Feature Mapping』：一般的に使用される ASA 機能とそれに相当する Threat Defense 機能が記載されています。ASA の各機能について、Threat Defense の同等の機能と、Cisco Secure Firewall Management Center または Cisco Defense Orchestrator（CDO）クラウド提供型 Firewall Management Center でその機能を設定するための UI パスが記載されています。
- 『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 脅威に対する防御 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 脅威に対する防御 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 脅威に対する防御 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 脅威に対する防御 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 脅威に対する防御 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 脅威に対する防御 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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。