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： FDM 管理対象デバイス 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 FDM 管理対象デバイス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 FDM 管理対象デバイスの機能とポリシーを自動的に 脅威に対する防御 に移行できます。サポートされていない機能はすべて、手動で移行する必要があります。

Cisco Secure Firewall 移行ツールは FDM 管理対象デバイス 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 FDM 管理対象デバイス構成項目。
- エラーのある FDM 管理対象デバイス構成行には、Cisco Secure Firewall 移行ツールが認識できない FDM 管理対象デバイスコンポーネント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。

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**、 FDM 管理対象デバイス構成、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** • Cisco 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。Cisco 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 Threat Defense 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、確認、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 Cisco 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制御リスト（ACL）を最適化できるようになりました。[設定の最適化、確認、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』ガイドの「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。 • 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。 FDM管理対象デバイスの管理センターへの移行（移行先の管理センターのバージョンが 7.3 以降で、移行元のデバイスマネージャのバージョンが 7.2 以降の場合に限ります）。 デバイスマネージャのバージョンは、移行先の管理センターのバージョン以下である必要があります。 移行には次のオプションを使用できます。 **1.** [Firepower Device Managerの移行（共有構成のみ）（Migrate Firepower Device Manager (Shared Configurations Only)）]：このオプションを使用すると、段階的な移行を行えます。この場合、最初にすべての共有構成を移行し、後で要件に応じてデバイス構成を移行できます。移行プロセスでは、共有構成のみが対象の管理センターに移行されます。デバイスマネージャから取得した構成バンドルをアップロードするか、デバイスマネージャの資格情報をツールに提供して、構成の詳細をフェッチすることができます。構成の詳細を自動フェッチする方法が推奨されます。 **2.** [Firepower Device Managerの移行（デバイスおよび共有構成を含む）（Migrate Firepower Device Manager (Includes Device & Shared Configurations)）]：このオプションを使用すると、デバイスと共有構成の両方をデバイスマネージャから対象の管理センターに移行できます。ソースデバイスとその構成が対象の管理センターに移行されると、FDM 管理対象デバイスが対象の管理センターデバイスになります。ツールが構成の詳細をフェッチするには、デバイスマネージャの資格情報を指定する必要があります。この移行オプションでは、構成の自動フェッチのみが許可されます。 **3.** [Firepower Device Manager（デバイスおよび共有構成を含む）のFTDデバイス（新しいハードウェア）への移行（Migrate Firepower Device Manager (Includes Device & Shared Configurations) to FTD Device (New Hardware)）]：このオプションを使用すると、デバイスと共有構成の両方を、対象の管理センターによって管理される Threat Defense デバイスに移行できます。この場合、移行プロセス中にソースデバイスは移行されず、デバイス構成のみが新しい Threat Defense デバイスに移行されます。デバイスマネージャから取得した構成バンドルをアップロードするか、デバイスマネージャの資格情報をツールに提供して、構成の詳細をフェッチすることができます。構成の詳細を自動フェッチする方法が推奨されます。

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

FDM 管理対象デバイス構成ファイルの要件と前提条件

FDM 管理対象デバイス構成バンドルは、手動で、または Cisco Secure Firewall 移行ツールからライブ FDM 管理対象デバイスに接続して取得できます。手動アップロードは、次のオプションでのみサポートされています。

- [Firepower Device Manager（デバイスおよび共有構成を含む）のFTDデバイス（新しいハードウェア）への移行（Migrate Firepower Device Manager (Includes Device & Shared Configurations) to FTD Device (New Hardware)）]
- [Firepower Device Managerの移行（共有構成のみ）（Migrate Firepower Device Manager (Shared Configurations Only)）]

（注） 手動アップロードは、[Firepower Device Managerの移行（デバイスおよび共有構成を含む）（Migrate Firepower Device Manager (Includes Device & Shared Configurations)）] オプションではサポートされていません。

Cisco Secure Firewall 移行ツールに手動でインポートする FDM 管理対象デバイス構成バンドルは、次の要件を満たしている必要があります。

- 有効なデバイスマネージャ CLI 構成のみを含んでいる。
- バージョン番号を含んでいる。
- 構成バンドルは .zip 形式でなければならない。
- デバイスマネージャからエクスポートされた完全エクスポート構成がある。28 ページの「FDM 管理対象デバイス構成ファイルのエクスポート」を参照してください。

- 構成を含む少なくとも 1 つの.txt ファイルが必要。
- 暗号化されたバンドルにキーを提供する必要がある。暗号化されていないバンドルの場合、暗号化キーは空のままでもよい。
- 構文エラーは含まれません。
- コードの手入力または手動変更をしていない。

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。FDM 管理対象デバイスの設定の 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。

- Threat Defense ハードウェアは、FDM 管理対象デバイスのモデル以上である必要があります。たとえば、ソース FDM 管理対象デバイスのモデルが 2100 の場合、接続先 Threat Defense モデルは 2100 または 3100 または 4100 または 9300 とすることができますが、2100 未満のモデルとすることはできません。
- 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 FDM 管理対象デバイス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、FDM 管理対象デバイス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。

FDM 管理対象デバイス構成のサポート

サポートされる FDM 管理対象デバイス構成

Cisco Secure Firewall 移行ツールは、次の FDM 管理対象デバイス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 移行ツールで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）
- アクセス コントロール ポリシー（Access Control Policy）
- 自動 NAT と手動 NAT
- 静的ルート、ECMP ルート
- 物理インターフェイス

- FDM 管理対象デバイスインターフェイス上のセカンダリ VLAN は 脅威に対する防御 に移行されません。
- サブインターフェイス（サブインターフェイス ID は、移行時に常に VLAN ID と同じ番号に設定されます）
- ポート チャネル
- 仮想トンネルインターフェイス（VTI）
- ブリッジグループ（トランスペアレントモードのみ）
- IP SLA のモニタ

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

  IP SLA モニタでは、モニタリング対象のアドレスへの接続ポリシーを定義し、そのアドレスへのルートの可用性をトラッキングします。静的ルートの可用性は、ICMP エコー要求を送信し、応答を待機することによって、定期的にチェックされます。エコー要求がタイムアウトすると、その静的ルートはルーティングテーブルから削除され、バックアップルートに置き換えられます。SLA モニタリングジョブは、デバイス設定から SLA モニタを削除していない限り、展開後すぐに開始して実行し続けます（つまり、ジョブはエージングアウトしません）。SLA モニタオブジェクトは、IPv4 静的ルートポリシーの [ルートトラッキング（Route Tracking）] フィールドで使用されます。IPv6 ルートでは、ルートトラッキングによって SLA モニタを使用することはできません.
- 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共有構成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

- 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 FDM 管理対象デバイスからターゲットの 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。

- [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 FDM 管理対象デバイス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。
  - FDM 管理対象デバイス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 FDM VPN
  - FDM 管理対象デバイスからの証明書ベースの VPN 移行
  - FDM 管理対象デバイスの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。
    - FDM 管理対象デバイスの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 FDM 管理対象デバイスから取得します。
- 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。

- マルウェアおよびファイル ポリシー
  - 移行ツールは、FDM 管理対象デバイスのマルウェアとファイルポリシーを、ターゲット管理センターにプッシュされるアクセス コントロール ポリシーのそれぞれのルールに追加します。
  - [マルウェアをすべてブロック（Block Malware All）] や [マルウェアクラウドルックアップ - ブロックなし（Malware Cloud Look up - No Block）] などのデフォルトのファイルポリシーは作成されません。
- SSL 復号ポリシー
- SNMP
  - SNMPv1 および SNMPv2 の場合は、[設定の最適化、確認、検証（Optimize, Review and Validate Configuration）] ページでコミュニティストリングが手動で更新されていることを確認します。
  - SNMPv3 の場合は、[設定の最適化、確認、検証（Optimize, Review and Validate Configuration）] でユーザー認証とユーザー暗号化パスワードが手動で指定されていることを確認します。

部分的にサポートされる FDM 管理対象デバイス構成

Cisco Secure Firewall 移行ツールは、次の FDM 管理対象デバイス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

サポートされていない FDM 管理対象デバイス構成

Cisco Secure Firewall 移行ツールは、次の FDM 管理対象デバイス構成の移行をサポートしていません。これらの構成が Management Center でサポートされている場合、移行の完了後に手動で構成できます。

- SGT ベースのアクセス コントロール ポリシー ルール
- SGT ベースのオブジェクト
- ユーザベースのアクセス コントロール ポリシー ルール
- ブロック割り当てオプションを使用して構成された NAT ルール
- サポートされていない ICMP タイプおよびコードを持つオブジェクト
- トンネリング プロトコルベースのアクセス コントロール ポリシー ルール

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

- SCTP で構成された NAT ルール
- ホスト '0.0.0.0' で構成された NAT ルール
- SLA トラッキングを使用した DHCP または PPPoE によって取得されたデフォルトルート
- sla monitor schedule
- トランスポートモードの IPsec のトランスフォームセット
- FDM 管理対象デバイスのトラストポイントの Management Center への移行
- BGP のトランスペアレント ファイアウォール モード
- SNMPv3 ユーザーグループおよびホストグループ

FDM 管理対象デバイスのオブジェクトと Threat Defense

FDM 管理対象デバイス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）
- ルーテッドモードでサポートされる BGP および EIGRP
- 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 属性マップ
- IKEv2 ポリシー
- IKEv2 IPsec プロポーザル
- 証明書マップ
- DAP
- 侵入ポリシー
- 侵入ルール

注意事項と制約事項

FDM 管理対象デバイスの移行ガイドライン

Cisco Secure Firewall 移行ツールを使用して FDM 管理対象デバイス構成を移行するためのガイドラインを以下に示します。

- 各 FDM 管理対象デバイス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。
- FDM 管理対象デバイスオブジェクトの名前に、管理センター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。
- FDM 管理対象デバイスオブジェクトの名前と構成が管理センターの既存オブジェクトと同じ場合：Cisco Secure Firewall 移行ツールは脅威防御構成に管理センターオブジェクトを再利用し、FDM 管理対象デバイスオブジェクトを移行しません。
- 複数の FDM 管理対象デバイスオブジェクトに、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、脅威防御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。

FDM 管理対象デバイス構成の制限事項

送信元 FDM 管理対象デバイス構成の移行には、次の制限があります。

- 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管理センターに移行されます。
- サポートされるすべての FDM 管理対象デバイス暗号マップ VPN は、管理センターの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。
- 脅威防御への動的ルーティングなど、一部の FDM 管理対象デバイス構成を移行することはできません。これらの構成は手動で移行してください。
- 管理センターでは、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、正確に同じ意味の管理センター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 FDM 管理対象デバイス構成にあり、これらのルールが FDM 管理対象デバイス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、脅威防御に移行すると、対応するルールは FDM 管理対象デバイス上と同じようには動作しません。脅威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 FDM 管理対象デバイス暗号マップは、ポイントツーポイント トポロジとして移行されます。
- 管理センターに同じ名前の 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 the management center, please resolve conflict in management center to proceed further）」

- ルートマップオブジェクトは、Cisco Secure 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。
- ID ポリシー、SSL ポリシー、セキュリティ インテリジェンス、SGT、ユーザーベースのルールなどのレイヤ 7 ポリシーは、API の制限により移行されません。

RA VPN の移行の制限事項

リモートアクセス VPN の移行は、次の制限付きでサポートされています。

- API の制限により、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 FDM 管理対象デバイス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。
- 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。

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 FDM 管理対象デバイス、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。

サポートされるソース FDM 管理対象デバイスプラットフォーム

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 FDM 管理対象デバイスプラットフォームから構成を移行できます。

- Firepower 1000 シリーズ

- Firepower 2100 シリーズ
- Secure Firewall 3100 シリーズ
- Firepower 4100 シリーズ
- Cisco Secure Firewall 4200 シリーズ
- Firepower 9300 シリーズ
- VMware、AWS、Azure、KVM 上の FDM 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 構成を移行できます。

- Firepower 1000 シリーズ
- Firepower 2100 シリーズ
- Secure Firewall 3100 シリーズ
- Firepower 4100 シリーズ
- 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。

サポートされる移行先の管理センター

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

Management Center

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

管理センターは、移行に関する次のガイドラインを満たす必要があります。

- 移行でサポートされる Mangement Center ソフトウェアバージョン（移行でサポートされるソフトウェアのバージョン （23 ページ）を参照）。
- 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、 FDM 管理対象デバイス、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。

サポートされる FDM 管理対象デバイスのバージョン

Cisco Secure Firewall 移行ツールは、Threat Defense ソフトウェアバージョン 7.2 以降を実行している FDM 管理対象デバイスからの移行をサポートしています。

ソース FDM 管理対象デバイス構成でサポートされる管理センターのバージョン

FDM 管理対象デバイスの場合、Cisco Secure Firewall 移行ツールは、バージョン 7.2 以降を実行している管理センターによって管理される Threat Defense デバイスからの移行をサポートしています。

（注）
- 一部の機能は、最新バージョンの管理センターおよび Threat Defense でのみサポートされます。
- 最適な移行時間を実現するには、管理センターを、software.cisco.com/downloads で言及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

FDM 管理対象デバイスの場合、Cisco Secure Firewall 移行ツールは、Threat Defense バージョン 7.2 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。

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

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