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： Fortinet 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 Fortinet 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。Cisco Secure Firewall 移行ツールを使用すると、サポートされている Fortinet 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 Fortinet 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 Fortinet 構成項目。
- エラーのある Fortinet 構成行には、Cisco Secure Firewall 移行ツールが認識できない Fortinet 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、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、アプリケーションをマッピングし、セキュリティゾーンをマッピングして、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**、 Fortinet 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。

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
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 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 に移行するコンテキストを 1 つ選択できます。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。Palo Alto Networks および Fortinet ファイアウォール移行ガイドの**「Cisco Secure Firewall 移行ツールの接続先パラメータの指定」**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。.
3.0.1	• ASA with FirePOWER Services、Check Point、Palo Alto Networks、および Fortinet の場合、Secure Firewall 3100 シリーズは宛先デバイスとしてのみサポートされます。
3.0	Cisco Secure Firewall 移行ツール 3.0 は、移行先の管理センターが 7.2 以降の場合、Fortinet からクラウド提供型 Firewall Management Center への移行をサポートするようになりました。
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、 Fortinet 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） Fortinet 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。

バージョン	サポートされる機能
2.3	• Fortinet ファイアウォール OS バージョン 5.0 以降をサポートしています。 • Cisco Secure Firewall 移行ツールを使用すると、次の FortiNet の構成要素を 脅威に対する防御 に移行できます。 • Interfaces • ゾーン • スタティック ルート • 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とグループ • アクセス コントロール リスト • NAT 依存オブジェクト（IPプール、仮想 IP） • NAT ルール • VDOM • 時間ベースオブジェクト：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。 （注） 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。

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

Fortinet ファイアウォール構成ファイルの要件と前提条件

Fortinet ファイアウォールの構成ファイルは手動で取得できます。

Cisco Secure Firewall 移行ツールに手動でインポートする Fortinet ファイアウォール構成ファイルは、次の要件を満たしている必要があります。

- Fortinet デバイスからエクスポートされた実行構成が含まれている。Firewall 移行ツールでは、グローバルと VDOM ごとのエクスポートの両方からの構成バックアップがサポートされています。詳細については、「Fortinet 構成ファイルのエクスポート」を参照してください。
- 有効な Fortinet ファイアウォール 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。Fortinet ファイアウォール構成を変更する場合は、変更した構成ファイルを Fortinet ファイアウォール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。

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。Fortinet ファイアウォールの設定の 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 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、Fortinet ファイアウォール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。

Fortinet 構成のサポート

サポートされる Fortinet ファイアウォール構成

Cisco Secure Firewall 移行ツールは、次の Fortinet ファイアウォール構成を完全に移行できます。

- ネットワークオブジェクトとグループ（ワイルドカードFQDN、ワイルドカードマスク、FortiNet ダイナミックオブジェクトを除く）
- サービス オブジェクト
- 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） 管理センター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展開します。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）
- アクセス ルール
- NAT ルール
- 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

- 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）
- 集約インターフェイス（ポートチャネル）
- Cisco Secure Firewall 移行ツールは、個別の Threat Defense デバイスとしての Fortinet ファイアウォールからの個々の VDOM の移行をサポートします。
- 時間ベースオブジェクト：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。[構成の最適化、確認および検証（Optimize, 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。このようなオブジェクトは、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 FortiNet からターゲットの Threat Defense 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管理センターバージョン 6.6 以降でサポートされています。

部分的にサポートされる Fortinet ファイアウォール構成

Cisco Secure Firewall 移行ツールは、次の Fortinet ファイアウォール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。管理センター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。

- サポートされていないアドレスオブジェクトを含むアドレスグループ。
- TCP、UDP、SCTP を含むプロトコルを使用するサービスオブジェクトを含むサービスグループ。

（注） SCTP プロトコルが削除され、サービスグループが部分的に移行されます。

サポートされていない Fortinet ファイアウォール構成

Cisco Secure Firewall 移行ツールは、次の Fortinet ファイアウォール構成の移行をサポートしません。これらの構成が管理センター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。

- ユーザーベース、デバイスベース、およびインターネットサービス ID ベースのアクセス コントロール ポリシー ルール
- サポートされていない ICMP タイプとコードを持つサービスオブジェクト
- 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
- 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
- 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
- 送信元または接続先に FQDN オブジェクトを含む NAT ルール
- 特殊文字で始まる、または特殊文字を含む FQDN オブジェクト
- ワイルドカード FQDN
- Fortinet では、IPv4 と IPv6 を組み合わせたポリシー（統合されたポリシー）を構成できます。

（注） このポリシーは、Cisco Secure Firewall 移行ツールではサポートされていません。

Fortinet ファイアウォール構成に関する注意事項と制限事項

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インターフェイス、オブジェクト、NAT ルール、およびルートは移行されません。
- 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。

Fortinet ファイアウォール構成の制限事項

送信元 Fortinet 構成の移行には、次の制限があります。

- 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、手動で移行する必要があります。
- タイプが仮想ワイヤ、冗長インターフェイス、トンネルインターフェイス、VDOM リンク、および SD-WAN インターフェイスまたはゾーンの Fortinet ファイアウォールインターフェイスはサポートされておらず、移行されません。

  FortiNet のハードウェアまたはソフトウェアスイッチの論理インターフェイスは、Threat Defense L3 インターフェイスとして移行されます。Cisco Secure Firewall 移行ツールでは、ハードウェアまたはソフトウェアスイッチメンバーインターフェイスは移行されません。
- ワイルドカード FQDN、ワイルドカード IP、ダイナミックオブジェクト、除外グループなどのオブジェクトの移行はサポートされていません。
- トランスペアレントモードまたはトランスペアレント VDOM の Fortinet ファイアウォールデバイスは移行できません。
- 管理センターでは、ネストされたサービス オブジェクト グループおよび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。

Fortinet ファイアウォールの移行ガイドライン

Cisco Secure Firewall 移行ツールは、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 Fortinet 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。

Threat Defense デバイスに関する注意事項と制約事項

構成を Threat Defense に移行することを計画する場合は、次の注意事項と制約事項を考慮してください。

- ルート、インターフェイスなど、Threat Defense 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、 構成から上書きします。

（注） デバイス（ターゲット Threat Defense）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。

- FortiNet のハードウェアまたはソフトウェアスイッチの論理インターフェイスは、Threat Defense L3 インターフェイスとして移行されます。Cisco Secure Firewall 移行ツールでは、ハードウェアまたはソフトウェアスイッチメンバーインターフェイスは移行されません。

  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。

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 Fortinet、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
- 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 （16 ページ）を参照）。
- Fortinet 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、 Fortinet、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 Fortinet Networks ファイアウォールのバージョン

Cisco Secure Firewall 移行ツールは、FortiNet ファイアウォール OS バージョン 5.0 以降を実行している 脅威に対する防御 への移行をサポートしています。

送信元 Fortinet ファイアウォール構成でサポートされている Management Center のバージョン

Fortinet ファイアウォールの場合、Cisco Secure Firewall 移行ツールは、バージョン 6.2.3.3 以降を実行している 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） 6.7 脅威に対する防御 デバイスへの移行は現在サポートされていません。そのため、デバイスに Management Center アクセス用のデータインターフェイスで設定されている場合、移行が失敗する可能性があります。

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。

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。