



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

- [このマニュアルについて](#) (1 ページ)
- [Cisco Secure Firewall 移行ツールについて](#) (1 ページ)
- [Cisco Secure Firewall 移行ツールの最新情報](#) (5 ページ)
- [Cisco Secure Firewall 移行ツールのライセンス](#) (20 ページ)
- [Cisco Secure Firewall 移行ツールのプラットフォーム要件](#) (20 ページ)
- [Cisco Multicloud Defense への移行に関する要件と前提条件](#) (20 ページ)
- [Multicloud Defense 向け Check Point ファイアウォール構成サポート](#) (21 ページ)
- [移行でサポートされるソフトウェアのバージョン](#) (21 ページ)
- [関連資料](#) (21 ページ)

このマニュアルについて

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。

Cisco Secure Firewall 移行ツールについて

Cisco Secure Firewall 移行ツールは、サポートされているチェックポイント構成を Multicloud Defense 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チェックポイント機能とポリシーを Multicloud Defense に自動的に移行できます。



(注) 移行前レポートで無視された構成について確認し、移行後にそれらを手動で構成する必要があります。

Cisco Secure Firewall 移行ツールは、チェックポイント 情報を収集し、解析して、最終的に Multicloud Defense 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。

- エラーのある Check Point 構成の XML または JSON の行
- Check Point には、Cisco Secure Firewall 移行ツールが認識できない Check Point XML または JSON の行がリストされています。**移行前レポート** とコンソールログのエラーセクションの下には、XML または JSON の構成行が記載されています。これにより、移行がブロックされています



(注) 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、構成の見直しと確認を実行します。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** のコピー、**移行後レポート** のコピー、チェックポイント 構成、および **Resources** フォルダ内のログを保存します。

Resources フォルダは、`<migration_tool_folder>\resources` にあります

未解析ファイル

Cisco Secure 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 Cisco Secure Firewall 移行ツールは、チェックポイント 構成ファイルを解析する際に、このファイルを作成します。

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)] ウィンドウの項目など、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 ～ 8331 およびポート 8888 の 12 ポートのうちの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。

通知センター

移行中にポップアップ表示される成功メッセージ、エラーメッセージ、警告を含むすべての通知は、通知センターでキャプチャされ、[成功 (Successes)]、[警告 (Warnings)]、および [エ

ラー (Errors)] に分類されます。移行中はいつでも右上隅にある  アイコンをクリックして、ポップアップしたさまざまな通知と、それらがツールにポップアップ表示された時刻を確認できます。

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
7.7.10.1	このリリースには、次の新機能が含まれています。 • Cisco Secure Firewall 移行ツールに、トランスペアレントモードとルーテッドモードのファイアウォール コンテキストを個別に選択するオプションが追加されました。これにより、コンテキストを個別に管理および移行できるようになり、移行プロセス中の柔軟性と制御が向上します。 参照：「Select the ASA Security Context」 サポートされる移行：Cisco Secure Firewall ASA • Secure Firewall 移行ツールの [構成の最適化、確認および検証 (Optimize, Review and Validate Configuration)] ウィンドウで、NAT ルールの送信元ゾーンと接続先ゾーンを編集するオプションが追加されました。 参照：「Optimize, Review and Validate the Configuration」 サポートされる移行：Cisco Secure Firewall ASA • Cisco Secure Firewall 移行ツールが、<code>negate</code> パラメータを使用したアクセス コントロール エントリ (ACE) の移行をサポートするようになりました。 参照：「Check Point Configuration Support」 サポートされる移行：Check Point Firewall • Cisco Secure Firewall 移行ツールは、インライン セキュリティ ゾーンへのインターフェイスマッピングをサポートするようになりました。これにより、きめ細やかなポリシーの適用とトラフィック制御が可能になります。 参照：「Map PAN Interfaces to Security Zones Interface Groups」 サポートされる移行：Palo Alto Networks ファイアウォール • Cisco Secure Firewall 移行ツールを使用して、VLAN タグオブジェクトおよびその他のサポートされているオブジェクトタイプを Threat Defense デバイスに移行できるようになりました。 参照：「Optimize, Review and Validate the Configuration」 サポートされる移行：Palo Alto Networks ファイアウォール

バージョン	サポートされる機能
7.7.10	このリリースには、次の新機能が含まれています。 • Cisco Secure Firewall 移行ツールを使用して、Microsoft Azure ネイティブファイアウォールから Firewall Threat Defense に設定を移行できるようになりました。詳細と移行手順については、『Migrating Microsoft Azure Native Firewall to Cisco Secure Firewall Threat Defense with the Migration Tool』を参照してください。 • Cisco Secure Firewall 移行ツールを使用して、Check Point ファイアウォールから Multicloud Defense に設定を移行できるようになりました。詳細と移行手順については、『Migrating Check Point Firewall to Cisco Multicloud Defense with the Migration Tool』を参照してください。 • Cisco Secure Firewall 移行ツールを使用して、Fortinet ファイアウォールから Multicloud Defense に設定を移行できるようになりました。詳細と移行手順については、『Migrating Fortinet Firewall to Cisco Multicloud Defense with the Migration Tool』を参照してください。 • Cisco Secure Firewall 移行ツールが、既存のセキュリティ グループ タグ オブジェクトの設定を検出するようになりました。この検出機能は、特定のタグをユーザー、デバイス、またはシステムに関連付けることでセキュリティポリシーの管理を簡素化し、動的でスケーラブルなアクセス制御を可能にします。 「構成の最適化、確認および検証」を参照してください サポートされる移行：Cisco Secure Firewall ASA • [設定の最適化、確認、検証 (Optimize, Review and Validate Configurations)] ページで、オブジェクトまたはオブジェクトグループを追加、削除、または変更してアクセスルールを編集できるようになりました。 「構成の最適化、確認および検証」を参照してください サポートされる移行：すべて • 移行前レポートと移行後レポートが強化され、ユーザー体験が向上しました。 各セクションの CSV ファイルをダウンロードして、詳細な分析を行えるようになりました。移行後レポートに比較チャートが導入され、移行前レポートと移行後レポートでカテゴリごとに設定数を比較できます。 「構成の最適化、確認および検証」を参照してください サポートされる移行：すべて

バージョン	サポートされる機能
7.7	このリリースには、次の新機能が含まれています。 • Cisco Secure Firewall 移行ツールを使用して、Secure Firewall ASA から Multicloud Defense に構成を移行できるようになりました。詳細と移行手順については、『Migrating Cisco Secure Firewall ASA to Cisco Multicloud Defense with the Migration Tool』を参照してください。 • Cisco Secure Firewall 移行ツールを使用して、Palo Alto Networks ファイアウォールから Multicloud Defense に構成を移行できるようになりました。詳細と移行手順については、『Migrating Palo Alto Networks Firewall to Cisco Multicloud Defense with the Migration Tool』を参照してください。

バージョン	サポートされる機能
7.0.1	

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。 • ASA および FDM 管理対象デバイスやサードパーティ製ファイアウォールなどのシスコファイアウォールから Cisco Secure Firewall 1200 シリーズ デバイスに設定を移行できるようになりました。 「Cisco Secure Firewall 1200 Series」を参照してください • 複数のサイト間 VPN トンネル設定の事前共有キーを一度に更新できるようになりました。[構成の最適化、確認および検証 (Optimize, Review and Validate Configuration)] ページのサイト間 VPN テーブルを Excel シートにエクスポートし、それぞれのセルに事前共有キーを指定して、シートをアップロードします。移行ツールは、Excel から事前共有キーを読み取り、テーブルを更新します。 「構成の最適化、確認および検証」を参照してください サポートされる移行：すべて • 移行を妨げる誤った設定を無視し、移行の最終プッシュを続行することを選択できるようになりました。以前は、単一のオブジェクトのプッシュがエラーのために失敗した場合でも、移行全体が失敗していました。また、移行を手動で中止してエラーを修正し、移行を再試行することもできるようになりました。 「移行された構成の Management Center へのプッシュ」を参照してください サポートされる移行：すべて • Secure Firewall 移行ツールは、ターゲットの Threat Defense デバイスの既存のサイト間 VPN 設定を検出し、Management Center にログインせずに削除するかどうかを選択するように求めます。[いいえ (No)] を選択し、Management Center から手動で削除して移行を続行できます。 「構成の最適化、確認および検証」を参照してください サポートされる移行：すべて • 移行先の Management Center によって管理される Threat Defense デバイスのいずれかに既存のハブアンドスポークトポロジが設定されている場合は、移行ツールから、ターゲットの Threat Defense デバイスをスポークの 1 つとして既存のトポロジに追加できます。Management Center で手動で行う必要はありません。 「構成の最適化、確認および検証」を参照してください サポートされる移行：Cisco Secure Firewall ASA • サードパーティ製ファイアウォールを移行するときに、高可用性ペ

バージョン	サポートされる機能
	アの一部である Threat Defense デバイスをターゲットとして選択できるようになりました。以前は、スタンドアロンの Threat Defense デバイスのみをターゲットデバイスとして選択できました。 サポートされる移行：Palo Alto Networks、Check Point、および Fortinet ファイアウォールの移行 • Cisco Secure Firewall 移行ツールは、より強化された直感的なデモモードを提供し、すべてのステップでガイド付きの移行手順が提供されるようになりました。さらに、要件に基づいて選択してテストするターゲット Threat Defense デバイスのバージョンを確認することもできます。 サポートされる移行：すべて

バージョン	サポートされる機能
7.0	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 - 移行先の Management Center に Threat Defense の高可用性（HA）ペアを設定し、Cisco Secure Firewall ASA HA ペアから Management Center に設定を移行できるようになりました。[ターゲットの選択（Select Target）] ページで [HAペア設定を続行（Proceed with HA Pair Configuration）] を選択し、アクティブデバイスとスタンバイデバイスを選択します。アクティブな Threat Defense デバイスを選択する場合は、HA ペア設定を成功させるために、Management Center に同一のデバイスがあることを確認してください。詳細については、『Migrating Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense with the Migration Tool』の「Specify Destination Parameters for the Secure Firewall Migration Tool」を参照してください。 - ASA デバイスからサイト間 VPN 設定を移行するときに、Threat Defense デバイスを使用してサイト間ハブアンドスポーク VPN トポロジを設定できるようになりました。[構成の最適化、確認および検証（Optimize, Review and Validate Configuration）] ページの [サイト間VPNトンネル（Site-to-Site VPN Tunnels）] の下にある [ハブアンドスポークトポロジの追加（Add Hub & Spoke Topology）] をクリックします。詳細については、『Migrating Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense with the Migration Tool』の「構成の最適化、確認および検証」を参照してください。 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、SSL VPN および中央 SNAT 設定の IPv6 および複数のインターフェイスとインターフェイスゾーンを移行できるようになりました。詳細については、『Migrating Fortinet Firewall to Cisco Secure Firewall Threat Defense with the Migration Tool』の「Fortinet Configuration Support」を参照してください。

バージョン	サポートされる機能
6.0.1	

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 から Threat Defense に設定を移行する際に、ネットワークとポートのオブジェクトを最適化できるようになりました。[構成の最適化、確認および検証 (Optimize, Review and Validate Configuration)] ページの該当するタブでこれらのオブジェクトを確認し、[オブジェクトとグループの最適化 (Optimize Objects and Groups)] をクリックして、移行先の Management Center に移行する前にオブジェクトのリストを最適化します。移行ツールは、同じ値を持つオブジェクトとグループを識別し、どちらを保持するかを選択するように求めます。詳細については、「構成の最適化、確認および検証」を参照してください。 Cisco Secure Firewall Threat Defense への FDM 管理対象デバイスの移行 • FDM 管理対象デバイスから Threat Defense デバイスに DHCP、DDNS、および SNMPv3 の設定を移行できるようになりました。[機能の選択 (Select Features)] ページで、[DHCP] チェックボックスと [サーバー (Server)]、[リレー (Relay)]、および [DDNS] 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。詳細については、「構成の最適化、確認および検証」を参照してください。 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 URL オブジェクトを他のオブジェクトタイプに加えて移行できるようになりました。移行中に、[構成の最適化、確認および検証 (Optimize, Review and Validate Configuration)] ページの [オブジェクト (Objects)] ウィンドウの [URL オブジェクト (URL Objects)] タブを確認します。詳細については、「構成の最適化、確認および検証」を参照してください。 Palo Alto Networks ファイアウォールの Cisco Secure Firewall Threat Defense への移行 • Palo Alto Networks ファイアウォールから Threat Defense デバイスに URL オブジェクトを他のオブジェクトタイプに加えて移行できるようになりました。移行中に、[構成の最適化、確認および検証 (Optimize, Review and Validate Configuration)] ページの [オブジェクト (Objects)] ウィンドウの [URL オブジェクト (URL Objects)] タブを必ず確認します。詳細については、「構成の最適化、確認および検証」を参照してください。

バージョン	サポートされる機能
	Cisco Secure Firewall Threat Defense への Check Point ファイアウォールの移行 • Check Point ファイアウォールから Threat Defense デバイスにポートオブジェクト、FQDN オブジェクト、およびオブジェクトグループを移行できるようになりました。移行中に、[構成の最適化、確認および検証 (Optimize, Review and Validate Configuration)] ページの [オブジェクト (Objects)] ウィンドウを確認します。詳細については、「構成の最適化、確認および検証」を参照してください。

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。 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。

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、CDO テナントと Multicloud Defense は、必要なライセンスを保持している必要があります。

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

Cisco Multicloud Defense への移行に関する要件と前提条件

Check Point から Multicloud Defense に構成を移行するには、次の要件と前提条件を満たす必要があります。

- Multicloud Defense が有効になっている CDO テナントがある。

- Multicloud Defense の必要な運用ライセンスを購入している。



(注) 90 日の無料トライアル期間中でも有料サブスクリプションの完全な機能を体験していただけるため、この期間であっても Multicloud Defense に構成を移行できます。

- Multicloud Defense のベース URL と CDO テナント名を保持している。
- API キーを作成し、API キー作成時に、Multicloud Defense が生成する **API キー ID** と **API キーシークレット** もコピーした。詳細については、「[Create an API Key in Multicloud Defense](#)」を参照してください。

Multicloud Defense 向け Check Point ファイアウォール構成サポート

サポートされている構成

Cisco Secure Firewall 移行ツールは、Multicloud Defense への移行時に次の Check Point 構成をサポートしています。

- アクセス コントロール リスト
- ネットワーク オブジェクト
- ポート オブジェクト
- FQDN オブジェクト

移行でサポートされるソフトウェアのバージョン

Cisco Secure Firewall 移行ツールは、Check Point (r80 ~ r81) バージョンの Multicloud Defense への移行をサポートしています。

関連資料

この項では、Multicloud Defense 関連のさまざまなユーザーガイドの概要を示します。

- [Cisco Multicloud Defense User Guide](#) [英語]
- [Multicloud Defense リリースノート](#)
- [Multicloud Defense の命名規則](#)

- [Multicloud Defense コンポーネントの推奨バージョン](#)
- [Cisco Security Provisioning and Administration の Multicloud Defense](#)

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。