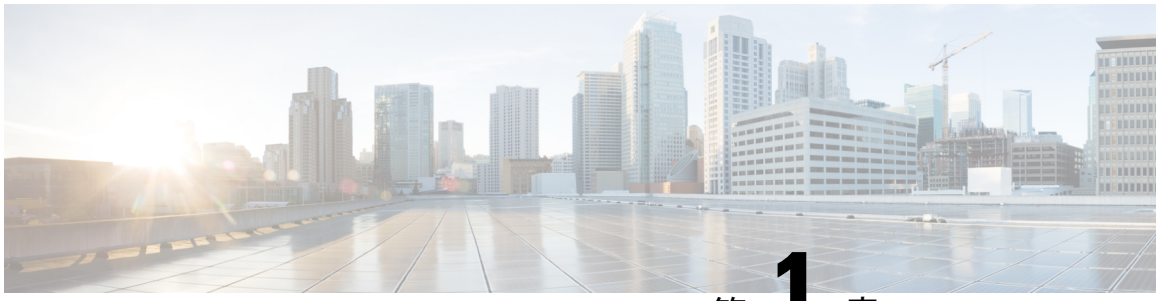
移行ツールを使用したPalo Alto Networksファイアウォールを Cisco Multicloud Defenseへの移行

最終更新：2025年7月25日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

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。

Cisco Secure Firewall 移行ツールは、サポートされている PAN 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 PAN 機能とポリシーを Multicloud Defense に自動的に移行できます。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、 PAN 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 PAN 構成の XML 行
- PAN には、Cisco Secure Firewall 移行ツールが認識できない PAN XML 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 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

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、PAN 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、 PAN 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 **Search**（🔍） 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。

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	

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 脅威に対する防御 に構成を移行できるようになりました。詳細および移行手順については、「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 Cisco Secure Firewall Threat Defense に移行する」を参照してください。 • Cisco Secure Firewall 移行ツールを使用して、チェック ポイント 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、「移行ツールを使用してチェック ポイント ファイアウォールから Cisco Multicloud Defense に移行する」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、「移行ツールを使用して Fortinet ファイアウォールから Cisco Multicloud Defenseに移行する」を参照してください。 • Cisco Secure Firewall 移行ツールは、既存のセキュリティ グループ タグ オブジェクト構成を検出できるようになりました。この検出により、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 • **[構成の最適化、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、または変更することにより、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、詳細な分析ができ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構成数を比較できます。 「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、「移行ツールを使用して Cisco Secure Firewall ASA から Cisco Multicloud Defense に移行する」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、「移行ツールを使用して Palo Alto Networks ファイアウォールから Cisco Multicloud Defense に移行する」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、Security Cloud Control 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

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 Security Cloud Control 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 Security Cloud Control 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、「Multicloud Defense で API キーを作成する」を参照してください。

Multicloud Defense 向け PAN 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 への次の PAN 構成移行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
- サービス オブジェクト
- URL オブジェクト

Multicloud Defense への移行に関するガイドラインと制限事項

Cisco Secure Firewall 移行ツールは、変換中に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 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。

サポートされている PAN 構成

Cisco Secure Firewall 移行ツールは、Multicloud Defense への次の PAN 構成移行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およびグループ
- サービス オブジェクト
- URL オブジェクト
- サービス オブジェクト グループ
- ポートオブジェクト
- 完全修飾ドメイン名（FQDN）オブジェクト

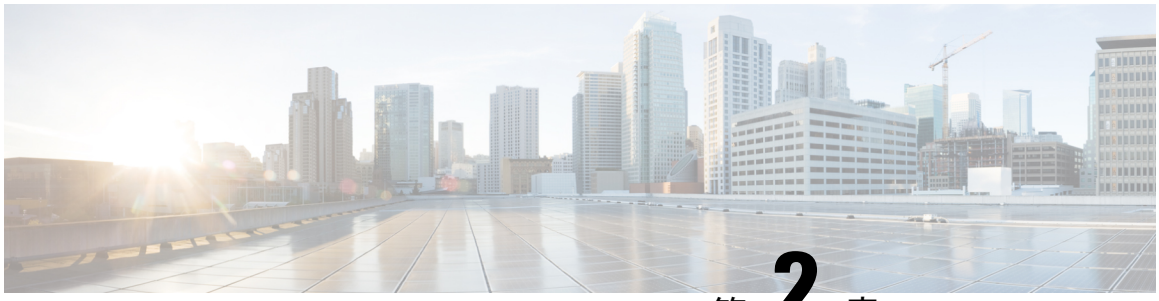
移行でサポートされるソフトウェアのバージョン

Cisco Secure Firewall ツールは、PAN ファイアウォール オペレーティング システム バージョン 8.0 以降を実行している Multicloud Defense への移行をサポートします。

関連資料

このセクションでは、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。

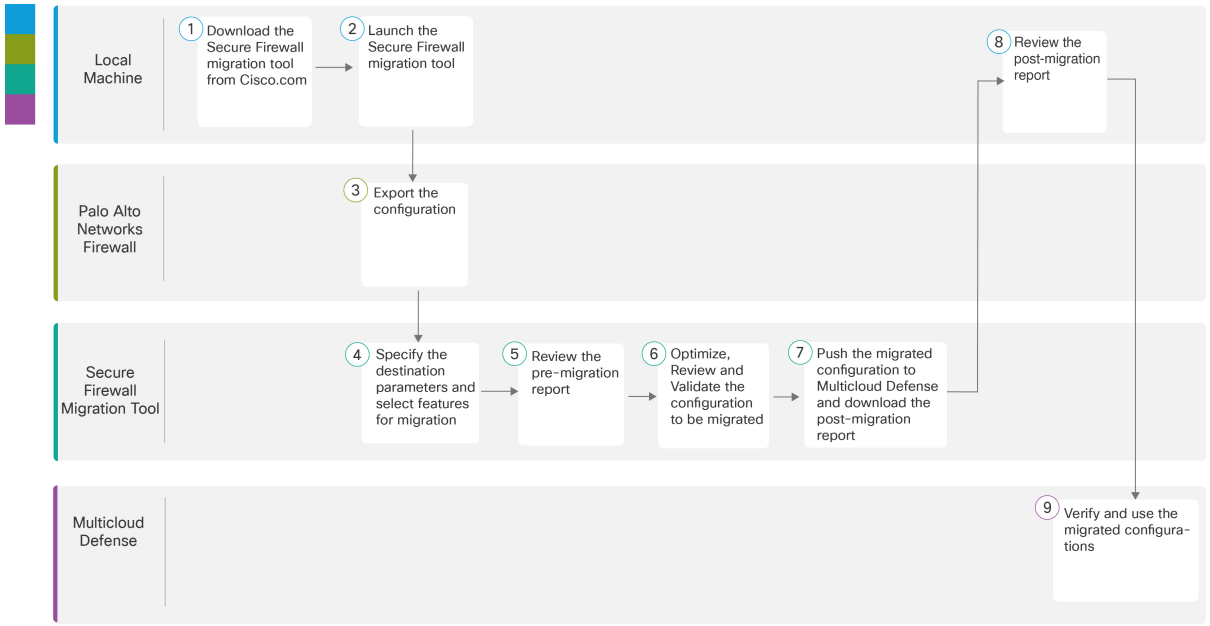
- Cisco Multicloud Defense User Guide [英語]
- Multicloud Defense リリースノート
- Multicloud Defense の命名規則
- Multicloud Defense コンポーネントの推奨バージョン
- Cisco Security Provisioning and Administration の Multicloud Defense



第 2 章

PAN から Multicloud Defense への移行フロー

エンドツーエンドの手順



	ワークスペース	手順
1	ローカルマシン	Cisco.com から Cisco Secure Firewall 移行ツールをダウンロードします。 詳細な手順については、「Cisco.com からの Cisco Secure Firewall 移行ツールのダウンロード」を参照してください。
2	Local Machine	ローカルマシンで、Cisco.comからdkした、アプリケーションファイルをダブルクリックして、Cisco Secure Firewall 移行ツールを開始します。
3	Palo Alto Networks ファイアウォール	構成ファイルをエクスポートする：Palo Alto Networks ファイアウォールから構成ファイルをエクスポートするには、「Palo Alto Networks ファイアウォールからの構成のエクスポート （29 ページ）」を参照してください。
4	Cisco Secure Firewall 移行ツール	この手順の実行中、Multicloud Defense の接続先パラメータを指定できます。手順の詳細については、Multicloud Defense の接続先パラメータを指定する （31 ページ）を参照してください。
5	Cisco Secure Firewall 移行ツール	移行前レポートをダウンロードした場所に移動し、レポートを確認します。手順の詳細については、移行前レポートの確認 （33 ページ）を参照してください。
6	Cisco Secure Firewall 移行ツール	構成を慎重に最適化して確認し、それが正しいことを確認します。手順の詳細については、移行する構成の最適化、確認および検証 （34 ページ）を参照してください。
7	Cisco Secure Firewall 移行ツール	移行プロセスのこの手順では、移行済み構成を Multicloud Defense に送信し、移行後レポートをダウンロードできるようにします。手順の詳細については、Multicloud Defense に構成をプッシュする （37 ページ）を参照してください。
8	Local Machine	移行後レポートをダウンロードした場所に移動し、レポートを確認します。手順の詳細については、移行後レポートの確認と移行の完了 （38 ページ）を参照してください。
9	Multicloud Defense	移行済み構成を確認し、必要に応じて、構成ゲートウェイで使用します。

移行の前提条件

PAN 構成を移行する前に、次のアクティビティを実行します。

Cisco.com からの Cisco Secure Firewall 移行ツールのダウンロード

始める前に

Cisco.com へのインターネット接続が可能な Windows 10 64 ビットまたは macOS バージョン 10.13 以降のマシンが必要です。

Security Cloud Control でホストされている Cisco Secure Firewall 移行ツールのクラウドバージョンを使用する場合は、手順 4 に進みます。

手順

ステップ 1 コンピュータで、Cisco Secure Firewall 移行ツール用のフォルダを作成します。

このフォルダには、他のファイルを保存しないことをお勧めします。Cisco Secure Firewall 移行ツールを起動すると、ログ、リソース、およびその他すべてのファイルがこのフォルダに配置されます。

（注）
Cisco Secure Firewall 移行ツールの最新バージョンをダウンロードする場合は、必ず新しいフォルダを作成し、既存のフォルダは使用しないでください。

ステップ 2 https://software.cisco.com/download/home/286306503/type を参照し、[Firewall移行ツール（Firewall Migration Tool）] をクリックします。

上記のリンクをクリックすると、[Firewall NGFWバーチャル（Firewall NGFW Virtual）] の [Cisco Secure Firewall移行ツール（Firewall Migration Tool）] に移動します。脅威に対する防御 デバイスのダウンロード領域から Cisco Secure Firewall 移行ツールをダウンロードすることもできます。

ステップ 3 Cisco Secure Firewall 移行ツールの最新バージョンを、作成したフォルダにダウンロードします。

Windows 用または macOS マシン用の適切な Cisco Secure Firewall 移行ツール実行可能ファイルをダウンロードします。

ステップ 4 Security Cloud Control ユーザーでそこにホストされている移行ツールを使用する場合は、Security Cloud Control テナントにログインして、左側のペインで、**[管理（Administration）]** > **[移行（Migration）]** > **[ファイアウォール移行ツール（Firewall Migration Tool）]** に移動して、移行インスタンスを作成します。

移行の実行

Cisco Secure Firewall 移行ツールの起動

このタスクは、デスクトップバージョンの Cisco Secure Firewall 移行ツールを使用している場合にのみ適用されます。Security Cloud Control でホストされている移行ツールのクラウドバージョンを使用している場合は、「Palo Alto Networks ファイアウォールからの設定のエクスポート」に進みます。

（注） 移行ツールのデスクトップバージョンを起動すると、別のウィンドウでコンソールが開きます。移行が進むのに合わせて、Cisco Secure Firewall 移行ツールの現在のステップの進行状況がコンソールに表示されます。画面にコンソールが表示されない場合は、Cisco Secure Firewall 移行ツールの背後にある可能性があります。

始める前に

- Cisco.com からの Cisco Secure Firewall 移行ツールのダウンロード
- Cisco Secure Firewall 移行ツールを実行するために、最新バージョンの Google Chrome ブラウザがコンピュータにインストールされていることを確認します。Google Chrome をデフォルトのブラウザとして設定する方法については、「Set Chrome as your default web browser」を参照してください。
- 大規模な構成ファイルを移行する場合は、移行プッシュ中にシステムがスリープ状態にならないようにスリープ設定を構成します。

手順

ステップ 1 コンピュータで、Cisco Secure Firewall 移行ツールをダウンロードしたフォルダに移動します。

ステップ 2 次のいずれかを実行します。

- Windows マシンで、Cisco Secure Firewall 移行ツールの実行可能ファイルをダブルクリックして、Google Chrome ブラウザで起動します。

  プロンプトが表示されたら、[はい（Yes）] をクリックして、Cisco Secure Firewall 移行ツールがシステムに変更を加えることができるようにします。

  （注）
  ログインポップアップの表示を妨げる可能性があるため、ブラウザのポップアップブロッカーを必ず無効にします。

Cisco Secure Firewall 移行ツールは、すべての関連ファイルを作成し、Cisco Secure Firewall 移行ツールの存在するフォルダに保存します（ログおよびリソースのフォルダを含む）。

- Mac では、Cisco Secure Firewall 移行ツールの `*.command` ファイルを目的のフォルダに移動し、ターミナルアプリケーションを起動して、Cisco Secure Firewall 移行ツールがインストールされているフォルダを参照し、次のコマンドを実行します。

  ```
  # chmod 750 Firewall_Migration_Tool-version_number.command
  ```

  ```
  # ./Firewall_Migration_Tool-version_number.command
  ```

  Cisco Secure Firewall 移行ツールは、すべての関連ファイルを作成し、Cisco Secure Firewall 移行ツールの存在するフォルダに保存します（ログおよびリソースのフォルダを含む）。

ヒント
Cisco Secure Firewall 移行ツールを開こうとすると、警告ダイアログが表示されます。これは、身元が明らかな開発者によって Cisco Secure Firewall 移行ツールが Apple に登録されていないためです。身元不明の開発者によるアプリケーションを開く方法については、「開発元が不明な Mac アプリを開く」を参照してください。

（注）
MAC のターミナルの zip メソッドを使用します。

ステップ 3 [エンドユーザライセンス契約（End User License Agreement）] ページで、テレメトリ情報をシスコと共有する場合は、[Cisco Success Network と情報を共有することに同意（I agree to share data with Cisco Success Network）] をクリックし、それ以外の場合は [後で行う（I'll do later）] をクリックします。

Cisco Success Network に統計を送信することに同意すると、Cisco.com アカウントを使用してログインするように求められます。Cisco Success Network に統計を送信しないことを選択した場合は、ローカルログイン情報を使用して Cisco Secure Firewall 移行ツールにログインします。

ステップ 4 Cisco Secure Firewall 移行ツールのログインページで、次のいずれかを実行します。

- Cisco Success Network と統計を共有するには、[CCOでログイン（Login with CCO）] リンクをクリックし、シングルサインオンログイン情報を使用して Cisco.com アカウントにログインします。Cisco.com アカウントがない場合は、Cisco.com のログインページで作成します。

  Cisco.com アカウントを使用してログインしている場合は、ステップ 8 に進みます。

- インターネットにアクセスできないエアギャップネットワークにファイアウォールを展開した場合は、Cisco TAC に連絡して、管理者のログイン情報で動作するビルドを入手してください。このビルドでは使用状況の統計がシスコに送信されず、TAC がログイン情報を提供できることに注意してください。

ステップ 5 [パスワードのリセット（Reset Password）] ページで、古いパスワードと新しいパスワードを入力し、新しいパスワードを確認します。

新しいパスワードは 8 文字以上で、大文字と小文字、数字、および特殊文字を含める必要があります。

ステップ 6 [リセット（Reset）] をクリックします。

ステップ 7 新しいパスワードでログインします。

（注）
パスワードを忘れた場合は、既存のすべてのデータを <*migration_tool_folder*> から削除し、Cisco Secure Firewall 移行ツールを再インストールします。

ステップ 8 移行前チェックリストを確認し、記載されているすべての項目を完了していることを確認します。

チェックリストの項目を 1 つ以上完了していない場合は、完了するまで続行しないでください。

ステップ 9 [新規移行（New Migration）] をクリックします。

ステップ 10 **[ソフトウェアアップデートを確認（Software Update Check）]** 画面で、Cisco Secure Firewall 移行ツールの最新バージョンを実行しているかどうかが不明な場合は、Cisco.com でバージョンを確認します。

ステップ 11 [続行（Proceed）] をクリックします。

次のタスク

次のステップに進むことができます。

- Cisco Secure Firewall 移行ツールを使用して PAN ファイアウォールから情報を抽出する必要がある場合は、「Palo Alto Networks ファイアウォールからの構成のエクスポート」に進みます。

Cisco Secure Firewall 移行ツールでのデモモードの使用

Cisco Secure Firewall 移行ツールを起動し、[送信元設定の選択（Select Source Configuration）] ページで、[移行の開始（Start Migration）] を使用して移行を開始するか、[デモモード（Demo Mode）] に入るかを選択できます。

デモモードでは、ダミーデバイスを使用してデモ移行を実行し、実際の移行フローがどのようになるかを可視化できます。移行ツールは、[送信元ファイアウォールベンダー（Source Firewall Vendor）] ドロップダウンでの選択に基づいてデモモードをトリガーします。構成ファイルをアップロードするか、ライブデバイスに接続して移行を続行することもできます。デモ FMC、デモ FTD デバイスまたは Multicloud Defenseやなどの送信元デバイスや対象デバイスを選択すると、デモの移行を実行できます。

⚠

注意 [デモモード（Demo Mode）] を選択すると、既存の移行ワークフローがあれば消去されます。[移行の再開（Resume Migration）] にアクティブな移行があるときにデモモードを使用すると、アクティブな移行は失われ、デモモードを使用した後に最初から再開する必要があります。

移行前レポートをダウンロードして確認し、実際の移行ワークフローで実行するその他のアクションを実行することもできます。ただし、デモ移行は設定の検証までしか実行できません。これはデモモードにすぎないため、選択したデモターゲットデバイスに設定をプッシュすることはできません。検証ステータスと概要を確認し、[デモモードの終了（Exit Demo Mode）] をクリックして [送信元設定の選択（Select Source Configuration）] ページに再度移動し、実際の移行を開始できます。

（注） デモモードでは、設定のプッシュを除く Cisco Secure Firewall 移行ツールのすべての機能セットを活用して、実際の移行を行う前にエンドツーエンドの移行手順のトライアルを実行できます。

Palo Alto Networks ファイアウォールからの構成のエクスポート

構成ファイルは、次の方法でエクスポートできます。

Palo Alto ファイアウォールからの構成ファイル（Panorama の管理対象外）

ゲートウェイから構成を抽出するには、次の手順を実行します。

手順

ステップ 1 [Device] > [Setup] > [Operations] に移動し、[Save Named Configuration <file_name.xml>] を選択します。

ステップ 2 [OK] をクリックします。

ステップ 3 [Device] > [Setup] > [Operations] に移動し、[Export Named Configuration] をクリックします。

ステップ 4 <file_name.xml> ファイルを選択します。

ステップ 5 [OK] をクリックします。

ステップ 6 実行構成 <file_name.xml> を含む XML ファイルを選択し、[Ok] をクリックして構成ファイルをエクスポートします。

ステップ 7 エクスポートしたファイルをファイアウォールの外部の場所に保存します。このバックアップを使用すると、構成を移行できる Cisco Secure Firewall 移行ツールをアップロードできます。

ステップ 8 （任意）接続先 NAT に同じ送信元ゾーンと接続先ゾーンがある NAT ポリシーがある場合は、次の手順を実行します。

a) ファイアウォールで CLI から **show routing route** コマンドを実行します。

b) ルーティングテーブルを .txt ファイルにコピーします。

c) この .txt ファイルをフォルダに追加します。このフォルダで .txt ファイルと .xml ファイル（panconfig.xml を含む）を圧縮します。

これらのステップは、移行に必須ではありません。これらのステップを実行しないと、接続先ゾーンは Cisco Secure Firewall 移行ツールでの移行中にマッピングされず、移行レポートに含まれます。

（注）
show routing route コマンドを使用して、ルーティングテーブルの詳細を抽出します。抽出した出力をメモ帳に貼り付けます。

Palo Alto ファイアウォールからの構成ファイル（Panorama の管理対象）

デバイスが Panorama で管理されている場合は、ゲートウェイから設定を抽出する必要があります。Panorama 設定をゲートウェイと統合し、設定を抽出します。

Cisco Secure Firewall 移行ツールのユーザーインターフェイスで、次の手順を実行します。

始める前に

スーパーユーザーアカウントを使用して、Palo Alto ファイアウォールの Web UI にログインします。

手順

ステップ 1 **[デバイス（Device）] > [サポート（Support）] > [テクニカルサポートファイル（Tech Support File）]**に移動します。

ステップ 2 **[テクニカルサポートファイルの生成（Generate Tech Support File）]**をクリックします。

ステップ 3 生成されたファイルが利用可能になったら、[テクニカルサポートファイルのダウンロード（Download Tech Support File）] をクリックします。

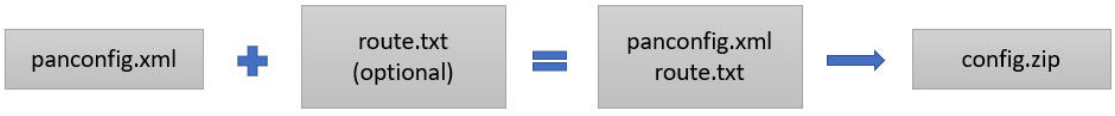
ステップ 4 ファイルを解凍して展開し、パス *\opt\pancfg\mgmt\saved-configs* に移動して、*merged-running-config.xml* ファイルを取得します。

次のタスク

エクスポートされたファイルの圧縮

エクスポートされたファイルの圧縮

Palo Alto Gateway ファイアウォールの panconfig.xml、および route.txt をエクスポートします（同じ送信元ゾーンと宛先ゾーンを持つ NAT ルールがある場合）。



Multicloud Defense の接続先パラメータを指定する

始める前に

- Multicloud Defense が有効JTAPIになっている Security Cloud Control テナントがある。
- Multicloud Defense に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 Security Cloud Control 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、「Multicloud Defense で API キーを作成する」を参照してください。

手順

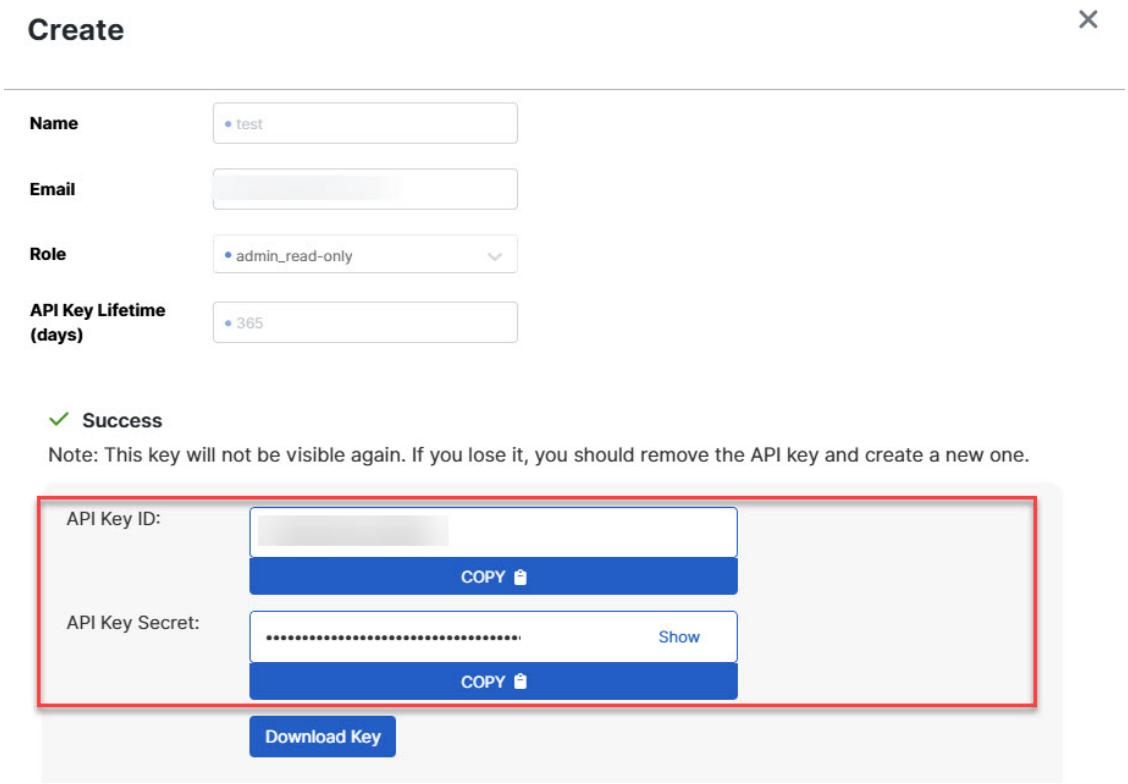
ステップ 1 **[ターゲットを選択（Select Target）]** ウィンドウで、**Multicloud Defense** を選択します。

ステップ 2 対応するフィールドに次のパラメータを指定して、移行ツールと Multicloud Defense 間の接続を確立します。

- **ベース URL の入力**：これは、Multicloud Defense コントローラに接続する際にブラウザで確認できるベース URL です。たとえば、コントローラダッシュボードで、**/dashboard** の部分を除くブラウザ上のリンクをコピーします。URL は https://xxxx.mcd.apj.cdo.cisco.com のようになります。
- **テナント名の入力**：Security Cloud Control テナントの名前。Multicloud Defense ウィンドウにいる場合は、右上の [プロファイル（Profile）] ドロップダウンから、Security Cloud Control ウィンドウにいる場合は、**[管理（Administration）]** > **[一般設定（General Settings）]** からコピーします。
- **API キー ID の入力**：**[システムとアカウント（System and Accounts）]** > **[API キー（API Keys）]** の順番に選択して、API キーを作成する際に、Multicloud Defense コントローラが生成する**API キー ID**。キーの名前、E メールアドレス、API キーに必要なロール、API キーに付与するロールおよびキーを生成するための API キーの有効期間を指定します。キーのデフォルトの有効期間は、365 日に設定されています。
- **APIキーシークレットの入力**：APIキーの作成時に Multicloud Defense コントローラが生成する **API キーシークレット** 。

（注）

API キーの作成時にのみ表示される **API キー ID** と **API キーシークレット**の両方をコピーしてください。コピーし忘れた場合は、作成した API キーを削除して新しいキーを生成し、今回は必ずコピーしてください。



ステップ 3 **[接続（Connect）]** をクリックし、Multicloud Defense への接続試行が成功したことを確認する**「正常に収集済み」**メッセージを受信するまで待機します。

ステップ 4 **[機能を選択（Select Features）]** を使用すると、Multicloud Defense に移行する構成を選択できます。**[アクセス制御（Access Control）]** および **[参照オブジェクトのみを移行（Migrate Only Reference Objects）]** チェックボックスはデフォルトでオンになっています。

この移行では、インターフェイスやルートなどの送信元ファイアウォールからのその他の構成はサポートされていないのでご注意ください。

ステップ 5 **[続行（Proceed）]**、**[変換を開始（Start Conversion）]** の順に選択します。移行ツールが送信元の構成を解析するまで待機します。

ステップ 6 Cisco Secure Firewall 移行ツールによって変換された要素の概要を確認します。

構成ファイルが正常にアップロードおよび解析されたかどうかを確認するには、移行を続行する前に**移行前レポート**をダウンロードして確認します。

ステップ 7 [レポートのダウンロード（Download Report）] をクリックし、**移行前レポート**を保存します。

移行前レポートのコピーも、Cisco Secure Firewall 移行ツールと同じ場所にある *Resources* フォルダに保存されます。

ステップ 8 **[次へ（Next）]** をクリックします。

移行前レポートの確認

移行中に移行前レポートをダウンロードし忘れた場合は、次のリンクを使用してダウンロードしてください。

移行前レポートのダウンロードエンドポイント：http://localhost:8888/api/downloads/pre_migration_summary_html_format

（注） レポートは、Cisco Secure Firewall 移行ツールの実行中にのみダウンロードできます。

手順

ステップ 1 移行前レポートをダウンロードした場所に移動します。

移行前レポートのコピーも、Cisco Secure Firewall 移行ツールと同じ場所にある `Resources` フォルダに保存されます。

ステップ 2 移行前レポートを開き、その内容を慎重に確認して、移行が失敗する原因となる問題を特定します。

移行前レポートには、次の情報が含まれています。

- 脅威に対する防御 または Multicloud Defense への移行に成功したサポートされている 構成要素と移行用に選択された特定の 機能のサマリー。
- **エラーがある構成行**：Cisco Secure Firewall 移行ツールが解析できなかったために正常に移行できない 構成要素の詳細。 構成でこれらのエラーを修正し、新しい構成ファイルをエクスポートしたら、新しい構成ファイルを Cisco Secure Firewall 移行ツールにアップロードして、続行します。
- **無視された構成**：Multicloud Defense または Cisco Secure Firewall 移行ツールがサポートしていないために無視された 構成要素の詳細。Cisco Secure Firewall 移行ツールはこれらの行を解析しません。これらの行を確認し、各機能が Multicloud Defense でサポートされているかどうかを確認します。サポートされている場合は、機能を手動で構成することを計画します。

ステップ 3 **移行前レポート**で修正措置が推奨されている場合は、インターフェイスで、これらの修正を完了し、再度 構成ファイルをエクスポートし、更新された構成ファイルをアップロードして、続行します。

ステップ 4 構成ファイルを正常にアップロードし、解析したら、Cisco Secure Firewall 移行ツールに戻り、**[次へ（Next）]** をクリックして移行を続行します。

移行する構成の最適化、確認および検証

始める前に

[設定の最適化、確認および検証（Optimize, Review and Validate Configuration）] ページでは、ターゲット Multicloud Defense に移行しようとしている構成パラメータを確認および検証できます。このステップでは、移行ツールは Multicloud Defense の既存の構成に対して構成を検証し、ターゲット Multicloud Defense での重複を避けるために、アクセス制御ルールの関連付けやオブジェクト名の変更など、移行を成功させるために実行する必要がある変更を提案します。

検証後にタブが点滅している場合は、タブで実行する必要があるアクションがあることを示します。

手順

ステップ 1 すべてのアクセス制御リスト（ACL）エントリを一覧する **[アクセス制御（Access Control）]** タブで、次を実行します。

- **[ACLを最適化（Optimize ACL）]** をクリックすると、移行ツールがすべてのシャドウ ACL と冗長 ACL を識別し、無効な ACL として移行するか、移行から除外するかを選択できます。

  Cisco Secure Firewall 移行ツールの ACL 最適化の概要

  Cisco Secure Firewall 移行ツールは、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。たとえば、2 つのルールが同じネットワーク上で FTP および IP トラフィックを許可し、アクセスを拒否するルールが定義されていない場合、最初のルールを削除できます。
  - 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。2 つのルールに同様のトラフィックがある場合、2 番目のルールはアクセスリストの後半に表示されるため、どのトラフィックにも適用されません。2 つのルールがトラフィックに対して異なるアクションを指定している場合、シャドウイングされたルールを移動するか、いずれかのルールを編集して必要なポリシーを実装できます。たとえば、特定の送信元または宛先に対して、基本ルールで IP トラフィックを拒否し、シャドウイングされたルールで FTP トラフィックを許可できます。

Cisco Secure Firewall 移行ツールは、ACL 最適化のルールを比較する際に次のパラメータを使用します。

- 無効化された ACL は、最適化プロセス中に考慮されません。
- 送信元の ACL は、対応する ACE（インライン値）に展開された後、次のパラメータについて比較されます。
  - 送信元と宛先のネットワーク
  - 送信元/宛先ポート

[レポートのダウンロード（Download Report）] をクリックして、ACL 名と、対応する冗長 ACL およびシャドウされた ACL を Excel ファイルで表形式で確認します。ACL の詳細情報を表示するには、[詳細なACL情報（Detailed ACL Information）] シートを使用します。

[続行（Proceed）] をクリックして、最適化プロセスを開始します。

- テーブル内の各エントリについて、マッピングを確認し、それらが正しいことを確認します。

  移行済みのアクセスポリシールールは、ACL名をプレフィックスとして使用し、ACLルール番号を追加することで、構成ファイルにマッピングしやすくします。たとえば、ACLの名前が、「inside_access」の場合、ACL の最初のルール（または ACE）行の名前は、「inside_access_#1.」になります。TCP または UDP の組み合わせ、拡張サービスオブジェクト、またはその他の理由でルールを拡張する必要がある場合、Cisco Secure Firewall 移行ツールは名前に番号付きサフィックスを追加します。たとえば、許可ルールが移行のために 2 つのルールへ拡張される場合、それらのルールには "inside_access_#1-1" と "inside_access_#1-2" という名前が付けられます。

  サポートされていないオブジェクトを含むルールの場合、Cisco Secure Firewall 移行ツールは名前に "_UNSUPPORTED" というサフィックスを追加します。

- 移行しない場合、または一部の ACL を無効として移行する場合は、行のチェックボックスをオンにし、**[アクション（Actions）]**をクリックして、該当するオプションを選択します。一括変更を実行するには、**[すべてのエントリを選択（Select all entries）]** チェックボックスをオンにします。
- アクセス制御リストポリシーを編集するには。ポリシーのチェックボックスをオンにして行を選択し、**[アクション（Actions）]** > **[編集（Edit）]** の順に選択します。

  該当しないすべてのルールは、テーブルでグレーアウトされます。

ステップ 2 **[オブジェクト（Objects）]** タブでは、次を実行できます。

次のタブを選択し、マッピングを確認します。

- 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

- URL オブジェクト

オブジェクト名を変更する場合は、オブジェクトの行のチェックボックスをオンにし、**[アクション（Actions）]** をクリックして **[名前を変更（Rename）]** を選択します。一括変更を実行するには、**[すべてのエントリを選択（Select all entries）]** チェックボックスをオンにします。

ステップ 3 確認が完了したら、[検証（Validate）] をクリックします。注意が必要な必須フィールドは、値を入力するまで点滅し続けることに注意してください。**[検証（Validate）]** ボタンは、すべての必須フィールドに入力した後にのみ有効になります。

検証中、Cisco Secure Firewall 移行ツールは Multicloud Defense に接続し、既存のオブジェクトを確認し、それらのオブジェクトを移行対象オブジェクトのリストと比較します。オブジェクトがすでに Multicloud Defense に存在する場合、Cisco Secure Firewall 移行ツールは次の処理を実行します。

- オブジェクトの名前と構成が同じ場合、Cisco Secure Firewall 移行ツールは既存のオブジェクトを再利用し、Multicloud Defense に新しいオブジェクトを作成しません。
- オブジェクトの名前が同じで構成が異なる場合、Cisco Secure Firewall 移行ツールはオブジェクトの競合を報告します。

検証の進行状況はコンソールで確認できます。

ステップ 4 検証が完了し、[検証ステータス（Validation Status）] ダイアログボックスに 1 つ以上のオブジェクトの競合が表示された場合は、次の手順を実行します。

a) [競合の解決（Resolve Conflicts）] をクリックします。

Cisco Secure Firewall 移行ツールは、オブジェクトの競合が報告された場所に応じて、[ネットワークオブジェクト（Network Objects）] タブまたは [ポートオブジェクト（Port Objects）] タブのいずれかまたは両方に警告アイコンを表示します。

b) タブをクリックし、オブジェクトを確認します。
c) 競合がある各オブジェクトのエントリを確認し、**[アクション（Actions）]** > **[競合の解決（Resolve Conflicts）]** を選択します。
d) [競合の解決（Resolve Conflicts）] ウィンドウで、推奨アクションを実行します。

たとえば、既存の Multicloud Defense オブジェクトとの競合を避けるために、オブジェクト名にサフィックスを追加するように求められる場合があります。デフォルトのサフィックスを受け入れるか、独自のサフィックスに置き換えることができます。

e) [解決（Resolve）] をクリックします。
f) タブ上のすべてのオブジェクトの競合を解決したら、[保存（Save）] をクリックします。
g) [検証（Validate）] をクリックして構成を再検証し、すべてのオブジェクトの競合を解決したことを確認します。

ステップ 5 検証が完了し、**[検証状態（Validation Status）]** ダイアログボックスに、**「検証成功」** というメッセージが表示されたら、引き続き Multicloud Defense に構成をプッシュします。

Multicloud Defense に構成をプッシュする

始める前に

構成を正常に検証しておらず、すべてのオブジェクト競合を解決していない場合、構成を Multicloud Defense にプッシュできません。

（注） Cisco Secure Firewall 移行ツールが 構成を Multicloud Defense に送信中は、構成を変更したりデバイスにデプロイしたりしないでください。

手順

ステップ 1 [検証ステータス（Validation Status）] ダイアログボックスで、検証の概要を確認します。

ステップ 2 **[構成をプッシュ（Push Configuration）]** をクリックして、送信元ファイアウォール構成を Multicloud Defense に送信します。

Cisco Secure Firewall 移行ツールに、移行の進行状況の概要が表示されます。コンソールに、Multicloud Defense にプッシュされているコンポーネントの詳細な進行状況を行ごとに表示できます。

（注）
一括設定プッシュの実行中にエラーのある設定がある場合、移行ツールは警告をスローし、移行を中止してエラーを手動で修正するか、誤った設定を除外して移行を続行することを求めます。エラーのある設定を表示してから、[移行の続行（Continue with migration）] または [中止（Abort）] を選択できます。移行を中止する場合は、トラブルシューティング バンドルをダウンロードし、分析のために Cisco TAC と共有できます。

移行を続行する場合は、移行ツールは移行を部分的に成功した移行として扱います。移行後レポートをダウンロードして、プッシュエラーが原因で移行されなかった設定のリストを表示できます。

ステップ 3 移行が完了したら、[レポートのダウンロード（Download Report）] をクリックして、移行後レポートをダウンロードして保存します。

移行後レポートのコピーも、Cisco Secure Firewall 移行ツールと同じ場所にある `Resources` フォルダに保存されます。

ステップ 4 移行できなかった場合、移行後レポート、ログファイル、未解析構成ファイルを慎重に確認し、失敗の原因を把握します。

トラブルシューティングについては、サポートチームに問い合わせることもできます。

移行の失敗のサポート

移行に失敗する場合は、サポートにお問い合わせください。

1. [移行完了（Complete Migration）] 画面で、[サポート（Support）] ボタンをクリックします。

   [ヘルプ（Help）] サポートページが表示されます。

2. [サポートバンドル（Support Bundle）]チェックボックスをオンにして、ダウンロードする構成ファイルを選択します。

   （注）
   ログファイルと DB ファイルは、デフォルトでダウンロード用に選択されています。

3. [ダウンロード（Download）] をクリックします。

   サポートバンドルファイルは、ローカルパスに.zip としてダウンロードされます。zip フォルダを解凍して、ログファイル、DB、構成ファイルを確認します。

4. [Email us] をクリックして、テクニカルチームに障害の詳細を電子メールで送信します。

   ダウンロードしたサポートファイルを電子メールに添付することもできます。

5. [TAC ページに移動（Visit TAC page）] をクリックして、シスコのサポートページで TAC ケースを作成します。

   （注）
   TAC ケースは、移行中にいつでもサポートページからオープンできます。

移行後レポートの確認と移行の完了

始める前に

移行後レポートには、さまざまなカテゴリの ACL カウント、ACL 最適化、および構成ファイルで実行された最適化の全体的なビューに関する詳細が表示されます。

手順

ステップ 1 **移行後レポート**をダウンロードした場所に移動します。

ステップ 2 移行後レポートを開き、その内容を慎重に確認して、ソース構成がどのように移行されたかを理解します。

1. **移行の概要**：Multicloud Defense へのソースファイアウォールから正常に移行された構成の概要。

   また、移行前の状態と移行後の状態の差異を示す比較チャートも確認できます。

2. **オブジェクト競合処理**：Multicloud Defense に既存しているオブジェクトと競合していると識別されたオブジェクトの詳細。オブジェクトの名前と設定が同じ場合、Cisco Secure Firewall 移行ツールは Multicloud Defense オブジェクトを再利用しています。オブジェクト

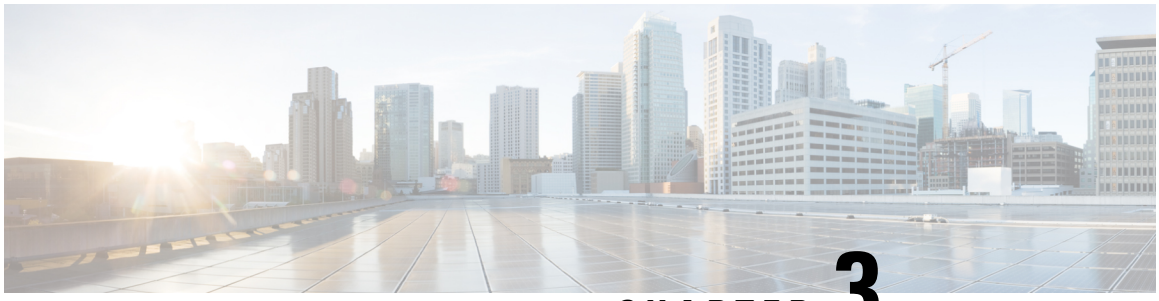
の名前が同じで構成が異なる場合は、管理者がそれらのオブジェクトの名前を変更しています。これらのオブジェクトを慎重に確認し、競合が適切に解決されたことを確認します。

3. **移行しないと判断したアクセス制御ルール**：Cisco Secure Firewall ツールを使用して移行しないと判断したルールの詳細。Cisco Secure Firewall 移行ツールによって無効化され、移行されなかったこれらのルールを確認します。これらの行を確認し、選択したすべてのルールがこのセクションにリストされていることを確認します。必要に応じて、これらのルールを手動で構成できます。
4. **一部移行済み構成**：高度なオプションなしで移行できる高度なオプション付きルールを含む、一部のみ移行されたルールの詳細。これらの行を確認し、詳細オプションが Multicloud Defense でサポートされているかどうかを確認します。サポートされている場合は、これらのオプションを手動で構成します。
5. **サポートされない構成**：Cisco Secure Firewall 移行ツールがこれらの機能の移行をサポートしないため、移行されなかったソースファイアウォール構成要素の詳細。これらの行を確認し、各機能が Multicloud Defense でサポートされているかどうかを確認します。その場合は、Multicloud Defense でこれらの機能を手動で構成します。
6. **拡張アクセス制御ポリシー**：移行中に単一ポイントルールから複数 Multicloud Defense ルールに拡張されたソースファイアウォールのアクセス制御ポリシーの詳細。
7. **Actions Taken on Access Control Rules**
   - **移行しないと判断したアクセスルール**：Cisco Secure Firewall ツールを使用して移行しないと判断したアクセス制御の詳細。これらの行を確認し、選択したすべてのルールがこのセクションにリストされていることを確認します。必要に応じて、Multicloud Defense でこれらのルールを手動で構成できます。
   - Access Rules with Rule Action Change：Cisco Secure Firewall 移行ツールを使用して「ルールアクション」が変更されたすべてのアクセス コントロール ポリシー ルールの詳細。ルールアクションの値は、Allow、Trust、Monitor、Block、Block with reset です。これらの行を確認し、選択したすべてのルールがこのセクションにリストされていることを確認します。必要に応じて、Multicloud Defense でこれらのルールを手動で構成できます。

（注）
サポートされていないルールが移行されなかった場合、不要なトラフィックがファイアウォールを通過する問題が発生します。このトラフィックがブロックされるように、Multicloud Defense でルールを構成することをお勧めします。

ステップ 3 **移行前レポート**を開き、Multicloud Defense で手動で移行する必要がある構成項目をメモします。

ステップ 4 移行されたすべての構成パラメータが、Multicloud Defense で使用できることを確認します。



CHAPTER 3

Cisco Success Network：テレメトリデータ

Cisco Success Network - テレメトリデータ

Cisco Success Network は、Cisco Secure Firewall 移行ツールの常時接続使用状況の情報とメトリックの収集機能であり、移行ツールと Cisco Cloud 間のセキュアなクラウド接続を介して使用統計を収集および送信します。これらの統計は、未使用の機能に関する追加のサポートを提供し、製品を改善するのに役立ちます。Cisco Secure Firewall 移行ツールで移行プロセスを開始すると、対応するテレメトリデータファイルが生成され、固定の場所に保存されます。

移行済み 構成を Management Center またはMulticloud Defense にプッシュすると、プッシュサービスはその場所からテレメトリデータファイルを読み取り、データがクラウドに正常にアップロードされた後に削除します。

移行ツールには、テレメトリデータのストリーミング用に、**[限定（Limited）]** と **[広範（Extensive）]** の 2 つのオプションが用意されています。

Cisco Success Network を **[限定（Limited）]** に設定すると、次のテレメトリデータポイントが収集されます。

表 *1*:限定的なテレメトリ

データ ポイント	説明	値の例
時刻	テレメトリデータが収集された日時	2025-03-17 17:02:01
ソース タイプ	送信元デバイスタイプ	Palo Alto
Source Device Version	Palo Alto デバイスのバージョン	N/A
送信元のバージョン	Palo Alto のバージョン	8.0

データ ポイント	説明	値の例
Target Management Version	管理センターのターゲットバージョン	6.2.3 以降
Target Management Type	ターゲット管理デバイスのタイプ、つまり管理センター	Management Center
Target Device Version	ターゲットデバイスのバージョン	7.6
Target Device Model	ターゲットデバイスのモデル	Cisco Firepower Threat Defense for VMware
Migration Tool Version	移行ツールのバージョン	7.7
移行ステータス	Management Center への Palo Alto 構成の移行状態	SUCCESS

次の表に、**Cisco Success Network** が **[広範（Extension）]** に設定されている場合のテレメトリデータポイント、その説明、およびサンプル値に関する情報を示します。

表 *2:* 広範なテレメトリ

データ ポイント	説明	値の例
オペレーティングシステム	Cisco Secure Firewall 移行ツールを実行するオペレーティングシステム。Windows7、Windows10 64-bit、macOS High Sierra を使用できます	Windows 7
ブラウザ	Cisco Secure Firewall 移行ツールの起動に使用されるブラウザ。Mozilla/5.0、Chrome/68.0.3440.106、Safari/537.36 を使用できます	Mozilla/5.0

表 *3:* ターゲット管理デバイス（*Management Center*）情報

データ ポイント	説明	値の例
Target Management Type	ターゲット管理デバイスのタイプ（Management Center）	Management Center
Target Device Version	ターゲットデバイスのバージョン	75
Target Device Model	ターゲットデバイスのモデル	VMware 向け Cisco Secure Firewall Threat Defense

表 *4 :* 移行の概要

データ ポイント	説明	値の例
アクセス コントロール ポリシー		
Name	アクセス コントロール ポリシーの名前	存在しない
Partially Migrated ACL Rule Counts	部分的に移行された ACL ルールの合計数	3
Expanded ACP Rule Counts	拡張 ACP ルールの数	0
NAT ポリシー		
Name	NAT ポリシーの名前	存在しない
NAT Rule Counts	移行された NAT ルールの合計数	0
Partially Migrated NAT Rule Counts	部分的に移行された NAT ルールの合計数	0
その他の移行詳細		
Interface Counts	更新されたインターフェイスの数	0
Sub Interface Counts	更新されたサブインターフェイスの数	0
Static Routes Counts	静的ルートの数	0
Objects Counts	作成されたオブジェクトの数	34
Object Group Counts	作成されたオブジェクトグループの数	6
Security Zone Counts	作成されたセキュリティゾーンの数	3
Network Object Reused Counts	再利用されたオブジェクトの数	21
Network Object Rename Counts	名前が変更されたオブジェクトの数	1
Port Object Reused Counts	再利用されたポートオブジェクトの数	0
Port Object Rename Counts	名前が変更されたポートオブジェクトの数	0

表 *5 : Cisco Secure Firewall* 移行ツールのパフォーマンスデータ

データ ポイント	説明	値の例
Conversion Time	構成行の解析にかかった時間（分）	14
Migration Time	エンドツーエンドの移行にかかった合計時間（分）	592

データ ポイント	説明	値の例
Config Push Time	最終構成のプッシュにかかった時間（分）	7
Migration Status	構成の Management Center への移行のステータス	SUCCESS
Error Message	Cisco Secure Firewall 移行ツールによって表示されるエラーメッセージ	null
Error Description	エラーが発生した段階および考えられる根本原因に関する説明	null

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。