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

最終更新：2025年2月27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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.

目 次

第 1 章

Cisco Secure Firewall 移行ツールのスタートアップガイド 1

Cisco Secure Firewall 移行ツールについて 1

Cisco Secure Firewall 移行ツールの最新情報 5

Cisco Secure Firewall 移行ツールのライセンス 19

Cisco Secure Firewall 移行ツールのプラットフォーム要件 19

Threat Defense デバイスの要件および前提条件 20

注意事項と制約事項 20

移行がサポートされるプラットフォーム 24

サポートされる移行先の管理センター 25

移行でサポートされるソフトウェアのバージョン 27

第 2 章

Palo Alto Networks ファイアウォールから Threat Defense への移行ワークフロー 29

エンドツーエンドの手順 29

移行の前提条件 31

Cisco.com からの Cisco Secure Firewall 移行ツールのダウンロード 31

移行の実行 32

Cisco Secure Firewall 移行ツールの起動 32

Cisco Secure Firewall 移行ツールでのデモモードの使用 34

Palo Alto Networks ファイアウォールからの構成のエクスポート 35

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） 35

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） 36

エクスポートされたファイルの圧縮 36

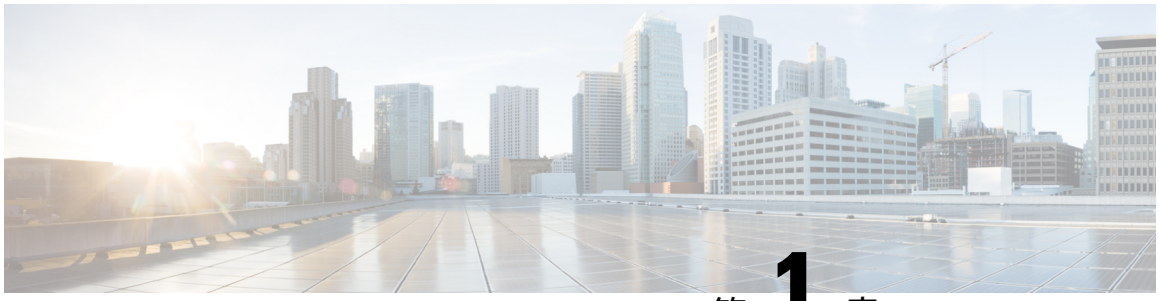
Cisco Secure Firewall 移行ツールの接続先パラメータの指定 37

移行前レポートの確認 41

PAN ファイアウォール 構成と Threat Defense インターフェイスのマッピング 42
セキュリティゾーンインターフェイスグループ への PAN インターフェイスのマッピング 44
構成とアプリケーションのマッピング 45
最適化、 構成の確認と検証 48
移行された構成の以下へのプッシュ： Management Center 55
移行後レポートの確認と移行の完了 57
解析のサマリー 60
移行の失敗 61
Cisco Secure Firewall 移行ツールのアンインストール 61
移行例： PAN から Threat Defense 2100 へ 62
メンテナンス期間前のタスク 62
メンテナンス期間のタスク 63

第 3 章 **Cisco Success Network：テレメトリデータ** 65
Cisco Success Network - テレメトリデータ 65

第 4 章 **移行の問題のトラブルシューティング** 69
Cisco Secure Firewall 移行ツールのトラブルシューティング 69
トラブルシューティングに使用されるログおよびその他のファイル 70
PAN のトラブルシューティング例：オブジェクトグループのメンバーが見つからない 70



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 （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 （19 ページ）
- Cisco Secure Firewall 移行ツールのプラットフォーム要件 （19 ページ）
- Threat Defense デバイスの要件および前提条件 （20 ページ）
- 注意事項と制約事項 （20 ページ）
- 移行がサポートされるプラットフォーム （24 ページ）
- サポートされる移行先の管理センター （25 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 （27 ページ）

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： PAN から Threat Defense 2100 へ）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 PAN 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 PAN 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 PAN 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。

- 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

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**、 PAN 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。

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
7.0.1	

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。 • Secure Firewall 移行ツール は、ルールごとのアプリケーションによるアクセス制御リスト（ACL）の分割をサポートするようになりました。Palo Alto Networks ファイアウォール設定に、1 つのルールが複数のアプリケーションに設定されたACLが含まれている場合は、**ルールごとのアプリケーションによる ACL の分割**オプションを使用して、1 つのルールにつきアプリケーションが 1 つの複数のルールに分割できます。移行ツールは、1 つのアプリケーションに対して1つのルールが設定されるように新しいルールを作成します。これにより、設定の確認と検証がより明確になります。 • 移行ツールは、ダイナミック IP またはポートフォールバック アドレスの送信元ファイアウォールのNAT設定を検証し、フォールバックアドレスが宛先ゾーンアドレスと同じである場合にのみ設定を移行するようになりました。これは Cisco Secure Firewall Management Center が、ダイナミック IP またはポート フォールバック インターフェイスとして宛先アドレスしか持てないためです。 • 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。.

バージョン	サポートされる機能
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。 • Secure Firewall 移行ツール は、Management Center バージョン 7.1 以降に移行するときに、変換された宛先で完全修飾ドメイン名（FQDN）オブジェクトを使用するネットワークアドレス変換（NAT）ルールをサポートするようになりました。 **重要** 変換されたソースに FQDN オブジェクトまたは FQDN オブジェクトグループがある NAT ルール、元のソースと宛先の両方に FQDN オブジェクトと FQDN オブジェクトグループがある NAT ルール、および変換された宛先に FQDN オブジェクトグループがある NAT ルールはサポートされていません。 • ACL の最適化が強化され、最適化されたアプリケーションを一覧表示する新しい [アプリケーション（Application）] 列が移行後レポートに含まれるようになりました。
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、Palo Alto Networks 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。

バージョン	サポートされる機能
2.1	• PAN OS バージョン 6.1.x 以降をサポートします。 • Cisco Secure Firewall 移行ツールを使用すると、次の PAN の構成要素を 脅威に対する防御 に移行できます。 • インターフェイス • 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 • ポートオブジェクトおよびポートグループ • アクセスコントロールリスト（ポリシー） • ゾーン • アプリケーション • NAT ルール • [確認と検証（Review and Validate）] ページで使用可能なコンテンツベースの検索機能。 • UI の機能が強化され、進行状況バーが表示されるようになりました。

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

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。PAN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。
- ターゲットの Threat Defense デバイスは、高可用性構成にすることができます。
- 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。クラスタの一部になることは**できません**。
  - 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、PAN 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。

注意事項と制約事項

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 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、NAT ルール、およびルートを移行しません。

PAN 構成の制約事項

送信元 PAN 構成の移行には、次の制限があります。

- Cisco Secure Firewall 移行ツールを使用すると、マルチ VSYS を移行できます。
- システム構成は移行されません。
- Management Center では、ネストされたサービス オブジェクト グループまたはポートグループはサポートされていません。変換の一環として、Cisco Secure Firewall 移行ツールは、参照されているネストされたオブジェクトグループまたはポートグループの内容を展開します。
- Cisco Secure Firewall 移行ツールは、1 つの回線にある送信元ポートと宛先ポートを持つ拡張サービスのオブジェクトまたはグループを、複数の回線にまたがる異なるオブジェクトに分割します。このようなアクセスコントロールルールの参照は、同じ意味の Management Center ルールに変換されます。

PAN 移行の注意事項

Cisco Secure Firewall 移行ツールは、次のような 脅威に対する防御 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、脅威に対する防御 のベストプラクティスに従います。ルールのログオプションは、送信元PAN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。

サポートされる PAN 構成

Cisco Secure Firewall 移行ツールは、次の PAN 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
- ゾーン（レイヤ 2、レイヤ 3、仮想ワイヤ）
- 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（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 変換のサポート（インターフェイス、スタティックルート、オブジェクト、ACL）
- アクセス ルール
- NAT ルール

（注） サービスに「application-default」が設定されているすべてのポリシーは、「any」として移行されます。脅威に対する防御 には同等の機能がないためです。

変換済み送信元と元の宛先には、「any」オブジェクトが Management Center で事前定義されていません。したがって、0.0.0.0/0 を持つ Obj_0.0.0.0 という名前のオブジェクトが作成され、プッシュされます。

- 変換された宛先に FQDN オブジェクトがある NAT ルール（バージョン 7.1 以降を実行している Secure Firewall Threat Defense に移行する場合）
- 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、移行時に常に VLAN ID と同じ番号に設定されます）
- 集約インターフェイス（ポートチャネル）
- 静的ルート（移行されない Next VR および ECMP のルートとしてネクストホップが設定されているルートを除く）

（注） 送信元ファイアウォール（PAN）に静的ルートとして設定されたルートが接続されている場合、プッシュの失敗が発生します。Management Center では、接続済みルートの静的ルートを作成できません。そのようなルートを削除し、移行を続行します。

（注） 仮想ワイヤインターフェイスは移行されませんが、仮想ワイヤゾーンは移行されます。移行後、脅威に対する防御 で BVI インターフェイスを手動で作成する必要があります。

部分的にサポートされる PAN 構成

Cisco Secure Firewall 移行ツールは、次の PAN 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。

- プロファイルを使用したアクセス コントロール ポリシー ルール
- 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 タイプが削除され、サービスグループが部分的に移行されます。

- サポートされているオブジェクトとサポートされていないオブジェクトを含むオブジェクトグループは、サポートされていないオブジェクトを削除することによって移行されます。

サポートされない PAN 構成

Cisco Secure Firewall 移行ツールは、次の PAN 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。

- 時間ベースのアクセス コントロール ポリシー ルール
- ユーザーベースのアクセス コントロール ポリシー ルール
- プロトコル SCTP を使用するサービスオブジェクト
- 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
- SCTP で構成された NAT ルール
- 変換済み送信元に FQDN オブジェクトと FQDN オブジェクトグループを含む NAT ルール
- 元の送信元と宛先の両方に FQDN オブジェクトと FQDN オブジェクトグループを含む NAT ルール
- 変換済み接続先に FQDN オブジェクトグループを含む NAT ルール
- IPv6 NAT
- URL フィルタリングを使用するポリシー

脅威に対する防御 でサポートされていない機能を構成するには、『Threat Defense Configuration Guide』を参照してください。

（注） サポートされているポリシーもサポートされていないポリシーもすべて Management Center に移行されます。サポートされていないポリシーは、無効として移行されます。これらのポリシーは、回避策の後、または Management Center に従って構成した後に、有効にすることができます。

プロファイル URL フィルタリング、ユーザー ID、送信元、または宛先ネゲートを含むポリシーは**サポートされていません**。

Threat Defense デバイスに関する注意事項と制約事項

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

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

移行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 PAN 、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
- 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 Management Center ソフトウェアバージョン（移行でサポートされるソフトウェアのバージョン （27 ページ）を参照）。

- PAN の移行でサポートされる Management Center ソフトウェアバージョンは 6.1.x 以降です。
- PAN 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 Security Cloud Control（旧 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。

Security Cloud Control からクラウド提供型 Firewall Management Center にアクセスできます。Security Cloud Control 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、Security Cloud Control の地域を追加し、Security Cloud Control ポータルから API トークンを生成する必要があります。

Security Cloud Control の地域

Security Cloud Control 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 : Security Cloud Control* の地域と *URL*

地域	Security Cloud Control URL
欧州	https://eu.manage.security.cisco.com/
US	https://us.manage.security.cisco.com/
APJC	https://apj.manage.security.cisco.com/
Australia	https://au.manage.security.cisco.com/
インド	https://in.manage.security.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、 PAN 、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 Palo Alto Networks のファイアウォールのバージョン

Cisco Secure Firewall 移行ツールは、PAN ファイアウォール OS バージョン 6.1.x 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 PAN 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

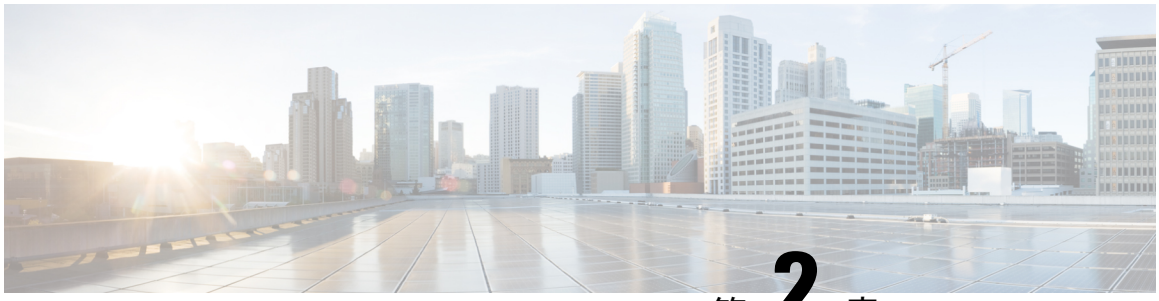
PAN ファイアウォールの場合、Cisco Secure Firewall 移行ツールは、バージョン 6.2.3.3 以降を実行している Management Center によって管理される Management Center デバイスへの移行をサポートしています。

（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。



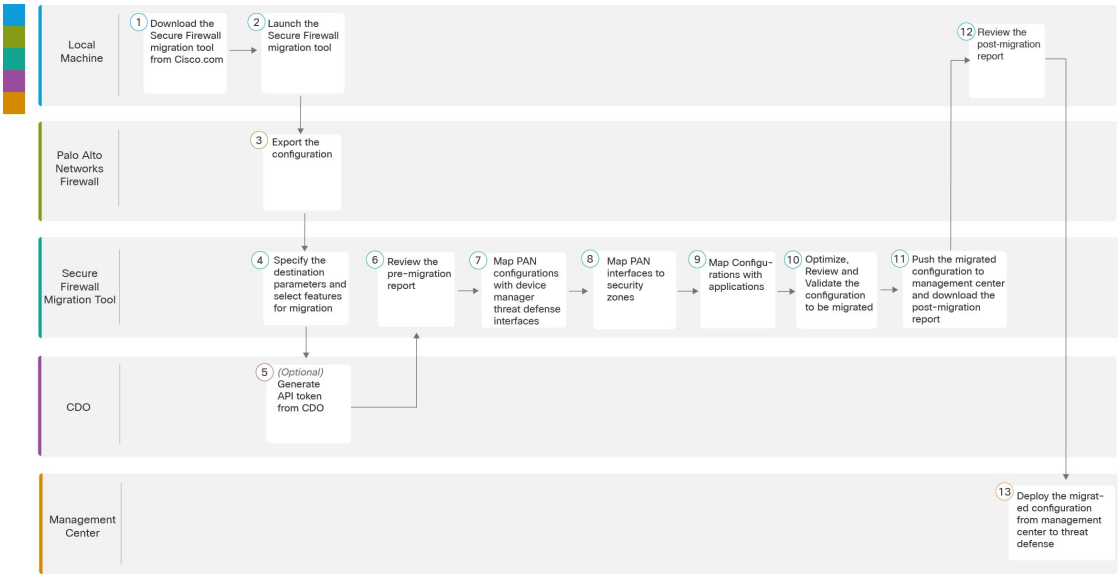
第 2 章

Palo Alto Networks ファイアウォールから Threat Defense への移行ワークフロー

- エンドツーエンドの手順 （29 ページ）
- 移行の前提条件 （31 ページ）
- 移行の実行 （32 ページ）
- Cisco Secure Firewall 移行ツールのアンインストール （61 ページ）
- 移行例： PAN から Threat Defense 2100 へ （62 ページ）

エンドツーエンドの手順

次のフローチャートは、Cisco Secure Firewall 移行ツールを使用して、Palo Alto Networks ファイアウォールを Threat Defense に移行するワークフローを示しています。



	ワークスペース	手順
1	Local Machine	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 Secure Firewall 移行ツールを起動します。「Cisco Secure Firewall 移行ツールの起動」を参照してください。
3	Palo Alto Networks ファイアウォール	構成ファイルのエクスポート：Palo Alto Networks ファイアウォールから構成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」を参照してください。
4	Cisco Secure Firewall 移行ツール	このステップでは、移行の接続先パラメータを指定できます。詳細な手順については、「Cisco Secure Firewall 移行ツールの接続先パラメータの指定」を参照してください。
5	Security Cloud Control	（オプション）この手順はオプションであり、クラウドで提供される Firewall Management Center を移行先管理センターとして選択した場合にのみ必要です。詳細な手順については、「Cisco Secure Firewall移行ツールの接続先パラメータの指定」を参照してください。
6	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。詳細な手順については、「移行前レポートの確認」を参照してください。
7	Cisco Secure Firewall 移行ツール	PAN 構成が正しく移行されるように、PAN インターフェイスを適切な Threat Defense インターフェイス オブジェクト、セキュリティゾーン、およびインターフェイスグループにマッピングします。詳細な手順については、「PAN ファイアウォール 構成と Threat Defense インターフェイスのマッピング」を参照してください。
8	Cisco Secure Firewall 移行ツール	PAN インターフェイスを適切なセキュリティゾーンにマッピングします。詳細な手順については、「セキュリティゾーンインターフェイスグループ への PAN インターフェイスのマッピング」をご覧ください。
9	Cisco Secure Firewall 移行ツール	PAN 構成を対応するターゲットアプリケーションにマップできます。詳細な手順については、「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。
10	Cisco Secure Firewall 移行ツール	構成を慎重に確認し、それが適切で Threat Defense デバイスの構成内容と一致することを確認します。詳細な手順については、「最適化、 構成の確認と検証」を参照してください。

	ワークスペース	手順
11	Cisco Secure Firewall 移行ツール	移行プロセスのこのステップでは、移行された構成を管理センターに送信し、移行後レポートをダウンロードできるようにします。詳細な手順については、「移行された構成の以下へのプッシュ：Management Center」を参照してください。
12	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。詳細な手順については、「移行後レポートの確認と移行の完了」を参照してください。
13	Management Center	移行した構成を管理センターから Threat Defense に展開します。詳細な手順については、「移行後レポートの確認と移行の完了」を参照してください。

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。

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。

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） Cisco Secure Firewall 移行ツールを起動すると、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
- サポートされる移行先の管理センター （25 ページ）セクションで要件を確認します。
- 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。

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の確認（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、リンクをクリックし、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 ファイアウォールからの構成ファイル（Panorama の管理対象外）」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 デバイスやデモ FTD デバイスなどのデモのソースデバイスとターゲットデバイスを選択して、デモ移行の実行を進められます。

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。

また、実際の移行ワークフローと同様に、移行前レポートのダウンロードと確認、インターフェイスのマッピング、セキュリティゾーンのマッピング、インターフェイスグループのマッピングなどのすべて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して Cisco Secure Firewall 移行ツールにアップロードし、構成を 脅威に対する防御 に移行できます。

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。

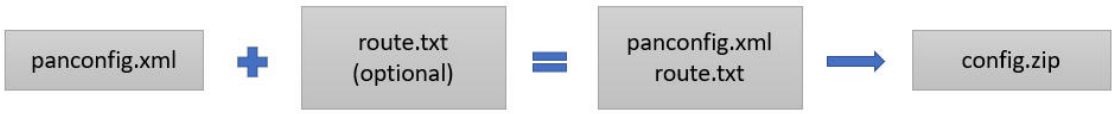
ステップ 4 ファイルを解凍して展開し、パス *\opt\pancfg\mgmt\saved-configs* に移動して、*merged-running-config.xml* ファイルを取得します。

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）。



Cisco Secure Firewall 移行ツールの接続先パラメータの指定

始める前に

Security Cloud Controlでホストされるクラウドバージョンの移行ツールを使用している場合は、ステップ 3 に進んでください。

- オンプレミス Firewall Management Center の Management Center の IP アドレスを取得します。
- Cisco Secure Firewall 移行ツール 3.0 以降では、オンプレミスの Firewall Management Center またはクラウド提供型 Firewall Management Center を選択できます。
- クラウド提供型 Firewall Management Center の場合、リージョンと API トークンを指定する必要があります。詳細については、「サポートされる移行先の管理センター」を参照してください。
- （任意） インターフェイスやルートなどのデバイス固有の構成を移行する場合は、ターゲット 脅威に対する防御 を Management Center に追加します。「Adding Devices to the Firewall Management Center」を参照してください。
- [確認と検証（Review and Validate）] ページで IPS またはファイルポリシーを ACL に適用する必要がある場合は、移行前に Management Center でポリシーを作成することを強くお勧めします。Cisco Secure Firewall 移行ツールは接続された Management Center からポリシーを取得するため、同じポリシーを使用します。新しいポリシーを作成して複数のアクセス制御リストに割り当てると、パフォーマンスが低下し、プッシュが失敗する可能性があります。

手順

ステップ 1 [ターゲットの選択（Select Target）] 画面の [ファイアウォール管理（Firewall Management）] セクションで、次の手順を実行します。オンプレミスのファイアウォール管理センターまたはクラウド提供型ファイアウォール管理センターへの移行を選択できます。

- オンプレミスのファイアウォール管理センターに移行するには、次の手順を実行します。

a) [オンプレミス FMC（On-Prem FMC）] オプションボタンをクリックします。
b) 管理センターの IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。
c) [ドメイン（Domain）] ドロップダウンリストで、移行先のドメインを選択します。

脅威に対する防御 デバイスに移行する場合は、選択したドメインで使用可能な 脅威に対する防御 デバイスにのみ移行できます。

d) [接続（Connect）] をクリックして、**手順 2** に進みます。

- クラウド提供型 Firewall Management Center に移行するには、次の手順を実行します。

a) [クラウド提供型 FMC（Cloud-delivered FMC）] オプションボタンをクリックします。

b) リージョンを選択し、Security Cloud Control API トークンを貼り付けます。Security Cloud Control から API トークンを生成するため、以下の手順に従います。

1. Security Cloud Control にログインします。
2. 右上隅から、**[設定（Preferences）] > [一般設定（General Preferences）]**に移動し、[マイトークン（My Tokens）] セクションから API トークンをコピーします。

c) [接続（Connect）] をクリックして、**手順 2** に進みます。

ステップ 2 [Firewall Management Centerへのログイン（Firewall Management Center Login）] ダイアログボックスで、Cisco Secure Firewall 移行ツール専用アカウントのユーザー名とパスワードを入力し、[ログイン（Login）] をクリックします。

Cisco Secure Firewall 移行ツールは Management Center にログインし、その Management Center による管理対象 脅威に対する防御デバイスのリストを取得します。この手順の進行状況はコンソールで確認できます。

ステップ 3 [続行（Proceed）] をクリックします。

ステップ 4 [FTDの選択（Choose FTD）] セクションで、次のいずれかを実行します。

- [FTDデバイスの選択（Select FTD Device）] ドロップダウンリストをクリックし、構成を移行するデバイスをオンにします。

  選択した Management Center ドメイン内のデバイスが、[IPアドレス（IP Address）]、[名前（Name）]、[デバイスモデル（Device Model）]、および [モード（Mode）]（ルーテッドまたはトランスペアレント）別に表示されます。

  （注）
  少なくとも、選択するネイティブ 脅威に対する防御デバイスには、移行する 構成と同じ数の物理インターフェイスまたはポートチャネルインターフェイスが必要です。少なくとも、脅威に対する防御デバイスのコンテナインスタンスには、同じ数の物理インターフェイスまたはポートチャネルインターフェイスとサブインターフェイスが必要です。 構成と同じファイアウォールモードでデバイスを構成する必要があります。ただし、これらのインターフェイスは、両方のデバイスで同じ名前である必要はありません。

  （注）
  サポートされているターゲット Threat Defense プラットフォームが、管理センターバージョン 6.5 以降を備えた Firewall 1010である場合にのみ、FDM 5505 移行サポートは共有ポリシーに適用され、デバイス固有のポリシーには適用されません。Threat Defense なしで続行すると、Cisco Secure Firewall 移行ツールは構成またはポリシーを Threat Defense にプッシュしません。したがって、Threat Defense のデバイス固有の構成であるインターフェイスとルート、およびサイト間 VPN は移行されません。ただし、NAT、ACL、ポートオブジェクトなど、サポートされている他のすべての構成（共有ポリシーとオブジェクト）は移行されます。リモートアクセス VPN は共有ポリシーであり、Threat Defense なしでも移行できます。

  リモート展開が有効になっている Management Center または 脅威に対する防御 6.7 以降への Palo Alto Networks ファイアウォールの移行は、Cisco Secure Firewall 移行ツールでサポートされています。インターフェイスとルートの移行は手動で行う必要があります。

- [FTD を使用せず続行（Proceed without FTD）] をクリックして、構成を Management Center に移行します。

  脅威に対する防御 なしで続行すると、Cisco Secure Firewall 移行ツールは 脅威に対する防御 に構成またはポリシーをプッシュしません。したがって、脅威に対する防御 のデバイス固有の校正であるインターフェイスとルート、およびサイト間 VPN は移行されず、Management Center で手動で構成する必要があります。ただし、NAT、ACL、ポートオブジェクトなど、サポートされている他のすべての構成（共有ポリシーとオブジェクト）は移行されます。リモートアクセス VPN は共有ポリシーであり、Threat Defense なしでも移行できます。

ステップ 5 [続行（Proceed）] をクリックします。

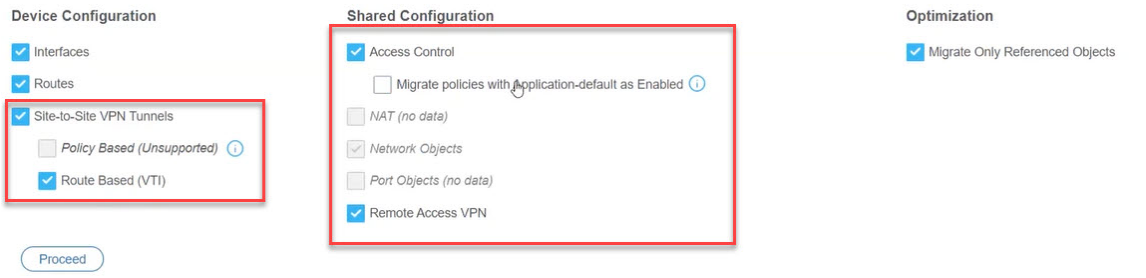
移行先に応じて、Cisco Secure Firewall 移行ツールを使用して移行する機能を選択できます。

ステップ 6 [機能の選択（Select Features）] セクションをクリックして、移行先に移行する機能を確認して選択します。

- 接続先 脅威に対する防御 デバイスに移行する場合、Cisco Secure Firewall 移行ツールは、[デバイスの構成（Device Configuration）] セクションと [共有構成（Shared Configuration）] セクションで、 構成から移行できる機能を自動的に選択します。要件に応じて、デフォルトの選択をさらに変更できます。
- Management Center に移行する場合、Cisco Secure Firewall 移行ツールは、[デバイス設定（Device Configuration）]、[共有構成（Shared Configuration）]、および [最適化（Optimization）] セクションで、 構成から移行できる機能を自動的に選択します。要件に応じて、デフォルトの選択をさらに変更できます。
- PAN の場合は、[Shared Configuration] で、関連する [Access Control] オプションを選択します。

  Migrate policies with Application-Default as Enabled：このオプションを選択すると、PAN アプリケーションが移行されます。このチェックボックスをオンにした場合にのみ、[Migrate policies with Application-Default as Enabled] オプションが表示されます。

  （注）
  [Application Mapping] は、ポリシーが移行対象として選択されている場合にのみ有効になります。



VPN が設定された Palo Alto Networks ファイアウォールから設定を移行する場合は、[デバイス設定（Device Configuration）] ペインで **サイト間 VPN トンネル**を、[共有設定（Shared Configuration）] ペインで**リモートアクセス VPN** を選択または選択解除できます。ポリシーベースのサイト間 VPN 設定は、Palo Alto Networks ファイアウォールでサポートされていないため、サポートされないことに注意してください。

サービスが "application-default" であるポリシー

サービスが "**application-default**" であり、アプリケーションが参照されているメンバーまたはグループを持つポリシーは、[機能の選択（Feature Selection）] ページでの選択に従って移行されます。Management Center には **application-default** と同等の設定がないため、このようなポリシーはサービス "any" でプッシュされます。**application-default** と同様の機能を複製する場合は、アプリケーションが使用するポートを Palo Alto Networks ファイアウォールから見つけ、Management Center の [ポリシー（Policy）] のポートセクションでそのポートを構成します。

たとえば、"**web-browsing**" を持ち、サービスが"**application-default**" であるポリシーは、アプリケーションHTTP（web-browsing と同等）と "**any**" ポートとして移行されます。"**application-default**" と同じ機能を複製するには、ポートを TCP/80 および TCP/8080 として構成します。web-browsing は、ポート TCP 80 および TCP 8080 を使用します。ポリシーに複数のアプリケーションがある場合は、各アプリケーションで使用されるポートを構成します。

ポリシーに複数のアプリケーションがある場合は、ポートを構成する前にポリシーを分割することを推奨します。これにより、他のアプリケーションへの追加アクセスが許可される可能性があるためです。

"**any**" として構成されたアプリケーションと "**application-default**" として構成されたサービスが設定されているポリシーは、[機能の選択（Feature Selection）]ページで選択できる項目（アプリケーションは "**any**"、サービスは "**any**"）に関係なく、無効として移行されます。これが許容可能な動作である場合は、アプリケーションを有効にして変更をコミットします。それ以外の場合は、必要なアプリケーションまたはサービスを選択し、ポリシーを有効にします。

ルールごとのアプリケーションによるアクセス制御リストの分割

複数のアプリケーションに設定された 1 つのルールを含むアクセス制御リストを移行する場合は、ACL の分割を選択できます。これによりそのルールは、1 つのルールにつきアプリケーションが 1 つの複数のルールに分割されます。これを行うには、[ルールごとにアプリケーションで ACL を分割する（Split ACLs with applications with rules per rule）] チェックボックスをオンにします。ただし、移行しようとしている設定に、アクセスルールごとに設定された複数のアプリケーションが含まれていない場合、チェックボックスは表示されません。

各ルールは、1 つのルールにつきアプリケーションが 1 つの複数のルールに変換されます。これは、[設定の最適化、確認、検証（Optimize, Review, and Validate Configuration）] ページで確認できます。

- Cisco Secure Firewall 移行ツールは、ターゲット管理センターが 7.2 以降の場合はリモートアクセス VPN の移行をサポートします。リモートアクセス VPN は、Threat Defense なしで移行できる共有ポリシーです。Threat Defense を使用する移行を選択した場合、Threat Defense のバージョンは 7.0 以降である必要があります。
- （任意）[Optimization] セクションで、[Migrate only referenced objects] を選択して、アクセス コントロール ポリシーと NAT ポリシーで参照されているオブジェクトのみを移行します。

  （注）
  このオプションを選択すると、 構成内の参照されていないオブジェクトは移行されません。これにより、移行時間が最適化され、未使用のオブジェクトが構成から消去されます。

ステップ 7　[続行（Proceed）] をクリックします。

ステップ 8 [Rule Conversion/ Process Config] セクションで、[Start Conversion] をクリックして変換を開始します。

ステップ 9 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 10 [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。

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 に正常に移行できるサポート対象 構成要素と、移行対象として選択された特定の機能のサマリー。
- [エラーのある構成行（Configuration Lines with Errors）]：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 の構成要素の詳細。 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てから、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、続行してください。
- [部分的なサポート構成（Partially Supported Configuration）]：部分的にのみ移行可能な 構成要素の詳細。これらの構成要素には、詳細オプションを含むルールとオブジェクトが含まれているため、詳細オプションを使用せずにルールまたはオブジェクトを移行できます。これらの行を確認し、詳細オプションが Management Center 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、 Cisco Secure Firewall 移行ツールを使用して移行を完了した後に、これらのオプションを手動で構成することを計画します。

- [未サポートの構成（Unsupported Configuration）]：Cisco Secure Firewall 移行ツールがこれらの機能の移行をサポートしていないため、移行できない 構成要素の詳細。これらの行を確認し、各機能が Management Center 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、 Cisco Secure Firewall 移行ツールを使用して移行を完了した後に、機能を手動で構成することを計画します。
- [無視される構成（Ignored Configuration）]： Management Center または Cisco Secure Firewall 移行ツールでサポートされていないために無視される 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 Management Center 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。

Management Center と 脅威に対する防御 でサポートされる機能の詳細については、『Management Center Configuration Guide』[英語] を参照してください。

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 で修正を完了し、 構成ファイルを再度エクスポートしてから、更新された構成ファイルをアップロードし、続行してください。

ステップ 4 構成ファイルが正常にアップロードおよび解析されたら、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。

次のタスク

PAN ファイアウォール 構成と Threat Defense インターフェイスのマッピング

PAN ファイアウォール 構成と Threat Defense インターフェイスのマッピング

脅威に対する防御デバイスには、構成で使用されている数以上の物理インターフェイスとポート チャネル インターフェイスが必要です。これらのインターフェイスは、両方のデバイスで同じ名前である必要はありません。インターフェイスのマッピング方法を選択できます。

インターフェイスから 脅威に対する防御 インターフェイスへのマッピングは、脅威に対する防御 デバイスタイプによって異なります。

- ターゲット 脅威に対する防御 がネイティブタイプの場合は次のようになります。
  - 脅威に対する防御には、使用するPANインターフェイスまたはポートチャネル（PC）データインターフェイスまたはサブインターフェイスが同数以上必要です（PAN構成の管理専用を除く）。同数未満の場合は、ターゲット 脅威に対する防御 に必要なタイプのインターフェイスを追加します。
  - サブインターフェイスは、物理インターフェイスまたはポートチャネル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 脅威に対する防御 がコンテナタイプの場合は次のようになります。

- 脅威に対する防御 には、使用する PAN 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、またはポート チャネル サブインターフェイスが同数以上必要です（ 構成の管理専用を除く）。同数未満の場合は、ターゲット 脅威に対する防御 に必要なタイプのインターフェイスを追加します。たとえば、ターゲット脅威に対する防御 の物理インターフェイスと物理サブインターフェイスの数が PAN での数より 100 少ない場合、ターゲット 脅威に対する防御 に追加の物理または物理サブインターフェイスを作成できます。

始める前に

Management Center に接続し、接続先として 脅威に対する防御 を選択していることを確認します。詳細については、「Cisco Secure Firewall 移行ツールの接続先パラメータの指定 （37 ページ）」を参照してください。

（注） 脅威に対する防御 デバイスなしで Management Center に移行する場合、この手順は適用されません。

手順

ステップ 1 インターフェイスマッピングを変更する場合は、[FTDインターフェイス名（FTD Interface Name）]のドロップダウンリストをクリックし、そのインターフェイスにマッピングするインターフェイスを選択します。

管理インターフェイスのマッピングは変更できません。脅威に対する防御 インターフェイスがすでにインターフェイスに割り当てられている場合は、ドロップダウンリストからそのインターフェイスを選択できません。割り当て済みのすべてのインターフェイスはグレー表示され、使用できません。

サブインターフェイスをマッピングする必要はありません。Cisco Secure Firewall 移行ツールは、 構成内のすべてのサブインターフェイスについて 脅威に対する防御 デバイスのサブインターフェイスをマッピングします。

（注）
送信元ファイアウォールのインターフェイスの数がターゲットファイアウォールのインターフェイスの数よりも多い場合は、ターゲットファイアウォールにサブインターフェイスを作成し、移行を再試行します。

ステップ 2 各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たら、[次へ（Next）]をクリックします。

次のタスク

PAN インターフェイスを適切な 脅威に対する防御 インターフェイス オブジェクトとセキュリティゾーンにマッピングします。詳細については、「セキュリティゾーンインターフェイスグループ への PAN インターフェイスのマッピング」を参照してください。

セキュリティゾーンインターフェイスグループへのPANインターフェイスのマッピング

構成が正しく移行されるように、インターフェイスを適切な 脅威に対する防御 インターフェイス オブジェクト、セキュリティゾーン にマッピングします。 構成では、アクセス コントロール ポリシーと NAT ポリシーはインターフェイス名（nameif）を使用します。Management Center では、これらのポリシーはインターフェイス オブジェクトを使用します。さらに、Management Center ポリシーはインターフェイス オブジェクトを次のようにグループ化します。

- セキュリティゾーン：インターフェイスは、1 つのセキュリティゾーンにのみ属することができます。

Cisco Secure Firewall 移行ツールでは、セキュリティゾーンとインターフェイスを 1 対 1 でマッピングできます。セキュリティゾーンがインターフェイスにマッピングされている場合、他のインターフェイスへのマッピングには使用できませんが、Management Center では許可されます。 Management Centerのセキュリティゾーンの詳細については、『Cisco Secure Firewall Management Center Device Configuration Guide』 の「Security Zones and Interface Groups」を参照してください。

手順

ステップ 1 [セキュリティゾーンのマッピング（Map Security Zones）] 画面で、使用可能なインターフェイスとセキュリティゾーンを確認します。

ステップ 2 セキュリティゾーンおよびインターフェイスグループが Management Center に存在する場合、またはセキュリティ ゾーン タイプ オブジェクトとして 構成ファイルに存在し、ドロップダウンリストで使用可能な場合、これらにインターフェイスをマッピングするには、次の手順を実行します。

a) [セキュリティゾーン（Security Zones）] 列で、インターフェイスのセキュリティゾーンを選択します。
b) [インターフェイスグループ（Interface Groups）] 列で、インターフェイスのインターフェイスグループを選択します。

ステップ 3 Management Center に存在するセキュリティゾーンにインターフェイスをマッピングするには、[セキュリティゾーン（Security Zones）] 列で、そのインターフェイスのセキュリティゾーンを選択します。

ステップ 4 セキュリティゾーンは、手動でマッピングすることも自動で作成することもできます。

セキュリティゾーンを手動でマッピングするには、次の手順を実行します。

a) [セキュリティゾーンとインターフェイスグループの追加（Add SZ & IG）] をクリックします。
b) [セキュリティゾーンとインターフェイスグループの追加（Add SZ & IG）] ダイアログボックスで、[追加（Add）] をクリックして新しいセキュリティゾーンを追加します。
c) [セキュリティゾーン（Security Zone）] 列にセキュリティゾーン名を入力します。使用できる最大文字数は 48 です。
d) [閉じる（Close）] をクリックします。

セキュリティゾーンを自動作成によってマッピングするには、次の手順を実行します。

a) [自動作成（Auto-Create）] をクリックします。
b) [自動作成（Auto-Create）] ダイアログボックスで、[ゾーンマッピング（Zone Mapping）] をオンにします。
c) [自動作成（Auto-Create）] をクリックします。

[自動作成（Auto-Create）] をクリックすると、送信元ファイアウォールゾーンが自動的にマッピングされます。同じ名前のゾーンが Management Center にすでに存在する場合、そのゾーンは再利用されます。マッピングページには、再利用ゾーンに対して "(A)" が表示されます。たとえば、**inside** "(A)" となります。

ステップ 5 すべてのインターフェイスを適切なセキュリティゾーンにマッピングしたら、[次へ（Next）] をクリックします。

構成とアプリケーションのマッピング

アプリケーションを対応するターゲットアプリケーションにマッピングできます。アプリケーションに基づくルールを移行できます。

Management Center の定義済みアプリケーションと、構成ファイルに含まれる一部のアプリケーションのリストが、このタブにリストされます。Management Center に存在する定義済みマッピングの一部がマップされます。

（注） 定義済みマッピングを編集することはできません。

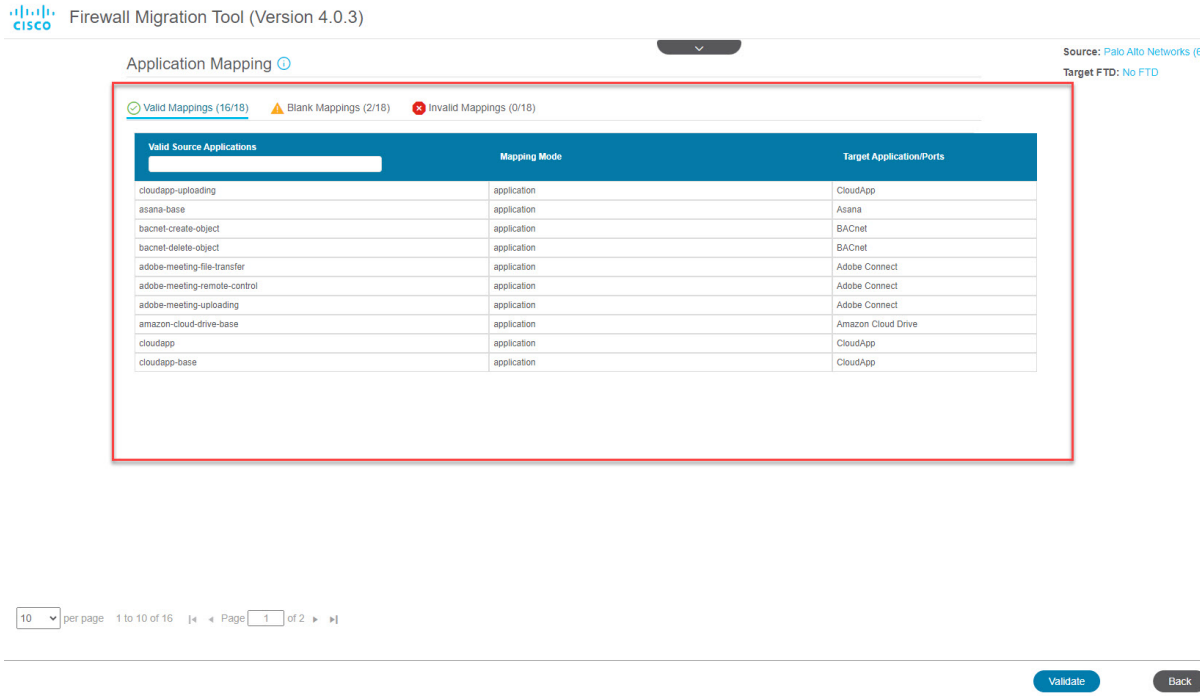
[Application Mapping] ページには、次のタブが表示されます。

- Invalid Mappings：その移行で無効なマッピングのリストを表示します。

  マッピングは、次のシナリオで **Invalid** と呼ばれます。

  - [Mapping Mode] に [Application] または [Port] が選択されているが、[Target] が空の場合。
  - [Mapping Mode] が [Port] で、ポートの構文が正しくない場合。移行を続行するには、[Invalid Mapping] をゼロにする必要があります。

（注） 正しい検証が行われるまで、[Next] ボタンは無効になります。



送信元からマッピングの定義済みリストを取得すると、自動的にマップされる定義済みアプリケーションがあります。マップされていないアプリケーションがある場合は、ポートまたはアプリケーションに手動でマップする必要があります。

- Blank Mappings：マッピングされていないアプリケーションを表示し、ユーザーアクションを要求します。**アプリケーション**は、**アプリケーション**または**ポート**にマッピングされている必要があります。

（注） すべての**アプリケーション**エントリをマッピングすることを推奨しますが、必須ではありません。

マッピングモードが選択され、ターゲットアプリケーションに有効なデータがある場合、それは有効なマッピングです。

（注） デフォルトでは、すべての定義済みマッピングを [Valid Mappings] タブで使用できます。

- Valid Mappings：正しいマッピングを表示します。Cisco Secure Firewall 移行ツールには、一般的に使用されるアプリケーション用に PAN および 脅威に対する防御 のアプリケーションとの定義済みマッピングのデータベースが独自に用意されています。PAN アプリケーションが定義済みマッピング DB と一致する場合、それらのアプリケーションは自動的にマッピングされ、有効なマッピングの下に表示されます。

アプリケーションが [Blank Mapping] で**アプリケーション**または**ポート**にマッピングされると、検証後に [Valid Mapping] に移動されます。

（注） 定義済みマッピングは編集できません。

無効、有効、およびブランクのマッピング数は、移行に基づいて変化し続けます。

次の表に、アプリケーションマッピングのプロパティを示します。

表 *2:* アプリケーション マッピング テーブル プロパティ

フィールド	説明
送信元アプリケーション（Source Application）	Palo Alto Networks ファイアウォールで使用されているアプリケーションのリストを表示します。
マッピングモード（Mapping Mode）	[Application] または [Port(s)] のいずれかのマッピングモードを選択します。 • Application：マッピングに使用可能なターゲットアプリケーションのリストから選択します。マッピングできるアプリケーションは 1 つだけです。 • Port(s)：マッピングに使用できるポートのリストから選択します。[Ports] を選択する場合は、指定された形式で関連するポート情報を入力します。たとえば、tcp/80 や udp/80 です。 （注） 文字間のスペースは使用できません。
対象のアプリケーション（Target Application）	マッピングモードに基づくターゲットアプリケーションまたはポートのリストを表示します。

ICMP および Ping のアプリケーションは、**ICMP** および **ping** のサービスとして移行されます。これは Cisco Secure Firewall 移行ツールによって自動的に実行されるため、[アプリケーションマッピング（Application Mapping）] ページには表示されません。

手順

ステップ 1 [Valid Mappings] タブをクリックして、その移行に有効なマッピング数を表示します。**有効な送信元アプリケーション**と、有効な**マッピングモード**および**ターゲットアプリケーション**をマッピングします。

マッピングが有効になると、有効なマッピング数の増加を確認できます。

ステップ 2 [Blank Mappings] をクリックして、その移行のブランクマッピングのリストを表示します。**ブランク送信元アプリケーション**と、有効な**マッピングモード**および**ターゲットアプリケーション**をマッピングします。

たとえば、マッピングモードを選択し、ターゲット接続先を入力せずに保存すると、ブランクマッピング数が増加します。タブを確認して正しくマッピングし、移行を続行します。

（注）
ブランクマッピングがある場合でも、移行を続行できます。

ステップ 3 [Invalid Mappings] タブをクリックして、無効なマッピングのリストを表示します。次の手順を実行します。

a) Invalid Application：移行中に無効なマッピングが表示されます。
b) Mapping Mode：[Application] または [Port] のいずれかのマッピングモードを選択します。
c) Target Application：アプリケーションマッピングのターゲットアプリケーションを選択します。

たとえば、マッピングモードを選択したが、別のターゲット接続先にマップした場合、他のタブに進むことはできません。[Invalid Mappings] タブを確認し、正しいターゲットアプリケーションを入力して、アプリケーションマッピングを実行します。

ステップ 4 各タブで [Validate] をクリックして、その移行の無効なマッピング、ブランクマッピング、または有効なマッピングを検証します。

ステップ 5 [Next] をクリックして続行します。

ステップ 6 検証前に手動で実行したマッピングをクリアするには、[マップされたデータのクリア（Clear Mapped Data）] をクリックします。検証をクリックしてマッピングが有効になった後はマッピングを元に戻すことができないため、実行しているマッピングに完全な確信がある場合にのみ[検証（Validate）] をクリックすることをお勧めします。

次のタスク

最適化、 構成の確認と検証

最適化、 構成の確認と検証

移行した 構成を Management Center にプッシュする前に、構成を慎重に確認し、それが適切で脅威に対する防御デバイスの構成内容と一致することを確認します。点滅しているタブは、次の一連のアクションを実行する必要があることを示しています。

（注） [構成の最適化、確認および検証（Optimize, Review and Validate Configuration）] 画面で Cisco Secure Firewall 移行ツールを閉じると、進行状況が保存され、後で移行を再開できます。この画面の前に Cisco Secure Firewall 移行ツールを閉じると、進行状況は保存されません。解析後に障害が発生した場合、[インターフェイスマッピング（Interface Mapping）] 画面から Cisco Secure Firewall 移行ツールを再起動します。

これで、Cisco Secure Firewall 移行ツールは、Management Center にすでに存在する侵入防御システム（IPS）ポリシーとファイルポリシーを取得し、移行するアクセスコントロールルールにそれらを関連付けることができます。

ファイルポリシーは、システムが全体的なアクセス制御設定の一環として、ネットワークの高度なマルウェア防御とファイル制御を実行するために使用する一連の設定です。この関連付けにより、アクセスコントロールルールの条件と一致するトラフィック内のファイルを通過させる前に、システムは必ずファイルを検査するようになります。

同様に、トラフィックが接続先に向かうことを許可する前に、システムの最終防御ラインとして IPS ポリシーを使用できます。侵入ポリシーは、セキュリティ違反に関するトラフィックの検査方法を制御し、インライン展開では、悪意のあるトラフィックをブロックまたは変更することができます。システムが侵入ポリシーを使用してトラフィックを評価する場合、システムは関連付けられた変数セットを使用します。セット内の大部分の変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスとポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。

タブで特定の構成項目を検索するには、列の上部にあるフィールドに項目名を入力します。テーブルの行はフィルタ処理され、検索語に一致する項目のみが表示されます。

（注） デフォルトでは、[インライングループ化（Inline Grouping）] オプションが有効になっています。

[構成の最適化、確認および検証（Optimize, Review and Validate Configuration）] 画面で Cisco Secure Firewall 移行ツールを閉じると、進行状況が保存され、後で移行を再開できます。この画面の前に閉じると、進行状況は保存されません。解析後に障害が発生した場合、[インターフェイスマッピング（Interface Mapping）] 画面から Cisco Secure Firewall 移行ツールを再起動します。

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。

（注） PAN 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

- 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。
  - 送信元と宛先のゾーン
  - 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。

ダイナミック IP/ポート フォールバック インターフェイス

Palo Alto Networks から Threat Defense への移行のため、[設定の最適化、確認、および検証（Optimize, Review and Validate Configuration）] ページで NAT 設定を確認する場合は、NAT ルールに**ダイナミック IP/ポートフォールバック**設定があるかどうか、およびルールが移行または削除されているかどうかも確認できます。

設定したダイナミック IP またはポート フォールバック インターフェイス アドレスが宛先ゾーンアドレスと同じである場合、Cisco Secure Firewall 移行ツールは NAT ルールを移行します。異なる場合、ルールは移行されず、サポート対象外としてリストされます。これは Cisco Secure Firewall Management Center が、ダイナミック IP またはポート フォールバック インターフェイスとして宛先アドレスしか持てないためです。NAT ルールにフォールバック設定がない場合、移行は検証なしで実行され、[ダイナミック IP/ポートフォールバック（Dynamic IP/Port-fallback）] 列には [適用なし（Not Applicable）] と表示されます。

手順

ステップ 1 [設定の最適化、確認、および検証（Optimize, Review and Validate Configuration）] 画面で、[アクセス制御ルール（Access Control Rules）] をクリックし、次の手順を実行します。

a) 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。

b) 1つ以上のアクセス制御リストポリシーを移行しない場合は、ポリシーのボックスをオンにして行を選択し、**[アクション（Actions）]** > **[移行しない（Do not migrate）]**を選択して、[保存（Save）] をクリックします。

移行しないことを選択したすべてのルールは、テーブルでグレー表示されます。

c) Management Center ファイルポリシーを 1 つ以上のアクセス コントロール ポリシーに適用する場合は、該当する行のボックスをオンにし、**[アクション（Actions）]** > **[ファイルポリシー（File Policy）]** を選択します。

[ファイルポリシー（File Policy）] ダイアログで、適切なファイルポリシーを選択し、選択したアクセス コントロール ポリシーに適用して、[保存（Save）] をクリックします。

d) Management Center IPS ポリシーを 1 つ以上のアクセス コントロール ポリシーに適用する場合は、該当する行のボックスをオンにし、**[アクション（Actions）]** > **[IPS ポリシー（IPS Policy）]** を選択します。

[IPS ポリシー（IPS Policy）] ダイアログで、適切な IPS ポリシーと対応する変数セットを選択し、選択したアクセス コントロール ポリシーに適用して、[保存（Save）] をクリックします。

e) ロギングが有効になっているアクセスコントロールルールのロギングオプションを変更する場合は、該当する行のボックスをオンにし、**[アクション（Actions）]** > **[ログ（Log）]** を選択します。

[ログ（Log）] ダイアログでは、接続の開始時または終了時、またはその両方でイベントのロギングを有効にできます。ロギングを有効にする場合は、接続イベントを**イベントビューア**または **Syslog** のいずれか、または両方に送信することを選択する必要があります。接続イベントを syslog サーバに送信することを選択した場合、Management Center ですでに構成されている syslog ポリシーを [Syslog] ドロップダウンメニューから選択できます。

f) [アクセスコントロール（Access Control）] テーブル内の移行されたアクセスコントロールルールのアクションを変更する場合は、該当する行のボックスをオンにし、**[アクション（Actions）]** > **[ルールアクション（Rule Action）]** を選択します。

ヒント
アクセス制御ルールにアタッチされている IPS およびファイルのポリシーは、[許可（Allow）] オプションを除くすべてのルールアクションに対して自動的に削除されます。

ACE カウントは、昇順、降順、等しい、大なり、および小なりのフィルタリング順序シーケンスでフィルタ処理できます。

フィルタリング条件をクリアするには、[フィルタのクリア（Clear Filter）] をクリックします。

（注）

ACE に基づいた ACL のソート順序は、表示のみを目的としています。ACL は、発生した時間順に基づいてプッシュされます。

ステップ 2 次のタブをクリックし、構成項目を確認します。

- アクセス制御（Access Control）
- オブジェクト（Objects）（ネットワークオブジェクト（Network Objects）、ポートオブジェクト（Port Objects）、URLオブジェクト（URL Objects））
- NAT
- インターフェイス（Interfaces）
- ルート（Routes）
- サイト間 VPN トンネル（Site-to-Site VPN Tunnels）
- リモートアクセス VPN（Remote Access VPN）

（注）
サイト間およびリモートアクセス VPN の設定では、VPN フィルタ設定とそれらに関連する拡張アクセスリストオブジェクトが移行され、それぞれのタブで確認できます。

1 つ以上の NAT ルールまたはルートインターフェイスを移行しない場合は、該当する行のボックスをオンにし、**[アクション（Actions）]** > **[移行しない（Do not migrate）]** を選択して、**[保存（Save）]** をクリックします。

移行しないことを選択したすべてのルールは、テーブルでグレー表示されます。

ステップ 3 （任意）構成の確認中に、オブジェクトを選択して**[アクション（Actions）]** > **[名前の変更（Rename）]** を選択することで、**[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）]** タブで 1 つ以上のネットワークオブジェクトまたはポートオブジェクトの名前を変更できます。

名前が変更されたオブジェクトを参照するアクセスルールと NAT ポリシーも、新しいオブジェクト名で更新されます。

ステップ 4 エントリを選択して**[アクション（Actions）]** > **[移行しない（Do not migrate）]**を選択することで、[ルート（Routes）] エリアからルートを表示し、移行しないルートを選択できます。

ステップ 5 [サイト間VPNトンネル（Site-to-Site VPN Tunnels）] セクションに、送信元ファイアウォール設定からの VPN トンネルが一覧表示されます。各行の [送信元インターフェイス（Source Interface）]、[VPNタイプ（VPN Type）]、[IKEv1] および [IKEv2] の設定などの VPN トンネルデータを確認し、すべての行に事前共有キーの値を指定していることを確認します。

ステップ 6 複数のサイト間 VPN トンネル設定を含む設定で、複数のエントリの事前共有キーを一度に更新するには、次の手順に従います。

- 事前共有キーを更新するサイト間 VPN 設定エントリを選択します。

- ダウンロード（ ）をクリックして、テーブルを編集可能な Excel シートにエクスポートします。
- 各 VPN 設定に対してそれぞれの列に事前共有キーを入力し、ファイルを保存します。IKEv1 と IKEv2 の両方のバージョンの IKE を含む VPN 設定の場合は、カンマで区切られた 2 つの値を列に入力します。
- アップロード（ ）をクリックします。移行ツールは Excel のエントリを読み取り、VPN 設定の対応する事前共有キー列に自動的に追加します。

（注）
一括更新の一部として更新されなかった事前共有キーを更新するには、エントリを選択して **[アクション（Actions）] > [事前共有キーの更新（Update Pre-Shared Key）]**を選択するデフォルトの方法を使用するか、Excel をエクスポートしてキーを更新し、インポートします。

ターゲットの Threat Defense デバイスにすでにサイト間 VPN トポロジが設定されている場合、移行ツールはそれを検出し、削除するかどうかを選択するように求めます。削除することを選択した場合は、Management Center にログインして手動で削除しなくても、移行ツールによって削除されます。[いいえ（No）] を選択した場合、移行を続行するには、ターゲットの Threat Defense デバイスの既存の VPN 設定を手動で削除する必要があります。

ステップ 7 [リモートアクセスVPN（Remote Access VPN）] セクションでは、リモートアクセス VPN に対応するすべてのオブジェクトが Palo Alto Networks ファイアウォールから管理センターに移行され、次のように表示されます。

- [ポリシーの割り当て（Policy Assignment）]：接続プロファイル、その VPN プロトコル、ターゲットデバイス、および VPN インターフェイスの名前を確認および検証します。接続プロファイルの名前を変更するには、対応するエントリを選択し、**[アクション（Actions）] > [名前の変更（Rename）]** の順に選択します。
- [IKEV2]：IKEv2 プロトコル設定（存在する場合）と、それらにマッピングされている送信元インターフェイスを確認および検証します。
- Anyconnect パッケージ：AnyConnect パッケージおよび AnyConnect プロファイルは、移行用に送信元 デバイスから取得する必要があります。

  移行前のアクティビティの一環として、すべての AnyConnect パッケージを管理センターにアップロードします。AnyConnect プロファイルは、管理センターに直接アップロードするか、Cisco Secure Firewall 移行ツールからアップロードすることができます。

  管理センターから取得した既存の Anyconnect、Hostscan、または外部ブラウザパッケージを選択します。1 つ以上の AnyConnect パッケージを選択する必要があります。 送信元の構成で使用可能な場合は、Hostscan、dap.xml、data.xml、または外部ブラウザを選択する必要もあります。AnyConnect プロファイルはオプションです。

正しい dap.xml ファイルが、送信元のファイアウォールから取得されている必要があります。検証は、構成ファイルで使用可能な dap.xml で実行されます。検証に必要なすべてのファイルを選択してアップロードする必要があります。更新に失敗すると不完全とマークされ、Cisco Secure Firewall 移行ツールは検証に進みません。

- [アドレスプール（Address Pool）]：ここに表示されすべての IPv4 プールと IPv6 プールを確認します。
- [グループポリシー（Group-Policy）]：この領域からユーザープロファイル、管理プロファイル、およびクライアントモジュールプロファイルを選択または削除します。この領域には、クライアントプロファイルを持つグループポリシー、管理プロファイル、クライアントモジュール、およびプロファイルを持たないグループポリシーが表示されます。プロファイルが [AnyConnectファイル（AnyConnect file）] 領域に追加されている場合は、事前に選択された状態で表示されます。ユーザープロファイル、管理プロファイル、およびクライアントモジュールプロファイルを選択または削除できます。
- [接続プロファイル（Connection Profile）]：ここに表示されるすべての接続プロファイル/トンネルグループを確認します。
- [トラストポイント（Trustpoints）]：PAN ファイアウォールから管理センターへのトラストポイントまたは PKI オブジェクトの移行は、移行前アクティビティの一環であり、リモートアクセス VPN の移行を正常に実行するために不可欠です。[リモートアクセスインターフェイス（Remote Access Interface）] セクションでグローバル SSL、IKEv2、およびインターフェイスのトラストポイントをマッピングして、移行を続行します。

  SAML オブジェクトが存在する場合、SAML IDP と SP のトラストポイントを SAML セクションでマッピングできます。SP 証明書のアップロードはオプションです。特定のトンネルグループについては、トラストポイントをオーバーライドすることもできます。オーバーライドされた SAML トラストポイント構成が送信元 で使用可能な場合は、**[SAMLのオーバーライド（Override SAML）]** で選択できます。

ステップ 8 （任意）グリッド内の各構成項目の詳細をダウンロードするには、[ダウンロード（Download）] をクリックします。

ステップ 9 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 Management Center 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 Management Center 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、Management Center 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 10 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 Management Center 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 11 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「Successfully Validated」というメッセージが表示されたら、移行された構成の以下へのプッシュ： Management Center （55 ページ）に進みます。

移行された構成の以下へのプッシュ： Management Center

構成の検証に成功せず、すべてのオブジェクトの競合を解決していない場合は、移行された構成を Management Center にプッシュできません。

移行プロセスのこのステップでは、移行された構成を Management Center に送信します。脅威に対する防御 デバイスに構成を展開しません。ただし、脅威に対する防御 上の既存の構成はこのステップで消去されます。

（注） Cisco Secure Firewall 移行ツールが移行された構成を Management Center に送信している間は、構成を変更したり、デバイスに展開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 [構成のプッシュ（Push Configuration）] をクリックして、移行した 構成を Management Center 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、Management Center 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 移行が失敗した場合は、移行後レポート、ログファイル、および未解析ファイルを慎重に確認して、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 フォルダを抽出して、ログファイル、DB、および構成ファイルを表示します。

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

移行後のレポートには、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。詳細については、最適化、 構成の確認と検証 （48 ページ）を参照してください。

オブジェクトを確認して検証します。

- **カテゴリ**
  - ACL ルール合計数（移行元の構成）
  - 最適化の対象とみなされる ACL ルールの合計数。冗長、シャドウなどがあります。
- 最適化の ACL カウントは、最適化の前後にカウントされた ACL ルールの合計数を示します。

移行中に移行後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。

移行後レポートのダウンロードエンドポイント：http://localhost:8888/api/downloads/post_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、 構成がどのように移行されたかを理解します。

- Migration Summary：ASA から 脅威に対する防御 正常に移行された構成の概要。 インターフェイス、Management Center ホスト名とドメイン、ターゲット 脅威に対する防御 デバイス（該当する場合）、および正常に移行された構成要素に関する情報が含まれます。
- Selective Policy Migration：移行用に選択された特定の 機能の詳細は、[デバイス構成機能（Device Configuration Features）]、[共有構成機能（Shared Configuration Features）]、および [最適化（Optimization）] の 3 つのカテゴリ内で使用できます。
- Interface to Threat Defense Interface Mapping：正常に移行されたインターフェイスの詳細と、 構成のインターフェイスを 脅威に対する防御 デバイスのインターフェイスにマッピングした方法。これらのマッピングが期待どおりであることを確認します。

（注）
このセクションは、宛先 脅威に対する防御デバイスを使用しない移行、または移行に**インターフェイス**が選択されて**いない**場合には適用されません。

- Source Interface Names to Threat Defense Security Zones：正常に移行された PAN 論理インターフェイスと名前の詳細、およびそれらを 脅威に対する防御 のセキュリティゾーンにマッピングした方法。これらのマッピングが期待どおりであることを確認します。

（注）
アクセス制御リストと **NAT** が移行に選択されて**いない**場合、このセクションは適用されません。

- Object Conflict Handling：Management Center の既存の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 Management Center 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。

- Access Control Rules, NAT, and Routes You Chose Not to Migrate：Cisco Secure Firewall 移行ツールで移行しないように選択したルールの詳細。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。

- Partially Migrated Configuration：詳細オプションなしでもルールを移行できる詳細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 Management Center 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。

- Unsupported Configuration：Cisco Secure Firewall 移行ツールがこれらの機能の移行をサポートしていないため、移行されなかった 構成要素の詳細。これらの行を確認し、各機能が 脅威に対する防御 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、Management Center でこれらの機能を手動で構成します。

- Expanded Access Control Policy Rules：移行時に単一の Point ルールから複数の 脅威に対する防御 ルールに拡張された アクセス コントロール ポリシー ルールの詳細。

- **Actions Taken on Access Control Rules**

  - Access Rules You Chose Not to Migrate：Cisco Secure Firewall 移行ツールで移行しないように選択した アクセスコントロールルールの詳細。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、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、これらのルールを手動で構成できます。

- Access Control Rules that have IPS Policy and Variable Set Applied：IPS ポリシーが適用されているすべての アクセス コントロール ポリシー ルールの詳細。これらのルールを慎重に確認し、この機能が 脅威に対する防御 でサポートされているかどうかを確認します。
- Access Control Rules that have File Policy Applied：ファイルポリシーが適用されているすべての アクセス コントロール ポリシー ルールの詳細。これらのルールを慎重に確認し、この機能が 脅威に対する防御 でサポートされているかどうかを確認します。
- Access Control Rules that have Rule 'Log' Setting Change：Cisco Secure Firewall 移行ツールを使用して「ログ設定」が変更された アクセスコントロールルールの詳細。ログ設定の値は、False、Event Viewer、Syslog 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、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 脅威に対する防御 によってブロックされるように、Management Center でルールを構成することを推奨します。

（注）
[確認と検証（Review and Validate）] ページで IPS またはファイルポリシーを ACL に適用する必要がある場合は、移行前に管理センターでポリシーを作成することを強くお勧めします。Cisco Secure Firewall 移行ツールは接続された管理センターからポリシーを取得するため、同じポリシーを使用します。新しいポリシーを作成して複数のポリシーに割り当てると、パフォーマンスが低下し、プッシュが失敗する可能性があります。

Management Center と 脅威に対する防御 でサポートされる機能の詳細については、『Management Center Configuration Guide, Version 6.2.3』[英語] を参照してください。

ステップ 3 **移行前レポート**を開き、脅威に対する防御デバイス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 Management Center で、次の手順を実行します。

a) 脅威に対する防御 デバイスの移行された構成を確認し、次を含むすべての期待されるルールおよびその他の構成項目が移行されたことを確認します。

- アクセス制御リスト（ACL）
- ネットワークアドレス変換規則
- ポートおよびネットワークオブジェクト
- ルート（Routes）
- インターフェイス
- 動的ルートオブジェクト

b) 一部がサポートされている、サポートされていない、無視された、無効化された、および移行されなかったすべての構成項目とルールを構成します。

これらの項目とルールを構成する方法の詳細については、『Management Center Configuration Guide』[英語] を参照してください。手動構成が必要な構成項目の例を次に示します。

- プラットフォーム設定（SSH アクセスと HTTPS アクセスを含む）（「Threat Defense プラットフォーム設定」を参照）
- Syslog 設定（「Configure Syslog」を参照）
- 動的ルーティング（「Routing Overview for Threat Defense」を参照）
- サービスポリシー（「FlexConfig Policies」を参照）
- VPN 構成（「Threat Defense VPN」を参照）
- 接続ログ設定（「Connection Logging」を参照）

ステップ 5 確認が完了したら、Management Center から 脅威に対する防御 デバイスに移行された構成を展開します。

サポートされていないルールと一部がサポートされているルールについて、データが**移行後レポート**に正しく反映されていることを確認します。

Cisco Secure Firewall 移行ツールは、ポリシーを 脅威に対する防御 デバイスに割り当てます。変更が実行中の構成に反映されていることを確認します。移行されるポリシーを識別しやすくするために、これらのポリシーの説明には 構成のホスト名が含まれています。

解析のサマリー

解析のサマリーには、オブジェクト、インターフェイス、NAT、ポリシー、およびアプリケーションの数が表示されます。サマリーには、[Pre-parse Summary]、[Parse Summary]、および [Pre-push Summary] の 3 つのコンポーネントがあります。

- Pre-parse Summary：構成のアップロード後に、解析前サマリーが表示されます。この段階で、Cisco Secure Firewall 移行ツールはさまざまなコンポーネントの数を表示します。カスタムアプリケーション、またはグループで使用されているアプリケーションのみが表示されます。構成がマルチ VSYS の場合、完全な VSYS のインターフェイス数が表示されます。ポリシーで直接呼び出されるアプリケーションはカウントされないため、解析前サマリーには一部のアプリケーションが表示されません。したがって、アプリケーション数は解析のサマリーと異なります。同様の動作が NAT にも適用されます。解析前サマリーの一部のコンポーネントにはゼロカウントが表示される場合がありますが、これはこれらの構成の構成要素が 0 であることを意味しません。
- Parse Summary：変換の開始をクリックすると、解析のサマリーが表示されます。この段階で、Cisco Secure Firewall 移行ツールは構成に対してアクションを実行し、サポートされていないすべての構成がサマリーカウントから削除されます。サポートされていないポリシーは無効として Management Center に移行されるため、サポートされていないポリシーはカウントの一部になります。構成の各コンポーネントが解析されます。解析のサマリーで表示されるカウントは、移行される正確な構成カウントです。
- Pre-push Summary：構成を Management Center にプッシュするよう求めるプロンプトが表示される前に、プッシュ前サマリーが表示されます。解析前サマリーのカウントは、Cisco

Secure Firewall 移行ツールによって実行されるアクションによって、解析のサマリーと異なる場合があります。NAT で直接参照される IP は、オブジェクトとしてプッシュされます。アプリケーションがポートにマッピングされると、サービスカウントが増加し、アプリケーションがダウンします。アプリケーションマッピングを空白のままにすると、アプリケーション数は減少します。静的ルートに重複するエントリがある場合、そのエントリは削除され、カウントは減少します。

移行の失敗

移行中の解析エラーは次のとおりです。

- **解析の失敗**：構成が Cisco Secure Firewall 移行ツールにアップロードされた後に解析が失敗します。インターフェイスの不良構成が原因です。複数の IP が構成されているか、/32 または /128 の IP がインターフェイスに割り当てられている場合、解析に失敗します。

  インターフェイスに複数の IP が割り当てられている場合、またはトンネリング、ループバック、VLANインターフェイスがルーティングの一部である場合は、プッシュの失敗が発生します。

  回避策：**移行前レポート**をダウンロードし、移行レポートの [Configuration lines with errors] セクションを参照します。このセクションには、問題の原因となっている構成の詳細が表示されます。問題を修正し、Cisco Secure Firewall 移行ツールに構成を再アップロードする必要があります。

  ルート内のトンネル、ループバック、または VLAN インターフェイスによってプッシュの失敗が発生した場合は、そのようなルートを削除して移行を再試行する必要があります。このようなインターフェイスは Management Center でサポートされていないためです。

- **プッシュの失敗**：Cisco Secure Firewall 移行ツールが構成を移行し、Management Center にプッシュされているときに、プッシュの失敗が発生します。プッシュの失敗は、**移行後レポート**でキャプチャされます。

  回避策：**移行後レポート**をダウンロードし、移行レポートの [Error Reporting] セクションを参照します。このセクションには、問題の原因となっている構成の詳細が表示されます。[確認と検証（Review and Validation）] ページで問題を修正する必要があります。これには、失敗が表示されているセクションで [移行しない（do not migrate）] オプションを選択するか、または送信元構成で問題を修正し、Cisco Secure Firewall 移行ツールに構成を再アップロードします。

Cisco Secure Firewall 移行ツールのアンインストール

すべてのコンポーネントは、Cisco Secure Firewall 移行ツールと同じフォルダに保存されます。

手順

ステップ 1 Cisco Secure Firewall 移行ツールを配置したフォルダに移動します。

ステップ 2 ログを保存する場合は、`log` フォルダを切り取りまたはコピーして別の場所に貼り付けます。

ステップ 3 移行前レポートと移行後レポートを保存する場合は、`resources` フォルダを切り取りまたはコピーして別の場所に貼り付けます。

ステップ 4 Cisco Secure Firewall 移行ツールを配置したフォルダを削除します。

ヒント
ログファイルはコンソールウィンドウに関連付けられています。Cisco Secure Firewall 移行ツールのコンソールウィンドウが開いている場合、ログファイルとフォルダは削除できません。

移行例： PAN から Threat Defense 2100 へ

（注） 移行の完了後にターゲットデバイスで実行できるテスト計画を作成します。

- メンテナンス期間前のタスク
- メンテナンス期間のタスク

メンテナンス期間前のタスク

始める前に

Management Center をインストールして展開していることを確認します。詳細については、適切な『Management Center Hardware Installation Guide』[英語] および適切な『Management Center Getting Started Guide』[英語] を参照してください。

手順

ステップ 1 ネットワークに Firepower 2100 シリーズ デバイスを展開し、インターフェイスを接続してアプライアンスの電源をオンにします。

詳細については、『Cisco Threat Defense for the 2100 Series Using Management Center Quick Start Guide』[英語] を参照してください。

ステップ 2 Management Center によって管理される Firepower 2100 シリーズ デバイスを登録します。

詳細については、「Add Devices to the Management Center」を参照してください。

ステップ 3 Cisco Secure Firewall 移行ツールの最新バージョンを https://software.cisco.com/download/home/286306503/type からダウンロードして実行します。

詳細については、Cisco.com からの Cisco Secure Firewall 移行ツールのダウンロード （31 ページ）を参照してください。

ステップ 4 Cisco Secure Firewall 移行ツールを起動し、接続先パラメータを指定する場合は、Management Center に登録した Firepower 2100 シリーズ デバイスを選択します。

詳細については、Cisco Secure Firewall 移行ツールの接続先パラメータの指定 （37 ページ）を参照してください。

ステップ 5 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ます。

（注）
Cisco Secure Firewall 移行ツールを使用すると、インターフェイスタイプを 脅威に対する防御 インターフェイスタイプにマッピングできます。

詳細については、「PAN ファイアウォール 構成と Threat Defense インターフェイスのマッピング」を参照してください。

ステップ 6 論理インターフェイスをセキュリティゾーンにマッピングするときに、[自動作成（Auto-Create）]をクリックして、Cisco Secure Firewall 移行ツールで新しいセキュリティゾーンを作成できるようにします。既存のセキュリティゾーンを使用するには、手動で 論理インターフェイスをセキュリティゾーンにマッピングします。

詳細については、「セキュリティゾーンインターフェイスグループ への PAN インターフェイスのマッピング」を参照してください。

ステップ 7 このガイドの手順に従って、移行する構成を順に確認および検証し、構成を Management Center にプッシュします。

ステップ 8 移行後レポートを確認し、手動で他の構成をセットアップして 脅威に対する防御 に展開し、移行を完了します。

詳細については、「」を参照してください。

ステップ 9 移行の計画時に作成したテスト計画を使用して、Firepower 2100 シリーズ デバイスをテストします。

メンテナンス期間のタスク

始める前に

メンテナンスウィンドウの前に実行する必要があるすべてのタスクが完了していることを確認します。「メンテナンス期間前のタスク （62 ページ）」を参照してください。

手順

ステップ 1 周辺スイッチング インフラストラクチャの Address Resolution Protocol（ARP）キャッシュをクリアします。

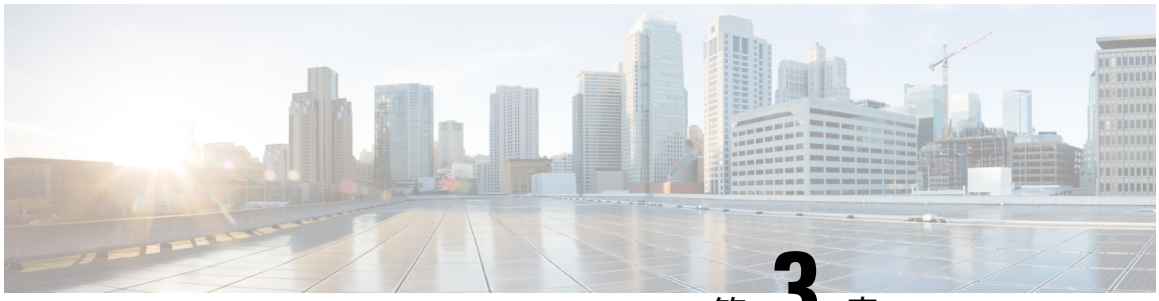
ステップ 2 周辺スイッチング インフラストラクチャから Firepower 2100 シリーズ デバイスインターフェイスの IP アドレスに対して基本的な ping テストを実行し、アクセス可能であることを確認します。

ステップ 3 Firepower 2100 シリーズ デバイスインターフェイスの IP アドレスに対するレイヤ 3 ルーティングが必要なデバイスから基本的な ping テストを実行します。

ステップ 4 Firepower 2100 シリーズ デバイスに新しい IP アドレスを割り当て、 に割り当てられた IP アドレスを再利用しない場合は、次の手順を実行します。

1. IP アドレスを参照する静的ルートを更新し、Firepower 2100 シリーズ デバイスの IP アドレスを指すようにします。
2. ルーティングプロトコルを使用している場合は、ネイバーが Firepower 2100 シリーズ デバイスの IP アドレスを予期される接続先のネクストホップとして認識していることを確認します。

ステップ 5 包括的なテスト計画を実行し、 Firepower 2100 デバイスの管理 Management Center 内でログをモニタリングします。



第 3 章

Cisco Success Network：テレメトリデータ

• Cisco Success Network - テレメトリデータ （65 ページ）

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。

移行した 構成を Management Center 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 *3*: 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	2023-04-25 10:39:19
ソース タイプ	送信元デバイスタイプ	ASA
デバイスのモデル番号	ASA のモデル番号	ASA5585-SSP-10, 5969 MB RAM, CPU Xeon 5500 series 2000 MHz, 1 CPU (4 cores)
送信元のバージョン	ASA のバージョン	9.2 (1)

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	6.5 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	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
Migration Tool Version	移行ツールのバージョン	1.1.0.1912
Migration Status	管理センターへの ASA 設定の移行のステータス	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 *4:* 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 *5:* 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 Version	Management Center のターゲットバージョン	6.2.3.3 (build 76)
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
Migration Tool Version	移行ツールのバージョン	1.1.0.1912

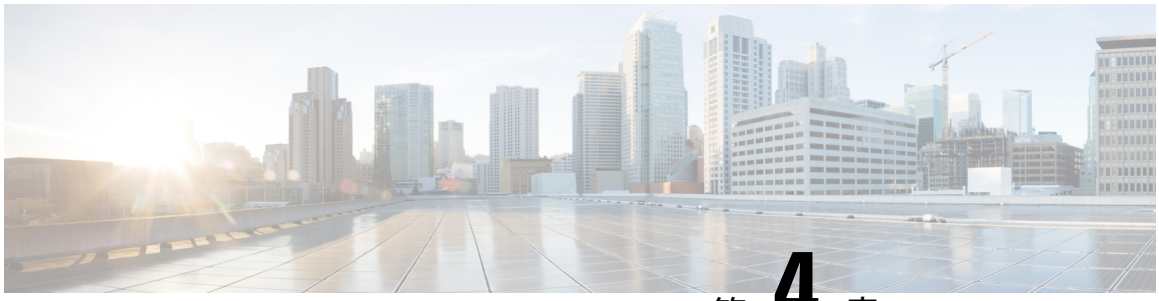
表 *6 :* 移行の概要

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
Access Rule Counts	移行された ACL ルールの合計数	0
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 *7 : 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

データ ポイント	説明	値の例
Migration Time	エンドツーエンドの移行にかかった合計時間（分）	592
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



第 4 章

移行の問題のトラブルシューティング

- Cisco Secure Firewall 移行ツールのトラブルシューティング （69 ページ）
- トラブルシューティングに使用されるログおよびその他のファイル （70 ページ）
- PAN のトラブルシューティング例：オブジェクトグループのメンバーが見つからない （70 ページ）

Cisco Secure Firewall 移行ツールのトラブルシューティング

移行が失敗するのは、通常、 PAN 構成ファイルをアップロードしているとき、または移行された構成を Management Center にプッシュしているときです。

予期しないファイル：PAN で無効なファイルが検出されました。たとえば、Mac OS を使用して zip 圧縮すると、Mac システムファイルが作成されます。Mac ファイルを削除してください。

Cisco Secure Firewall 移行ツールのサポートバンドル

Cisco Secure Firewall 移行ツールには、サポートバンドルをダウンロードして、ログファイル、DB、構成ファイルなどの役立つトラブルシューティング情報を抽出するオプションがあります。次の手順を実行します。

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フォルダを抽出して、ログファイル、DB、および構成ファイルを表示します。

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。

トラブルシューティングに使用されるログおよびその他のファイル

問題の特定とトラブルシューティングに役立つ情報は、次のファイルにあります。

ファイル	ロケーション
ログ ファイル	*<migration_tool_folder>*\logs
移行前のレポート	*<migration_tool_folder>*\resources
移行後のレポート	*<migration_tool_folder>*\resources
未解析ファイル	*<migration_tool_folder>*\resources
telemetry_sessionid_timestamp.json	*<migration_tool_folder>*\resources\telemetry_data

PANのトラブルシューティング例：オブジェクトグループのメンバーが見つからない

この例では、要素の構成にエラーがあるため、PAN構成ファイルのアップロードと解析が失敗します。

手順

ステップ1 エラーメッセージを確認して問題を特定します。

このエラーにより、次のエラーメッセージが生成されます。

参照先	エラー メッセージ
Cisco Secure Firewall 移行ツールのメッセージ	エラーを含む、解析済みの Check Point 構成ファイル。
ログ ファイル	[ERROR | objectGroupRules] > "ERROR, SERVICE_GROUP_RULE not applied for port-group object [services_epacity_nt_abc] as CheckPoint object [ica] does not exist in <service> table;" [INFO | objectGroupRules] > "Parsing object-group service:[services_gvxs06]" [INFO | objectGroupRules] > "Parsing object-group service:[services_iphigenia]" [INFO | objectGroupRules] > "Parsing object-group service:[Services_KPN_ISP]"

ステップ 2 PAN `services.xml` ファイルを開きます。

ステップ 3 services_gvxs06 という名前のオブジェクトグループを検索します。

ステップ 4 スマートダッシュボードを使用して、オブジェクトグループの欠落しているメンバーを作成します。

ステップ 5 構成ファイルをもう一度エクスポートします。詳細については、を参照してください。

ステップ 6 これ以上エラーがない場合は、新しい PAN 構成 zip ファイルを Cisco Secure Firewall 移行ツールにアップロードし、移行を続行します。

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