Cisco Secure Firewall 移行ツール リリースノート

最終更新：2024 年 8 月 21 日

Cisco Secure Firewall 移行ツールについて

Cisco Secure Firewall 移行ツールを使用すると、Management Center で管理されるサポート対象の Cisco Secure Firewall Threat Defense にファイアウォール設定を移行できます。この移行ツールでは、Cisco Secure Firewall ASA、ASA with FirePOWER Services（FPS）、FDM 管理対象デバイス、および Check Point、Palo Alto Networks、Fortinet のサードパーティ製ファイアウォールからの移行をサポートします。

このドキュメントでは、Cisco Secure Firewall 移行ツールについての重要かつリリース固有の情報について説明します。Cisco Secure Firewall のリリースに精通していて、移行プロセスを以前に経験したことがある場合でも、このドキュメントを読み、十分に理解しておくことをお勧めします。

新機能

リリースバージョン	新機能
6.0.1	**通知センター** 新しい通知センターを使用して、移行中の任意の時点で Firewall 移行ツールから送信されたすべての通知メッセージを確認できます。これらの通知は、[成功（Successes）]、[警告（Warnings）]、および [エラー（Errors）] に分類され、送信された時刻も示されます。
	Cisco Secure Firewall ASA から Threat Defense への移行 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。 詳細については、『*Migrating Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense with the Migration Tool*』ガイドの「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 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、『*Migrating an FDM-Managed Device to Cisco Secure Firewall Threat Defense with the Migration Tool*』ガイドの「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 URL オブジェクト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）] タブの [URLオブジェクト（URL Objects）] タブを確認します。 詳細については、『*Migrating Fortinet Firewall to Cisco Secure Firewall Threat Defense with the Migration Tool*』ガイドの「構成の最適化、確認および検証」を参照してください。

リリースバージョン	新機能
	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、『*Migrating Palo Alto Networks Firewall to Cisco Secure Firewall Threat Defense with the Migration Tool*』ガイドの「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 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）] タブを確認します。 詳細については、『*Migrating Check Point Firewall to Cisco Secure Firewall Threat Defense with the Migration Tool*』ガイドの「構成の最適化、確認および検証」を参照してください。
6.0.0.1	このパッチリリースにはバグ修正が含まれています。

リリースバージョン	新機能
6.0	**Cisco Secure Firewall ASA から Threat Defense への移行** • 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。 • ダイナミック仮想トンネルインターフェイス（DVTI）設定を Cisco Secure Firewall ASA から Threat Defense デバイスに移行できるようになりました。これらは、[セキュリティゾーン、インターフェイスグループ、およびVRF へのASAインターフェイスのマッピング（Map ASA Interfaces to Security Zones, Interface Groups, and VRFs）] ページでマッピングできます。この機能を適用するには、ASA のバージョンが 9.19(x) 以降であることを確認します。 • 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。 移行のためにこの機能を選択する方法については、『*Migrating Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense with the Migration Tool*』ガイドの「Specify Destination Parameters」を参照してください。

リリースバージョン	新機能
	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 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。 移行のためにこの機能を選択する方法については、『*Migrating an FDM-Managed Device to Secure Firewall Threat Defense with the Migration Tool*』ガイドの「Specify Destination Parameters」を参照してください。
	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。 移行のためにこの機能を選択する方法については、『*Migrating Check Point Firewall to Secure Firewall Threat Defense with the Migration Tool*』ガイドの「Specify Destination Parameters」を参照してください。
	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。 詳細については、『*Migrating Fortinet Firewall to Secure Firewall Threat Defense with the Migration Tool*』ガイドの「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 移行ツールの履歴情報については、次を参照してください。

- History of the ASA Firewall Migration Tool

- History of the ASA with FirePOWER Services Firewall to Threat Defense with the Firewall Migration Tool
- History of the Check Point Firewall Migration Tool
- History of the Palo Alto Networks Firewall Migration Tool
- History of the Fortinet Firewall Migration Tool
- History of the FDM-Managed Device Migration Tool

サポートされている構成

移行では、次の設定要素がサポートされています。

- ネットワークオブジェクトおよびグループ
- サービスオブジェクト（送信元と接続先に設定されたサービスオブジェクトを除く）

（注） Cisco Secure Firewall 移行ツールでは拡張サービスオブジェクト（送信元と接続先の構成）は移行しませんが、参照先の ACL と NAT のルールは完全な機能とともに移行されます。

- サービス オブジェクト グループ（ネストされたサービス オブジェクト グループを除く）

（注） Management Center ではネストはサポートされていないため、Cisco Secure Firewall 移行ツールは参照されるルールの内容を展開します。ただし、ルールは完全な機能とともに移行されます。

- IPv4 および IPv6 FQDN オブジェクトとグループ
- IPv6 変換サポート（インターフェイス、静的ルート、オブジェクト、ACL、および NAT）
- インバウンド方向とグローバル ACL のインターフェイスに適用されるアクセスルール
- 自動 NAT、手動 NAT、およびオブジェクト NAT（条件付き）
- 静的ルート、ECMP ルート、および PBR
- 物理インターフェイス
- ASA または ASA with FirePOWER Services インターフェイス上のセカンダリ VLAN は 脅威に対する防御 に移行されません。
- サブインターフェイス（サブインターフェイス ID は移行時の VLAN ID と同じ番号に常に設定されます）
- ポート チャネル

- 仮想トンネルインターフェイス（VTI）
- ブリッジグループ（トランスペアレントモードのみ）
- IP SLA のモニタ

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

（注） IP SLA モニターは、脅威に対する防御 以外のフローではサポートされていません。

- オブジェクトグループの検索

（注）
- オブジェクトグループ検索は、6.6 より前の Management Center または脅威に対する防御 のバージョンでは使用できません。
- オブジェクトグループ検索は脅威に対する防御以外のフローではサポートされていないため、無効になります。

- 時間ベースのオブジェクト

（注）
- 送信元の ASA、ASA with FirePOWER Services、および FDM 管理対象デバイスから送信先の 脅威に対する防御 にタイムゾーン構成を手動で移行する必要があります。
- 時間ベースのオブジェクトは脅威に対する防御以外のフローではサポートされていないため、無効になります。
- 時間ベースのオブジェクトは Management Center バージョン 6.6 以降でサポートされています。

- [サイト間 VPN トンネル（Site-to-Site VPN Tunnels）]
  - サイト間 VPN：Cisco Secure Firewall 移行ツールは、送信元 ASA および FDM 管理対象デバイスで暗号マップ構成を検出すると、暗号マップを Management Center VPN にポイントツーポイント トポロジとして移行します。
  - Palo Alto Networks および Fortinet ファイアウォールからのサイト間 VPN
  - ASA および FDM 管理対象デバイスからの暗号マップ（静的/動的）ベース VPN
  - ルートベース（VTI）の ASA および FDM VPN

- ASA、FDM 管理対象デバイス、Palo Alto Networks、Fortinet ファイアウォールからの証明書ベースの VPN 移行
- ASA、FDM 管理対象デバイス、Palo Alto Networks、および Fortinet のトラストポイントまたは証明書の Management Center への移行は手動で実行する必要があり、また、移行前のアクティビティに含まれている必要があります。

- 動的ルートオブジェクト、BGP、および EIGRP
  - ポリシーリスト
  - プレフィックスリスト
  - Community-List
  - 自律システム（AS）パス
  - [Route-Map]

- リモートアクセス VPN
  - SSL と IKEv2 プロトコル
  - 認証方式：[AAA のみ（AAA only）]、[クライアント証明書のみ（Client Certificate only）]、および [AAA とクライアント証明書（AAA + Client Certificate）]
  - AAA：Radius、ローカル、LDAP、および AD
  - 接続プロファイル、グループポリシー、動的アクセスポリシー、LDAP 属性マップ、および証明書マップ
  - 標準的な ACL と拡張 ACL
  - RA VPN カスタム属性と VPN ロードバランシング
  - 移行前のアクティビティの一環として、次の手順を実行します。
    - ASA、FDM 管理対象デバイス、Palo Alto Networks、および Fortinet ファイアウォールのトラストポイントを PKI オブジェクトとして手動で Management Center に移行します。
    - AnyConnect パッケージ、Hostscan ファイル（Dap.xml、Data.xml、Hostscan Package）、外部ブラウザパッケージ、および AnyConnect プロファイルを送信元 ASA および FDM 管理対象デバイスから取得します。
    - すべての AnyConnect パッケージを Management Center にアップロードします。
    - AnyConnect プロファイルを Management Center に直接アップロードするか、または Cisco Secure Firewall 移行ツールからアップロードします。
    - Live Connect ASA からプロファイルを取得できるようにするには、ASA で **ssh scopy enable** コマンドを有効にします。

- ACL 最適化

  ACL 最適化は、次の ACL タイプをサポートします。

  - 冗長 ACL：2 つの ACL の構成とルールのセットが同じ場合、基本以外の ACL を削除してもネットワークに影響はありません。
  - シャドウ ACL：最初の ACL は、2 番目の ACL の設定を完全にシャドウイングします。

（注） ACL の最適化は現在、Palo Alto Networks と ASA with FirePower Services（FPS）では使用できません。

Cisco Secure Firewall 移行ツールのサポートされている構成の詳細については、次を参照してください。

- サポートされている ASA の設定
- サポートされている ASA with FirePOWER Services の構成
- サポートされているチェックポイントの設定
- サポートされる PAN 構成
- サポートされている FortiNet の設定
- サポートされる FDM 管理対象デバイス構成

移行ワークフロー

Cisco Secure Firewall 移行ツールの移行ワークフローについては、次を参照してください。

- ASA 構成ファイルのエクスポート
- ASA with FirePOWER Services 構成ファイルのエクスポート
- Check Point 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の構成のエクスポート
- Fortinet ファイアウォールからの構成のエクスポート
- FDM 管理対象デバイス構成ファイルのエクスポート

移行レポート

Cisco Secure Firewall 移行ツールは、次のレポートを移行の詳細とともに HTML 形式で提供します。

- 移行前のレポート
- 移行後のレポート

Cisco Secure Firewall 移行ツールの機能

Cisco Secure Firewall 移行ツールは、次の機能を提供します。

- 分析およびプッシュ操作を含む移行全体の検証
- オブジェクト再利用機能
- オブジェクト競合の解決
- インターフェイス マッピング
- インターフェイス オブジェクトの自動作成または再利用（セキュリティゾーンとインターフェイス グループ マッピングに対する ASA name if）
- インターフェイス オブジェクトの自動作成または再利用
- 自動ゾーンマッピング
- ユーザー定義のセキュリティゾーンとインターフェイスグループの作成
- ユーザー定義のセキュリティゾーンの作成
- 送信先 Threat Defense デバイスのサブインターフェイス制限チェック
- サポートされるプラットフォーム：
  - ASA Virtual から Threat Defense Virtual へ
  - FDM Virtual から Threat Defense Virtual へ
  - 同じハードウェアでの移行（X から X デバイスへの移行）
  - X から Y デバイスへの移行（Y に多数のインターフェイスが存在）
- ACP ルールアクションに対する送信元 ASA、FDM 管理対象デバイス、Fortinet、および Checkpoint の ACL 最適化。

インフラストラクチャとプラットフォームの要件

Cisco Secure Firewall 移行ツールには、次のインフラストラクチャおよびプラットフォームが必要です。

- 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
- Google Chrome がシステムのデフォルト ブラウザ

ヒント　移行ツールを使用するときは、ブラウザで全画面表示モードを使用することをお勧めします。

- システムごとに Cisco Secure Firewall 移行ツールのシングルインスタンス
- Management Center と Threat Defense がバージョン 6.2.3.3 以降であること

（注）　新しいバージョンをダウンロードする前に、以前のビルドを削除する。

未解決および解決済みの問題

未解決の問題

不具合 ID	説明
CSCwi97232	Fortinet ファイアウォールの NAT 設定が解析されません。
CSCwi93856	特殊文字が原因で、Fortinet の移行で設定のプッシュエラーが発生します。

解決済みの問題

不具合 ID	説明
CSCwj25133	ASA VPN オブジェクトのプッシュ中にエラーが発生します - ローカル変数ペイロード。
CSCwj23453	PAN 準備の概要で、すべての機能のエントリが 0 と表示されます。
CSCwj10882	新しいハードウェアへの FDM の移行がプッシュ段階で失敗します。

不具合 ID	説明
CSCwj13908	Fortinet ファイアウォールの VPN 設定が、同じインターフェイスにマッピングされます。
CSCwi89163	Fortinet ファイアウォールの移行が、解析時にオブジェクトグループエラーで失敗します。
CSCwi76132	Fortinet ファイアウォールの移行の [RA VPN] タブが予期したとおりに点滅せず、[AnyConnect] タブが空白になります。
CSCwi75821	50 を超えるオブジェクトが移行されても、ASA 移行の [SNMP] タブに次のページの情報が表示されません。
CSCwi63611	Fortinet ファイアウォールの移行が ACL 解析エラーで失敗します。
CSCwi37184	FDM 共有設定の移行が、地理位置情報オブジェクトのプッシュ障害で失敗します。
CSCwi83826	Fortinet RA VPN 設定オブジェクトの再使用が機能しません。

未解決の警告および解決済みの警告

このリリースで未解決の警告には、Cisco バグ検索ツールを使用してアクセスできます。この Web ベースツールから、この製品やその他のシスコハードウェアおよびソフトウェア製品でのバグと脆弱性に関する情報を保守するシスコバグトラッキングシステムにアクセスできます。

（注） Cisco Bug Search Tool にログインしてこのツールを使用するには、Cisco.com アカウントが必要です。アカウントを持っていない場合は、Cisco.com でアカウントに登録できます。バグ検索ツールの詳細については、「Bug Search Tool（BST）ヘルプおよび FAQ」を参照してください。

Cisco Secure Firewall 移行ツールの未解決および解決済みの警告の最新リストについては、未解決の警告および解決済みの警告ダイナミッククエリを使用してください。

関連資料

- Migrating ASA Firewall to Firewall Threat Defense with the Secure Firewall Migration Tool

- Migrating ASA Firewall with FirePOWER Services to Firewall Threat Defense with the Secure Firewall Migration Tool
- Cisco Secure Firewall ASA から Threat Defense への機能マッピング
- 移行ツールを使用した Cisco Secure Firewall Threat Defense への FDM 管理対象デバイスの移行
- Migrating Check Point Firewall to Firewall Threat Defense with the Secure Firewall Migration Tool
- Migrating Palo Alto Networks Firewall to Firewall Threat Defense with the Secure Firewall Migration Tool
- Migrating Fortinet Firewall to Firewall Threat Defense with the Secure Firewall Migration Tool
- Cisco Defense Orchestrator を利用した FDM 管理対象デバイスへの ASA の移行
- Navigating the Cisco Secure Firewall Migration Tool Documentation
- Cisco Secure Firewall Migration Tool Compatibility Guide
- Cisco Secure Firewall Migration Tool Error Messages
- Open Source Used in Cisco Secure Firewall Migration Tool

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。