Cisco Secure Firewall 移行ツール 7.7.10.4 リリースノート

最終更新：2026 年 1 月 19 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 Microsoft Azure、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	機能	説明
7.7.10.4	パッチリリース	このパッチリリースにはバグ修正が含まれています。詳細については、「未解決および解決済みの問題」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 Firepower Threat Defense 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 FMC に移行します。

（注） IP SLA モニターは、Firepower Threat Defense 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 FMC または Firepower Threat Defense 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 Firepower Threat Defense 以外のフローではサポートされていないため、無効になります。

- 時間ベースのオブジェクト

（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 Firepower Threat Defense にタイムゾーン構成を手動で移行する必要があります。
- 時間ベースのオブジェクトは Firepower Threat Defense 以外のフローではサポートされていないため、無効になります。
- 時間ベースのオブジェクトは FMC 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 FMC 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 FMC 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 FMC 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 FMC にアップロードします。
    - AnyConnect プロファイルを FMC 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。

- 無効化されたACL：ファイアウォールの設定で明示的にオフになっているACL。ルールは構成ファイルに存在しますが、Cisco Secure Firewall移行ツールはトラフィックを処理するときにそれらを無視します。

（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
- Microsoft Azure ネイティブファイアウォール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

解決済みの問題

不具合 ID	説明
CSCwq44215	拡張ACLは、個別のネットワークオブジェクトとしてではなく、サイト間VPN内の保護されたネットワークの下でマッピングされます。
CSCwq83914	Cisco Secure Firewall 移行ツールは、ホスト値とリテラル値に対して新しいオブジェクトを作成するのではなく、ホストエントリとリテラルエントリを FMC に直接移行する必要があります。
CSCwq91811	設定が FMC にプッシュされると、誤って移行された NAT インターフェイスが原因で、Cisco Secure Firewall 移行ツールを使用した Check Point ファイアウォールの移行が失敗します。
CSCwr35492	Firewall 移行ツールを使用した適応型セキュリティアプライアンス（ASA）with FirePOWER Services（FPS）の FTD への移行が、解析ステージ中に失敗します。
CSCwr51172	Cisco Secure Firewall 移行ツールを使用して Check Point ファイアウォールから FTD に設定を移行するときに、ツールが ACL ルールを誤った順序で移行します。
CSCwr51177	Cisco Secure Firewall 移行ツールを使用した Check Point ファイアウォールの FTD への移行で、ACL ルール名が正しく移行されません。
CSCwr51179	Cisco Secure Firewall 移行ツールを使用して Check Point ファイアウォールから FTD に設定を移行するときに、ツールが NAT ルールを誤った順序で移行します。

不具合 ID	説明
CSCwr51265	Cisco Secure Firewall 移行ツールでの ASA から FTD への移行が失敗し、次のエラーが表示されます。 `'Port-channel1: Invalid interface name passed or this name is used'`
CSCwr55462	ACL 最適化で、同じ設定が複数回実行されると、誤った一意の結果カウントが表示されます。
CSCwr55468	エアギャップビルドでは、ユーザーが最初にログインしたときに、`"You will be redirected to cisco.com Login Page"` というダイアログボックスは表示されません。ただし、ログアウトして再度ログインしようとすると、ダイアログボックスが表示されます。
CSCwr61478	読み取り専用リソースに関連するエラーと繰り返しの深度の問題が原因で、サイト間 VPN プッシュ中に Firewall 移行ツールでの ASA から FTD への移行が失敗します。
CSCwr63983	Firewall 移行ツールでの ASA 移行タスクで、オブジェクトが FMC のサブドメインまたは別のドメインにすでに存在する場合、オブジェクトの作成または再利用に失敗します。その結果、エラーが発生し、オブジェクトの移行が妨げられます。

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

- Navigating the Cisco Secure Firewall Migration Tool Documentation
- 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
- Cisco Secure Firewall 移行ツールを使用した Microsoft Azure ネイティブファイアウォールから Cisco Secure Firewall Threat Defense への移行
- 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
- Migrating Cisco Secure Firewall ASA to Cisco Multicloud Defense with the Migration Tool
- Migrating Palo Alto Networks Firewall to Cisco Multicloud Defense with the Migration Tool
- Cisco Secure Firewall Migration Tool Compatibility Guide

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。