Cisco Secure Firewall 移行ツール 10.0 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
10.0	CSF220 シリーズデバイスの移行サポート	このリリースでは、CSF200 シリーズデバイスの包括的な移行サポートが導入されています。 サポートされる移行：すべて
	Firewall Management Center および Firewall Threat Defense 10.0 リリースの移行サポート	このリリースへのスムーズな移行を容易にするために設計された Firewall Management Center および Firewall Threat Defense 10.0 の移行サポート。 サポートされる移行：すべて
	テレメトリの機能強化	このリリースでは、テレメトリ機能が大幅に強化され、分析および障害対応のためのデータ収集が改善されています。 サポートされる移行：すべて
	解析パフォーマンスの向上	このリリースでは、解析パフォーマンスが大幅に強化され、システムの応答性と効率性が向上しています。 サポートされている移行：Check Point ファイアウォールから Firewall Threat Defense へ、Palo Alto Networks ファイアウォールから Firewall Threat Defense へ、ASA ファイアウォールから Firewall Threat Defense への移行。
	デュアル NAT サポートの機能強化	デュアル ネットワーク アドレス変換（NAT）機能を強化し、ユーザー体験を向上させます。 参照：「Check Point Configuration Support」 サポートされる移行：Check Point ファイアウォールから Firewall Threat Defense への移行

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
CSCwq68720	移行された設定に IPv4 マッピングされた IPv6 アドレスが含まれている場合、解析は失敗します。
CSCwq90564	Firewall 移行ツール 7.7.10.1 バージョンを使用した ASA から Firewall Threat Defense への移行では、部分的なサイト間 VPN が無視されます。
CSCwr42202	ファイアウォール移行ツールを使用して ASA 設定を Firewall Management Center に移行する場合、リモートアクセス VPN（RAVPN）機能が移行対象としてマークされると、アクセス制御リスト（ACL）は無視されます。
CSCwr76541	移行中に最適化が正しく機能しません。
CSCwr77655	Firewall 移行ツールを使用した ASA から Firewall Threat Defense への移行中、解析後に [次へ（Next）] ボタンがグレー表示されます。
CSCwr77681	Firewall 移行ツールを使用した Fortinet ファイアウォールから Firewall Threat Defense への移行中、解析後に [次へ（Next）]、[ログアウト（Logout）]、[設定（Settings）] などのボタンがグレー表示されます。
CSCwr81648	Firewall 移行ツールを使用して ASA から Firewall Threat Defense に移行するときに、ターゲットの Firewall Threat Defense がデータインターフェイスとして管理されている場合、このツールではデバイス設定（インターフェイス、ルート、またはサイト間 VPN）を解析またはプッシュできません。
CSCwr85336	Firewall 移行ツールを使用した Palo Alto から Firewall Threat Defense への移行では、解析概要ページに NAT が表示されません。
CSCwr96827	Firewall 移行ツールを使用した Fortinet ファイアウォールから Firewall Threat Defense への移行では、アプリケーション マッピング ステージでエラーがスローされます。
CSCwr98247	Firewall Management Center バージョン 10.0 が選択されると、Firewall 移行ツールの [Firewall Management Center] 選択ページにエラーメッセージが表示されます。
CSCws16819	Fortinetファイアウォールの Firewall Threat Defense ACL設定への移行は、解析ステージで失敗します。
CSCws22470	Firewall 移行ツールを使用した Palo Alto から Firewall Threat Defense への移行が失敗し、次のエラーメッセージが表示されます。 `"Str" object has no attribute "toXML"`

不具合 ID	説明
CSCws23077	Firewall 移行ツールを使用した ASA から Firewall Threat Defense への移行では、オブジェクトグループの設定が移行されません。
CSCws24428	移行が完了した後も、システムによる remaining_time API の呼び出しが続きます。
CSCws24481	ユーザーグループ設定の解析中に見積の処理が失敗するとエラーが発生します。
CSCws24497	一部のオブジェクト名に、IPアドレスの形式を模倣した下線が含まれています。設定パーサーがこれらの名前にサブネット表記が含まれていると誤って解釈し、「/」を使用してアドレスを分割しようとします。その結果、ValueError が発生します。
CSCws24608	Firewall 移行ツールを使用した ASAから Firewall Threat Defense への移行ですべての ACL がすでに最適化されていますが、[続行（Proceed）] ボタンをクリックすると [最適化（Optimization）] ダイアログボックスが表示されます。
CSCws25006	Firewall 移行ツールを使用した FDM 管理対象デバイスから Cisco Secure Firewall Threat Defense デバイスへの移行の際、DHCP 設定のプッシュ中にエラーが発生しました。
CSCws25852	次の解析ステージでエラーが発生しました。 `Object Network range rule has failed, too many values to unpack (expected 2)`
CSCws25865	Firewall 移行ツールを使用した ASA から Firewall Threat Defense への移行で、部分的なサイト間 VPN が Firewall 移行ツールバージョン 7.7.10.1 によって無視されます。
CSCws25869	Firewall 移行ツールを使用して ASA から Firewall Threat Defense に移行する際、[事前共有キー（Preshared Key）] フィールドへの入力中に情報メッセージが繰り返し表示されます。
CSCws25870	Firewall 移行ツールを使用した ASA から Firewall Threat Defense への移行で、ツールが解析ステージでサイト間トンネル設定を無視します。
CSCws25950	Firewall 移行ツールを使用した ASA から Firewall Threat Defense への移行に失敗しました。エラーメッセージが次のように表示されます。 `"Error while pushing s2s vpn: Object for Type Ike2 and UUID null is not found"`
CSCws26263	Firewall 移行ツールを使用した ASA から Firewall Threat Defense への移行中に、ページが更新された後でも、AnyConnect ファイルが Firewall Management Center によって取得されません。

不具合 ID	説明
CSCws27417	Firewall 移行ツールを使用した Palo Alto から Firewall Threat Defense への移行で、[設定の最適化、確認、および検証（Optimize, Review and Validate the Configuration）] ページに警告メッセージが表示されます。
CSCws27468	Firewall 移行ツールを使用した Palo Alto から Firewall Threat Defense への移行で、設定の解析後にルートと VPN がサポートされません。
CSCws27674	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）から Firewall Threat Defense への移行で、RA VPN のプッシュ中に、次のエラーにより移行が失敗します。 `External proxy invoked LwVPNApi commitWithDomain method and ran into an unexpected error com.cisco.nm.vms.rpc.shared.exception.USMException: Invalid Reference One or more of the selected objects was not found, or may have been deleted by another user or activity. Check the Audit Report to see if any of the selected objects was deleted.`
CSCws27993	Firewall 移行ツールが「`inside_access_in`」という名前のルールを解析した後に ACL の解析を停止します。
CSCws28174	Firewall 移行ツールでの ASA から Firewall Threat Defense への移行が、サイト間 VPN プッシュ中に失敗し、次のエラーが表示されます。 `Unsupported or Invalid value for endpoint interface. VPN supports only routed mode interfaces. In case of VRF enabled device, only interfaces that are part of global VRF are supported.`
CSCws28557	[セキュリティゾーンのマッピング（Map Security Zones）] ページで、Firewall 移行ツールが Palo Alto から Firewall Threat Defense への移行をブロックします。
CSCws28568	Firewall 移行ツールを使用した ASA から Firewall Threat Defense への移行で、設定に ACL がない場合でも、ツールが ACL 最適化の必要性を示します。
CSCws29822	Firewall 移行ツールを使用した ASA から Firewall Threat Defense への移行が、拡張 ACL のプッシュ中に失敗します。
CSCws29832	Firewall 移行ツールを使用した ASA から Firewall Threat Defense への移行で、グループポリシーのプッシュ中にエラーが発生します。
CSCws29839	Firewall 移行ツールが API トークンを使用して クラウド提供型 Firewall Management Center に接続できません。
CSCws30006	デモモードとアップロードタイプがテレメトリ電子メールに表示されません。
CSCws31190	デバイス名が重複しているため、FDM 管理対象デバイスから Firewall Threat Defense デバイスへの登録に失敗しました。

不具合 ID	説明
CSCws32615	Firewall 移行ツールを使用した ASA から Firewall Threat Defense への移行の際、すべての ACL がすでに最適化されています。それでも、[ACLの最適化（Optimize ACL）] ボタンが引き続き表示されます。
CSCws32977	Firewall 移行ツールを使用した Fortinet ファイアウォールから Firewall Threat Defense への移行で、RA VPN のプッシュ中に次のエラーにより移行が失敗します。 `Error while pushing ra vpn: External proxy invoked LwVPNApi commitWithDomain method and ran into an unexpected error com.cisco.nm.vms.rpc.shared.exception.ValidationException: Configure at least one security zone or interface group in access interfaces to enable Remote Access VPN.`
CSCws33225	Cisco Secure Firewall 移行ツールを使用した Fortinet ファイアウォールから Firewall Threat Defense への移行が、RA VPN のプッシュ中に次のエラーによりブロックされます。 `Only IPv4 Network or Host types are allowed for objects. An object that is not in IPv4 format has been introduced. Please remove the object or modify the object to meet the requirements.`
CSCws34300	Firewall 移行ツールを使用した Check Point（r80-r81）から Firewall Threat Defense への移行が、設定の解析中に次のエラーにより失敗します。 `cannot access local variable 'extracted_dual_nat_acls' where it is not associated with a value`
CSCws34347	Firewall 移行ツールを使用した Check Point から Firewall Threat Defense への移行で、設定の解析後に移行前レポートをダウンロードできません。

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。

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

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。

関連資料

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

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、以下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、以下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。

ファイアウォール移行ツールのドキュメントへのリンク

- 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。