

Cisco Secure Firewall 移行ツール 7.7.10.3 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
7.7.10.3	オブジェクト競合の修復	<p>Cisco Secure Firewall 移行ツールは、FMC に設定を展開するときに、オブジェクト名または値の重複によって引き起こされる競合を特定できるようになりました。その後ツールは、これらの競合を解決するために適切なアクションを実行するようにユーザーに求めます。</p> <p>「Push the Migrated Configuration to Firewall Management Center」を参照してください。</p> <p>サポートされる移行：すべて</p>
	パフォーマンスの最適化	<p>パフォーマンスを向上させるために、ACL 最適化分析時間が短縮されました。[設定の最適化、確認、検証 (Optimize, Review and Validate Configuration)] ウィンドウにバナーが表示され、[ACL最適化 (Optimize ACL)] を選択してから [続行 (Proceed)] をクリックすると、ACL 最適化分析にかかるおおよその時間が示されます。</p> <p>参照：「Optimize, Review and Validate the Configuration」</p> <p>サポートされる移行：すべて</p>
	無効化された ACL ルール	<p>[設定の最適化、確認、検証 (Optimize, Review and Validate Configuration)] > [ACL最適化 (Optimize ACL)] ウィンドウで、無効化された ACL のリストを表示できるようになりました。この機能強化により、移行プロセスがより効率的になります。</p> <p>参照：「Optimize, Review and Validate the Configuration」</p> <p>サポートされる移行：すべて</p>
	設定の最適化	<p>移行中の最適化プロセスを合理化するために、Cisco Secure Firewall 移行ツールは、すべての属性が最適化されていることを確認します。[設定の最適化、確認、検証 (Optimize, Review and Validate Configuration)] ウィンドウで [検証 (Validate)] をクリックすると、欠落している属性が [設定の最適化 (Optimize Your Configuration)] ダイアログボックスに表示されます。</p> <p>参照：「Optimize, Review and Validate the Configuration」</p> <p>サポートされる移行：すべて</p>

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 チャンネル

- 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す、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

未解決の問題

不具合 ID	説明
CSCwq91811	Cisco Secure Firewall 移行ツールでの Check Point ファイアウォールの移行の場合、設定を FMC に適用した後、送信元インターフェイスと宛先インターフェイスの両方に同じインターフェイスマッピングが表示されるため、設定のエクスポートが失敗します。

解決済みの問題

不具合 ID	説明
CSCwq69641	<p>設定を Palo Alto ファイアウォールから FTD に移行するために CDO から Firewall 移行ツールを起動した後、設定のエクスポートが失敗します。</p> <p>次のエラーメッセージが表示されます。</p> <p>Blocked - division by zero</p>

不具合 ID	説明
CSCwr02764	<p>Firewall 移行ツールでの Palo Alto 設定の移行が、FMC への設定のプッシュ中に失敗し、次のエラーメッセージが表示されます。</p> <p>The object name 'object_name_' already exists. 新しい名前を入力します。</p> <p>移行元のプラットフォームで名前に含まれるスペースがサポートされている場合、Firewall 移行ツールによってスペースが下線に置き換えられます。FMC に下線付きの類似した名前がすでに存在する場合、検証の際、ツールはその名前を重複としてレポートしません。その結果、エラーにより移行が失敗します。</p>
CSCwr08989	<p>Live Connect を介した CP 設定の抽出中に、Cisco Secure Firewall 移行ツールを使用した Check Point (CP) ファイアウォールの移行が失敗します。</p>
CSCwr48003	<p>macOS で、Finder UI から [圧縮 (Compress)] オプションを使用して構成 zip ファイルを作成する際に、Cisco Secure Firewall 移行ツールへのアップロードが失敗します。ただし、コマンドラインインターフェイスを使用して同じ zip ファイルを作成すると、Cisco Secure Firewall 移行ツールへのアップロードは正常に動作します。</p>

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。