Cisco Secure Firewall Threat Defense バージョン 7.4 モデル移行ガイド

改訂：2024 年 1 月 18 日

Cisco Secure Firewall Threat Defense モデルの移行について

Firewall Threat Defense のモデル移行ウィザードを使用すると、古い脅威防御モデルから新しいモデルに、デバイス固有の設定とインターフェイス設定を移行できます。また、ソースデバイスに割り当てられているすべてのポリシー（サイト間 VPN ポリシーを除く）をターゲットデバイスに移行することもできます。

移行でサポートされるデバイス

サポートされているソースデバイス

- Cisco Firepower 1120
- Cisco Firepower 1140
- Cisco Firepower 1150
- Cisco Firepower 2110
- Cisco Firepower 2120
- Cisco Firepower 2130
- Cisco Firepower 2140

（注） ソースデバイスはバージョン 7.0 以降である必要があります。

サポートされるターゲットデバイス

- Cisco Secure Firewall 3105
- Cisco Secure Firewall 3110
- Cisco Secure Firewall 3120
- Cisco Secure Firewall 3130
- Cisco Secure Firewall 3140

（注） Cisco Secure Firewall 3110、3120、3130、および 3140 デバイスは、バージョン 7.1 以降である必要があります。Cisco Secure Firewall 3105 は、バージョン 7.3 以降である必要があります。

移行用のライセンス

スマート ライセンス アカウントにデバイスを登録する必要があります。移行すると、ソースデバイスのライセンスがターゲットデバイスにコピーされます。

移行の前提条件

- ソースデバイスとターゲットデバイスを Management Center に登録する必要があります。
- スマート ライセンス アカウントには、ターゲットデバイスのソフトウェア利用資格が必要です。
- ターゲットデバイスは、何も設定されていない新しく登録されたデバイスにすることを推奨します。
- ソースデバイスとターゲットデバイスは以下の点が同じである必要があります。
  - ドメイン
  - ファイアウォールモード：ルーテッドまたはトランスペアレント
  - コンプライアンスモード
- ターゲットデバイスは以下の状態にはできません。
  - マルチインスタンスモード
  - クラスタの一部
- ユーザーは、デバイスの変更権限を持っている必要があります。
- ソースデバイスの設定は有効で、エラーがない必要があります。
- ソースデバイスには、保留中の展開を設定できます。ただし、移行中は、いずれのデバイスでも展開、インポート、またはエクスポートタスクを実行しないでください。
- ソースデバイスが HA ペアの一部である場合、ターゲットデバイスが HA ペアの一部である必要はなく、その逆も同様です。移行によって HA ペアが形成されることも、分断されることもありません。

ウィザードで移行される設定

移行ウィザードにより、次の設定が送信元デバイスからターゲットデバイスにコピーされます。

- ライセンス
- インターフェイス設定
- インラインセット設定
- ルーティング設定
- DHCP および DDNS 構成
- 仮想ルータ設定
- ポリシー

- 関連するオブジェクトとオブジェクトのオーバーライド
- プラットフォーム設定
- リモートブランチ展開の構成

移行ウィザードにより、次のポリシー設定が送信元デバイスからターゲットデバイスにコピーされます。

- 正常性ポリシー
- NAT ポリシー
- QoS ポリシー
- リモートアクセス VPN ポリシー
- FlexConfig ポリシー
- アクセス コントロール ポリシー
- プレフィルタ ポリシー
- IPS ポリシー
- DNS ポリシー
- SSL ポリシー
- マルウェアポリシーとファイルポリシー
- アイデンティティ ポリシー

移行ウィザードにより、次のルーティング設定が送信元デバイスからターゲットデバイスにコピーされます。

- ECMP
- BFD
- OSPFv2/v3
- EIGRP
- RIP
- BGP
- ポリシーベースルーティング
- Static Route
- マルチキャスト ルーティング
- [仮想ルータ（Virtual Router）]

移行ウィザードにより、次のインターフェイスが送信元デバイスからターゲットデバイスにコピーされます。

- 物理インターフェイス

- サブインターフェイス
- EtherChannel インターフェイス
- □ブリッジ グループ インターフェイス
- VTI インターフェイス
- VNI インターフェイス
- ループバック インターフェイス

移行の制限事項

- ウィザードは移行しません。
  - サイト間 VPN ポリシー
  - SNMP の構成

    移行後、デバイスのプラットフォーム設定を使用して SNMP を設定できます。
- 一度に実行できる移行は 1 つだけです。
- 送信元インターフェイスの速度、自動ネゴシエーション、およびデュプレックス設定がターゲットデバイスのマッピングされたインターフェイスに対して有効な場合、値がコピーされます。有効でない場合、これらのパラメータはデフォルト値に設定されます。
- リモートアクセス VPN トラストポイント証明書が登録されていません。トラストポイント証明書は、展開前に手動で登録する必要があります。
- デフォルトでは、移行後にソースデバイスで Snort 2 が使用されている場合でも、ターゲットデバイスでは Snort 2 ではなく Snort 3 が使用されます。
- HA デバイスの場合：
  - ターゲットデバイス：フェールオーバー構成の一部であるインターフェイスはマッピングできません。それらのインターフェイスは、ウィザードで無効化されています。
  - ソースデバイスとターゲットデバイス：ウィザードでは、監視対象インターフェイス、フェールオーバーのトリガー基準、インターフェイス MAC アドレスなどの HA 構成は移行されません。移行後に、必要なパラメータを手動で設定する必要があります。

Cisco Secure Firewall Threat Defense の移行

始める前に

移行に関する前提条件と制限事項を確認してください。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

ステップ 2 ページの右上にある [移行（Migrate）] をクリックします。

ステップ 3 [ようこそ（Welcome）] 画面で [開始（Start）] をクリックします。

ステップ 4 [ソースデバイス（Source Device）] ドロップダウンリストからデバイスを選択します。

デバイスが HA ペアの一部である場合、HA ペアのコンテナ名のみが表示されます。

ステップ 5 [Next] をクリックします。

ステップ 6 [ターゲットデバイス（Target Device）] ドロップダウンリストからデバイスを選択します。

デバイスが HA ペアの一部である場合、HA ペアのコンテナ名のみが表示されます。

ステップ 7 [Next] をクリックします。

ステップ 8 [インターフェイスの設定（Configure Interfaces）] ステップで、ソースデバイスの物理インターフェイスをターゲットデバイスの物理インターフェイスにマッピングします。

すべてのインターフェイスのマッピングは、必須ではありません。すべての名前付きインターフェイスと、他のインターフェイスの一部であるインターフェイスをマッピングする必要があります。HA フェールオーバー構成の一部であるインターフェイスはマッピングできません。それらのインターフェイスは、ウィザードで無効化されています。ウィザードでは、ユーザーが提供するインターフェイスマッピングに従って、論理インターフェイスが作成されます。

- [デフォルトのマッピング（Map Default）] をクリックして、デフォルトのインターフェイスマッピングを設定します。

  たとえば、ソースデバイスの Ethernet1/1 は、ターゲットデバイスの Ethernet1/1 にマッピングされます。

- すべてのマッピングをクリアするには、[すべてをクリア（Clear All）] をクリックします。

ステップ 9 [Next] をクリックします。

ステップ 10 [マッピングの表示（View Mappings）] をクリックして、インターフェイスマッピングを確認します。

ステップ 11 [送信（Submit）] をクリックして移行を開始します。

ステップ 12 [通知（Notifications）] > [タスク（Tasks）] ページに移行ステータスが表示されます。

次のタスク

移行が成功したら、デバイスを展開できます

展開は必須ではなく、構成を検証し、必要に応じて展開できます。ただし、展開前に、移行のベストプラクティス（7 ページ）に記載されているアクションを実行してください。

移行のベストプラクティス

移行が成功したら、展開前に次のアクションを実行することをお勧めします。

- 送信元デバイスが稼働中の場合は、インターフェイスの IP アドレスを変更します（それらのアドレスが送信元デバイスからターゲットデバイスにコピーされるため）。
- 必ず、変更した IP アドレスで NAT ポリシーを更新してください。
- 移行後にインターフェイスの速度がデフォルト値に設定される場合は、それらの速度を設定します。
- ターゲットデバイスにデバイス証明書がある場合は、再登録します。
- HA セットアップがある場合は、監視対象インターフェイス、フェールオーバーのトリガー基準、インターフェイス MAC アドレスなどの HA パラメータを設定します。
- 移行後にリセットされる診断インターフェイスを設定します。
- （任意）デバイスのプラットフォーム設定を使用して SNMP を設定します。
- （任意）リモートブランチ展開の設定を指定します。

  ソースデバイスまたはターゲットデバイスにデータインターフェイスを介したマネージャアクセス権があった場合、移行後にマネージャアクセス権が失われます。ターゲットデバイスのマネージャアクセス設定を更新します。詳細については、『Cisco Secure Firewall Management Center Device Configuration Guide』またはオンラインヘルプの「*Change the Manager Access Interface from Management to Data*」を参照してください。
- （任意）必要に応じてサイト間 VPN を設定します。これらの設定は、送信元デバイスから移行されません。
- 展開前に展開プレビューを表示します。[展開（Deploy）]>[高度な展開（Advanced Deploy）] を選択し、デバイスの **[プレビュー（Preview）]**（ ） アイコンをクリックします。

【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。

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/

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。