コンフィギュレーションのインポートとエクスポート

次のトピックでは、インポート/エクスポート機能を使用する方法について説明します。

コンフィギュレーションのインポート/エクスポートについて

インポート/エクスポート機能を使用して、アプライアンス間で構成をコピーできます。インポート/エクスポートはバックアップ ツールではありませんが、展開に新しいアプライアンスを追加するプロセスを簡素化できます。

単一の設定をエクスポートすることや、（同じタイプまたは異なるタイプの）一連の設定を単一操作でエクスポートすることができます。後に別のアプライアンスにパッケージをインポートするとき、パッケージ内のどの設定をインポートするかを選択できます。

エクスポートされたパッケージには、その構成のリビジョン情報が含まれ、これにより、別のアプライアンスにその構成をインポートできるかどうかが決まります。アプライアンスに互換性があるものの、パッケージに重複構成が含まれていると、解決オプションが示されます。

（注） インポート側とエクスポート側のアプライアンスは、同じバージョンの Firepower システムを実行している必要があります。アクセスコントロールとそのサブポリシー（侵入ポリシーを含む）の場合、侵入ルールの更新バージョンも一致している必要があります。バージョンが一致しない場合、インポートは失敗します。インポート/エクスポート機能を使用して侵入ルールを更新することはできません。代わりに、最新バージョンのルール更新をダウンロードして適用します。

インポート/エクスポートをサポートする構成

インポート/エクスポートは、次の構成でサポートされます。

- アクセス コントロール ポリシーとそれが呼び出すポリシー：プレフィルタ、ネットワーク分析、侵入、SSL、ファイル、Threat Defense サービス ポリシー
- 侵入ポリシー（アクセス コントロールとは無関係に）
- NAT ポリシー（Firepower Threat Defense のみ）
- FlexConfig ポリシー。ただし、すべての秘密鍵の変数の内容は、ポリシーをエクスポートする際にクリアされます。秘密鍵を使用するFlexConfigポリシーをインポートした後に手動ですべての秘密鍵の値を編集する必要があります。
- プラットフォーム設定
- 正常性ポリシー
- アラート応答
- アプリケーション ディテクタ（ユーザ定義およびCisco Professionalサービスによって提供されるディテクタ）
- ダッシュボード
- カスタム テーブル
- カスタム ワークフロー
- 保存済み検索
- カスタム ユーザ ロール
- レポート テンプレート
- サードパーティ製品および脆弱性マッピング

設定のインポート/エクスポートに関する特別な考慮事項

構成をエクスポートすると、他の必要な構成もエクスポートされます。たとえば、アクセス コントロール ポリシーをエクスポートすると、そのポリシーが呼び出すサブポリシー、使用しているオブジェクトとオブジェクト グループ、先祖ポリシー（マルチドメイン展開の場合）などもエクスポートされます。別の例として、外部認証が有効になっているプラットフォーム設定ポリシーをエクスポートした場合は、認証オブジェクトもエクスポートされます。ただし、いくつかの例外があります。

- システム提供のデータベースとフィード：URLフィルタリング カテゴリとレピュテーション データ、シスコ インテリジェンス フィード データ、または地理位置情報データベース（GeoDB）はエクスポートされません。展開内のすべてのアプライアンスがシスコから最新情報を取得していることを確認してください。

- グローバルなセキュリティインテリジェンスのリスト：エクスポートされた構成に関連するグローバルなセキュリティインテリジェンスのブラックリストとホワイトリストがエクスポートされます（マルチドメイン展開では、これは現在のドメインに関係なく実行されます。子孫ドメインのリストはエクスポートされ**ません**）。インポートプロセスはこれらのブラックリストとホワイトリストをユーザ作成リストに変換してから、インポートされた構成でそれらの新しいリストを使用します。これにより、インポートされたリストが既存のグローバルなブラックリストおよびホワイトリストと競合することはありません。インポートされた構成でインポート側の Firepower Management Center のグローバル リストを使用するには、これらを手動で追加します。
- 侵入ポリシー共有層：エクスポートプロセスにより、侵入ポリシー共有レイヤが切断されます。以前の共有レイヤはパッケージに含まれ、インポートされた侵入ポリシーには共有レイヤは含まれません。
- 侵入ポリシーのデフォルト変数セット：エクスポートパッケージには、カスタム変数とシステム提供の変数を含むデフォルト変数セットがユーザ定義値とともに含まれています。インポート プロセスでは、インポートされた値でインポート側の Firepower Management Center のデフォルト変数セットを更新します。ただし、インポートプロセスはエクスポート パッケージに存在しないカスタム変数を削除**しません**。また、エクスポート パッケージに設定されていない値については、インポート側の Firepower Management Center のユーザ定義値を元に戻しません。したがって、インポート側の Firepower Management Center で設定されているデフォルト変数が異なる場合は、インポートされた侵入ポリシーの動作が予想とは異なる可能性があります。
- カスタム ユーザ オブジェクト：Firepower Management Center でカスタム ユーザ グループまたはオブジェクトを作成済みで、そのようなカスタム ユーザ オブジェクトがアクセス コントロール ポリシーのいずれかのルールに含まれている場合、エクスポート ファイル（.sfo）にはそのユーザ オブジェクト情報が格納されません。このため、そうしたポリシーをインポートする際、これらのカスタム ユーザ オブジェクトへの参照が削除され、宛先 Firepower Management Center にはインポートされません。不明なユーザ グループが原因で検出の問題が発生するのを避けるには、カスタマイズされたユーザ オブジェクトを新しい Firepower Management Center に手動で追加し、インポート後にアクセス コントロール ポリシーを再設定します。

オブジェクトおよびオブジェクト グループをインポートする場合：

- 通常、インポートプロセスはオブジェクトとグループを新規としてインポートしますが、既存のオブジェクトとグループを置き換えることはできません。ただし、インポートされた設定のネットワークやポートのオブジェクトまたはグループが既存のオブジェクトまたはグループと一致する場合、インポートした設定は、新しいオブジェクト/グループを作成せずに、既存のオブジェクト/グループを再利用します。システムは、名前（自動生成される番号は除外します）および各ネットワークとポートのオブジェクト/グループの内容を比較して、一致するかどうかを判別します。
- インポートしたオブジェクトの名前がインポートする Firepower Management Center 上の既存のオブジェクトと一致する場合、システムはそれらの名前を一意にするため、インポートされたオブジェクトとグループの名前に自動生成した番号を付加します。

- インポートした設定で使用されているセキュリティ ゾーンとインターフェイス グループを、インポート側の Firepower Management Center で管理されているタイプが一致するゾーンとグループにマッピングする必要があります。
- 秘密キーを含むPKIオブジェクトを使用する構成をエクスポートすると、エクスポートの前に秘密キーが復号されます。インポート時に、キーはランダムに生成されたキーで暗号化されます。

設定のエクスポート

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

エクスポートされる設定の数や、それらのオブジェクトが参照する設定の数によっては、エクスポート プロセスに数分かかる場合があります。

ヒント

Firepowerシステムの多くのリストページには、リスト項目の横にエクスポートアイコン（  ）があります。このアイコンがある場合は、それを使用することにより、その後のエクスポート操作を簡単に代行させることができます。

始める前に

- インポートおよびエクスポートするアプライアンスが同じバージョンの Firepower システムを実行していることを確認します。アクセス制御とそのサブポリシー（侵入ポリシーを含む）の場合は、侵入ルールの更新バージョンも一致する必要があります。

手順

ステップ 1 **[System]** > **[Tools]** > **[Import/Export]**を選択します。

折りたたむ（  ）アイコンか、展開する（  ）アイコンをクリックし、使用可能な設定のリストを折りたたんだり、展開したりします。

ステップ 2 エクスポートする構成をチェックして [エクスポート（Export）] をクリックします。

ステップ 3 Webブラウザのプロンプトに従って、エクスポートされたパッケージをコンピュータに保存します。

設定のインポート

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

インポートされる設定の数や、それらのオブジェクトが参照する設定の数によっては、インポート プロセスに数分かかる場合があります。

（注） システムからログアウトした場合、別のドメインに変更した場合、または[インポート（Import）] をクリックした後にユーザ セッションがタイムアウトした場合、インポート プロセスは完了するまでバックグラウンドで続行されます。

始める前に

- インポートおよびエクスポートするアプライアンスが同じバージョンの Firepower システムを実行していることを確認します。アクセス制御とそのサブポリシー（侵入ポリシーを含む）の場合は、侵入ルールの更新バージョンも一致する必要があります。

手順

ステップ 1 インポートするアプライアンスで、**[System]** > **[Tools]** > **[Import/Export]** を選択します。

ステップ 2 [パッケージのアップロード（Upload Package）] をクリックします。

ステップ 3 エクスポートしたパッケージへのパスを入力するか、そのパッケージの場所を参照して [アップロード（Upload）] をクリックします。

ステップ 4 バージョンが一致していないなどの問題がない場合は、インポートする設定を選択して、[インポート（Import）] をクリックします。
競合の解決やインターフェイス オブジェクトのマッピングを実行する必要がない場合は、インポートが完了して、成功メッセージが表示されます。この手順の残りは省略してください。

ステップ 5 プロンプトが表示されたら、[インポートの競合解決（Import Conflict Resolution）] ページで、インポートする Firepower Management Center で管理されているインターフェイス タイプと一致するゾーンおよびグループに、インポートした設定で使用されている インターフェイス オブジェクトをマップします。

インターフェイス オブジェクト タイプ（セキュリティ ゾーンまたはインターフェイス グループ）およびインターフェイス タイプ（パッシブ、インライン、ルーテッドなど）が送信元と宛先で一致している必要があります。詳細については、インターフェイス オブジェクト：インターフェイスグループとセキュリティ ゾーンを参照してください。

インポートする設定が存在していないセキュリティ ゾーンまたはインターフェイス グループを参照する場合は、その設定を既存のインターフェイ オブジェクトにマップするか、新しいインターフェイ オブジェクトを作成します。

ステップ 6 [インポート（Import）] をクリックします。

ステップ 7 プロンプトが表示されたら、[インポートの解決（Import Resolution）] ページで、各設定を展開して適切なオプションを選択します。詳細については、インポート競合の解決 （6 ページ）を参照してください。

ステップ 8 [インポート（Import）] をクリックします。

次のタスク

- 必要に応じて、インポートした設定の概要を示すレポートを表示します。タスク メッセージの表示を参照してください。

インポート競合の解決

構成をインポートしようとすると、同じ名前とタイプの構成がアプライアンスにすでに存在するかどうかがシステムによって確認されます。マルチドメイン展開では、構成が現在のドメイン、またはその先祖あるいは子孫ドメインのいずれかで定義されている構成の複製であるかどうかが確認されます。（子孫ドメインの構成は表示できませんが、重複する名前の構成が子孫ドメインに存在する場合は、システムにより競合が通知されます）。インポートに重複構成が含まれている場合、次の中から展開に適切な解決オプションが表示されます。

- **既存のものを維持する（Keep existing）**

  その構成はインポートされません。

- **既存のものを置換する（Replace existing）**

  インポート用に選択した構成で現在の構成が上書きされます。

- **最新バージョンを残す（Keep newest）**

  選択した構成は、タイムスタンプがアプライアンスの現在の構成のタイムスタンプより新しい場合にのみインポートされます。

- **新たにインポート（Import as new）**

  選択した重複する構成はインポートされ、システム生成の番号が適用されて一意の構成になります。（インポートプロセスが完了する前にこの名前を変更できます）。アプライアンスの元の構成は変更されません。

表示される解決オプションは、展開でドメインを使用するかどうか、およびインポートされた構成が現在のドメインで定義されている構成の複製であるか、または現在のドメインの先祖あるいは子孫で定義された構成であるかどうかによって異なります。次の表に、どの場合に解決オプションが表示されるか表示されないかを示します。

解決オプション	Firepower Management Center		管理対象デバイス
	現在のドメインの複製	子孫または先祖ドメインの複製	
既存のものを維持する（**Keep existing**）	Yes	Yes	Yes
既存のものを置換する（**Replace existing**）	○	いいえ	○
最新バージョンを残す（**Keep newest**）	○	いいえ	○
新たにインポート（**Import as new**）	Yes	Yes	Yes

クリーンまたはカスタム定義ファイル リストを使用するファイル ポリシーとともにアクセス コントロール ポリシーをインポートし、ファイル リストに重複する名前競合が示されている場合、上記の表に示すように競合解決オプションが表示されますが、ポリシーおよびファイル リストに対して実行されるアクションは、次に表に示すように異なります。

解決オプション	システム アクション	
	アクセス コントロール ポリシーと関連ファイル ポリシーが新たにインポートされ、ファイル リストは統合される	既存のアクセス コントロール ポリシーと関連ファイル ポリシーおよびファイル リストは変更されない
既存のものを維持する（**Keep existing**）	×	○
既存のものを置換する（**Replace existing**）	○	いいえ
新たにインポート（**Import as new**）	○	いいえ
最新バージョンを残す（Keep newest）。インポートされるアクセス コントロール ポリシーが最新	○	いいえ
最新バージョンを残す（Keep newest）。既存のアクセス コントロール ポリシーが最新	×	○

アプライアンスにインポートされた構成を修正し、後で同じアプライアンスにその構成を再インポートする場合は、保持する構成のバージョンを選択する必要があります。