設定のインポートおよびエクスポート

インポート/エクスポート機能を使用して、ポリシーを含む複数のタイプの設定を、1つのアプライアンスから同じタイプの別のアプライアンスにコピーにできます。設定のインポートおよびエクスポートは、バックアップ ツールとして設計されてはいませんが、新しい ASA FirePOWER モジュールを追加するプロセスを簡素化するために使用できます。

以下の設定をインポートおよびエクスポートできます。

- アクセス コントロール ポリシーとその関連するネットワーク分析ポリシー、SSL ポリシー、およびファイル ポリシー
- 侵入ポリシー
- システム ポリシー
- アラート応答

エクスポートされた設定をインポートするには、両方の ASA FirePOWER モジュールで同じソフトウェアバージョンを実行している必要があります。エクスポートされた侵入ポリシーまたはアクセス コントロール ポリシーをインポートするには、両方のアプライアンスでルール更新のバージョンも一致している必要があります。

（注） バージョンが一致している場合、ASDM で管理された ASA with FirePOWER Services デバイスからエクスポートしたポリシーを、Firepower Management Center で管理されたデバイスにインポートできます。

設定のエクスポート

ライセンス：任意

設定のインポートおよびエクスポート

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）一連の設定を同時に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。

設定をエクスポートするとき、アプライアンスは、その設定のリビジョン情報もエクスポートします。ASA FirePOWER モジュールはその情報を使用して、別のアプライアンスにその設定をインポートできるかどうかを判別します。アプライアンスにすでに存在する設定リビジョンをインポートすることはできません。

また、設定をエクスポートするときには、その設定が依存するシステム設定も、アプライアンスによってエクスポートされます。

ヒント ASA FirePOWER モジュールの多くのリスト 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。

以下の設定をエクスポートできます。

- アラート応答：アラート応答は、アラートの送信先とする予定の外部システムと ASA FirePOWER モジュールが対話できるようにするための一連の設定です。
- アクセス コントロール ポリシー：アクセス コントロール ポリシーには、システムがネットワーク トラフィックをどのように管理するかを指定するために設定できる、さまざまなコンポーネントが含まれます。これらのコンポーネントには、アクセス コントロール ルール、関連する侵入ポリシー、ファイル ポリシー、およびネットワーク分析ポリシー、およびSSL ポリシー、および侵入の変数セットを含むルールとポリシーが使用するオブジェクトが含まれています。アクセス コントロール ポリシーをエクスポートすると、そのポリシーのすべての設定とコンポーネントもエクスポートされます。ただし、複数のアプライアンスで同等であり、ユーザが変更できない URL レピュテーションとカテゴリは（それらが存在しても）エクスポートされません。アクセス コントロール ポリシーをインポートするには、エクスポート元とインポート先の ASA FirePOWER モジュールでルール アップデートのバージョンが一致している必要があります。

エクスポートするアクセス コントロール ポリシー、またはそのポリシーが呼び出す SSL ポリシーには、地理位置情報データを参照するルールが含まれている場合、インポート先モジュールの地理位置情報データベース（GeoDB）のアップデート バージョンが使用されます。

- 侵入ポリシー：侵入ポリシーには、ネットワーク トラフィックを検査して侵入やポリシー違反を見つけるように設定できる、さまざまなコンポーネントが組み込まれています。これらのコンポーネントは、プロトコル ヘッダー値、ペイロード コンテンツ、特定のパケット サイズの特性、および他の詳細設定を検査する侵入ルールです。

侵入ポリシーをエクスポートすると、そのポリシーのすべての設定もエクスポートされます。たとえば、イベントを生成するルールを設定するように選択した場合、ルールの SNMP アラートを設定した場合、またはポリシーで機密データ プリプロセッサをオンにした場合は、エクスポートされるポリシー内にそれらの設定値が保持されます。カスタム ルール、カスタム ルールの分類、およびユーザ定義変数も、ポリシーと共にエクスポートされます。

設定のインポートおよびエクスポート

レイヤを使用する侵入ポリシーをエクスポートする場合、そのレイヤが2番目の侵入ポリシーによって共有されているときは、エクスポートするポリシーにその共有レイヤがコピーされて、共有関係はなくなることに注意してください。侵入ポリシーを別のアプライアンスにインポートするときは、インポートするポリシーをニーズに合うように編集できます。レイヤの削除、追加、共有などができます。

1 つの ASA FirePOWER モジュールから別の ASA FirePOWER モジュールに侵入ポリシーをエクスポートする場合、2 つ目の ASA FirePOWER モジュールのデフォルト変数の設定が異なっている場合は、インポートされたポリシーの動作が異なることがあります。

（注） インポート/エクスポート機能を使用して、脆弱性調査チーム（VRT）が作成したルールをアップデート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 アップデートをダウンロードして適用します。ルール更新とローカル ルール ファイルのインポートを参照してください。

- システム ポリシー：システム ポリシーは、時間設定や SNMP 設定などを含む、展開内の他の ASA FirePOWER モジュールに類似している可能性のある ASA FirePOWER モジュールの側面を制御します。

（注） 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。

一つ以上の設定をエクスポートする方法：

ステップ 1 設定のエクスポート元の ASA FirePOWER モジュールと設定のインポート先の ASA FirePOWER モジュールで、同じバージョンが実行されていることを確認します。侵入ポリシーまたはアクセス コントロール ポリシーをエクスポートする場合は、ルールのアップデート バージョンが一致することを確認します。

ASA FirePOWER モジュールのバージョン（および該当する場合はルールのアップデート バージョン）が一致しない場合、インポートは失敗します。

ステップ 2 [Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Import Export] の順に選択します。 > > >

[Import/Export] ページが開き、ASA FirePOWER モジュール上の設定のリストが表示されます。エクスポートする設定がない設定カテゴリは、このリストに表示されないことに注意してください。

ヒント 設定のリストは、設定タイプの横にある折りたたみアイコンをクリックして折りたたむことができます。設定を確認するには、設定タイプの横にあるフォルダ展開アイコンをクリックします。

ステップ 3 エクスポートする設定の横にあるチェック ボックスを選択して、[Export] をクリックします。

ステップ 4 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

ライセンス：任意

ASA FirePOWER モジュールから設定をエクスポートした後に、その設定が別のモジュールでもサポートされていれば、そのモジュールにインポートできます。

インポートしている設定のタイプに応じて、以下の点に注意する必要があります。

- 設定のインポート先の ASA FirePOWER モジュールと設定のエクスポートに使用した ASA FirePOWER モジュールで、同じバージョンが実行されていることを確認します。侵入ポリシーまたはアクセス コントロール ポリシーをインポートする場合は、両方のアプライアンスでルールのアップデート 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。

（注） バージョンが一致している場合、ASDM で管理された ASA with FirePOWER Services デバイスからエクスポートしたポリシーを、Firepower Management Center で管理されたデバイスにインポートできます。

- ゾーンに基づいてトラフィックを評価するアクセス コントロール ポリシーをインポートした場合、インポートしたポリシー内のゾーンを、インポート先の ASA FirePOWER モジュールのゾーンにマッピングする必要があります。ゾーンをマッピングするときは、それらのタイプが一致している必要があります。したがって、インポートを開始する前に、インポート先の ASA FirePOWER モジュールで必要となるゾーン タイプを作成する必要があります。セキュリティ ゾーンについて詳しくは、セキュリティ ゾーンの操作を参照してください。
- 既存のオブジェクトやグループと同一の名前を持つオブジェクトやオブジェクト グループを含むアクセス コントロール ポリシーをインポートする場合は、オブジェクトやグループの名前を変更する必要があります。
- アクセス コントロール ポリシーや侵入ポリシーをインポートする場合、インポート プロセスによって、デフォルト変数セットに含まれる既存のデフォルト変数が、インポートされたデフォルト変数に置換されます。既存のデフォルト変数セットに、インポートされたカスタム変数セットに存在しないカスタム変数が含まれる場合、一意的な変数が保持されます。
- 侵入ポリシーをインポートするとき、その侵入ポリシーが 2 番目の侵入ポリシーの共有レイヤを使用していた場合は、エクスポート プロセスによって共有関係が切断されて、それまで共有されていたレイヤがパッケージにコピーされます。つまり、インポートされた侵入ポリシーに共有レイヤは含まれません。

（注） インポート/エクスポート機能を使用して、脆弱性調査チーム（VRT）が作成したルールをアップデート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 アップデートをダウンロードして適用します。ルール更新とローカル ルール ファイルのインポートを参照してください。

1つのパッケージで複数の設定をエクスポートできるため、パッケージのインポート時に、パッケージ内のどの設定をインポートするかを選択する必要があります。

設定をインポートしようとすると、ASA FirePOWER モジュールは、その設定がアプライアンスにすでに存在しているかどうかを判別します。競合がある場合は、以下の操作が可能です。

- 既存の設定を維持する、
- 既存の設定を新しい設定に置き換える、
- 最新の設定を維持する、または
- 設定を新しい設定としてインポートする。

設定をインポートした後に、宛先システムで設定を変更してその設定を再インポートすると、保持する設定のバージョンを選択する必要があります。

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、プロセスに数分かかる場合があります。

一つ以上の設定をインポートする方法：

ステップ 1 設定のエクスポート元の ASA FirePOWER モジュールと設定のインポート先のモジュールで、同じバージョンが実行されていることを確認します。侵入ポリシーまたはアクセス コントロール ポリシーをインポートする場合は、ルールのアップデート バージョンが一致することも確認する必要があります。

ASA FirePOWER モジュールのバージョン（および該当する場合はルールのアップデート バージョン）が一致しない場合、インポートは失敗します。

ステップ 2 インポートする設定をエクスポートします。設定のエクスポート （1 ページ）を参照してください。

ステップ 3 設定をインポートするアプライアンスで、[Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Import Export] の順に選択します。 > > >

[Import Export] ページが表示されます。

ヒント 設定のリストを折りたたむには、設定タイプの横にある折りたたみアイコンをクリックします。設定を確認するには、設定タイプの横にあるフォルダ展開アイコンをクリックします。

ステップ 4 [Upload Package] をクリックします。

[Upload Package] ページが表示されます。

ステップ 5 次の 2 つのオプションから選択できます。

- アップロードするパッケージへのパスを入力します。
- [Upload File] をクリックして、パッケージを見つけます。

ステップ 6 [Upload] をクリックします。

アップロードの結果は、パッケージの内容によって異なります。

- パッケージ内の設定およびルールのバージョンが、アプライアンスにすでに存在するバージョンと正確に一致する場合、そのバージョンが存在することを示すメッセージが表示されます。アプライアンスに最新の設定が存在するので、それらをインポートする必要はありません。
- 使用するアプライアンスとパッケージのエクスポート元のアプライアンスとの間に、ASA FirePOWER モジュールまたは（該当する場合）ルールアップデートのバージョンの不一致がある場合、パッケージをインポートできないことを示すメッセージが表示されます。ASA FirePOWER モジュールまたはルール アップデートのバージョンを更新して、プロセスを再試行します。
- アプライアンスに存在しない設定やルールのバージョンがパッケージに含まれている場合、[Package Import] ページが表示されます。次の手順に進んでください。

ステップ 7 インポートする設定を選択して、[Import] をクリックします。

インポート プロセスが解決されて、以下のような結果になります。

- ASA FirePOWER モジュールに、インポートする設定の以前のリビジョンが存在しない場合、インポートは自動的に完了し、成功メッセージが表示されます。残りの手順は省略してください。
- セキュリティ ゾーンを含むアクセス コントロール ポリシーをインポートする場合、[アクセス コントロール インポートの解決（Access Control Import Resolution）] ページが表示されます。ステップ 8 に進みます。
- インポートする設定に対してアプライアンスに以前のリビジョンが存在する場合、[Import Resolution] ページが表示されます。ステップ 9 に進みます。

ステップ 8 取り込まれる各セキュリティ ゾーンの横で、同じタイプの既存のローカル セキュリティ ゾーンをマップ先として選択し、[Import] をクリックします。

ステップ 7 に戻ります。

ステップ 9 各設定を展開して、以下の該当するオプションを選択します。

- アプライアンスの設定を保持するには、[Keep existing] を選択します。
- アプライアンスの設定をインポートした設定に置き換えるには、[Replace existing] を選択します。
- 最新の設定を保持するには、[Keep newest] を選択します。
- インポートした設定を新しい設定として保存するには、[Import as new] を選択し、オプションとして設定名を編集します。

クリーン リストまたはカスタム検出リストが有効になっているファイル ポリシーを含むアクセス コントロール ポリシーをインポートする場合、[Import as new] オプションは使用できません。

- 従属オブジェクトを含むアクセス コントロール ポリシーや保存済み検索をインポートする場合、提案された名前を受け入れるか、またはオブジェクトの名前を変更します。システムは常にこれらの従属オブジェクトを新規としてインポートします。既存のオブジェクトを保存したり置き換えたりするオプションはありません。システムではオブジェクトもオブジェクト グループも同様に処理されることに注意してください。

ステップ 10 [Import] をクリックします。

設定がインポートされます。

次のタスク

セキュリティ インテリジェンス フィードを含むアクセス コントロール ポリシーのインポート後、そのポリシーを展開する前にセキュリティ インテリジェンス フィードを更新して最新のデータがダウンロードされるのを待つ必要があります。フィードの内容はエクスポートやインポートのプロセスの一部ではありません。そのため、こうすることで最新のフィードが常に使用されるようにします。

設定のインポートおよびエクスポート