Cisco Firepowerシステムでのパスルールの設定

内容

概要

このドキュメントでは、パスルール、その作成方法、および侵入ポリシーでそれを有効にする方法について説明します。

パスルールを作成すると、パスルールで定義された基準を満たすパケットが、アラートルールを無効にするのではなく、特定の状況でアラートルールをトリガーするのを防ぐことができます。デフォルトでは、パス· ルールはアラート· ルールを上書きします。Firepowerシステムは、パケットを各ルールで指定された条件と比較し、パケットデータがルールで指定されたすべての条件と一致する場合、ルールがトリガーされます。ルールがアラートルールの場合、侵入イベントが生成されます。パスルールの場合、トラフィックは無視されます。

たとえば、ユーザ「anonymous」としてFTPサーバにログインする試行を検索するルールをアクティブのままにしたい場合があります。ただし、ネットワークに1つ以上の正規の匿名FTPサーバがある場合は、特定のサーバに対して匿名ユーザが元のルールをトリガーしないことを指定するパスルールを作成してアクティブにすることができます。

> **注意**：パスルールの基になっている元のルールがリビジョンを受信しても、パスルールは自動的には更新されません。したがって、パス· ルールの維持が困難になる可能性があります。

> **注**：ルールの抑制機能を有効にすると、そのルールのイベント通知が抑制されます。ただし、ルールは引き続き評価されます。たとえば、ドロップルールを押すと、ルールに一致するパケットはサイレントにドロップされます。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

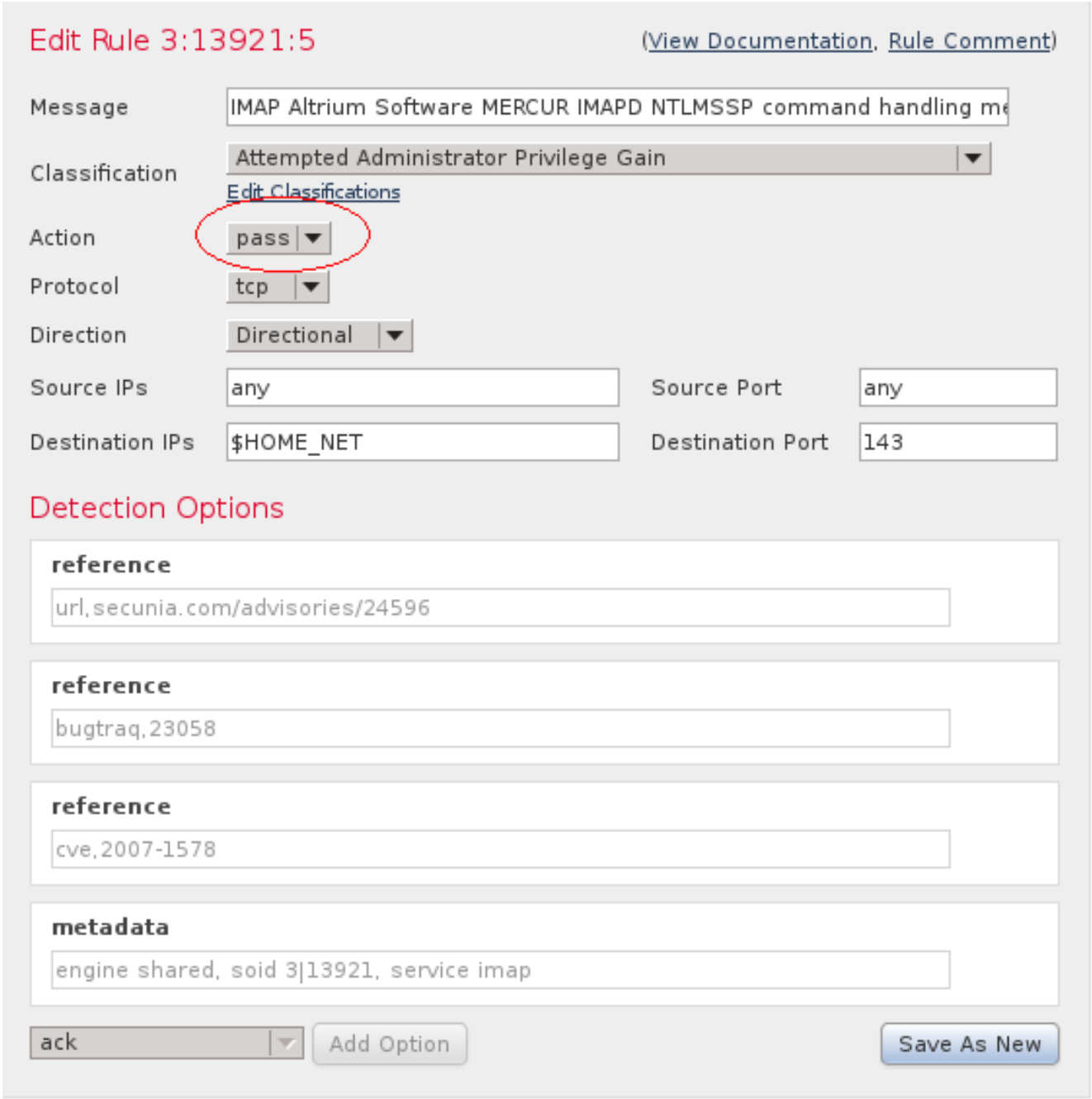
このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

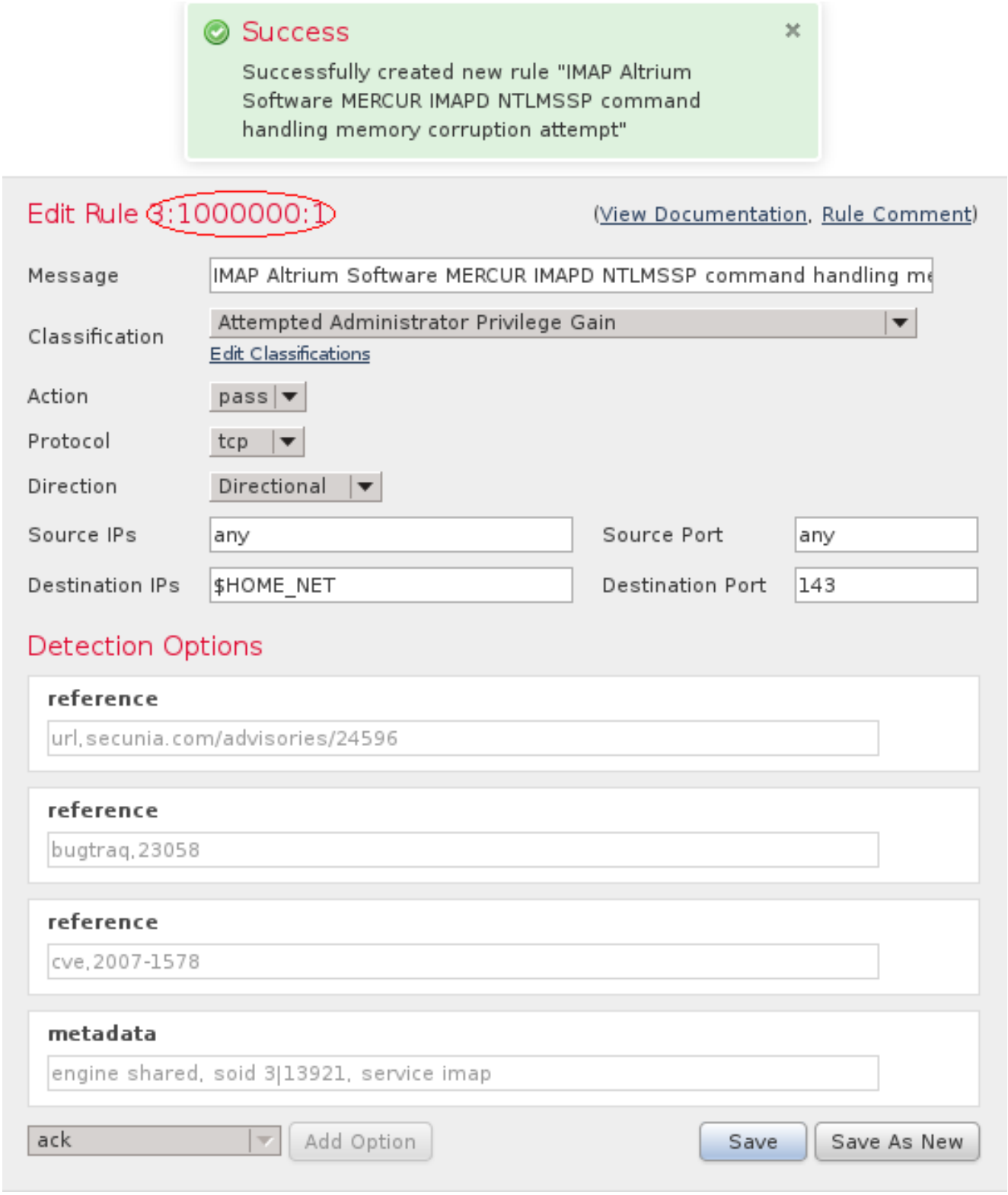
設定

パスルールの作成

1. **Objects > Intrusion Rules にすすんでください。**ルールカテゴリのリストが表示されます。
2. フィルタするルールに関連付けられているルールカテゴリを検索します。矢印アイコンを使用して、カテゴリリストからルールカテゴリを展開し、パスルールを作成するルールを検索します。または、ルール検索ボックスを使用することもできます。
3. 目的のルールが見つかったら、その横にある鉛筆アイコンをクリックしてルールを編集します。
4. ルールを編集する場合は、次の手順を実行します。 **ルールに適した Edit ボタンをクリックしてください。**Action **ドロップ** ダウン リストより、pass を選択してください。[Source IPs]フィールドと[Destination IPs]フィールドを、ルールを警告しないホストまたはネットワークに変更します。**Save As New をクリックしてください。**



5. 新しいルールのID番号をメモします。たとえば 1000000 と入力します。



パスルールの有効化

指定した送信元または宛先アドレスでトラフィックを渡すには、適切な侵入ポリシーで新しいルールを有効にする必要があります。パスルールを有効にするには、次の手順を実行します。

1. アクティブな侵入ポリシーを変更します。 [Policies] > [Access Control] > [Intrusion] の順に選択します。**Edit をクリックして有効な不正侵入ポリシーの隣にある Edit をクリックしてください。**
2. 新しいルールをルールリストに追加します。 **左側にある Rules をクリックしてください。** 前にメモしたルールIDをフィルタボックスに入力します。Rules **チェック ボックスを確認し**

て、Rule State を Generate Events に変更してください。**左側にある Policy Information をクリックしてください。Commit Changes をクリックしてください。**

3. **デバイスに変更を反映させるために、Deploy をクリックしてください。**

確認

定義された送信元または宛先IPアドレスに関するこの特定のルールに関するイベントが生成されないように、新しいイベントをしばらく監視する必要があります。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。