FireSIGHT システムでのパス ルールの設定

目次

概要

ルールをある特定の状況では引き起こすことからの ルールで定義される条件を満たす ルールを作成できま ルールをディセーブルにしますよりもむしろパケットを防ぐ。 デフォルトで、 ルール上書きする ルール。 SireSIGHT システムは各ルールおよび、ルール トリガーで規定 される条件に対してパケットデータがルールで規定 される条件すべてと一致すればパケットを比較します。 ルールが ルールである場合、不正侵入 イベントを生成します。 ルールである場合、トラフィックを無視します。

たとえば、アクティブのままになるために」匿名ユーザ「として FTP サーバにログイン する試みを探すルールがほしいと思うかもしれません。 ただし、ネットワークに 1つ以上の正当 な 匿名FTP サーバがあれば、それらの特定のサーバのために、匿名ユーザーはオリジナル ルールを引き起こさないこと規定 する ルールを書き、アクティブにする可能性があります。

それをおよび不正侵入 ポリシーでそれを作成する方法を ルールはであるものこの資料に、有効にする方法を記述されています。

> **注意**： ルールが基づいているオリジナル ルールが修正を受け取るとき、 ルールは自動的にアップデートされません。 従って、 ルールは維持しにくくないですかもしれません。

> **注:** ルールのための*抑制*機能を有効に する場合、そのルールのためのイベント 通知を抑制します。 ただしルールはまだ評価されますあります。 たとえば、ルールを抑制すれば、ルールを一致するパケットは無言で廃棄されます。

設定

パス ルールを作成して下さい

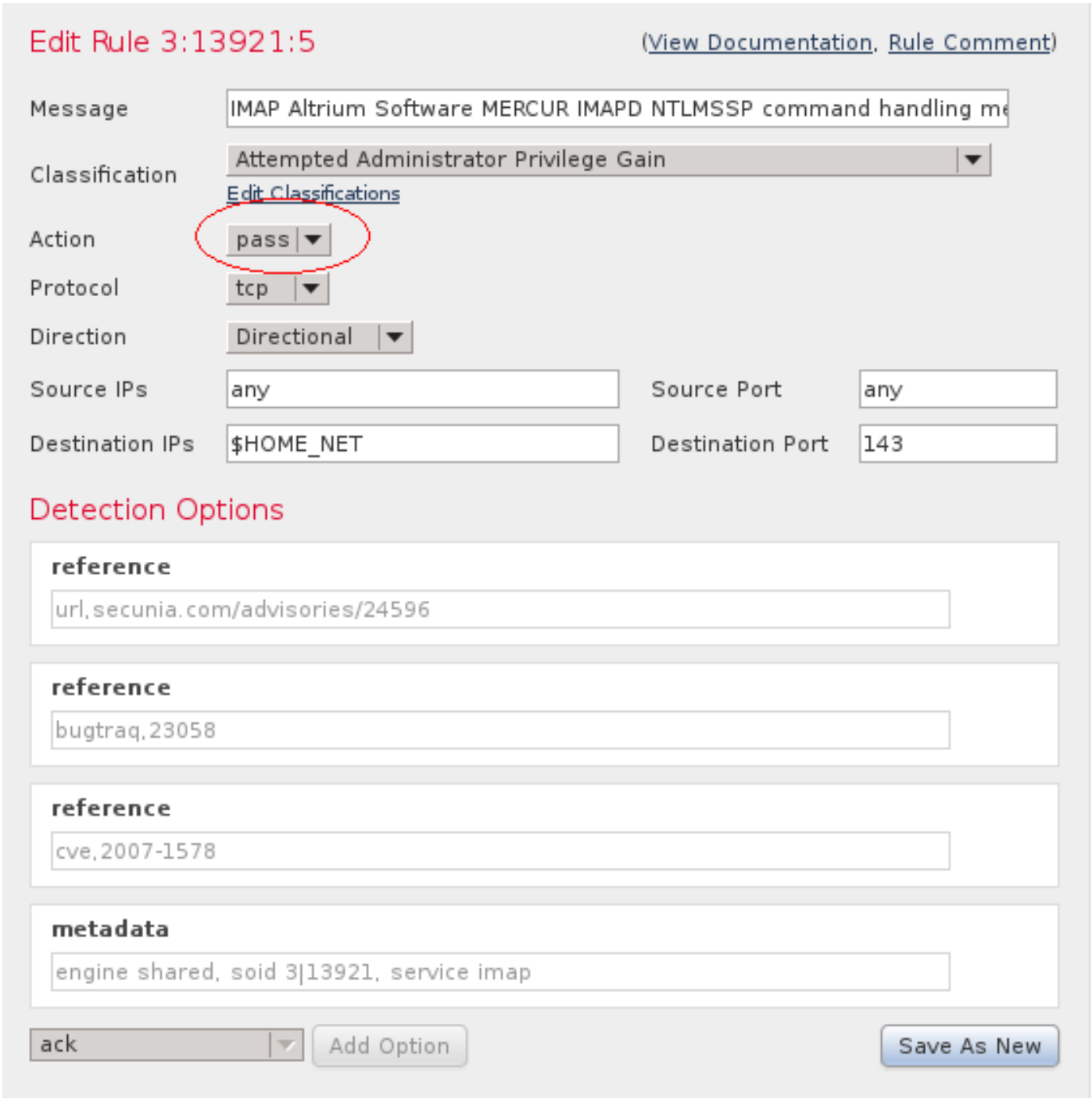
1. Webインターフェイスを使用しているルール エディタを開くために**ポリシー > 不正侵入 > ル**

ール エディタに、ナビゲート して下さい

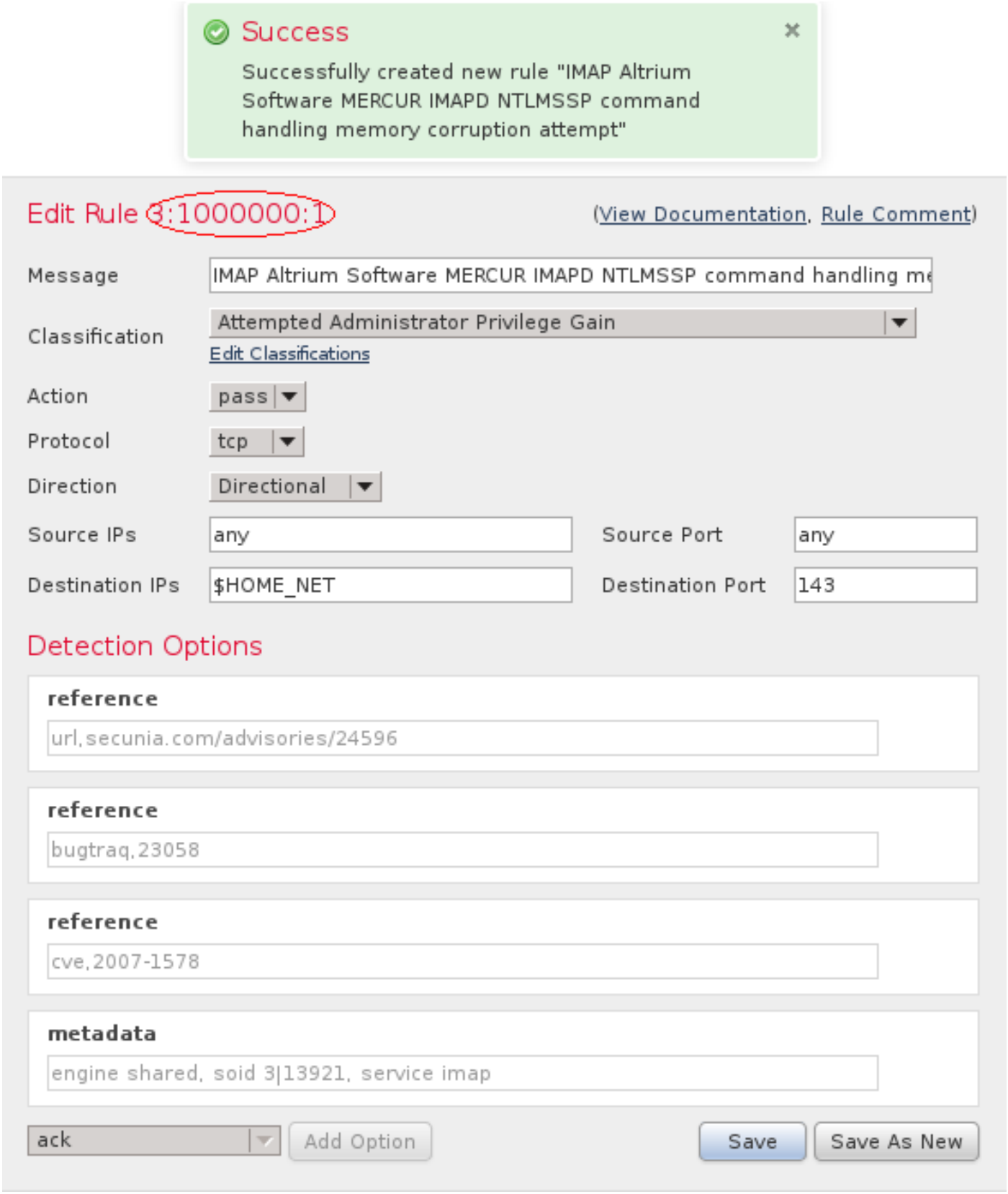
2. フィルタリングしたいと思うルールを見つけて下さい。 支配させるたいと思うルールを見つけるのに検索ボックスかカテゴリ リストを使用して下さい。

3. 条件を満たすルールを編集して下さい:

- ルールに相当して **Edit ボタンを**クリックして下さい。
- 警告 するルールがほしいと思わないことホストかネットワークに**出典 IP** および**宛先IP を**変更して下さい。
- **渡るためにアラート**から**処理を**変更して下さい。



4. **新しい**『Save As』 をクリック して下さい。 新しいルールの ID 番号に注意して下さい。 たとえば、1000000。



パス ルールを有効に して下さい

規定 した 送信元または宛先アドレスのトラフィックを通過させることを適切な不正侵入 ポリシーの新しいルールが可能にする必要があります。 ルールを有効に するために下記のステップに従って下さい:

1. アクティブな不正侵入 ポリシーを修正して下さい。

- [Policies] > [Intrusion] > [Intrusion Policy] に移動します。
- はたらくポリシーの隣で『Edit』 をクリック して下さい。

2. ルール リストに新しいルールを追加して下さい。

- 左側 ペインで『Rules』 をクリック して下さい。
- フィルタ ボックスで先に注意したルール ID を入力して下さい。
- Rules チェックボックスを選択し、**イベントを生成するために**ルール状態を変更して下さい。
- 左側 ペインの**ポリシー情報を**クリックして下さい。 **託します変更**ボタンをクリックして下さい。

3. 不正侵入 ポリシーの隣で**適用ポリシー** ボタンをクリックして下さい。 デバイスを選択し、**再適用します**クリックして下さい。

確認

イベントが定義された出典または宛先IP のこの特定のルールのために生成されないことを確かめるために新しいイベントをしばらくの間監視する必要があります。