一个帕斯规则的配置在FireSIGHT系统的

目录

简介

在特定的情况下您能创建规则防止满足在从触发规则的规则定义的标准的数据包，而不是禁用规则。默认情况下，规则覆盖规则。FireSIGHT系统对在每个规则，如果数据包数据匹配所有条件指定在规则，规则触发指定的条件比较数据包。如果规则是一个规则，生成入侵事件。如果它是规则，忽略流量。

例如，您也许想要寻找尝试登录FTP服务器作为用户“匿名”保持活动的规则。然而，如果您的网络有一个或更多合法匿名文件传送协议服务器，您可能写入和启动指定的规则，对于那些特定服务器，匿名用户不触发原始规则。

本文在入侵策略描述什么是规则，如何创建它和如何启用它。

> **Caution**:当规则根据时的一个原始规则接收版本，规则没有自动地更新。所以，规则可能是难维护。

> **Note**:如果启用规则的*抑制*功能，抑制该规则的事件通知。然而规则是仍然被评估。例如，如果抑制规则，匹配规则的数据包静静地被丢弃。

配置

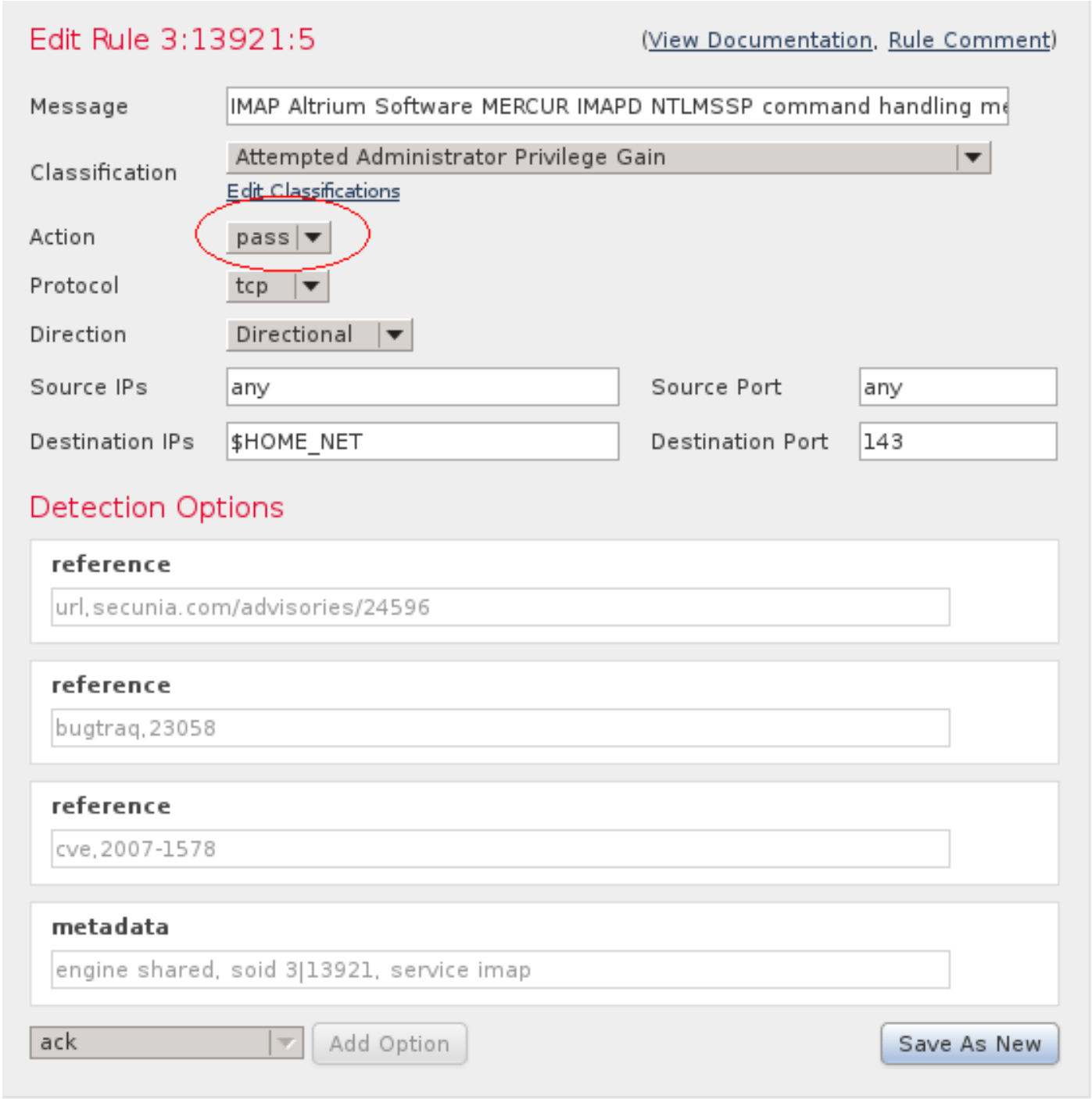
创建帕斯规则

1. 使用Web接口，导航到**策略>入侵>规则编辑器**，打开规则编辑器

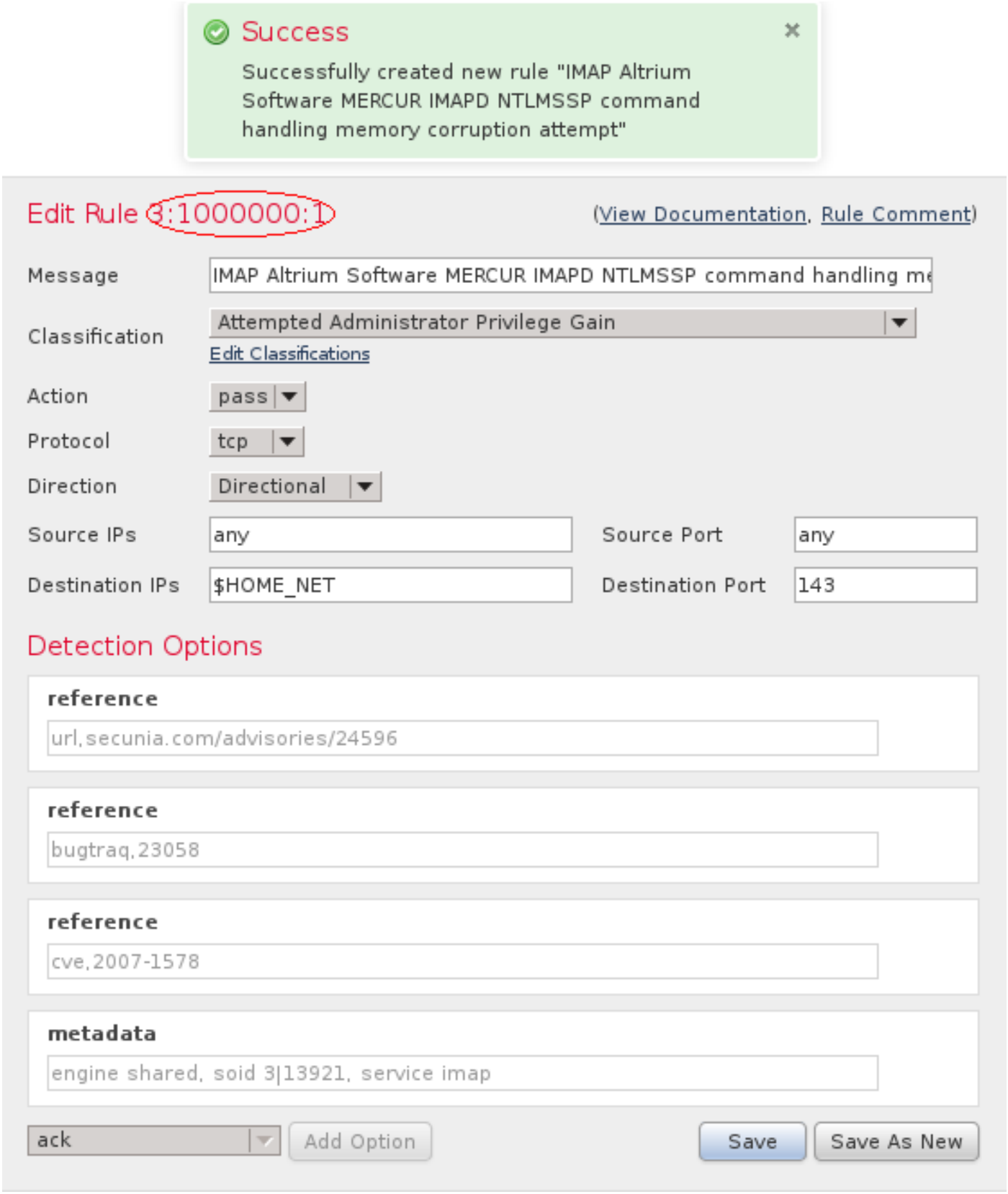
2. 查找您要过滤的规则。请使用搜索方框或类别列表查找您要做规定的规则。

3. 编辑规则匹配您的标准：

- 单击**编辑按钮**与规则相应。
- 更改**来源IP**和**目的地IP**对主机或网络您不想要规则警告。
- 更改从**警报的操作通过**。



4. 单击**"Save"如新建**。注释新规则的ID号码。例如， 1000000。



启用帕斯规则

您需要使您的在适当的入侵策略的新规则为了通过在您指定的来源或目的地址的流量。遵从下面步骤启用规则：

1. 修改活动入侵策略。

- 导航对**策略>入侵>入侵策略。**

- 单击在您工作的策略旁边**编辑**。

2. 添加新规则到规则列表。

- 点击在左侧窗格的**规则**。
- 输入您在过滤器方框注释前的规则ID。
- 选择规则复选框，并且更改规则状态**生成事件**。
- 点击关于左侧窗格的**策略信息**。点击**进行更改**按钮。

3. 在入侵策略旁边单击**应用策略**按钮。选择您的设备并且单击**重新应用**。

验证

您不应该有一段时间了监控新的事件确保事件为定义来源或目的地IP的此特定规则生成。