在Cisco Firepower系统上配置通过规则

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[配置](#)
[创建通过规则](#)
[启用通过规则](#)
[验证](#)
[故障排除](#)

简介

本文档介绍通过规则、如何创建它以及如何在入侵策略中启用它。

您可以创建通过规则，以防止符合通过规则中定义的条件的数据包在特定情况下触发警报规则，而不是禁用警报规则。默认情况下，通过规则会覆盖警报规则。Firepower系统将数据包与每个规则中指定的条件进行比较，如果数据包数据与规则中指定的所有条件匹配，则触发规则。如果规则是警报规则，它将生成入侵事件。如果是通过规则，则忽略流量。

例如，您可能希望一个规则保持活动状态，该规则会查找以用户“anonymous”身份登录FTP服务器的尝试。但是，如果您的网络有一个或多个合法的匿名FTP服务器，则可以编写并激活一个传递规则，该规则指定对于这些特定服务器，匿名用户不触发原始规则。

> **警告**：当基于通过规则的原始规则收到修订时，不会自动更新通过规则。因此，通过规则可能难以维护。

> **注意**：如果为规则启用抑制功能，则会抑制该规则的事件通知。但是，仍会评估规则。例如，如果您拒绝丢弃规则，匹配规则的数据包将以静默方式丢弃。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

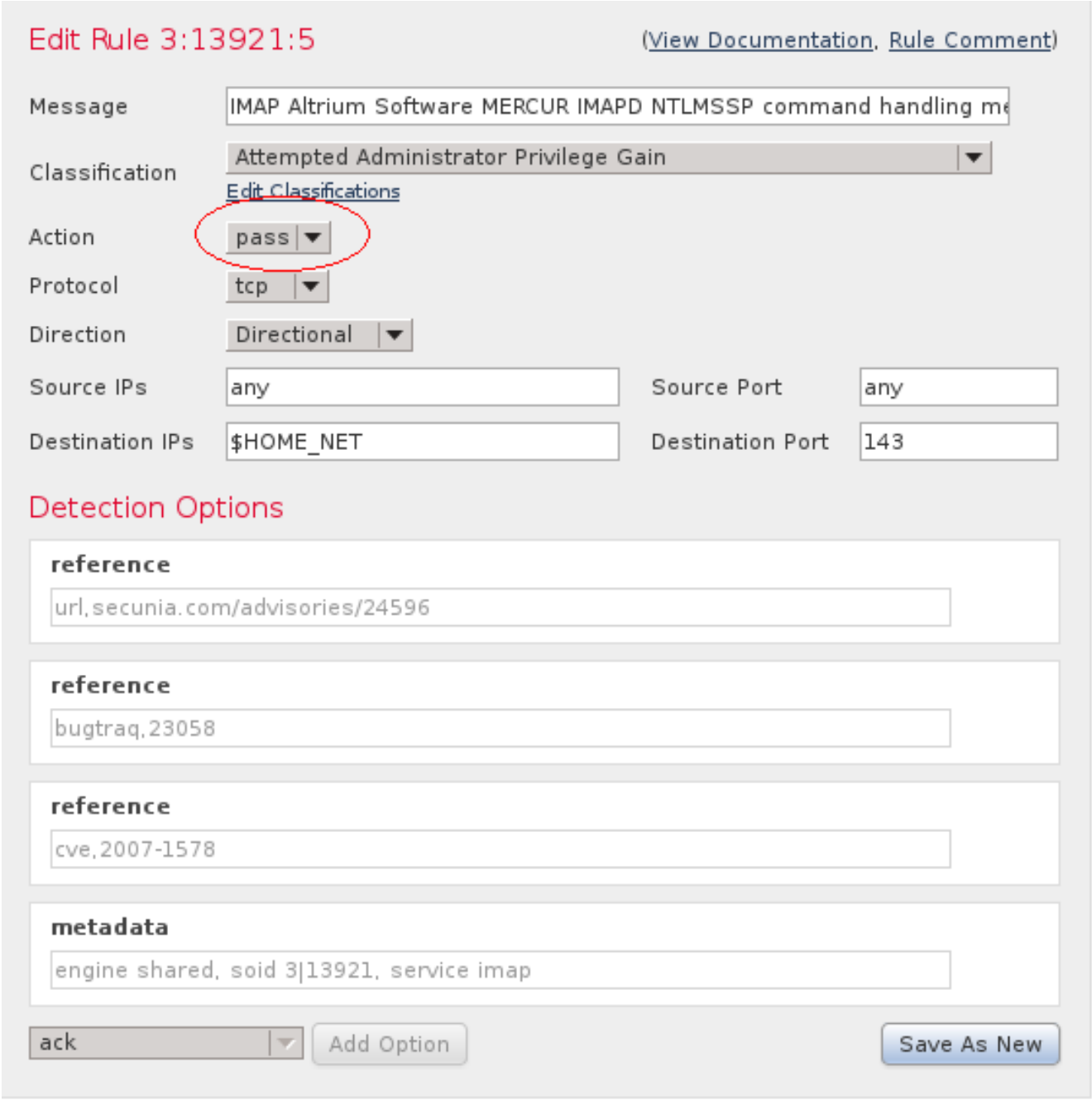
本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

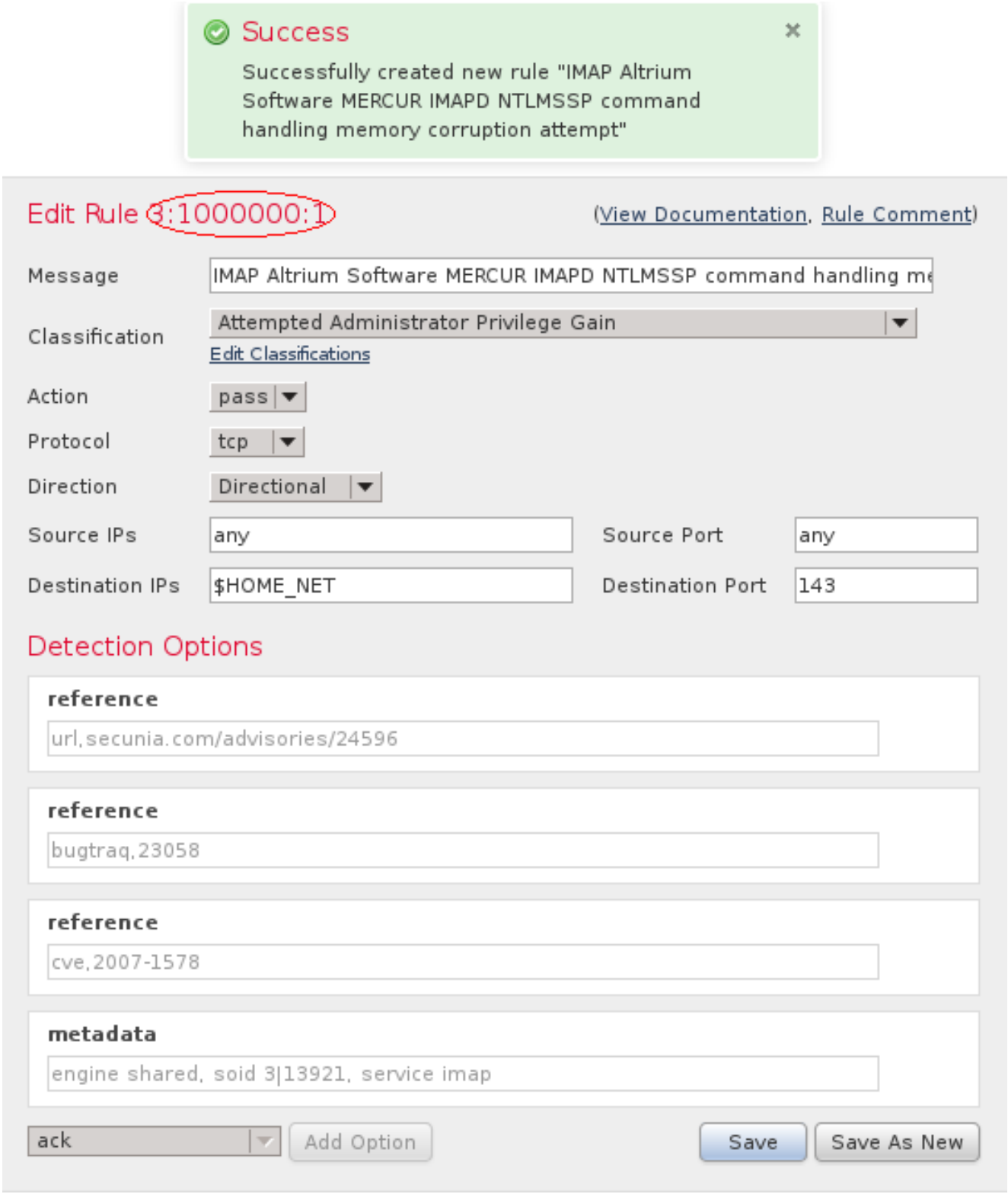
配置

创建通过规则

1. 导航至“对**象”(Objects)>“入侵规则**”(Intrusion Rules)。系统将显示规则类别列表。
2. 查找与要过滤的规则关联的规则类别。使用箭头图标从类别列表中展开规则类别，并查找要为其制定通过规则的规则。或者，您也可以使用规则搜索框。
3. 找到所需规则后，点击其旁边的铅笔图标以编辑规则。
4. 编辑规则时，请完成以下步骤： 单击与**规则**对应的Edit按钮。在“操作”下拉列表中，选择**pass**。将Source IPs（源IP）字段和Destination IPs（目标IP）字段更改为不希望规则发出警报的主机或网络。单击**另存为新**。



5. 注意新规则的ID号。例如1000000。



启用通过规则

您需要在适当的入侵策略中启用新规则，以便在指定的源地址或目标地址上传递流量。要启用通过规则，请执行以下步骤：

1. 修改活动入侵策略： 导航至**Policies > Access Control > Intrusion**。单击活动入侵策略旁的**Edit**。
2. 将新规则添加到规则列表： 单击左侧窗格中的**Rules**。输入您在过滤器框中前面记录的规则ID。选中Rules复选框，并将Rule State更改为**Generate Events**。单击左侧窗格中的**Policy Information**。单击“**Commit Changes**”。

3. 单击Deploy以在设备上部署更改。

验证

您应该监控一段时间的新事件，以确保没有为已定义的源或目标IP地址的此特定规则生成任何事件。

故障排除

目前没有针对此配置的故障排除信息。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。