在思科FireSIGHT系统的自定义本地喷鼻息规则

目录

简介

在FireSIGHT系统的一个自定义本地规则是您在从本地设备的一个ASCII文件格式导入的一个自定义标准的喷鼻息规则。使用Web接口， FireSIGHT系统允许您导入本地规则。导入本地规则的步骤是非常直接的。然而，写入一个最佳的本地规则，用户要求在喷鼻息和网络协议的深入的知识。

本文目的将提供您若干提示和协助写入一个自定义本地规则。关于创建本地规则的说明是可用的在*喷鼻息用户手册*，是可用的在snort.org。思科建议您下载并且读用户手册，在您写入一个自定义本地规则前。

> **Note**:由思科Talos安全智能和研究小组创建并且测试，并且Cisco技术支持中心(TAC)支持在Sourcefire规则更新(SRU)包提供的规则。Cisco TAC在文字或调整不提供援助一个自定义本地规则，然而，如果遇到与您的FireSIGHT系统的规则导入功能的任何问题，请与Cisco TAC联系。

> 警告：一个不足写入的自定义本地规则能影响可能导致整个网络的性能下降FireSIGHT系统的性能。如果遇到在您的网络的任何性能问题，并且有在您的FireSIGHT系统启用的一些自定义本地喷鼻息规则，思科推荐您禁用那些本地规则。

先决条件

要求

思科建议您有在喷鼻息规则和FireSIGHT系统的知识。

使用的组件

关于本文的信息根据这些硬件和软件版本：

- FireSIGHT管理中心(亦称防御中心)
- 软件版本5.2或以上

工作与自定义本地规则

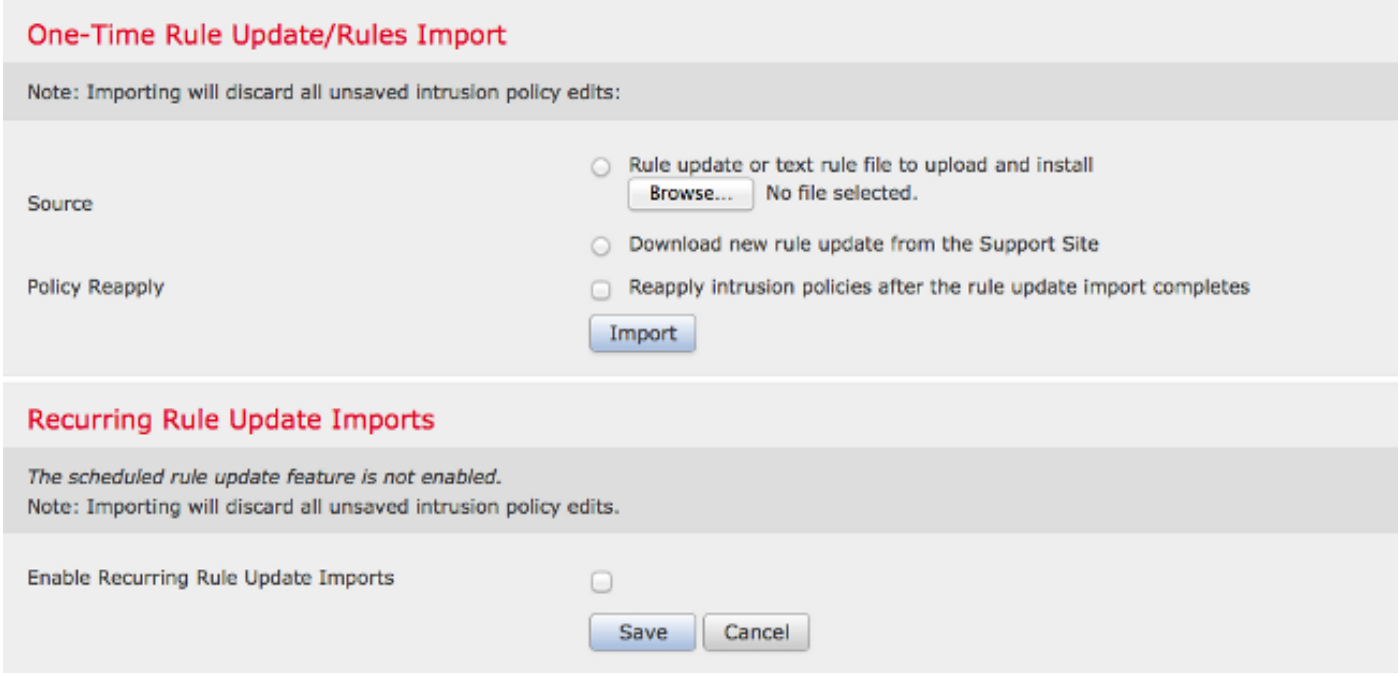
导入本地规则

在您开始前，您必须确保，在文件的规则不包含任何转义字符。使用ASCII或UTF-8编码，规则进口商需要所有海关规则导入。

以下步骤解释如何导入从本地设备的本地标准的文本规则：

1. 通过导航访问**规则编辑器**页到**策略>入侵>规则编辑器**。

2. 点击**导入规则**。**规则更新**页出版。



图：规则的屏幕画面校正页

3. 选择**规则更新或发短信给规则文件上传和安装**并且单击**浏览**选择规则文件。

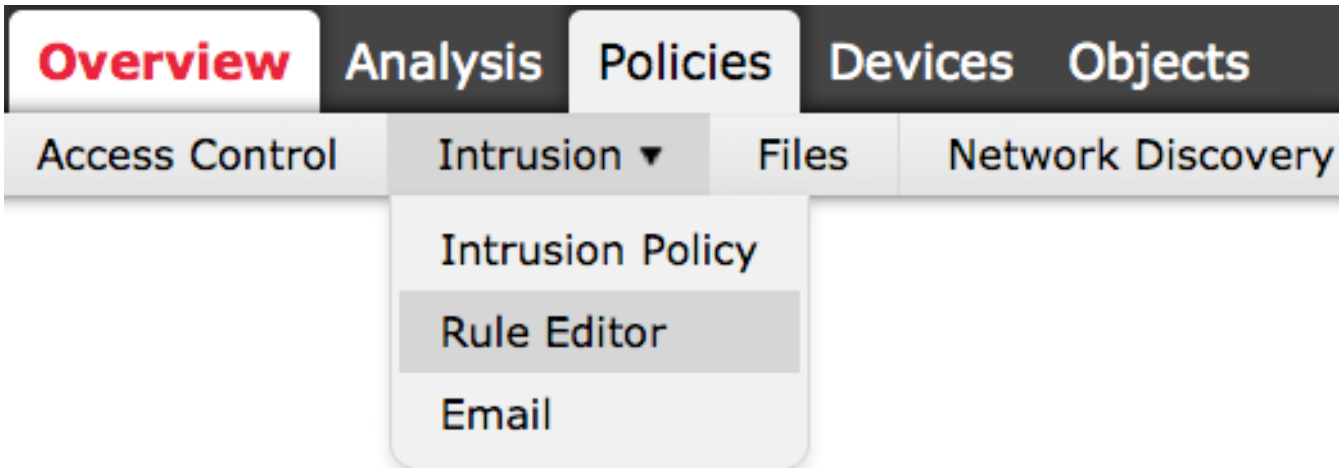
> **Note**:所有上传的规则在**本地规则**类别保存。

4. 单击 **Import**。规则文件导入。

Caution:FireSIGHT系统不使用设置的新规则检查。要启动一个本地规则，您在入侵策略需要启用它，然后运用策略。

查看本地规则

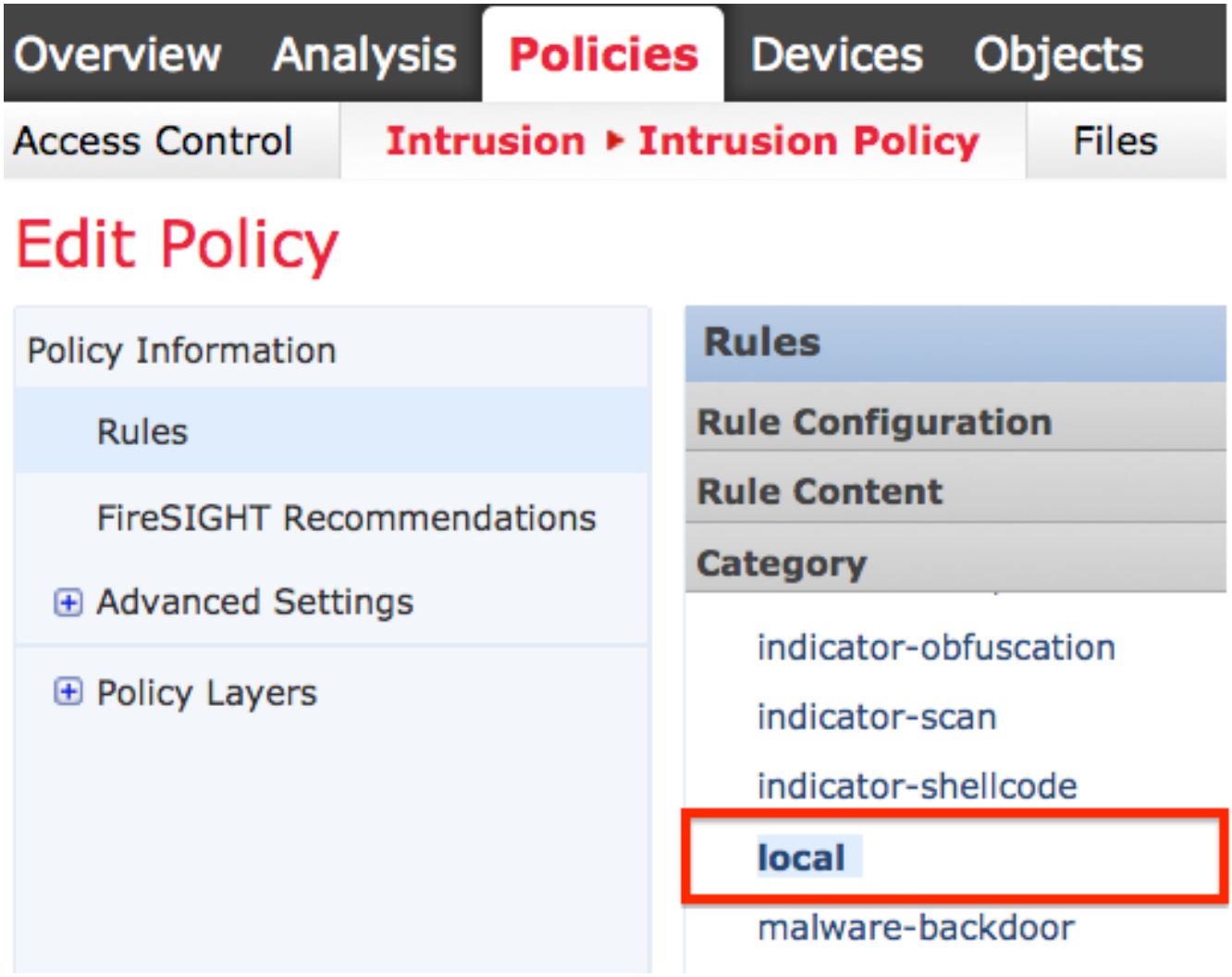
- 要查看一个当前本地规则的修订版号，请导航对**规则编辑器**页(**策略>入侵>规则编辑器**)。



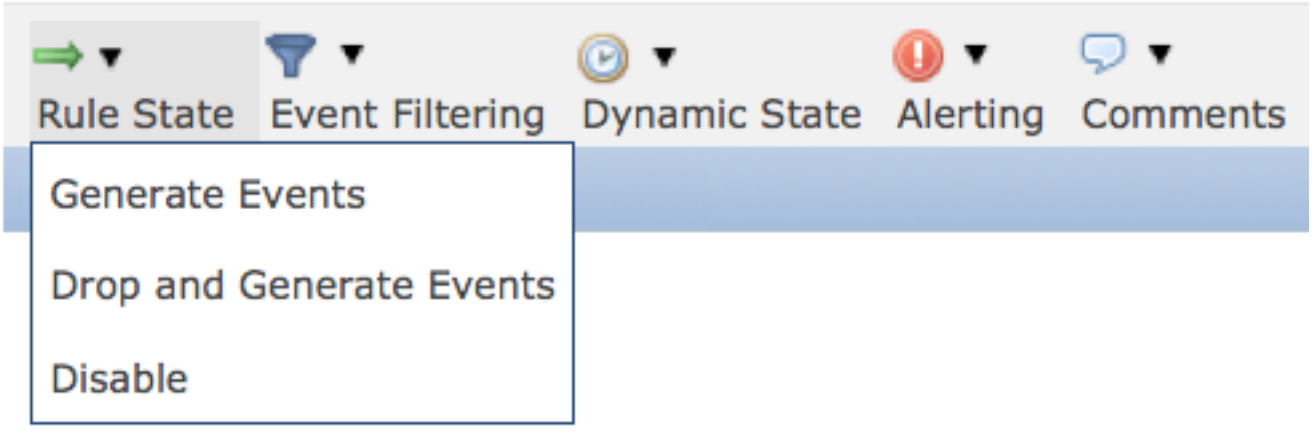
- 在规则编辑器页，请点击**本地规则**类别展开文件夹，然后单击在规则旁边**编辑**。
- 所有已导入本地规则在**本地规则**类别自动地保存。

Enable (event)本地规则

- 默认情况下， FireSIGHT系统在禁用状态设置本地规则。在您在您的入侵策略前，能使用他们您必须手工设置本地规则的状态。
- 为了启用一个本地规则，请导航对策略编辑器页(**策略>入侵>入侵策略**)。选择**规则**在左面板中。在**类别下**，请选择**本地**。若有所有本地规则应该出现。



- 在选择希望的本地规则以后，请选择规则的一状态。



- 一旦规则状态选择，请点击在左面板的**策略信息**选项。选择**进行更改**按钮。入侵策略验证。

  Note:策略验证发生故障，如果启用使用贬抑的阈值关键字与入侵事件门限功能的组合在入侵策略的一个已导入本地规则。

查看删除的本地规则

- 所有删除的本地规则移动从本地规则类别到删除的规则类别。
- 要查看一个删除的本地规则的修订版号，去**规则编辑器**页，点击**删除的**类别展开文件夹，然后

点击*铅笔*图标查看规则的详细信息在**规则编辑器**页的。

本地规则的编号

- 您不必须指定生成器(GID);如果，您能指定一个标准的文本规则的仅GID 1或138敏感数据的规定。
- 请勿指定喷鼻息ID (SID)或修订版号，当第一次时导入规则;这避免与其他规则Sids的冲突，包括删除的规则。
- FireSIGHT管理中心自动地分配下可用的海关规则SID 1000000或更加极大和修订版号1。
- 如果尝试导入与极大SID的一个入侵规则比2147483647，验证错误将出现。
- 您比当前修订版号必须包括IPS分配的SID和修订版号极大，当导入您以前导入一个本地规则的一个更新版本时。
- 您能复原您通过导入规则使用IPS分配的SID和修订版号极大比当前修订版号删除的一个本地规则。注意FireSIGHT管理中心自动地增加修订版号，当您删除一个本地规则;这是允许您复原本地规则的设备。