Cisco FireSIGHT系统上的自定义本地Snort规则

目录

简介

FireSIGHT系统上的自定义本地规则是自定义标准Snort规则，可从本地计算机以ASCII文本文件格式导入。FireSIGHT系统允许您使用Web界面导入本地规则。导入本地规则的步骤非常简单。但是，要编写最佳本地规则，用户需要深入了解Snort和网络协议。

本文档旨在为编写自定义本地规则提供一些提示和帮助。有关创建本地规则的说明，请参阅*Snort用户手册*，该手册位于snort.org。Cisco建议您在编写自定义本地规则之前下载并阅读《用户手册》。

> **注意**：Sourcefire规则更新(SRU)数据包中提供的规则由思科Talos安全情报和研究小组创建和测试，并由思科技术支持中心(TAC)提供支持。 思科TAC不提供编写或调整自定义本地规则方面的帮助，但是，如果您遇到FireSIGHT系统的规则导入功能有任何问题，请联系思科TAC。

> **警告**：编写不当的自定义本地规则可能会影响FireSIGHT系统的性能，从而降低整个网络的性能。如果网络出现任何性能问题，并且FireSIGHT系统上启用了某些自定义本地Snort规则，思科建议您禁用这些本地规则。

先决条件

要求

Cisco建议您了解Snort规则和FireSIGHT系统。

使用的组件

本文档中的信息基于以下硬件和软件版本：

- FireSIGHT管理中心（也称为防御中心）
- 5.2 或更高软件版本

使用自定义本地规则

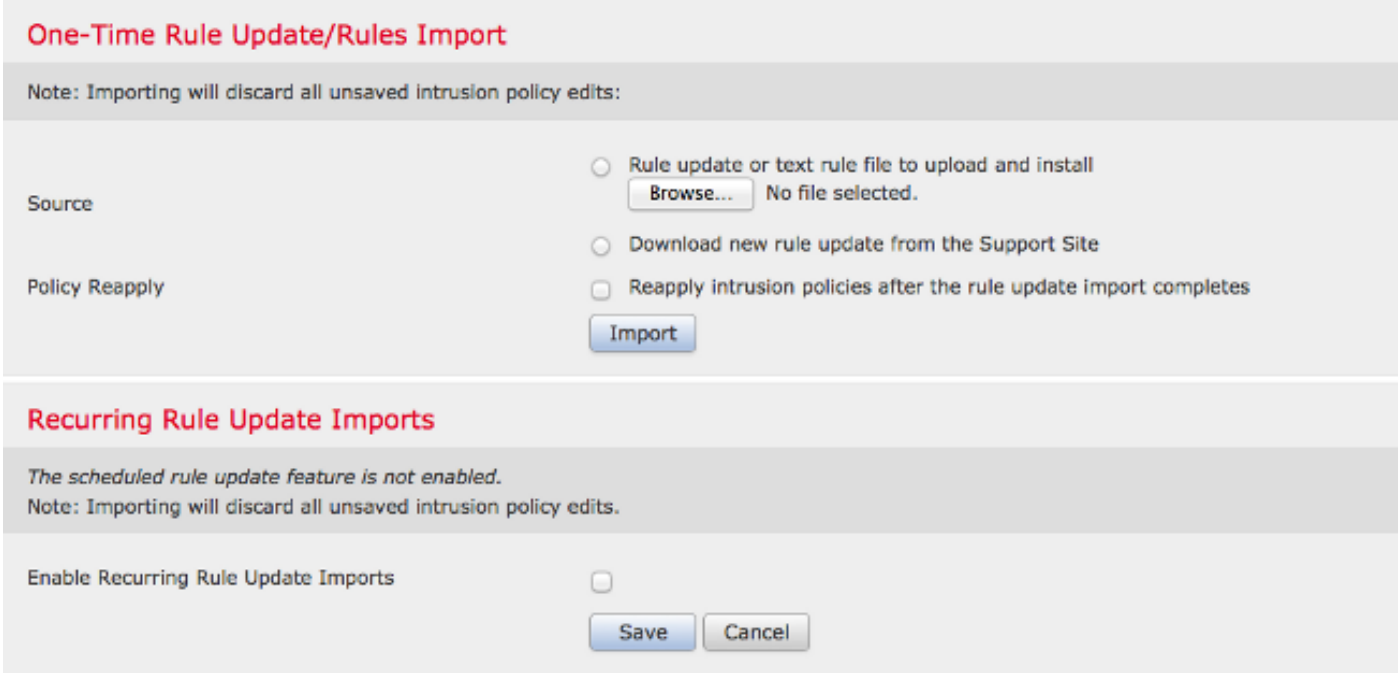
导入本地规则

开始之前，必须确保文件中的规则不包含任何转义字符。规则导入程序要求使用ASCII或UTF-8编码导入所有自定义规则。

以下步骤说明如何从本地计算机导入本地标准文本规则：

1.导航到**Policies > Intrusion > Rule Editor**，访问**Rule Editor**页。

2.单击**导入规则**。系统将显示**Rule Updates**页面。



图：Rule Updates页面的截图

3.选择**规则更新或文本规则文件以上载和安装**，然后单击**浏览**以选择规则文件。

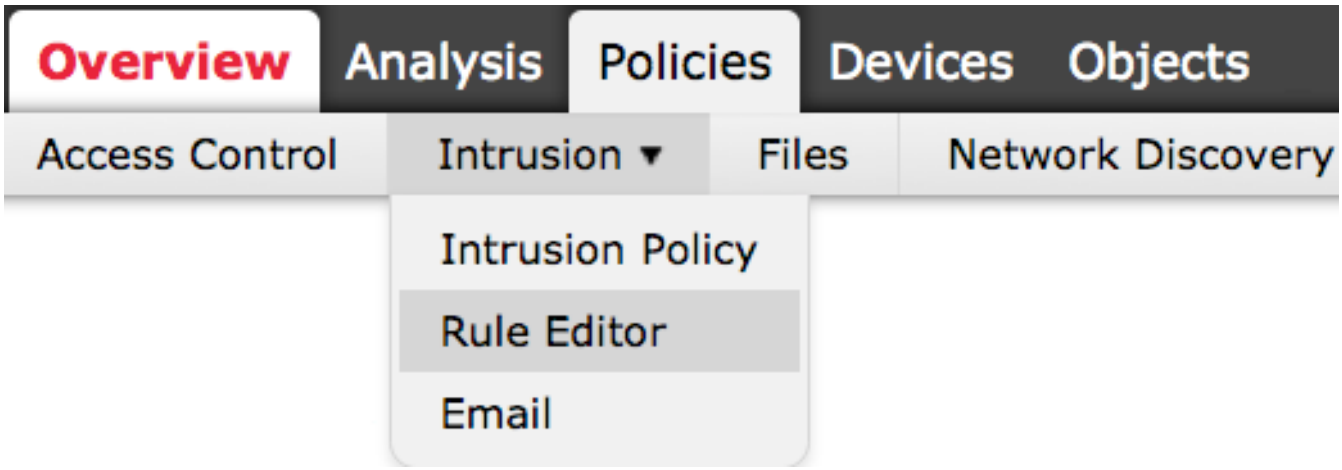
> **注意**：所有上传的规则都保存在本**地规则**类别。

4.单击**导入**。规则文件已导入。

警告：FireSIGHT系统不使用新规则集进行检查。要激活本地规则，需要在入侵策略中启用该规则，然后应用该策略。

查看本地规则

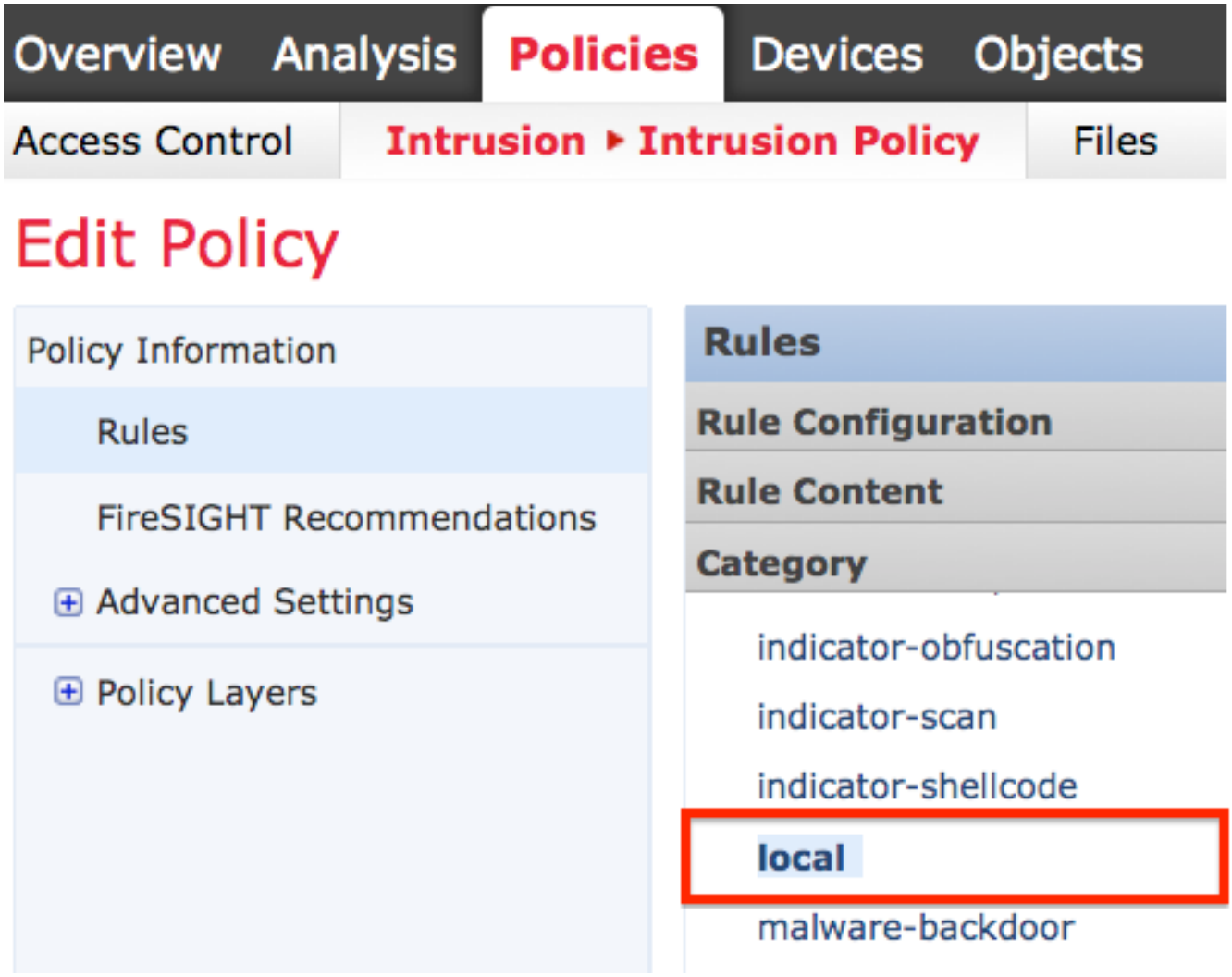
- 要查看当前本地规则的修订版号，请导航到**Rule Editor**页面(**Policies > Intrusion > Rule Editor**)。



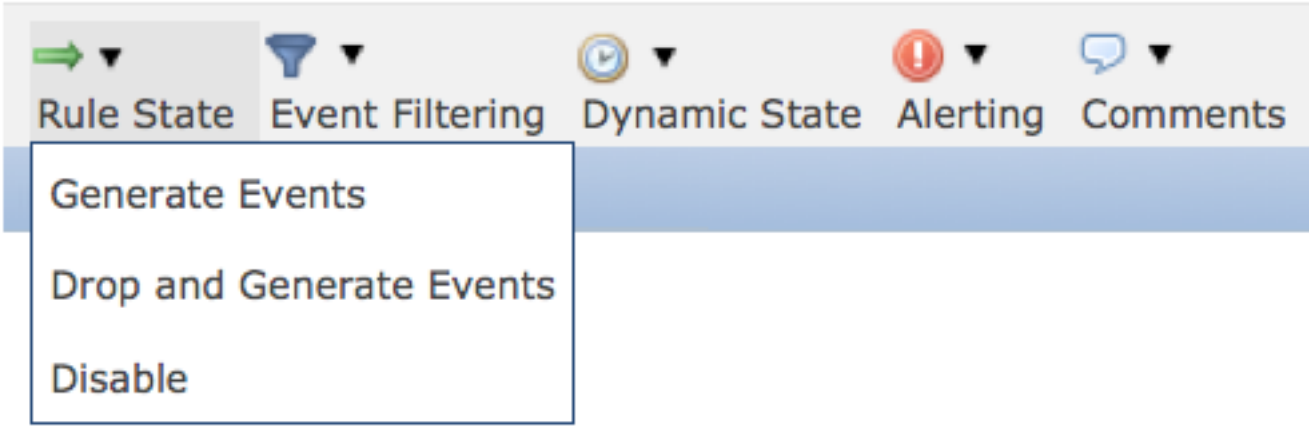
- 在Rule Editor页面中，点击**Local Rule**类别以展开文件夹，然后点击规则旁边的**Edit**。
- 所有导入的本地规则将自动保存在**本地规则**类别。

启用本地规则

- 默认情况下，FireSIGHT系统将本地规则设置为禁用状态。必须先手动设置本地规则的状态，然后才能在入侵策略中使用它们。
- 要启用本地规则，请导航到Policy Editor页面(**Policies > Intrusion > Intrusion Policy**)。 在左侧面板中选择**Rules**。在**Category**下，选择**local**。如果可用，应显示所有本地规则。



- 选择所需的本地规则后，选择规则的状态。



- 选择规则状态后，点击左侧面板上的**Policy Information**选项。选择**Commit Changes**按钮。入侵策略已验证。

  注意：如果启用一个导入的本地规则，该规则将precated threshold关键字与入侵策略中的入侵事件阈值功能结合使用，则策略验证失败。

查看已删除的本地规则

- 所有已删除的本地规则都将从本地规则类别移至已删除的规则类别。

- 要查看已删除的本地规则的修订版号，请转到**Rule Editor**页，单击**deleted**类别展开文件夹，然后单击**铅笔**图标在**Rule Editor**页中查看规则的详细信息。

本地规则编号

- 不必指定生成器(GID);如果这样做，则只能为标准文本规则指定GID 1，为敏感数据规则指定138。
- 首次导入规则时，请勿指定Snort ID(SID)或修订版号；这样可以避免与其他规则的SID发生冲突，包括已删除的规则。
- FireSIGHT管理中心会自动分配下一个可用的自定义规则SID 1000000或更大值，并且版本号为1。
- 如果尝试导入SID大于2147483647的入侵规则，则会发生验证错误。
- 导入先前导入的本地规则的更新版本时，必须包括IPS分配的SID以及大于当前修订号的修订版本号。
- 您可以恢复已删除的本地规则，方法是使用IPS分配的SID和大于当前修订号的修订号导入规则。请注意，删除本地规则时，FireSIGHT管理中心会自动增加修订版号；此设备允许您恢复本地规则。

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）。

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）。