

在Cisco FireSIGHT系统的自定义本地喷鼻息规则

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[自定义本地规则的使用](#)

[导入本地规则](#)

[查看本地规则](#)

[Enable \(event\)本地规则](#)

[查看被删除的本地规则](#)

[本地规则的编号](#)

Introduction

在FireSIGHT系统的一个自定义本地规则是您导入以ASCII文件格式从一个本地设备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。

本文的目的将提供您若干提示和协助写一个自定义本地规则。关于创建本地规则的指令是可用的在*喷鼻息用户手册*，是可用的在snort.org。Cisco建议您下载并且读用户手册，在您写一个自定义本地规则前。

Note:是由Cisco Talos安全智能和研究小组创建的并且测试，并且Cisco技术支持中心(TAC)支持在Sourcefire规则更新(SRU)程序包提供的规则。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：一个不足书面自定义本地规则能影响可能导致整个网络的性能降低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，Cisco推荐您禁用那些本地规则。

Prerequisites

Requirements

Cisco建议您有在喷鼻息规则和FireSIGHT系统的知识。

Components Used

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)
- 5.2 或更高软件版本

自定义本地规则的使用

导入本地规则

在您开始前，您必须确信，在文件的规则不包含任何换码字符。使用ASCII或UTF-8编码，规则进口商要求所有海关规则被导入。

以下程序解释如何导入从一个本地设备的本地标准的文本规则：

1. 通过连接访问**规则编辑器**页到**策略>闯入>规则编辑器**。
2. 点击**导入规则**。**规则更新**页出版。

The image shows two screenshots of a web interface for rule management. The top screenshot is titled "One-Time Rule Update/Rules Import" and contains a note: "Note: Importing will discard all unsaved intrusion policy edits:". Below the note, there are two sections: "Source" and "Policy Reapply". Under "Source", there are three radio button options: "Rule update or text rule file to upload and install" (selected), "Download new rule update from the Support Site", and "Reapply intrusion policies after the rule update import completes". The "Rule update or text rule file to upload and install" option has a "Browse..." button next to it, which shows "No file selected.". Below the radio buttons is an "Import" button. The bottom screenshot is titled "Recurring Rule Update Imports" and contains a note: "The scheduled rule update feature is not enabled." and another note: "Note: Importing will discard all unsaved intrusion policy edits:". Below the notes, there is a checkbox labeled "Enable Recurring Rule Update Imports" which is currently unchecked. At the bottom of this section are "Save" and "Cancel" buttons.

图：规则的屏幕画面校正页

3. 选择**规则更新**或**文本规则文件加载和安装**并且点击访问选择规则文件。

Note:所有被加载的规则在**本地规则**类别被保存。

4. 单击 **Import**。导入规则文件。

警告：FireSIGHT系统不使用设置的新规则检查。要启动一个本地规则，您需要enable (event)它在闯入策略，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本号，请连接对[规则编辑器页\(策略>闯入>规则编辑器\)](#)。



- 在规则编辑器页，请点击**本地规则**类别展开文件夹，然后点击在规则旁边**编辑**。
- 所有被导入的本地规则在**本地规则**类别自动地被保存。

Enable (event)本地规则

- 默认情况下，FireSIGHT系统设置在一个禁用状态的本地规则。在您在您的闯入策略前，能使用他们您必须手工设置本地规则状态。
- 为了enable (event)一个本地规则，连接对策略编辑器页([策略>闯入>闯入策略](#))。选择在左面板的**规则**。在**类别**下，请选择**本地**。若有所有本地规则应该出现。

Edit Policy

Policy Information

- Rules
- FireSIGHT Recommendations
- + Advanced Settings
- + Policy Layers

Rules

Rule Configuration

Rule Content

Category

- indicator-obfuscation
- indicator-scan
- indicator-shellcode
- local**
- malware-backdoor

- 在选择期望本地规则以后，为规则请选择一个状态。

→ Rule State
🔍 Event Filtering
🕒 Dynamic State
🚨 Alerting
💬 Comments

- Generate Events
- Drop and Generate Events
- Disable

- 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。闯入策略被验证。

Note:策略验证发生故障，如果您enable (event)使用贬抑的阈值关键字与闯入事件门限功能的组合在闯入策略的一个被导入的本地规则。

查看被删除的本地规则

- 所有被删除的本地规则从本地规则类别被移动向被删除的规则类别。
- 要查看一个被删除的本地规则的修订版本号，请去**规则编辑器**页，点击**被删除**的类别展开文件夹

，然后点击铅笔图标查看规则的详细资料在**规则编辑器**页的。

本地规则的编号

- 您不必指定生成器(GID);如果，您能为一个标准的文本规则指定仅GID 1或138敏感数据的规定。
- 请勿指定喷嘴ID (SID)或修订版本号，当第一次时导入规则;这避免与其他规则Sids的冲突，包括被删除的规则。
- 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本号1。
- 如果尝试导入与极大SID的闯入规则比2147483647，验证错误将出现。
- 您比当前修订版本号必须包括IPS分配的SID和修订版本号极大，当导入您以前导入了一个本地规则时的一个更新的版本。
- 您能复原您通过导入规则使用IPS分配的SID和修订版本号极大比当前修订版本号删除了的一个本地规则。注意FireSIGHT管理中心自动地增加修订版本号，当您删除一个本地规则;这是允许您复原本地规则的设备。