使用CLI和FMC GUI从Firepower传感器验证自定义SID列表

简介

本文档介绍如何使用CLI和FMC GUI从Firepower威胁防御(FTD)或FirePOWER模块获取自定义SID列表。如果导航到Objects > Intrusion Rules，则可在FMC GUI上找***到SID信息***。在某些情况下，从CLI获取可用SID列表是必要的。

先决条件

要求

思科建议您了解以下主题：

- 思科Firepower威胁防御(FTD)
- 具备FirePOWER服务的Cisco ASA
- 思科Firepower管理中心(FMC)
- Linux基础知识

使用的组件

本文档中的信息基于以下软件版本：

- Firepower管理中心6.6.0
- Firepower威胁防御6.4.0.9
- FirePOWER模块6.2.3.2

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

入侵***规则***是一组关键字和参数，系统使用它们来检测利用网络漏洞的尝试。当系统分析网络流量时，它会将数据包与每条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。对于内联部署中的丢弃规则，系统丢弃数据包并生成事件。您可以从Firepower管理中心Web控制台查看和评估入侵事件。

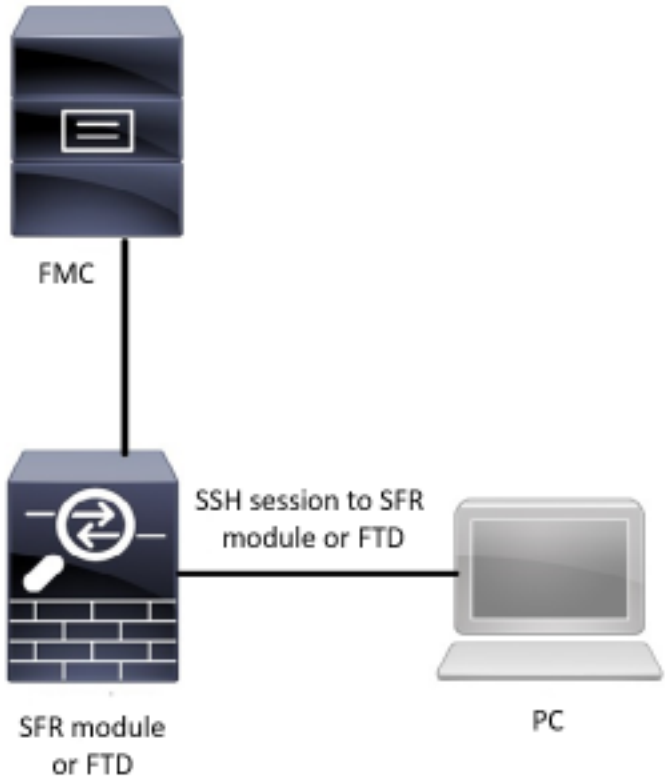
Firepower系统提供两种类型的入侵规则：***共享对象规***则和***标准文本规则***。思科Talos安全情报和研究小组(Talos)可以使用共享对象规则以传统标准文本规则无法的方式检测针对漏洞的攻击。无法创建共享对象规则。当入侵规则由您自己编写时，必须创建标准文本规则。自定义标准文本规则，以调整您可能看到的事件类型。通过编写规则并指定规则的事件消息，可以更轻松地识别指示攻击和策略规避的流量。

在自定义入侵策略中启用自定义标准文本规则时，请记住，某些规则关键字和参数要求首先以某种方式对流量进行解码或预处理。

Firepower***系统上的***自定义本地规则是自定义标准Snort规则，可以从本地计算机以ASCII文本文件格式导入。Firepower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。

> **警告：**确保在生产环境中使用规则之前使用受控网络环境测试所编写的任何入侵规则。编写不当的入侵规则可能会严重影响系统性能

网络图

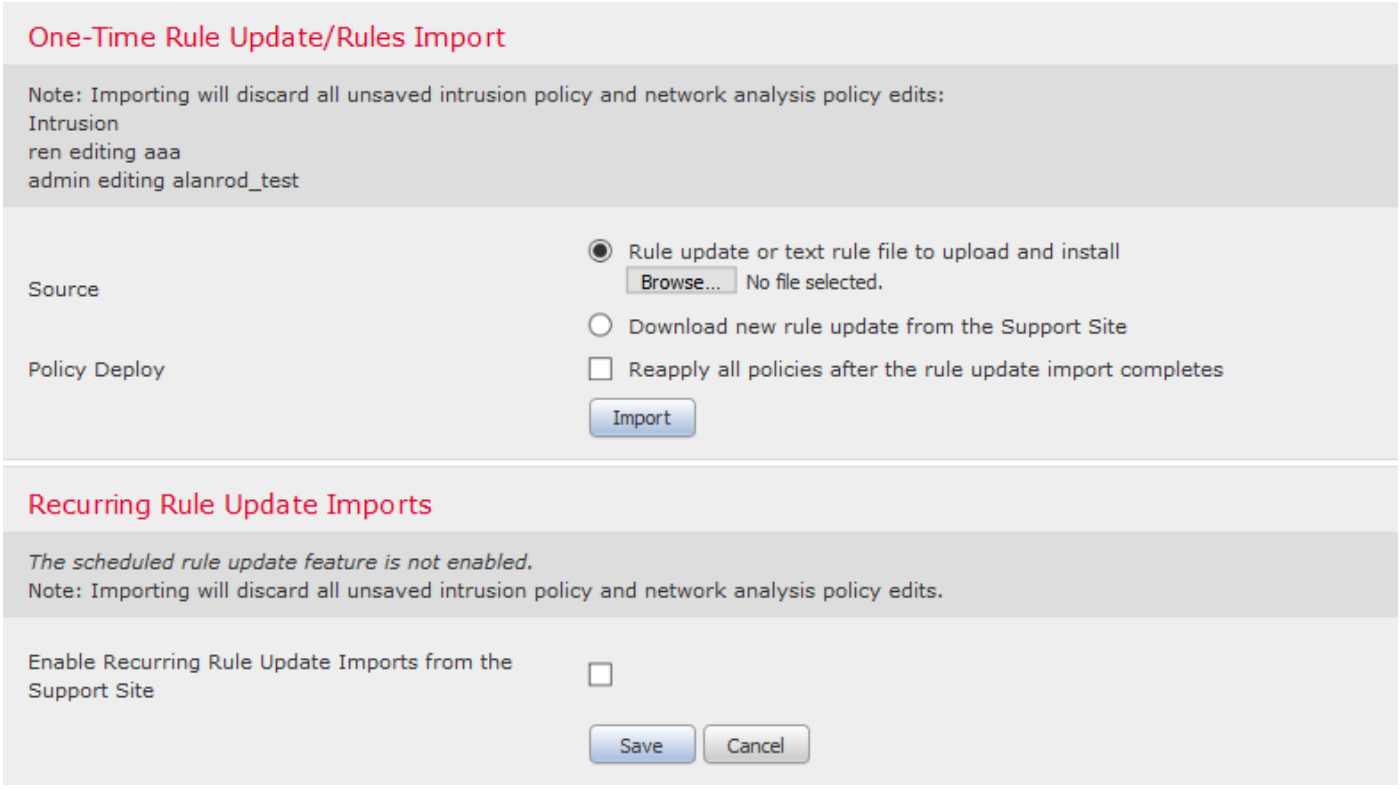


配置

导入本地规则

在开始之前，您需要确保自定义文件上列出的规则不包含任何特殊字符。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。下面显示的步骤说明如何从本地计算机导入本地标准文本规则。

步骤1.导航至“对**象”**(Objects)>“入侵规**则”(Intrusion Rules)>“导入规则”(Import Rules)选项卡。**系统将**显示Rule Updates页**面，如下图所示：



步骤2.选择要**上传和安装的规则更新或文本规则文件**，然**后单**击浏览以选择自定义规则文件

注意：所有上传的规则都保存在本**地规则类**别中

步骤3.单击“**导入”**。规则文件已导入

注意: Firepower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。

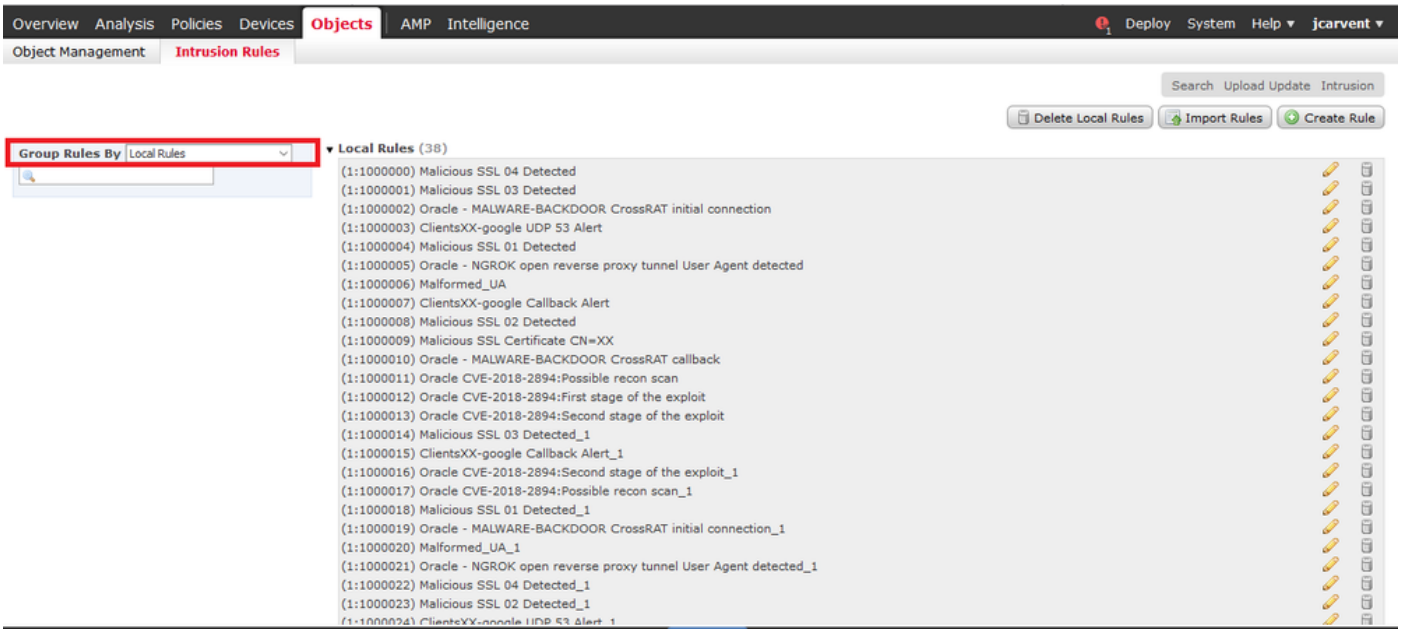
验证

从FMC GUI

1.查看从FMC GUI导入的本地规则

步骤1.导航至“对**象”>“入侵规则”**

步骤2.从组规**则中选**择本**地规则**



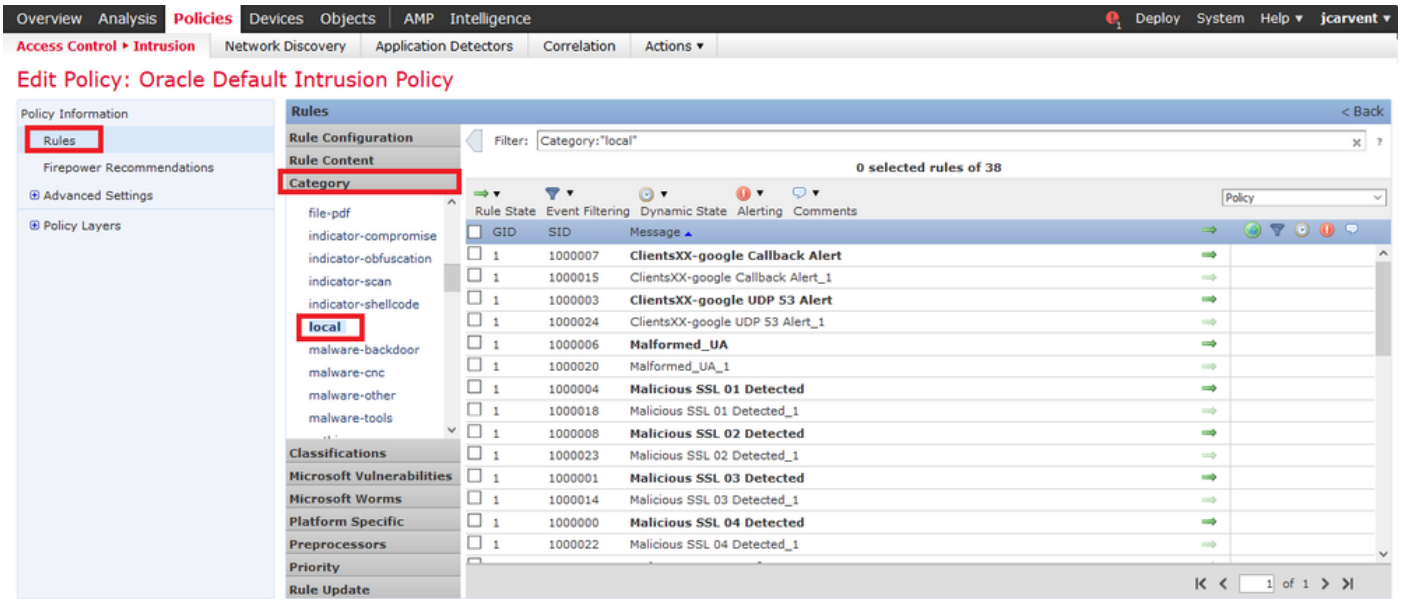
默认情况下，Firepower系统将本地规则设置为禁用状态。这些本地规则必须手动设置本地规则的状态，才能在入侵策略中使用它们。

2.从入侵策略启用本地规则

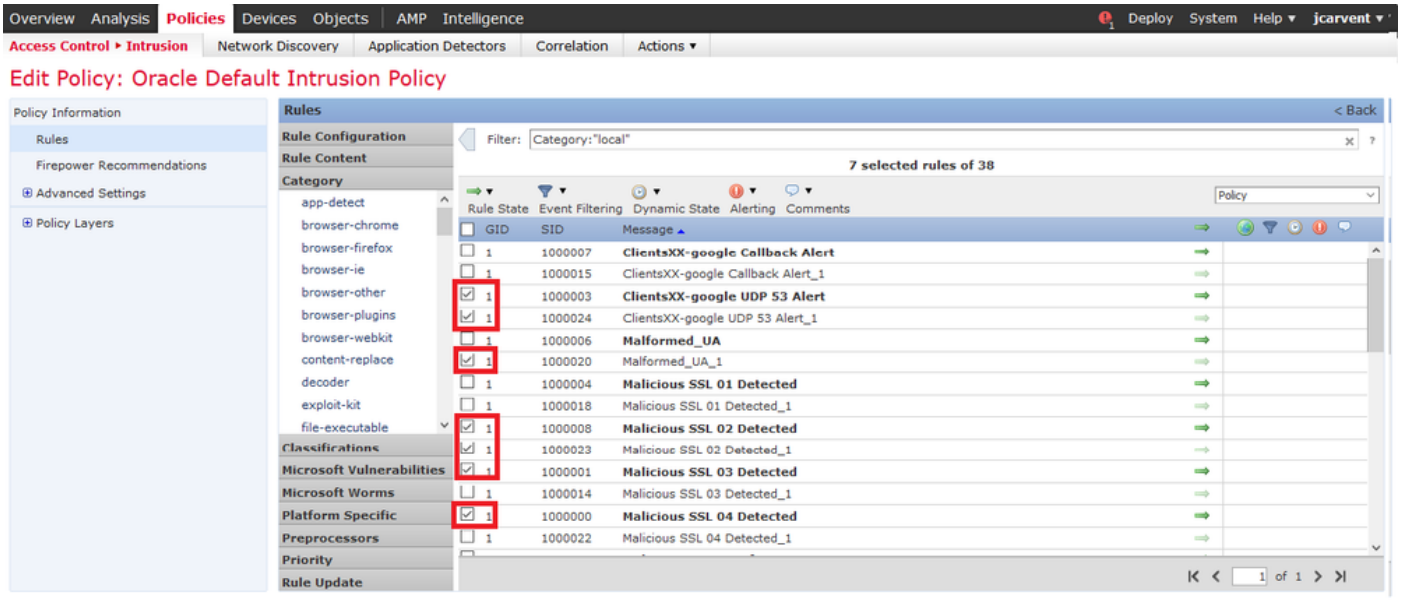
步骤1.导航至Policies > **Intrusion** > **Intrusion Policy**下的Policy Editor页

步骤2.在左**面**板中选择Rules

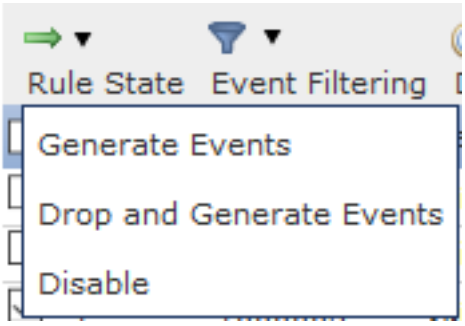
第3步。在"类**别**"下，选**择本**地。所有本地规则都应显示（如果可用）：



第四步： 选择所需的本地规则：



第五步：选择所需的本地规则后，从Rule State中选择**状态**



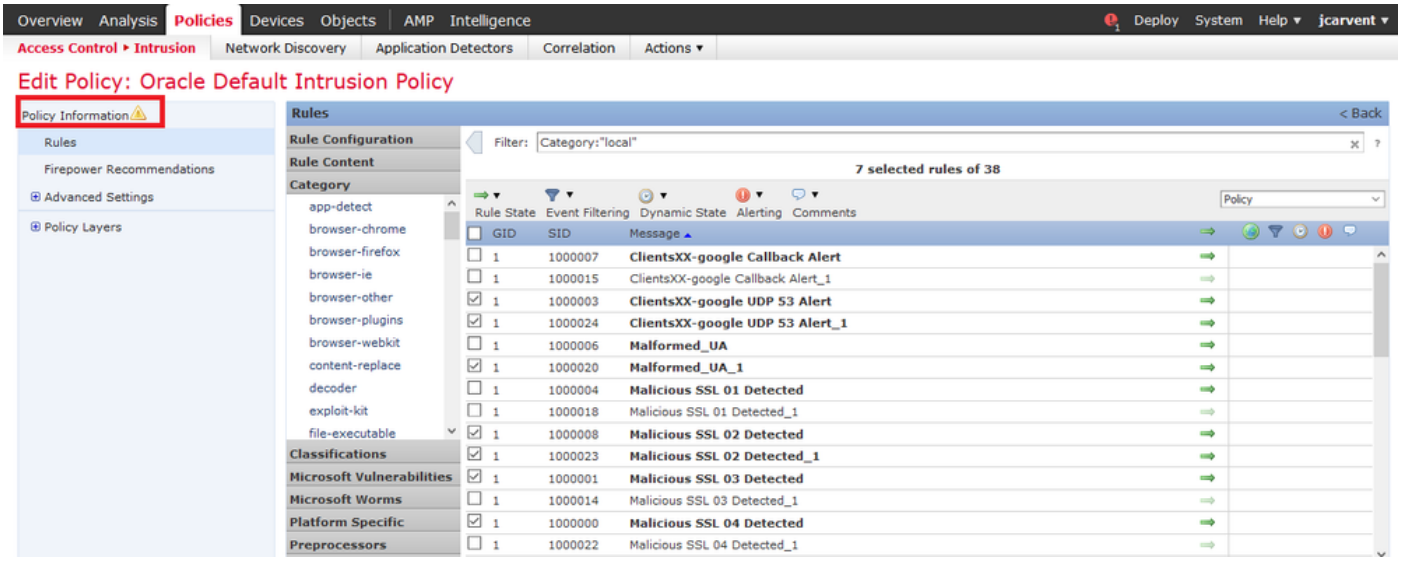
可以使用以下选项：

— 生成事件：启用规则并生成事件

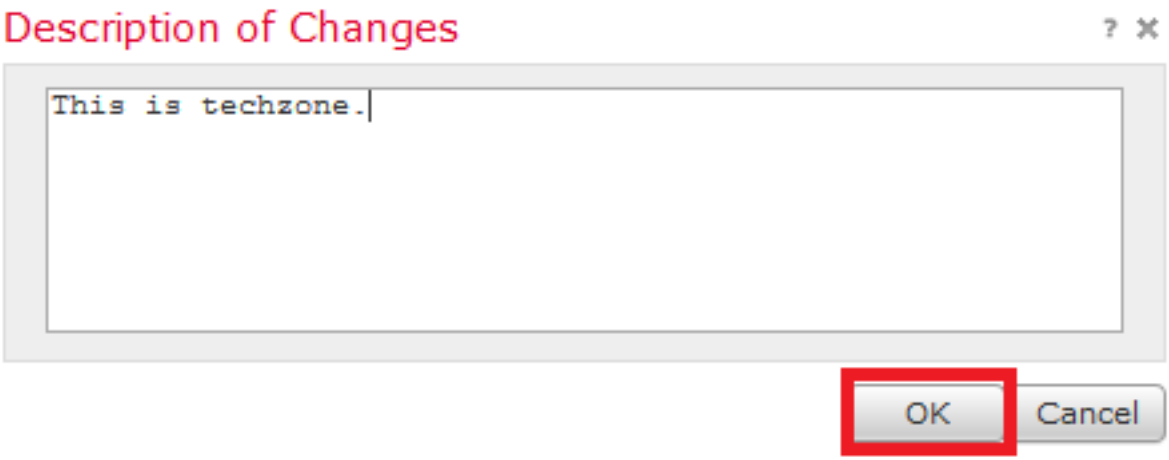
— 删除并生成事件：启用规则、丢弃流量并生成事件

-禁用:否启用规则，无事件

第六步： 选择规则状态后，点击 **左面板上的"策略信息"选项**



步骤7.选择Commit **Changes按**钮并提供更改的简要说明。单击“OK(**稍后**确定)”。入侵策略已验证。



注意：如果启用导入的本地规则，该规则使用已弃用的threshold关键字并结合入侵策略中的入侵事件阈值功能，则策略验证失败。

步骤8.部署更改

从FTD或SFR模块CLI

1.查看从FTD或SFR模块CLI导入的本地规则

步骤1.从SFR模块或FTD建立SSH或CLI会话

步骤2.导航至专家模式

```
> expert
admin@firepower:~$
```

步骤3.获取管理员权限

```
admin@firepower:~$ sudo su -
```

步骤4.键入密码

```
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
```

步骤5.导航至**/ngfw/var/sf/detection_engine/UUID/intrusion/**

```
root@firepower:/home/admin# cd /ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-
2369c038cbc9/intrusion/
root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#
```

注意：如果使用SFR模块，请勿使用/ngfw/var/sf/detection_engines/*/intrusion path。入侵用途**/var/sf/detection_engine/*/入侵**

步骤6.引入以下命令

```
grep -Eo "sid:*([0-9]{1,8})" */*local.rules
```
请参考下图作为工作示例：

```
root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#
grep -Eo "sid:*([0-9]{1,8})" */*local.rules
sid:1000008
sid:1000023
sid:1000007
sid:1000035
sid:1000004
sid:1000000
...
```
这将列出FTD或SFR模块启用的客户SID列表。

故障排除

步骤1.确保从FMC detection_engines建立到SFR模块或FTD的SSH会话未列出

步骤2.命令grep -Eo "sid:*([0-9]{1,8})" */*local.rules仅在入侵目录下工作，该命令不能从另一个目录使用

步骤3.使用命令grep -Eo "sid:*([0-9]{1,8})" */*.rules从所有类别中获取完整的SID列表

导入本地入侵规则的最佳实践

导入本地规则文件时，请遵守以下准则：

- 规则导入程序要求所有自定义规则都以ASCII或UTF-8编码的纯文本文件导入
- 文本文件名可以包含字母数字字符、空格和除下划线(_)、句点(.)和短划线(-)以外的任何特殊字符
- 系统导入以单磅字符(#)开头的本地规则，但这些规则被标记为已删除
- 系统导入以单磅字符(#)开头的本地规则，且不导入以两磅字符(##)开头的本地规则
- 规则不能包含任何转义字符
- 导入本地规则时，无需指定生成器ID(GID)。如果需要，请仅为标准文本规则指定GID 1
- 首次导入规则时，请执行 *不* 指定 Snort ID (SID)或修订号。这可避免与其他规则（包括已删除的规则）的SID发生冲突。系统将自动为规则分配下一个可用的自定义规则SID 1000000或更大，修订版号为1
- 如果必须导入带SID的规则，则SID必须是介于1,000,000和9,999,999之间的唯一数字
- 在多域部署中，系统将从上所有域使用的共享池将SID分配给导入的规则 Firepower 管理中心。如果多个管理员同时导入本地规则，则单个域内的SID可能显示为非顺序，因为系统将序列中的干预数字分配给了另一个域
- 在导入以前导入的本地规则的更新版本或恢复已删除的本地规则时，***必须***包括系统分配的SID和大于当前修订版号的修订版号。您可以通过编辑规则来确定当前或已删除规则的修订版号

  注：删除本地规则时，系统会自动增加修订号；这是允许您恢复本地规则的设备。所有已删除的本地规则都从本地规则类别移动到已删除的规则类别。

- 在高可用性对中的主Firepower管理中心上导入本地规则，以避免SID编号问题

- 如果规则包含以下任一项，导入将失败：SID大于2147483647长于64个字符的源或目标端口列表
- 如果启用导入的本地规则，该规则使用已弃用的***threshold***关键字并结合入侵策略中的入侵事件阈值功能，则策略验证失败
- 所有导入的本地规则将自动保存在本地规则类别中
- 系统始终将导入的本地规则设置为禁用的规则状态。在入侵策略中使用本地规则之前，必须手动设置其状态

相关信息

以下是一些与Snort SID相关的文档供参考：

更新入侵规则

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/System_Software_Updates.html#ID-2259-00000356

入侵规则编辑器

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/the_intrusion_rules_editor.html