在FTD的Snort3中配置自定义本地Snort规则

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

网络图

配置

- 方法 1.从Snort 2导入Snort 3
  - 步骤1:确认Snort版本
  - 第二步：在Snort 2中创建或编辑自定义本地Snort规则
  - 第三步：将自定义本地Snort规则从Snort 2导入Snort 3
  - 第四步：更改规则操作
  - 第五步：确认导入的自定义本地Snort规则
  - 第六步：将入侵策略与访问控制策略(ACP)规则相关联
  - 步骤 7.部署更改
- 方法 2.上传本地文件
  - 步骤1:确认Snort版本
  - 第二步：创建自定义本地Snort规则
  - 第三步：上传自定义本地Snort规则
  - 第四步：更改规则操作
  - 第五步：确认上传的自定义本地Snort规则
  - 第六步：将入侵策略与访问控制策略(ACP)规则相关联
  - 步骤 7.部署更改

验证

- 步骤1:设置HTTP服务器中的文件内容
- 第二步：初始HTTP请求
- 第三步：确认入侵事件

常见问题解答 (FAQ)

故障排除

参考

简介

本文档介绍在防火墙威胁防御(FTD)的Snort3中配置自定义本地Snort规则的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科Firepower管理中心(FMC)
- 防火墙威胁防御(FTD)

使用的组件

本文档中的信息基于以下软件和硬件版本：

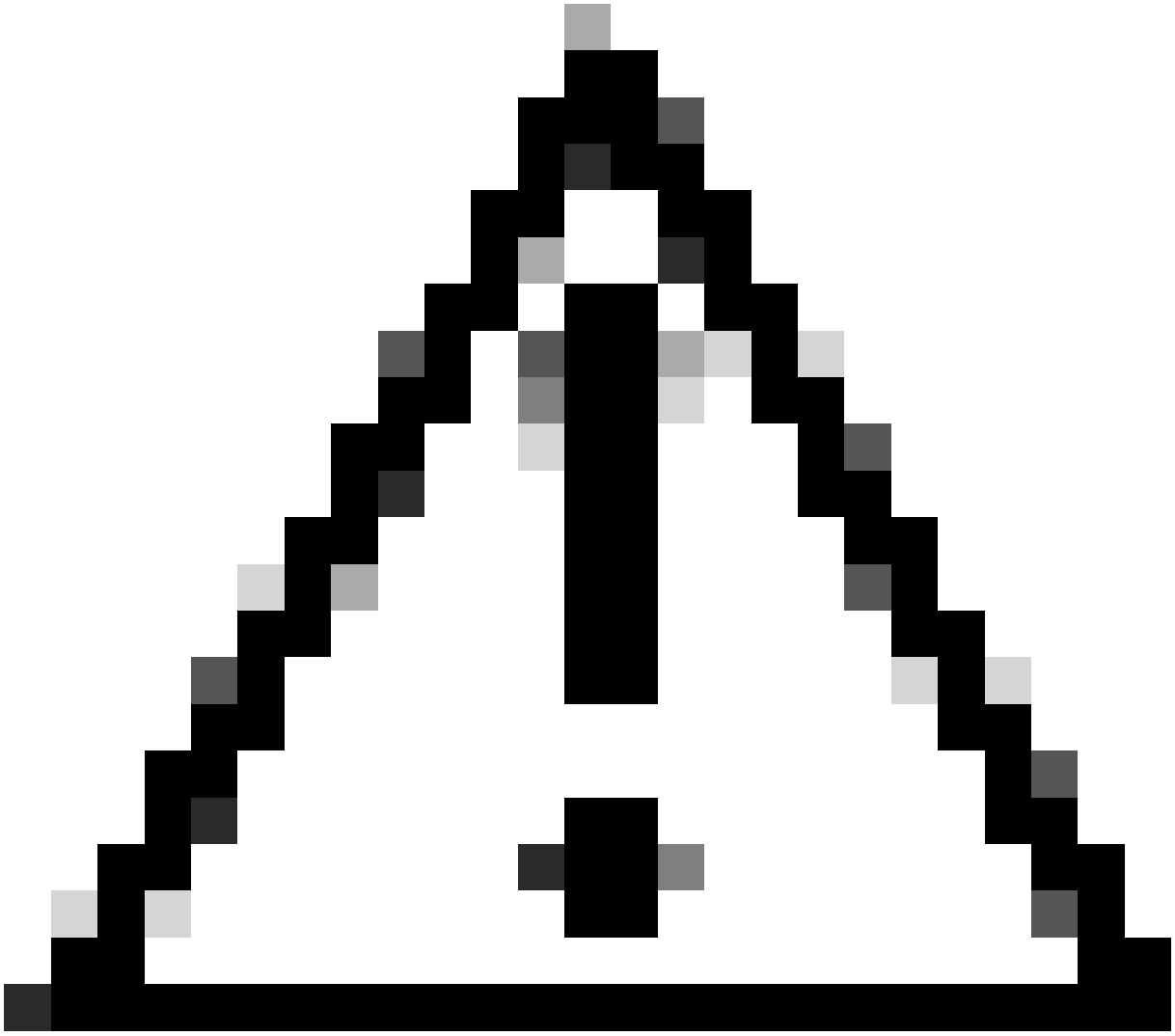
- 思科VMWare Firepower管理中心7.4.1
- 思科Firepower 2120 7.4.1

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

在管理中心威胁防御中对Snort 3的支持从7.0版开始。对于7.0版及更高版本的新设备和重新映象设备，Snort 3是默认检测引擎。

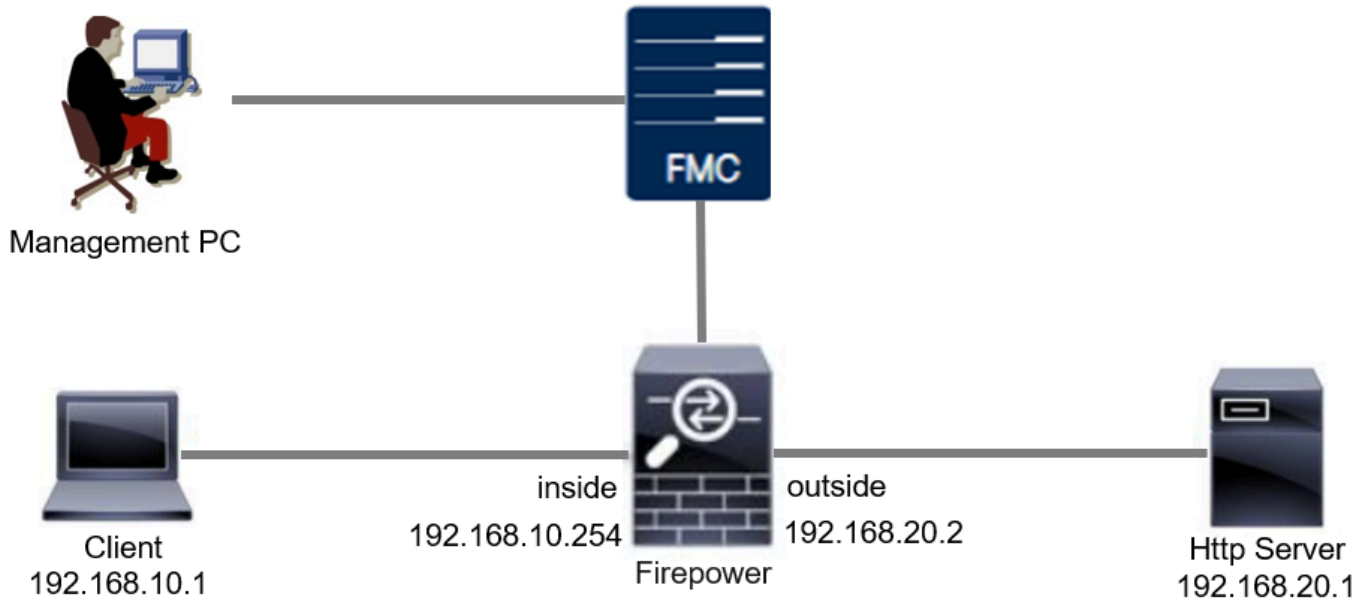
本文档提供了如何为Snort 3自定义Snort规则的示例，以及一个实际的验证示例。具体而言，介绍了如何使用自定义Snort规则配置和验证入侵策略，以丢弃包含特定字符串（用户名）的HTTP数据包。



注意：创建自定义本地Snort规则并为其提供支持不在TAC支持范围之内。因此，本文档只能用作参考，并要求您自行决定并自行负责创建和管理这些自定义规则。

网络图

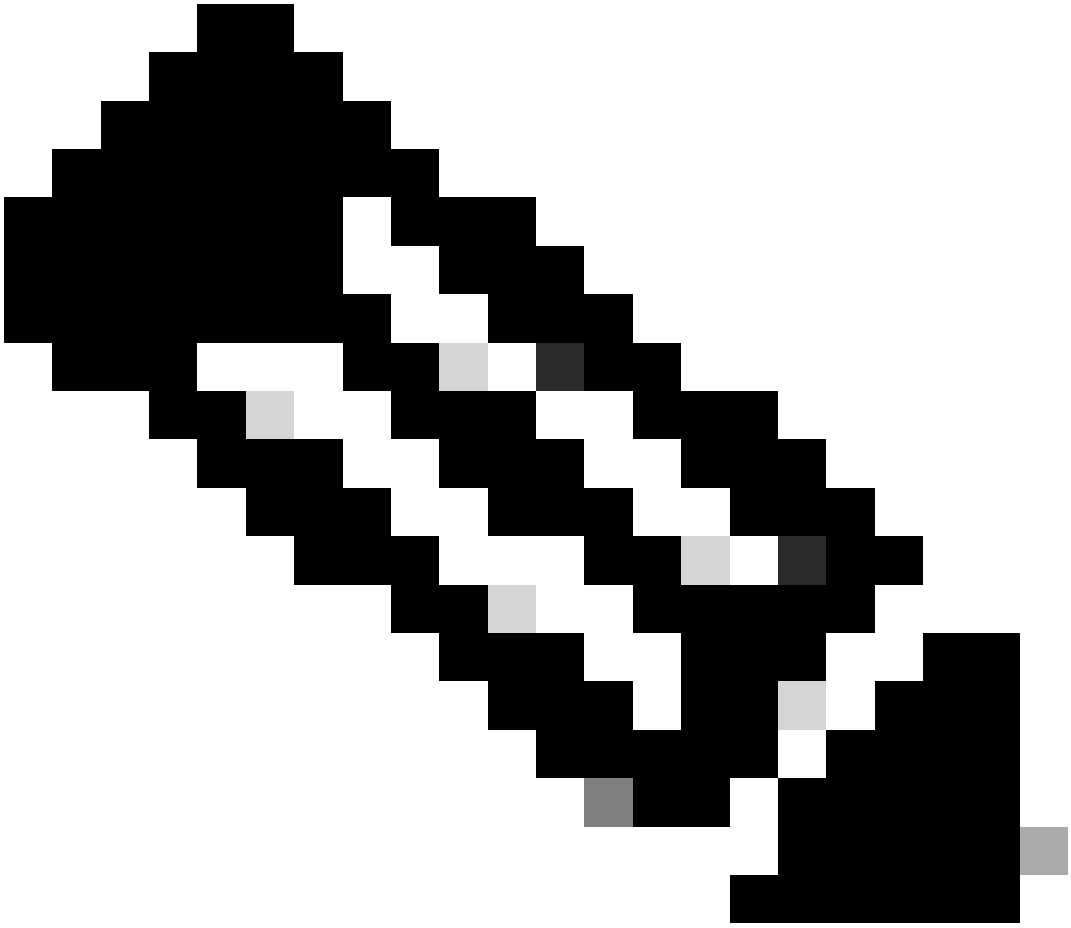
本文档介绍此图中Snort3中的自定义本地Snort规则的配置和验证。



网络图

配置

这是用于检测和丢弃包含特定字符串（用户名）的HTTP响应数据包的自定义本地Snort规则的配置。

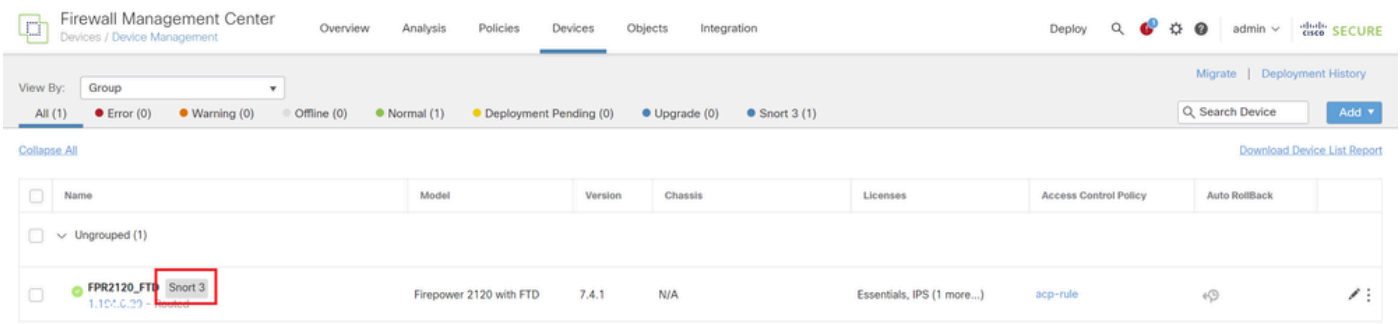


注意：到目前为止，无法在FMC GUI中从Snort 3 All Rules页面添加自定义本地Snort规则。您必须使用本文档中介绍的方法。

方法 1.从Snort 2导入Snort 3

步骤1.确认Snort版本

在FMC上导航到设备>设备管理，点击设备选项卡。确认snort版本为Snort3。



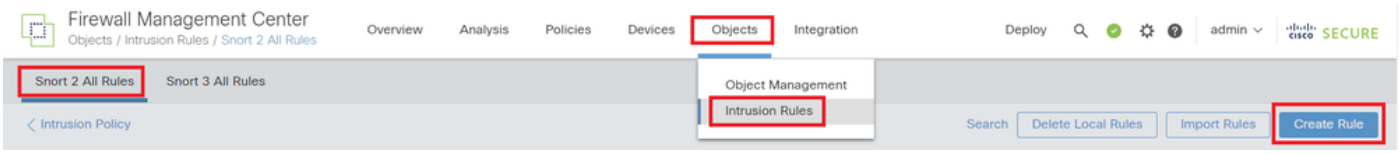
Snort版本

第二步：在Snort 2中创建或编辑自定义本地Snort规则

导航到对象(Objects) >入侵规则(Intrusion Rules) > Snort 2所有规则(Snort 2 All Rules)在FMC上。点击Create Rule按钮添加自定义本地Snort规则，或在FMC上导航到Objects > Intrusion Rules > Snort 2 All Rules > Local Rules，点击Edit按钮以编辑现有自定义本地Snort规则。

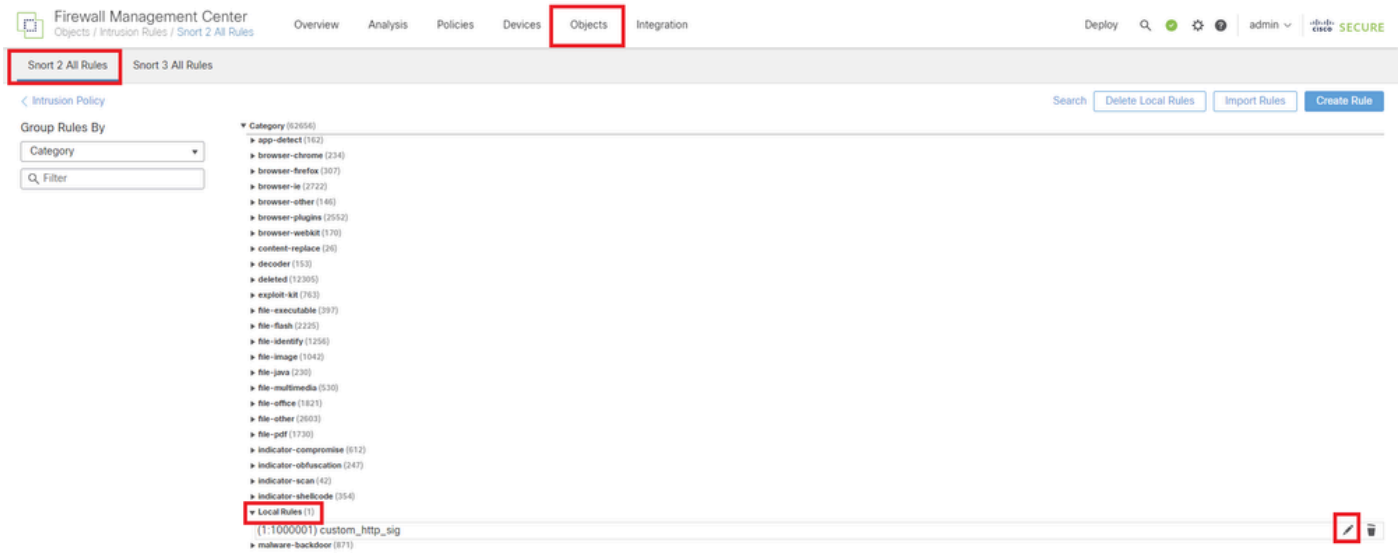
有关如何在Snort 2中创建自定义本地Snort规则的说明，请参阅在Snort2的FTD上配置自定义本地Snort规则。

添加新的自定义本地Snort规则，如图所示。



添加新的自定义规则

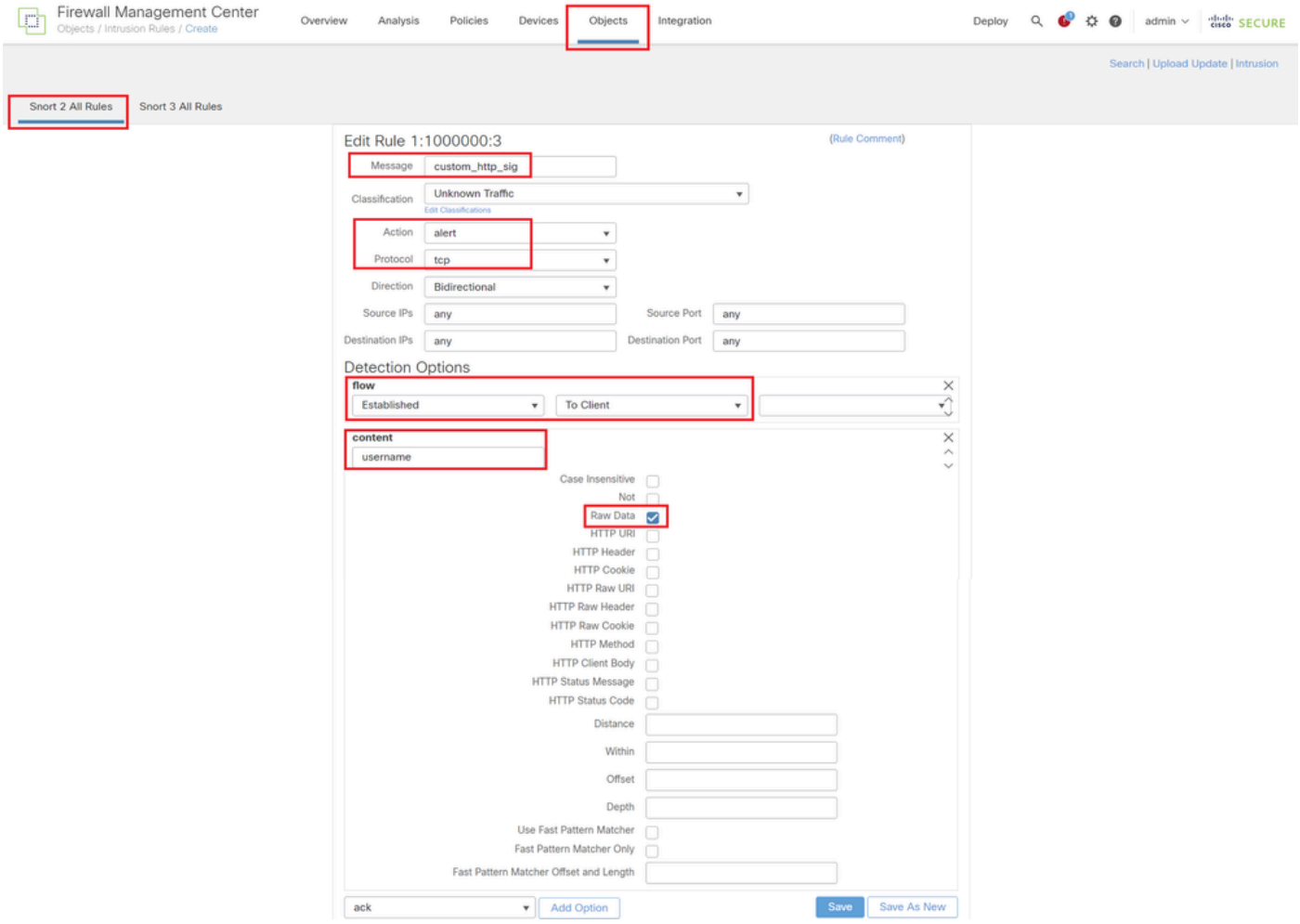
编辑现有自定义本地Snort规则，如图所示。在本示例中，编辑现有自定义规则。



编辑现有自定义规则

输入签名信息以检测包含特定字符串（用户名）的HTTP数据包。

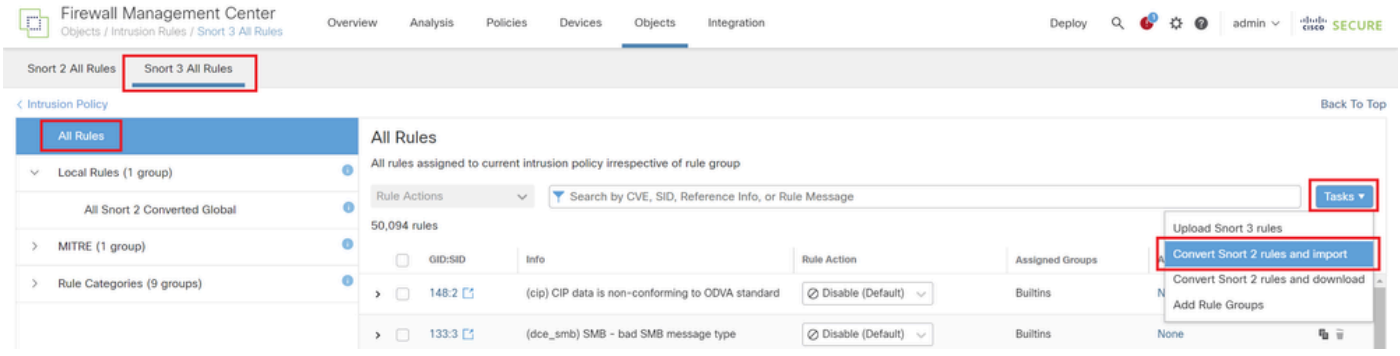
- 消息：custom_http_sig
- 操作：警报
- 协议：tcp
- 流：已建立，到客户端
- 内容：用户名（原始数据）



输入规则的必要信息

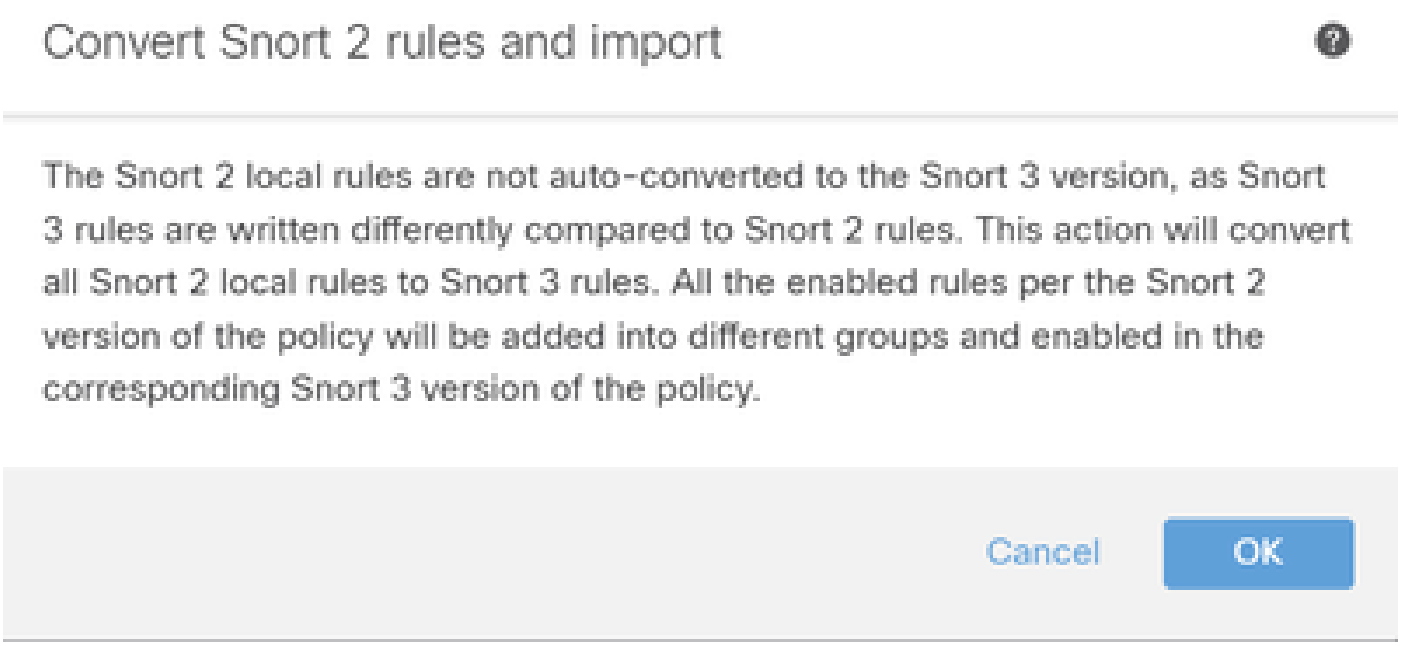
第三步：将自定义本地Snort规则从Snort 2导入Snort 3

在FMC上导航到对象>入侵规则> Snort 3所有规则>所有规则，单击任务下拉列表中的转换Snort 2规则和导入。



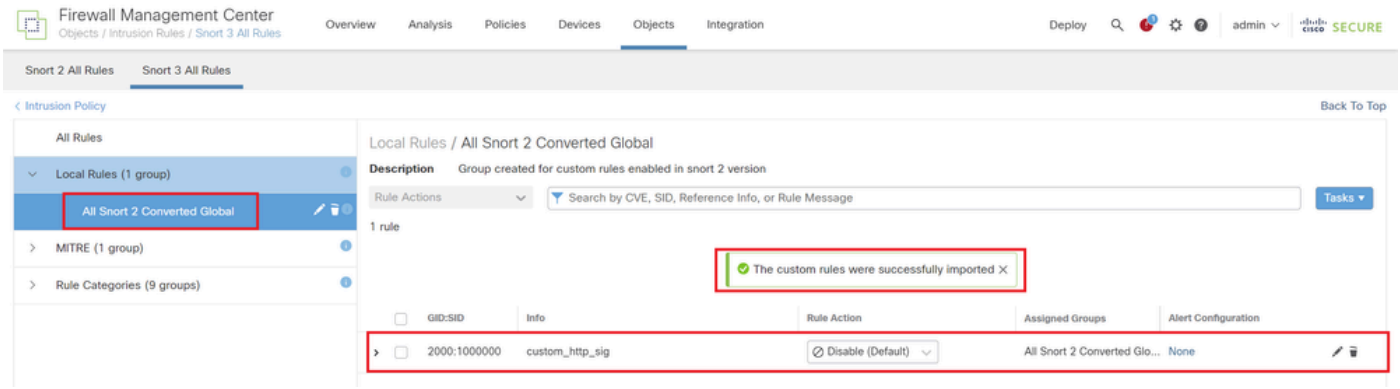
将自定义规则导入Snort 3

选中警告消息并单击确定。



警告消息

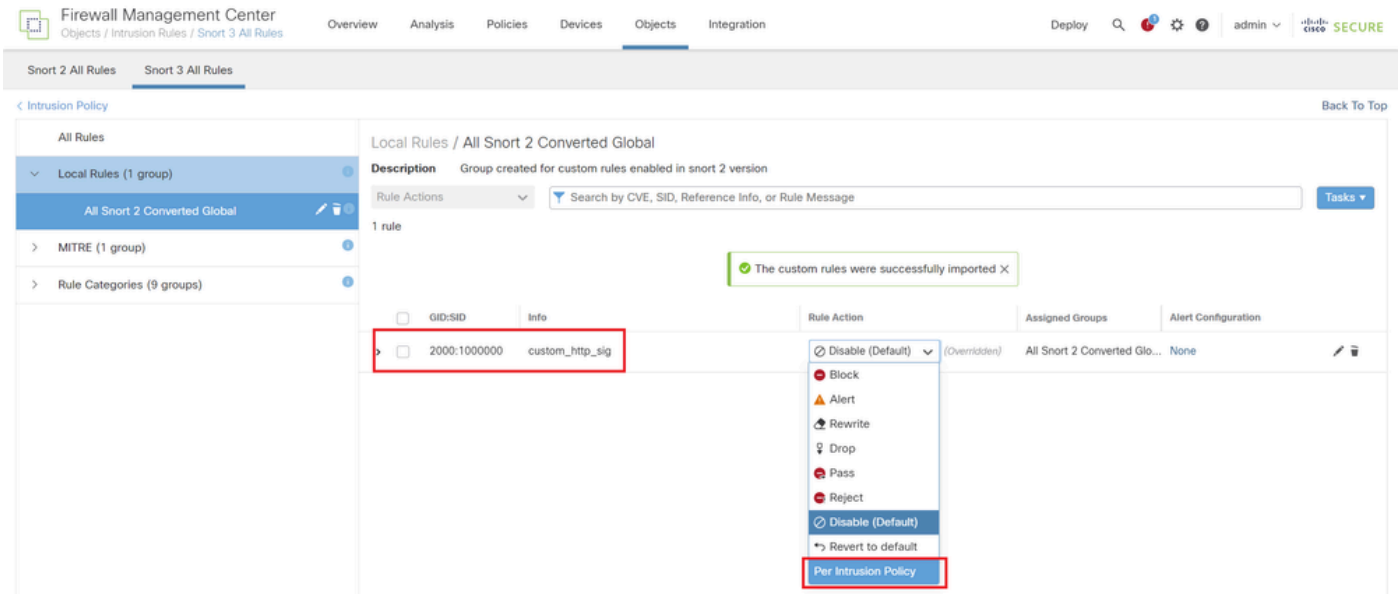
在FMC上导航到对象>入侵规则> Snort 3所有规则，点击所有Snort 2转换后的全局以确认导入的自定义本地Snort规则。



确认导入的自定义规则

第四步：更改规则操作

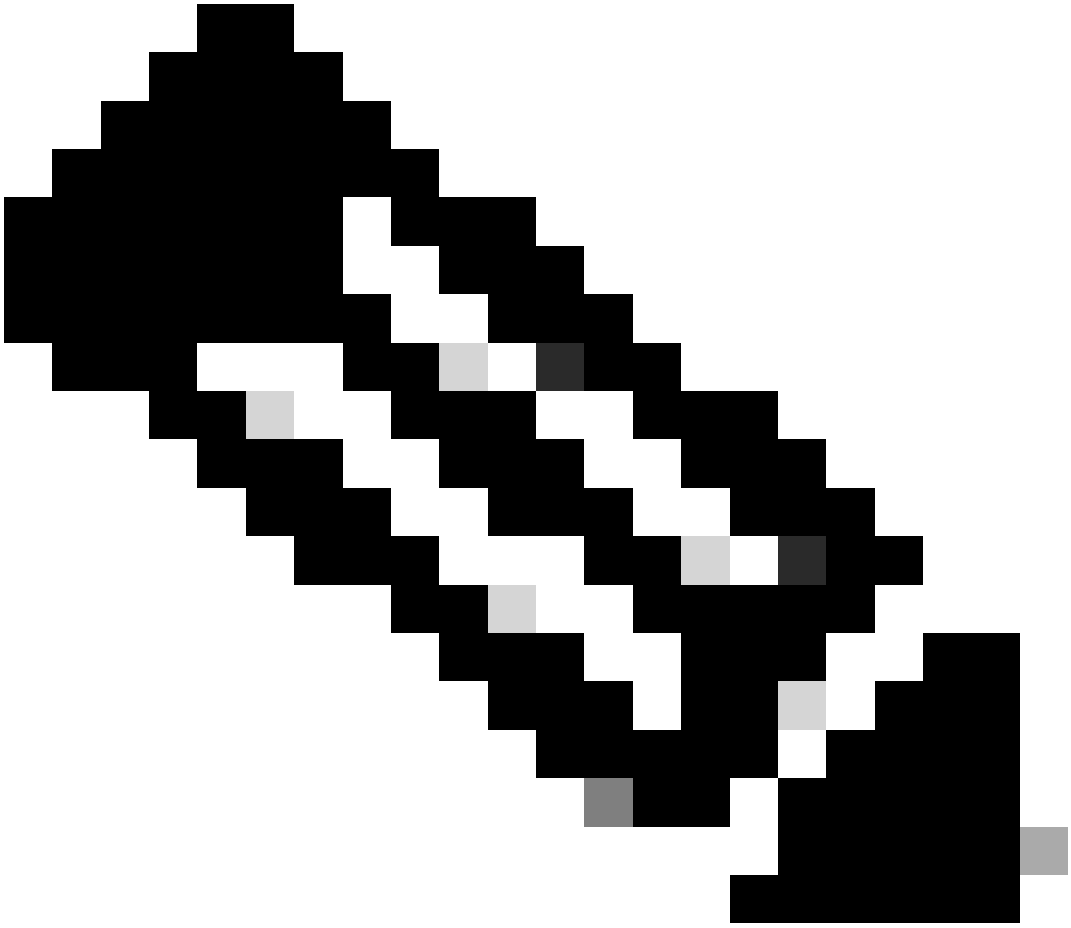
根据目标自定义规则的规则操作，单击Per Intrusion Policy。



更改规则操作

在Edit Rule Action屏幕中，输入Policy和Rule Action的信息。

- 策略：snort_test
- 规则操作：阻止



注意：规则操作包括：

Block -生成事件，阻塞当前匹配的数据包以及此连接中的所有后续数据包。

警报-仅为匹配的数据包生成事件，不会丢弃数据包或连接。

Rewrite -根据规则中的replace选项生成事件并覆盖数据包内容。

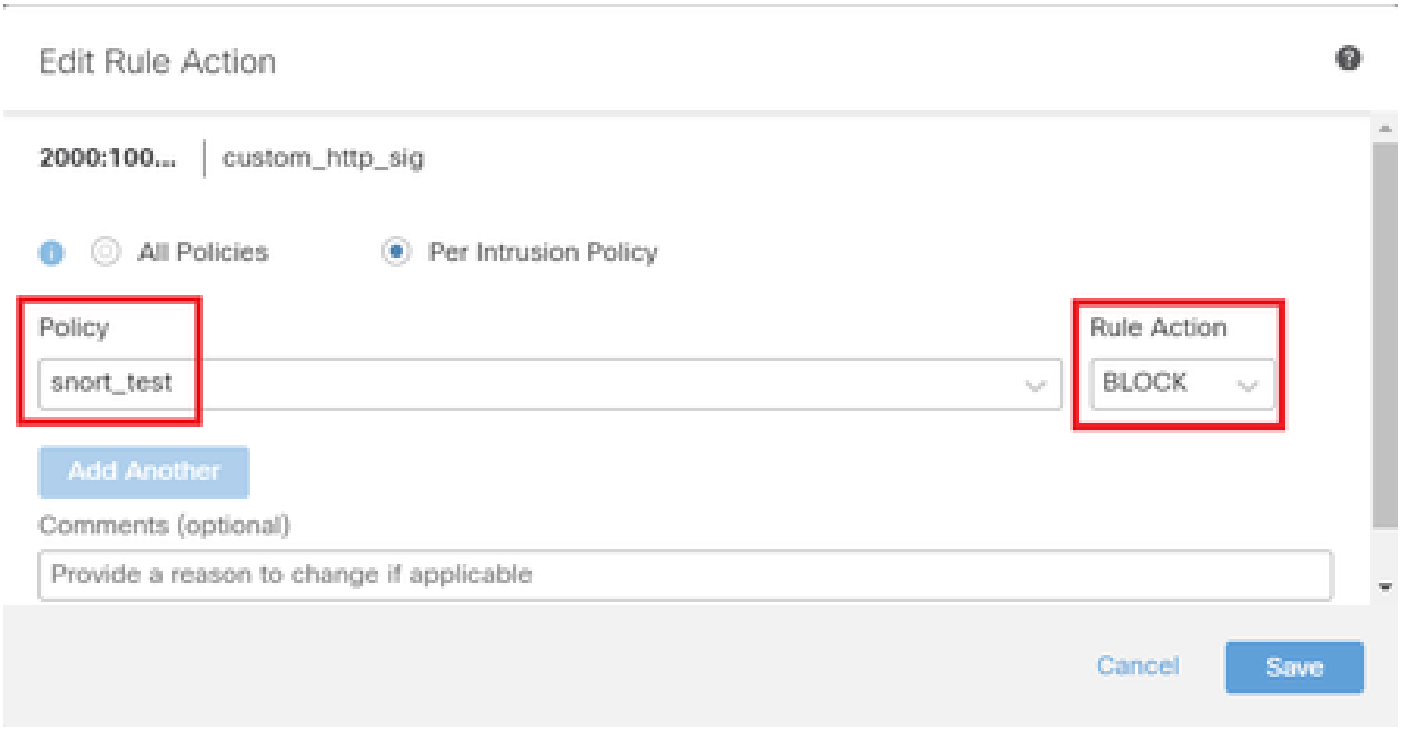
Pass -不生成任何事件，允许数据包通过，而无需任何后续Snort规则进一步评估。

Drop -生成事件，丢弃匹配的数据包，并且不阻塞此连接中的进一步流量。

Reject -生成事件，丢弃匹配的数据包，阻止此连接中的进一步流量，如果是TCP协议，则向源主机和目的主机发送TCP重置。

Disable -不匹配此规则的流量。不生成事件。

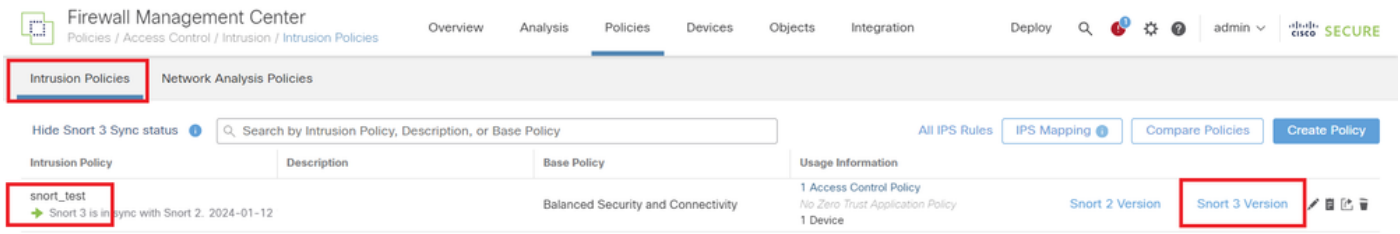
Default -恢复系统默认操作。



编辑规则操作

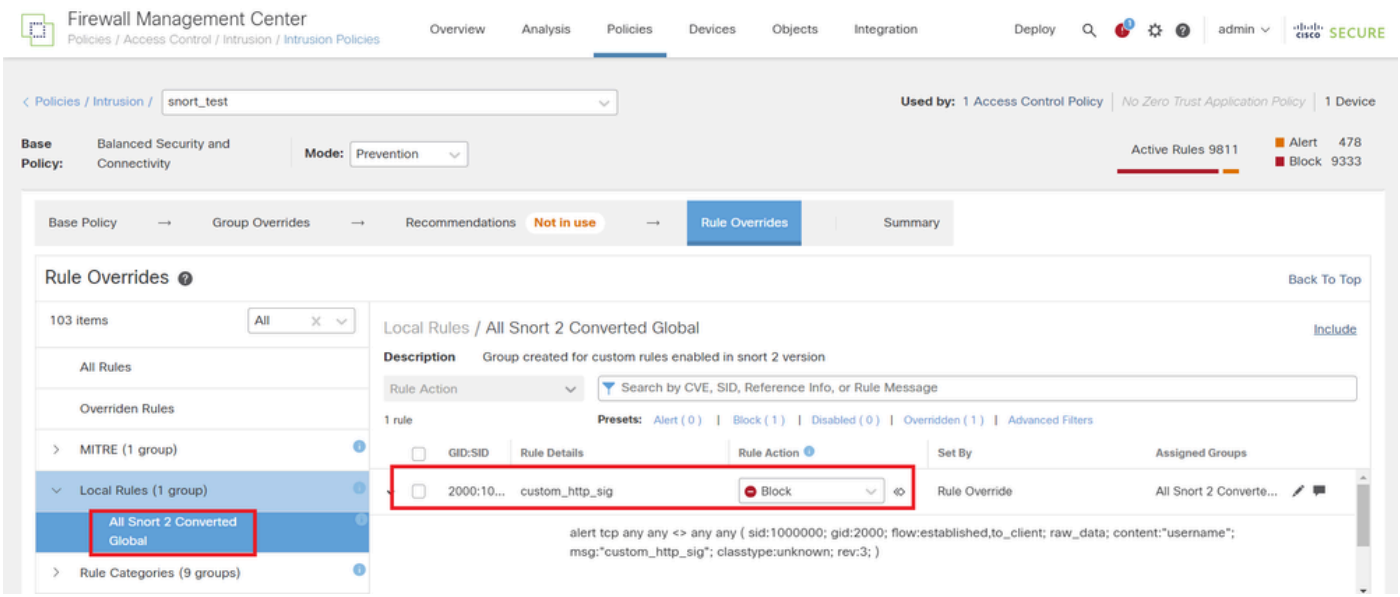
第五步：确认导入的自定义本地Snort规则

导航到FMC上的Policies > Intrusion Policies，点击与行中的目标入侵策略对应的Snort 3 Version。



确认导入的自定义规则

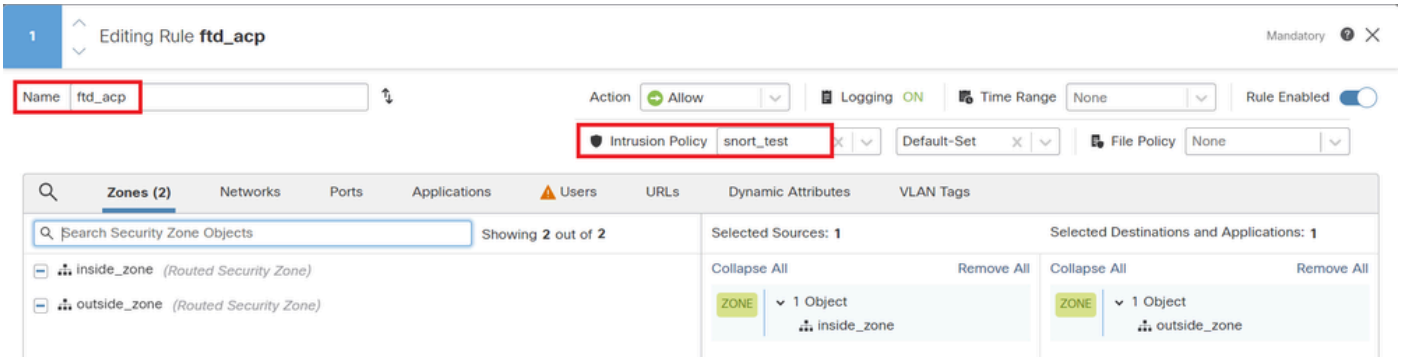
单击Local Rules > All Snort 2 Converted Global以检查自定义本地Snort规则的详细信息。



确认导入的自定义规则

第六步：将入侵策略与访问控制策略(ACP)规则相关联

导航到策略> 访问控制 FMC，将入侵策略与ACP关联。



与ACP规则关联

步骤 7.部署更改

将更改部署到FTD。

部署更改

方法 2.上传本地文件

步骤1:确认Snort版本

与方法1中的步骤1相同。

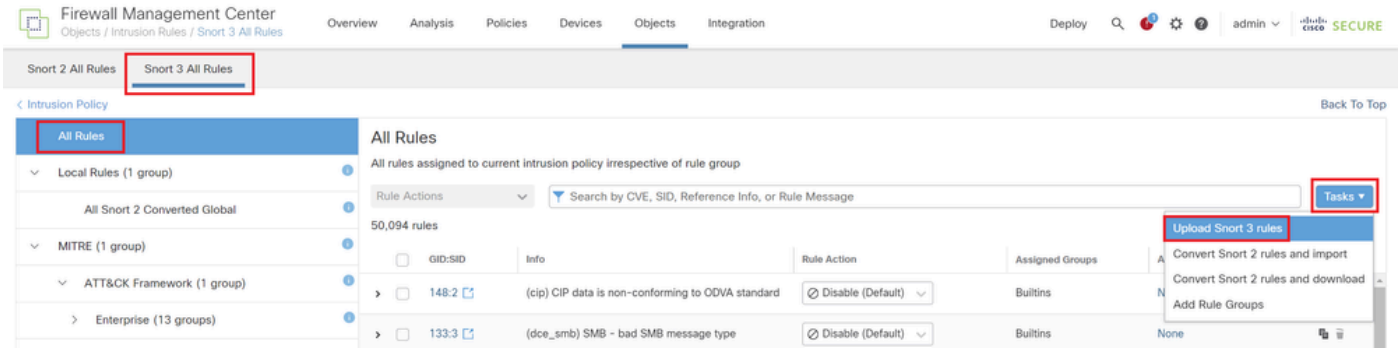
第二步：创建自定义本地Snort规则

手动创建自定义本地Snort规则并将其保存在名为custom-rules.txt的本地文件中。

```
alert tcp any any <> any any ( sid:1000000; flow:established,to_client; raw_data; content:"username"; m
```

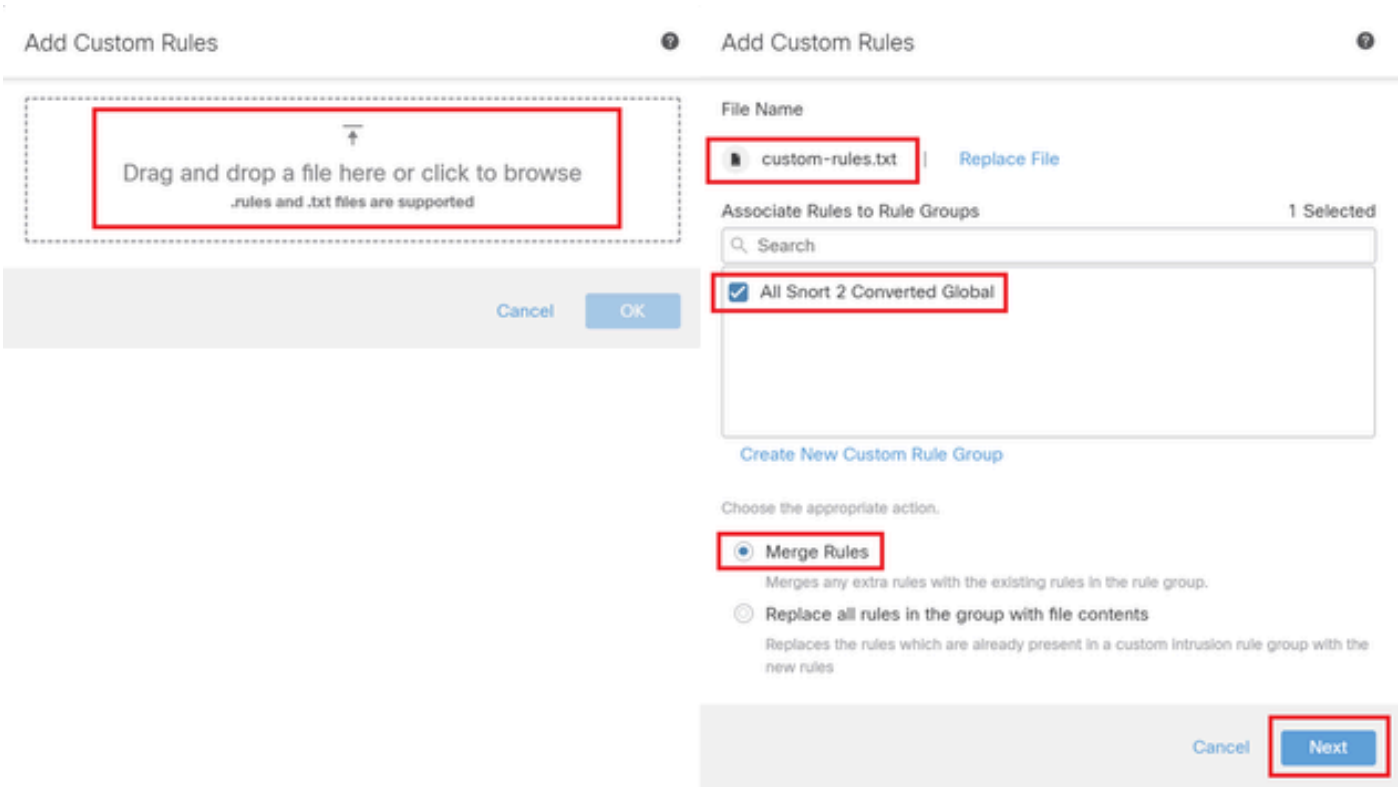
第三步：上传自定义本地Snort规则

在FMC上导航到对象>入侵规则> Snort 3所有规则>所有规则，从任务下拉列表中单击上传Snort 3规则。



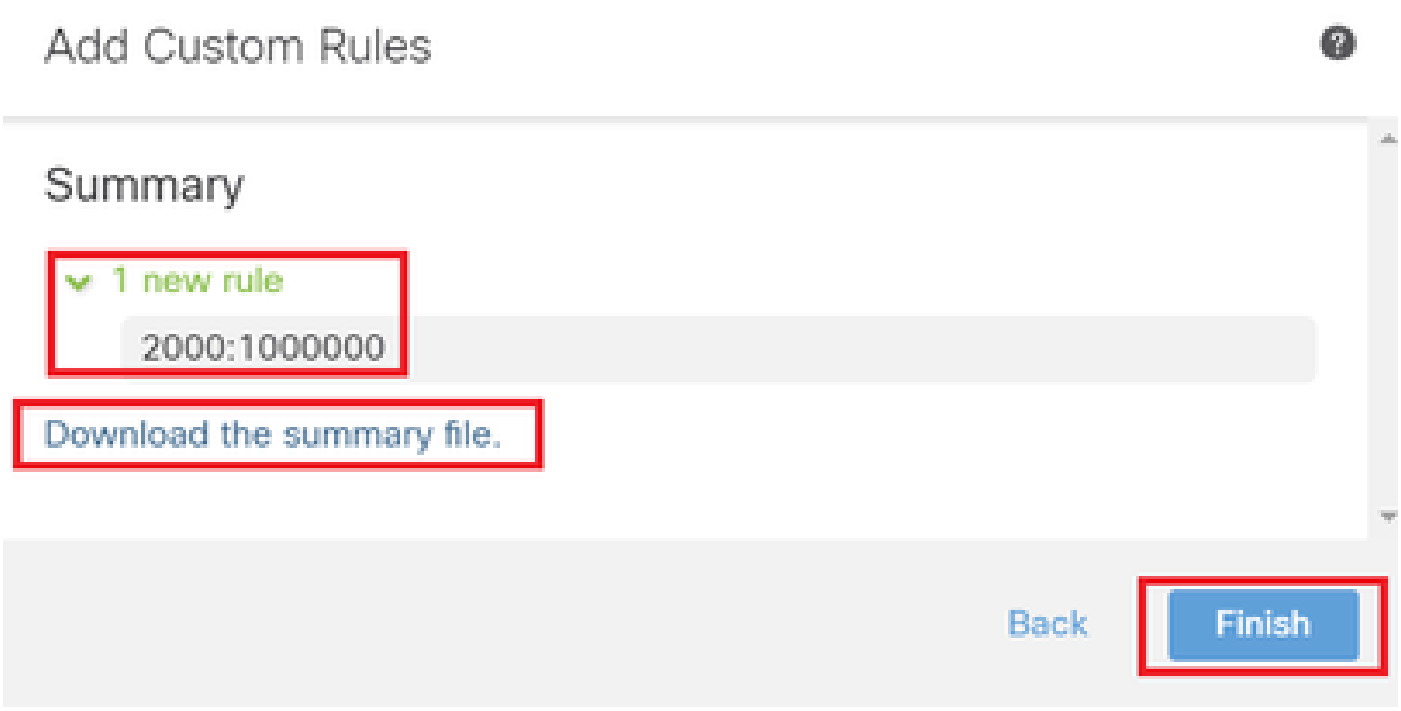
上传自定义规则

在Add Custom Rules屏幕中，拖放本地custom-rules.txt文件，选择Rule Groups和Appropriate Action（本示例中为Merge Rules），然后单击Next按钮。



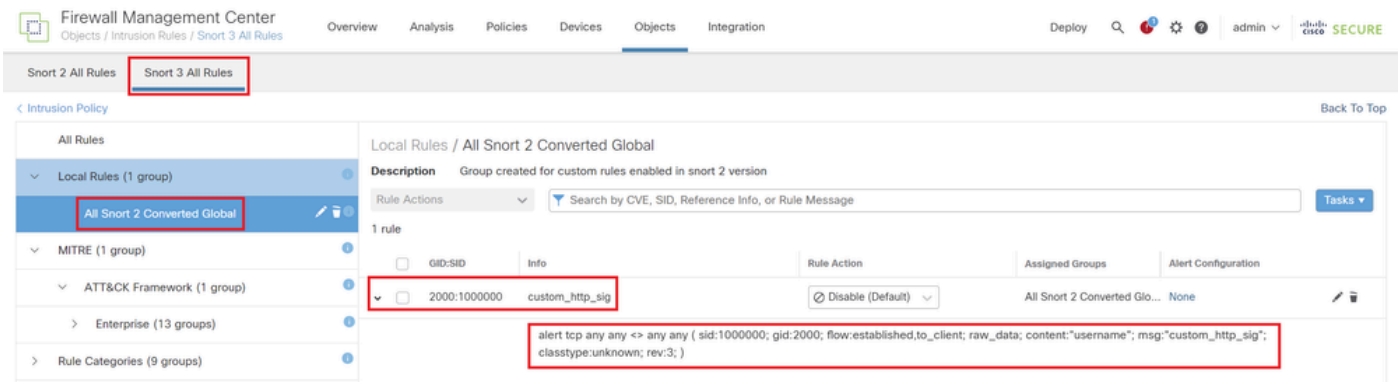
添加自定义规则

确认本地规则文件已成功上传。



确认上传结果

在FMC上导航到对象>入侵规则> Snort 3所有规则，点击所有Snort 2转换后的全局以确认上传的自定义本地Snort规则。



自定义规则详细信息

第四步：更改规则操作

与方法1中的步骤4相同。

第五步：确认上传的自定义本地Snort规则

与方法1中的步骤5相同。

第六步：将入侵策略与访问控制策略(ACP)规则相关联

与方法1中的步骤6相同。

步骤 7.部署更改

与方法1中的步骤7相同。

验证

步骤1:设置HTTP服务器中的文件内容

将HTTP服务器端的test.txt文件的内容设置为用户名。

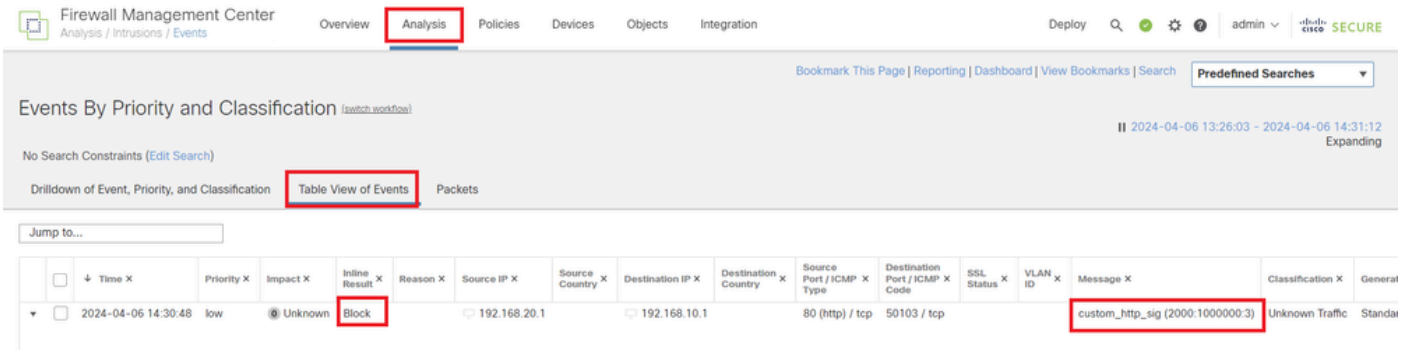
第二步：初始HTTP请求

从客户端浏览器(192.168.10.1)访问HTTP服务器(192.168.20.1/test.txt)，并确认已阻止HTTP通信。

初始HTTP请求

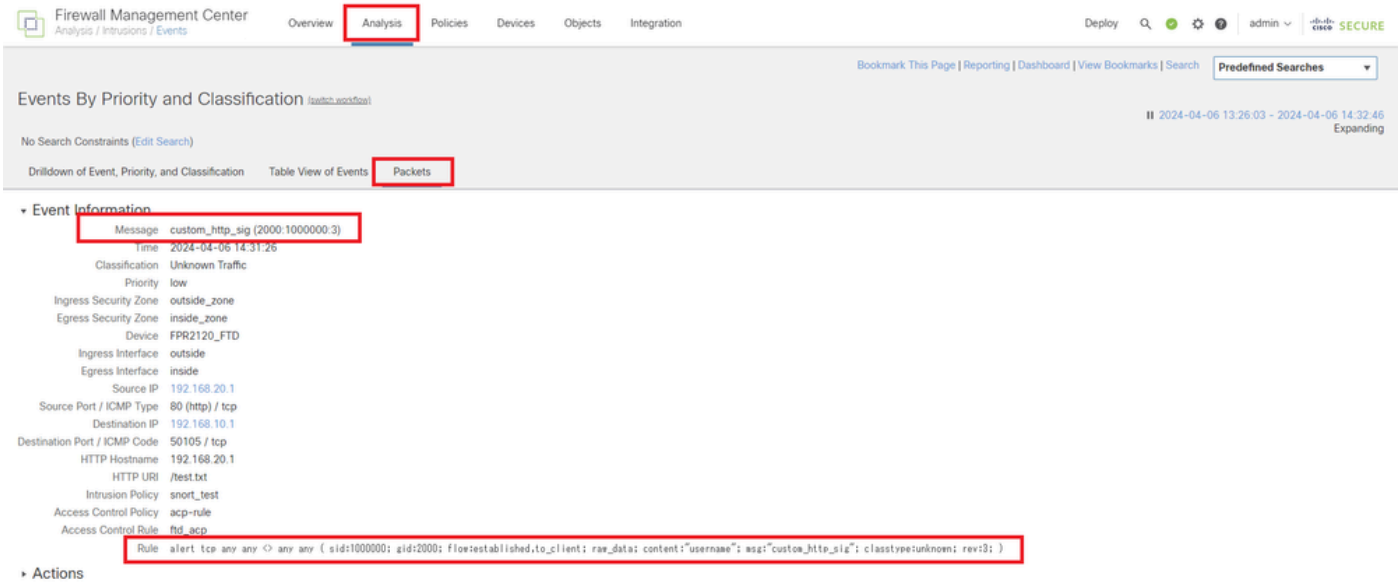
第三步：确认入侵事件

导航到分析>入侵>事件 FMC，确认入侵事件由自定义本地Snort规则生成。



入侵事件

点击Packetstab，确认入侵事件的详细信息。



入侵事件的详细信息

常见问题解答 (FAQ)

问：推荐使用哪一种，Snort 2或Snort 3 ？
答：与Snort 2相比，Snort 3具有更高的处理速度和新功能，因此更值得推荐。

问：从7.0之前的FTD版本升级到7.0或更高版本后，Snort版本是否自动更新为Snort 3 ？
答：否，检测引擎仍在Snort 2上。要在升级后使用Snort 3，您必须明确启用它。请注意，Snort 2计划在未来版本中弃用，强烈建议您立即停止使用。

问：在Snort 3中，是否可以编辑现有自定义规则？
A：否，您不能编辑它。要编辑特定自定义规则，必须删除相关规则并重新创建。

故障排除

运行system support trace命令以确认FTD上的行为。在本示例中，IPS规则(2000：1000000：3)阻止了HTTP流量。

```
<#root>

>

system support trace


Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.1
Please specify a client port:
Please specify a server IP address: 192.168.20.1
Please specify a server port:

192.168.10.1 50104 -> 192.168.20.1 80 6 AS=0 ID=4 GR=1-1 Firewall: allow rule, '

ftd_acp
```

', allow

192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1

Event

:

2000:1000000:3

, Action

block

192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict: blacklist
192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict Reason:

ips, block

参考

Cisco Secure Firewall Management Center Snort 3配置指南

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）。