在FTD的Snort2中配置自定义本地Snort规则

目录

简介

本文档介绍在防火墙威胁防御(FTD)的Snort2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：

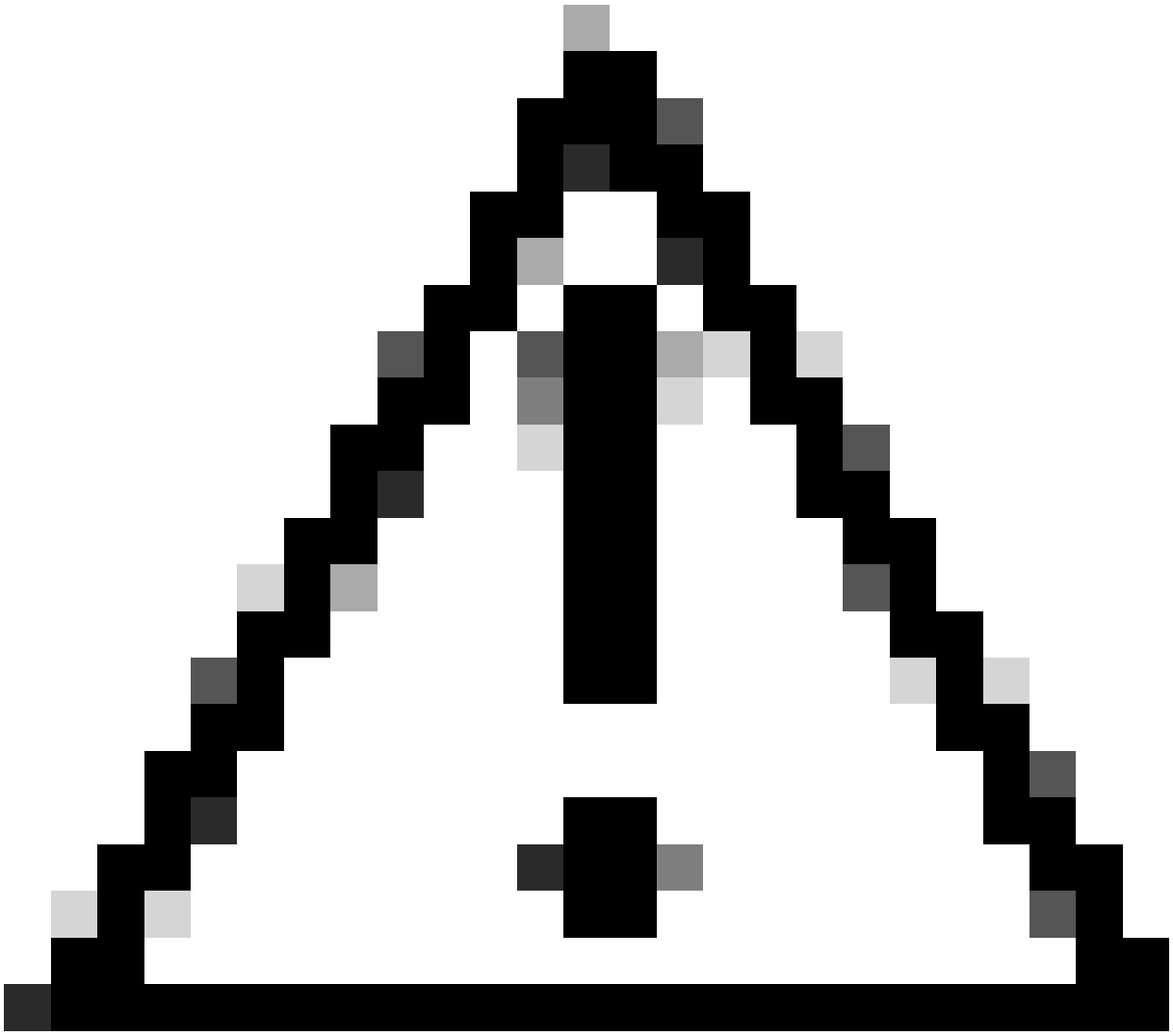
- 思科VMWare Firepower管理中心7.4.1
- 思科Firepower 2120 7.4.1

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

自定义本地Snort规则是指用户定义的规则，您可以在集成到FTD的Snort入侵检测和防御系统中创建和实施。当您在思科FTD中创建自定义本地Snort规则时，您实际上是在定义Snort引擎可以监视的新模式或条件集。如果网络流量匹配自定义规则中指定的条件，Snort可以采取规则中定义的操作，例如生成警报或丢弃数据包。 管理员使用自定义本地Snort规则解决一般规则集未涵盖的特定威胁。

本文档介绍了如何配置和验证旨在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。



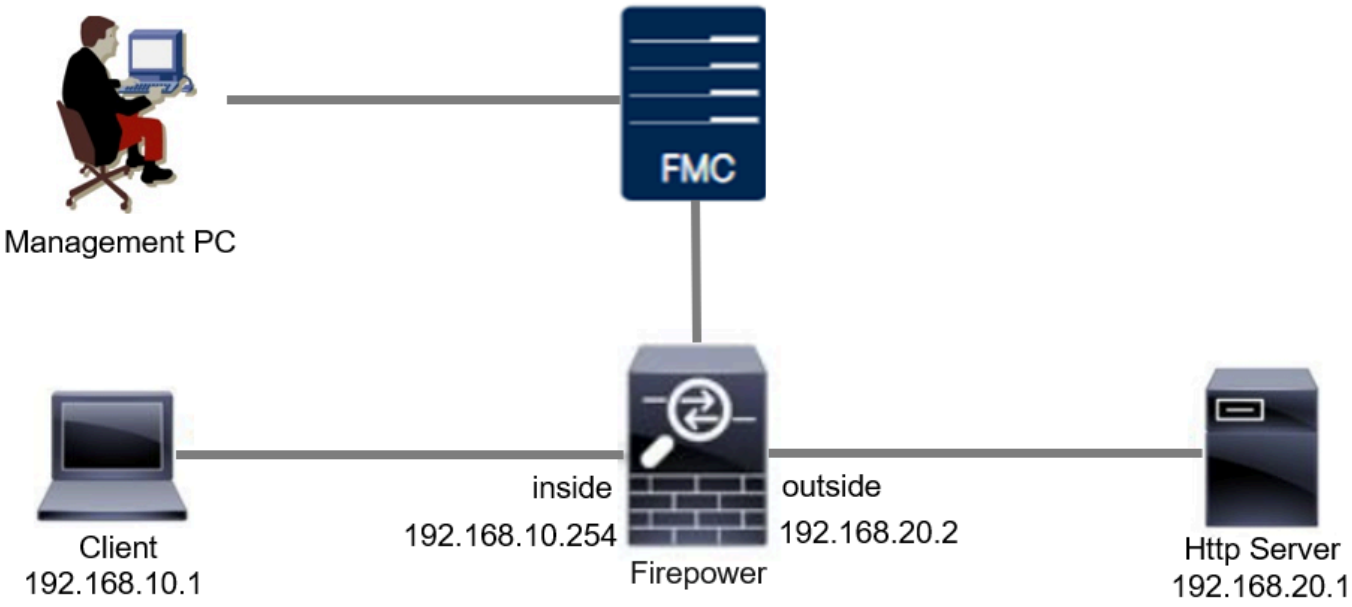
注意：创建自定义本地Snort规则并为其提供支持不属于TAC支持范围。因此，本文档只能

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。

配置

网络图

本文档介绍此图中Snort2中的自定义本地Snort规则的配置和验证。

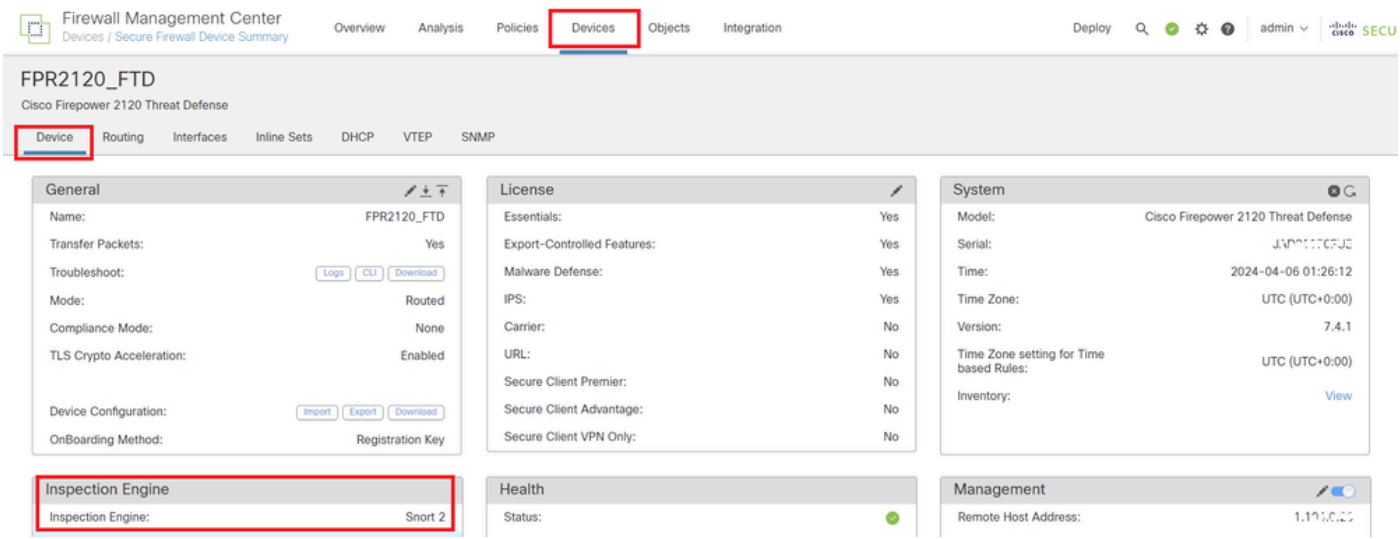


配置

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。

步骤1:确认Snort版本

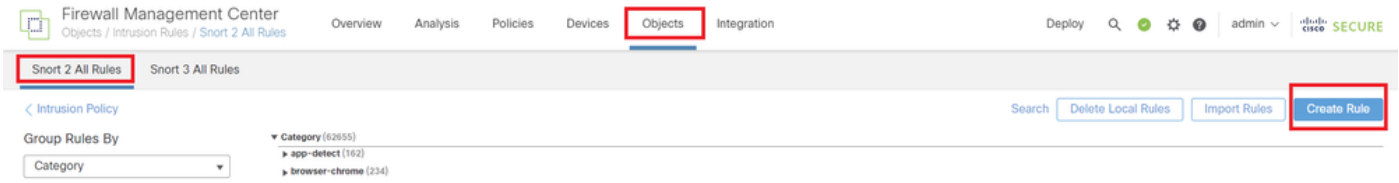
导航到FMC上的设备 > 设备管理，点击设备选项卡。确认Snort版本为Snort2。



Snort版本

第二步：在Snort 2中创建自定义本地Snort规则

在FMC上导航到对象 > 入侵规则 > Snort 2所有规则，点击创建规则按钮。

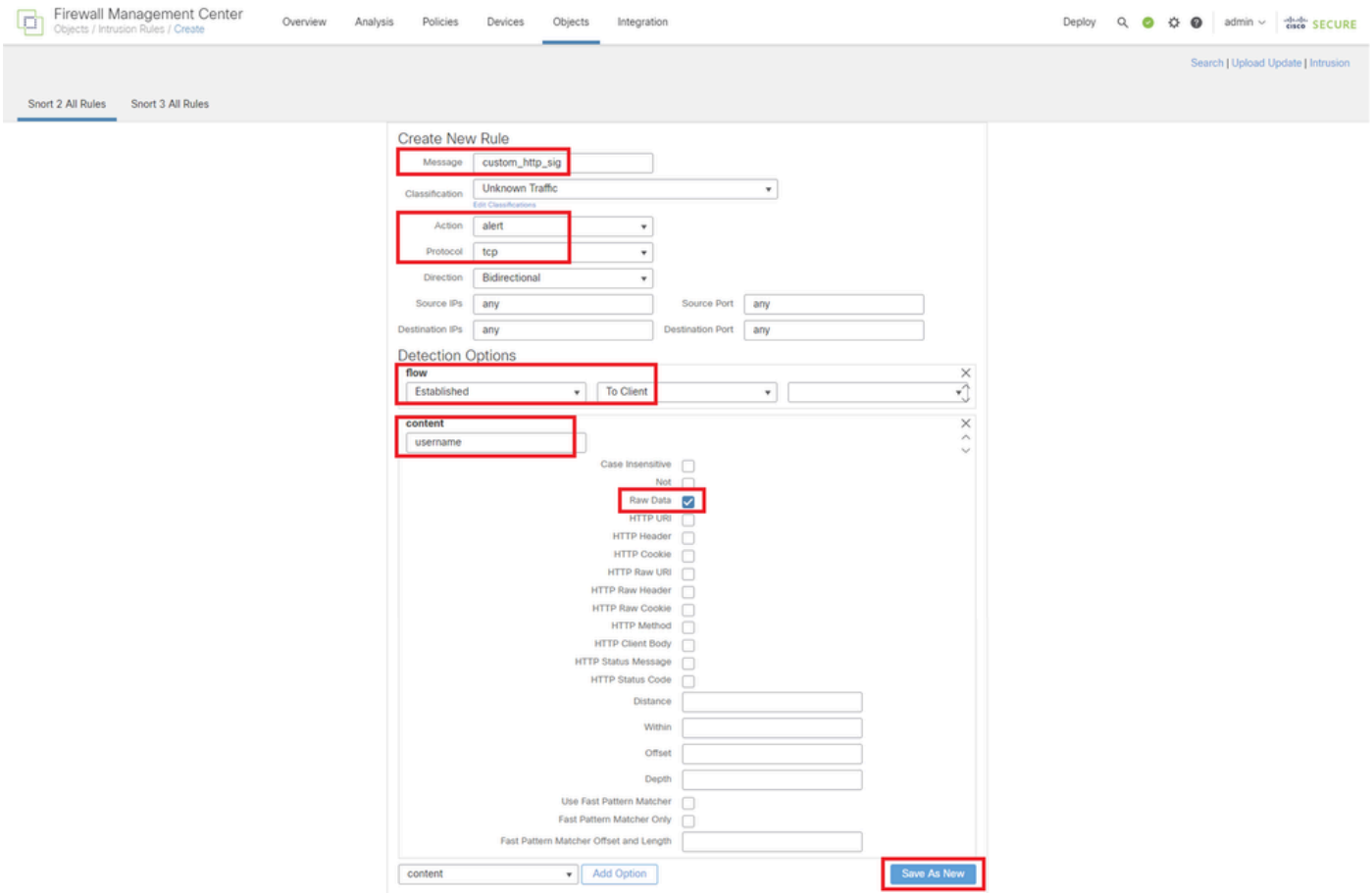


创建自定义规则

输入自定义本地Snort规则的必要信息。

- 入侵：custom_http_sig
- 操作：警报
- 协议：tcp
- 流：已建立，到客户端

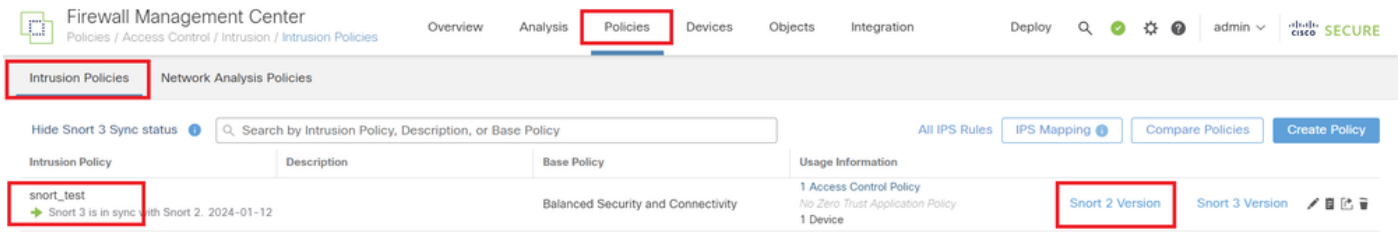
- 内容：用户名（原始数据）



输入规则的必要信息

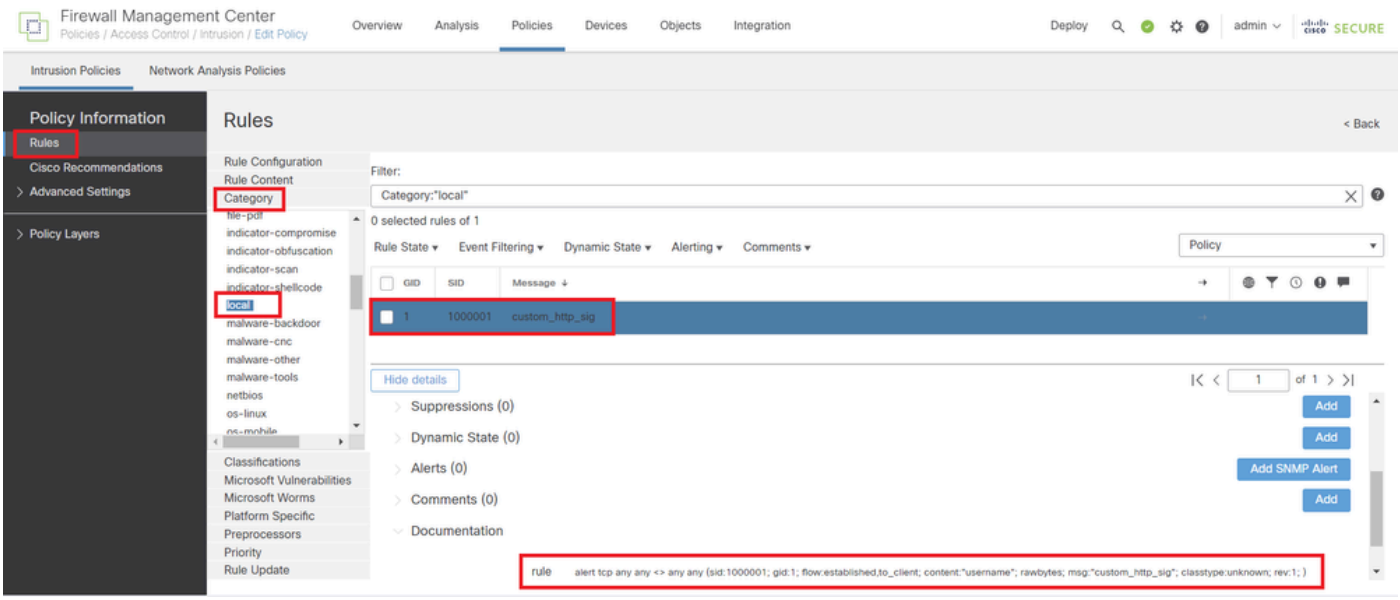
第三步：确认自定义本地Snort规则

在FMC上导航到策略 > 入侵策略，点击Snort 2版本按钮。



确认自定义规则

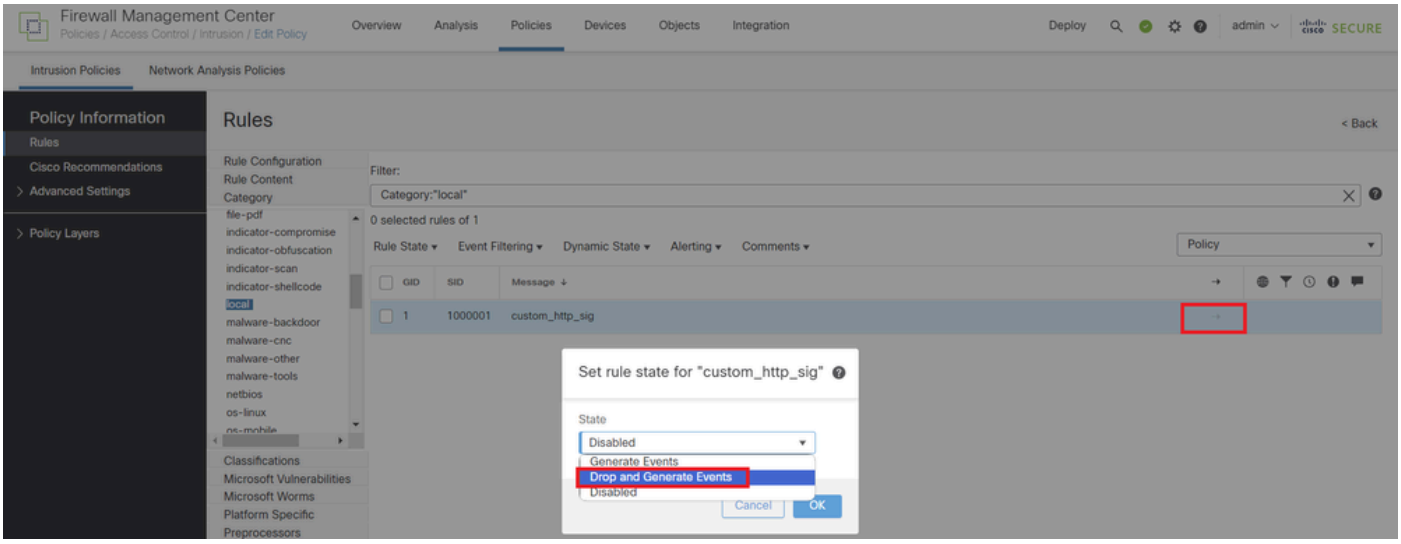
在FMC上导航到规则 >类别>本地，确认自定义本地Snort规则的详细信息。



自定义规则详细信息

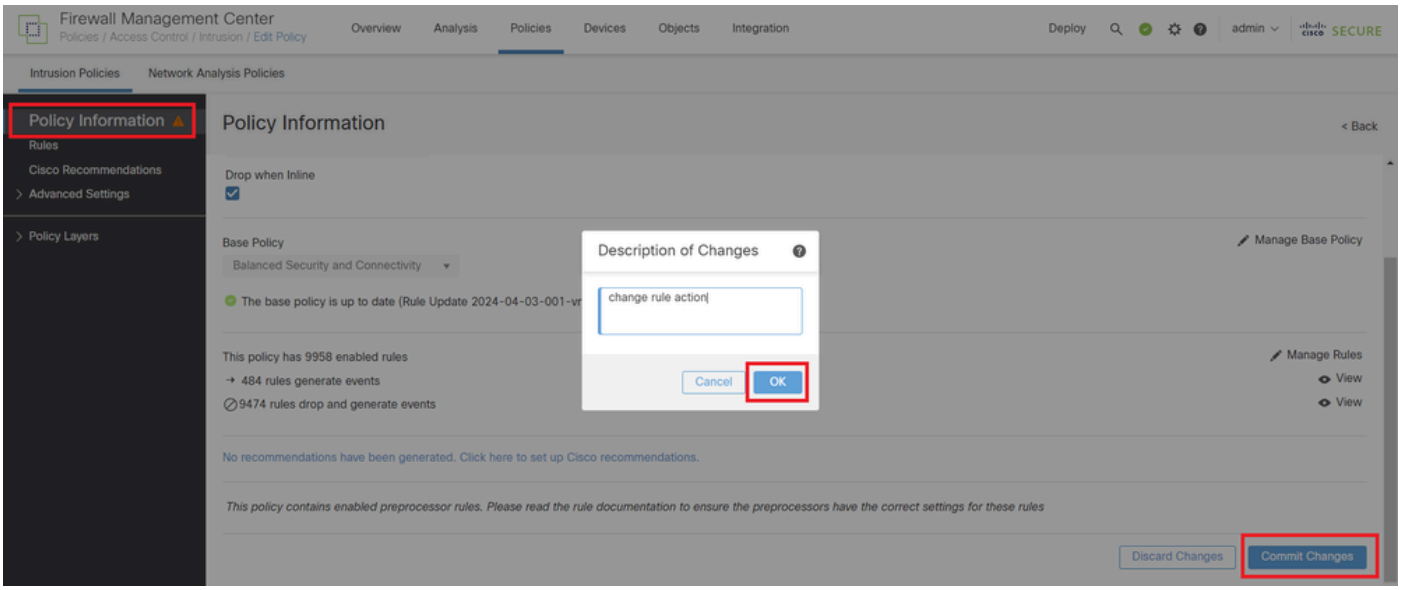
第四步：更改规则操作

单击State按钮，将State设置为Drop and Generate Events，然后单击OK按钮。



更改规则操作

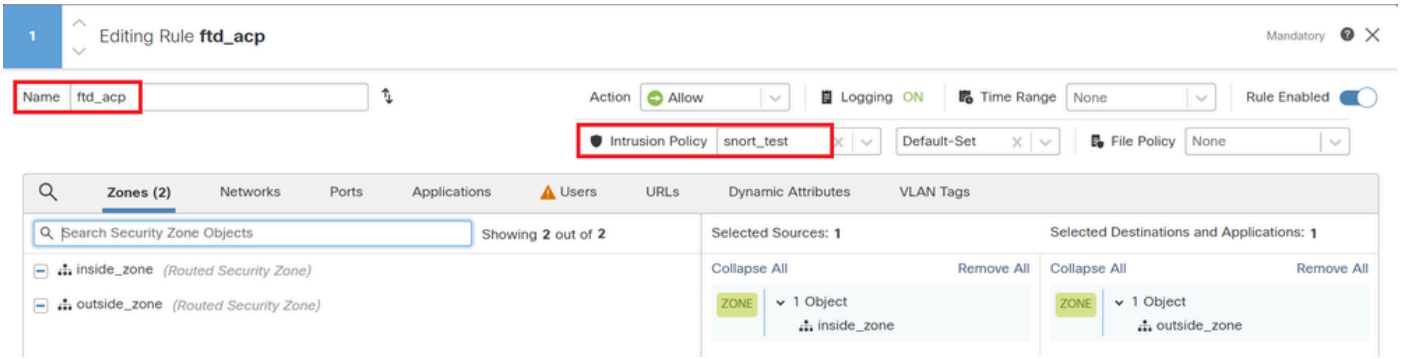
依次单击Policy Information 按钮和Commit Changes 按钮以保存更改。



提交更改

第五步：将入侵策略与访问控制策略(ACP)规则相关联

导航到FMC上的策略 > 访问控制，将入侵策略与ACP关联。



与ACP规则关联

第六步：部署更改

将更改部署到FTD。

部署更改

验证

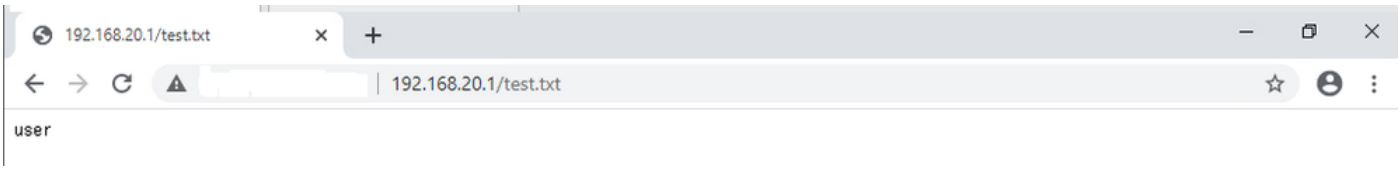
未触发自定义本地Snort规则

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。

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)，并确认允许HTTP通信。



初始HTTP请求

触发自定义本地Snort规则

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。

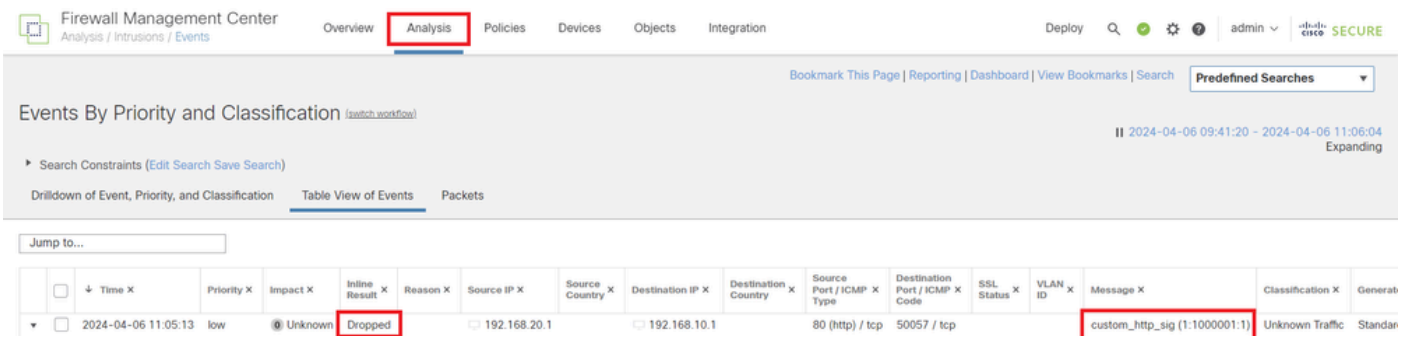
第二步：初始HTTP请求

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

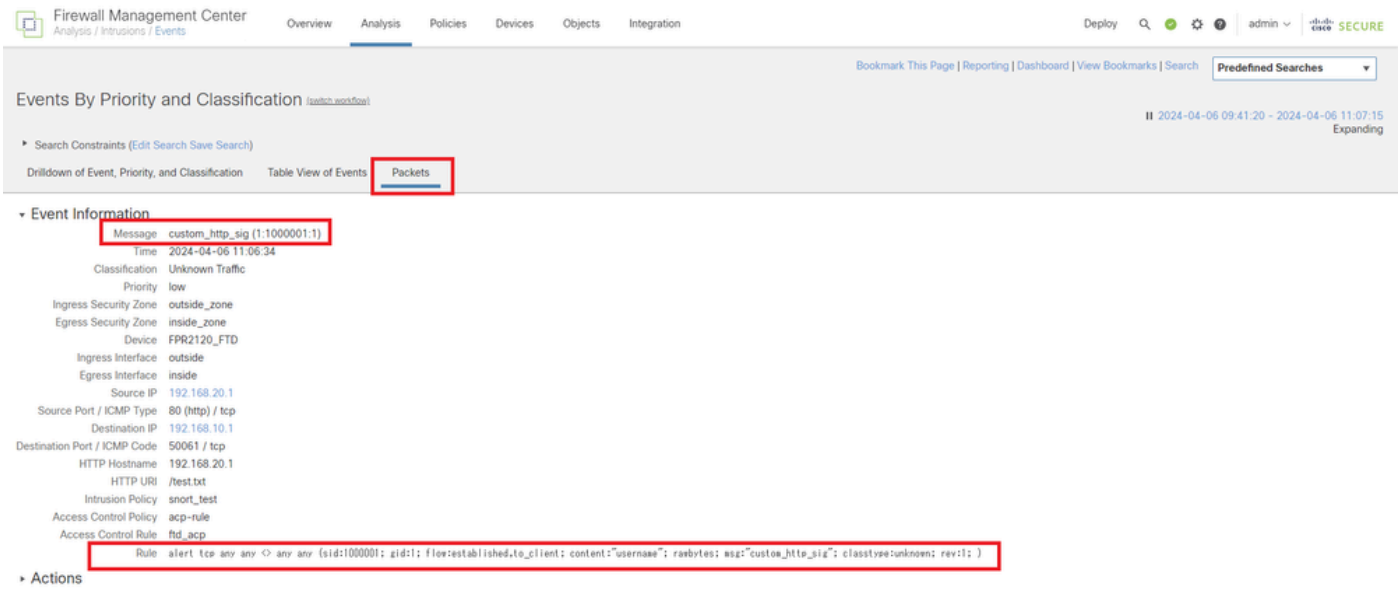
第三步：确认入侵事件

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



入侵事件

单击Packets选项卡，确认入侵事件的详细信息。



入侵事件的详细信息

故障排除

运行system support trace命令以确认FTD上的行为。在本示例中，HTTP流量被IPS规则阻止(gid 1， sid 1000001)。

```
<#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:

192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Firewall: allow rule, '

ftd_acp

', allow
192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0

IPS Event

:

gid 1

,

sid 1000001

, drop
```

```
192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Snort id 3, NAP id 2, IPS id 1, Verdict BLOCKFLOW
192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 ===>
```

Blocked by IPS

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）。