确定特定Snort实例处理的流量

目录

简介

本文档介绍如何确定思科Firepower威胁防御(FTD)环境中特定Snort实例处理的流量。

先决条件

要求

思科建议您了解以下产品：

- 安全Firepower管理中心(FMC)
- 安全Firepower威胁防御(FTD)
- 系统日志和SNMP
- REST API

使用的组件

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。用于本文的所有设备始于初始（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。

1. 使用命令行界面命令

使用FTD设备上的命令行界面(CLI)，您可以访问有关Snort实例及其处理的流量的详细信息。

- 此命令提供有关正在运行的Snort进程的详细信息。

```
show snort instances
```

下面是命令输出的示例。

```
> show snort instances
```

Total number of instances available - 1 +----------+----------+ | INSTANCE | PID | +----------+----------+ | **1** | **4765** | <<< One instance available and its process ID +----------+----------+

- 有关Snort实例处理的流量统计信息的更多详细信息，可以使用以下命令。这将显示各种统计信息，包括处理、丢弃的数据包数量以及每个Snort实例生成的警报。

show snort statistics

下面是命令输出的示例。

> show snort statistics Packet Counters: Passed Packets 3791881977 Blocked Packets 707722 Injected Packets 87 **Packets bypassed (Snort Down) 253403701** <<< Packets bypassed **Packets bypassed (Snort Busy) 0** Flow Counters: Fast-Forwarded Flows 294816 Blacklisted Flows 227 Miscellaneous Counters: Start-of-Flow events 0 End-of-Flow events 317032 Denied flow events 14230 Frames forwarded to Snort before drop 0 Inject packets dropped 0 TCP Ack bypass Packets 6412936 TCP Meta-Ack Packets 2729907 Portscan Events 0 Packet decode optimized 21608793 Packet decode legacy 6558642

show asp inspect-dp snort

下面是命令输出的示例。

> show asp inspect-dp snort

SNORT Inspect Instance Status Info Id Pid Cpu-Usage Conns Segs/Pkts Status tot (usr | sys) -- ----- ---------- ---------- ---------- -- -------- 0 16450 8% (7%| 0%) 2.2 K 0 READY 1 16453 9% (8%| 0%) 2.2 K 0 READY 2 16451 6% (5%| 1%) 2.3 K 0 READY 3 16454 5% (5%| 0%) 2.2 K 1 READY 4 16456 6% (6%| 0%) 2.3 K 0 READY 5 16457 6% (6%| 0%) 2.3 K 0 READY 6 16458 6% (5%| 0%) 2.2 K 1 READY 7 16459 4% (4%| 0%) 2.3 K 0 READY 8 16452 9% (8%| 1%) 2.2 K 0 READY **9 16455 100% (100%| 0%) 2.2 K 5 READY** <<<< High CPU utilization 10 16460 7% (6%| 0%) 2.2 K 0 READY -- ----- ---------- ---------- ---------- ---------- Summary 15% (14%| 0%) 24.6 K 7

-

使用Firepower管理中心(FMC)

如果您通过FMC管理FTD设备，则可以通过网络界面获得有关流量和Snort实例的详细见解和报告。

- 监控

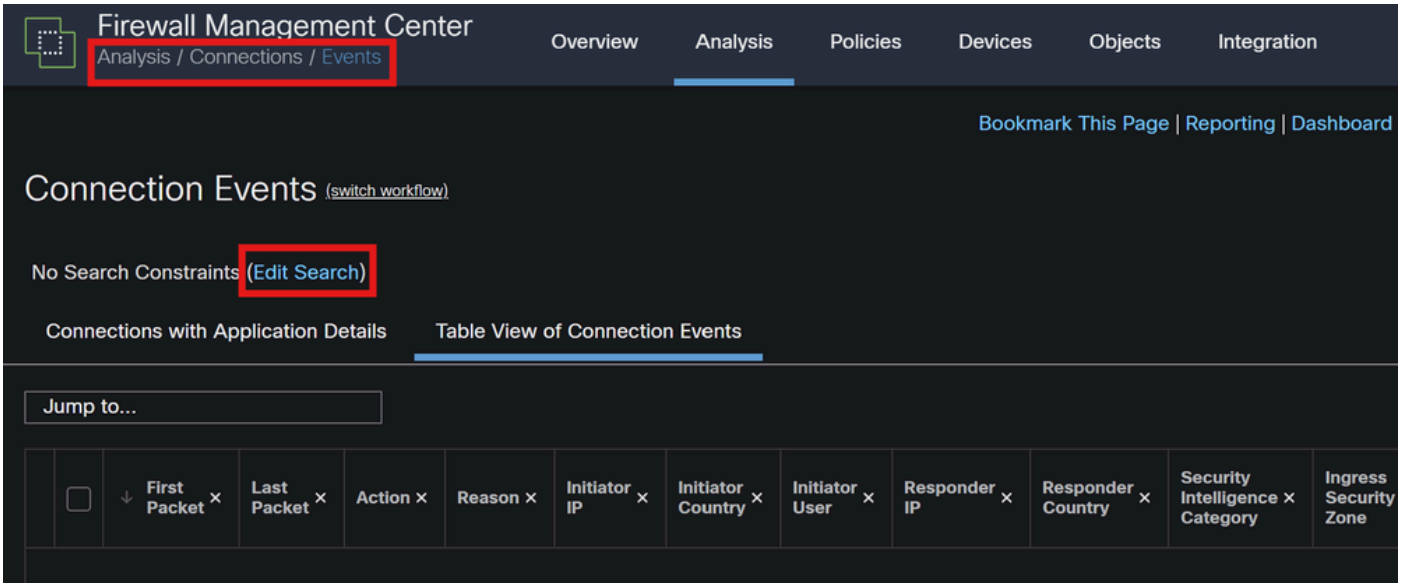
FMC控制面板(FMC Dashboard)：导航至控制面板，从中可以查看系统状态概述，包括Snort实例。

运行状况监控：在运行状况监控部分，您可以获得有关Snort进程的详细统计信息，包括已处理的流量。

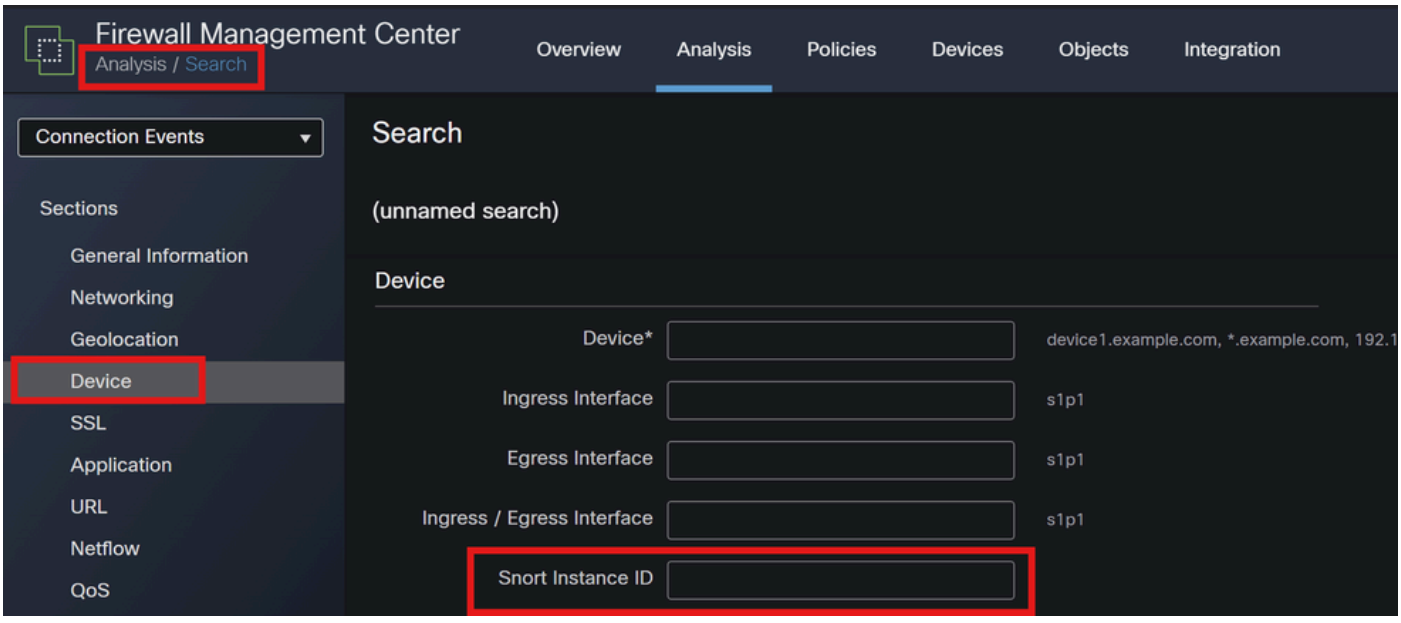
- 分析

分析：导航到**分析>**连接事件。

过滤器：使用过滤器将数据范围缩小到您感兴趣的特定Snort实例或流量。



连接事件



*Snort*实例*ID*

-

使用系统日志和SNMP

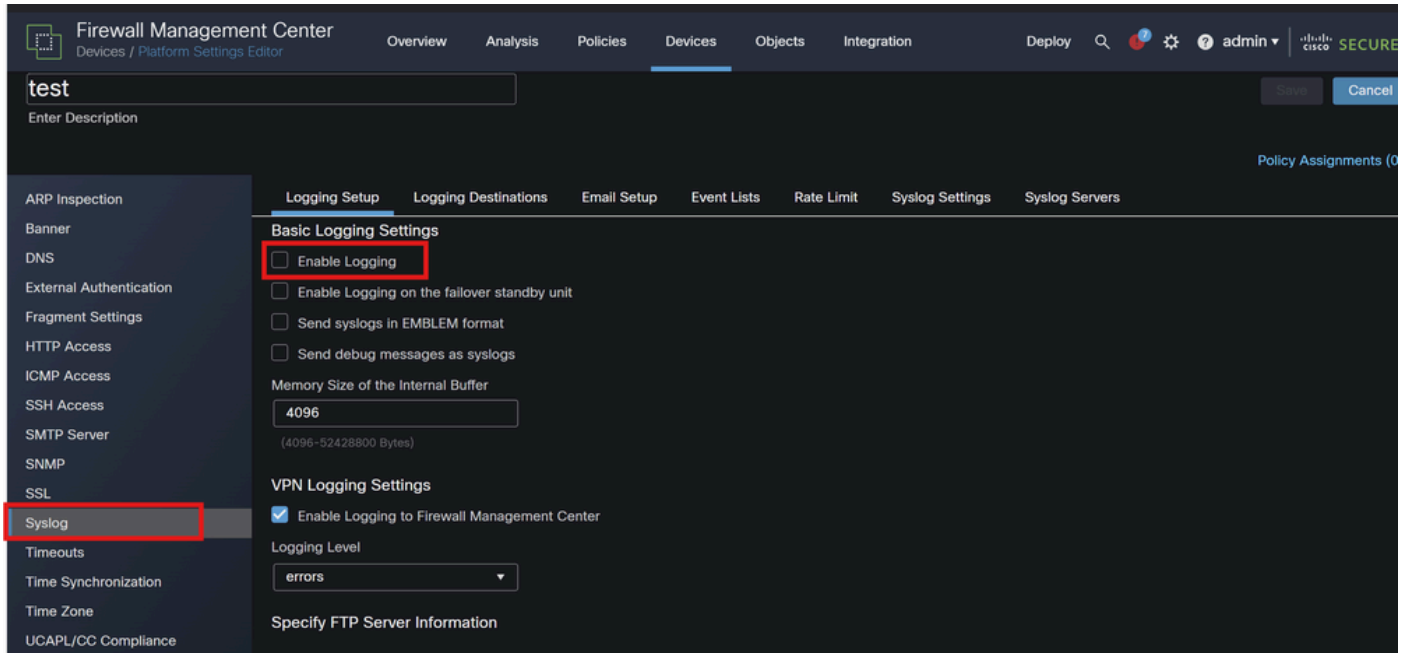
您可以将FTD配置为将系统日志消息或SNMP陷阱发送到可分析流量数据的外部监控系统。

- 系统日志配置

设备(Devices)：在FMC中，导航到设备(**Devices**) >平台设置(**Platform Settings**)。

创建或编辑策略(Create or Edit a Policy)：选择适当的平台设置策略。

系统日志：配置系统日志设置以包括Snort警报和统计信息。

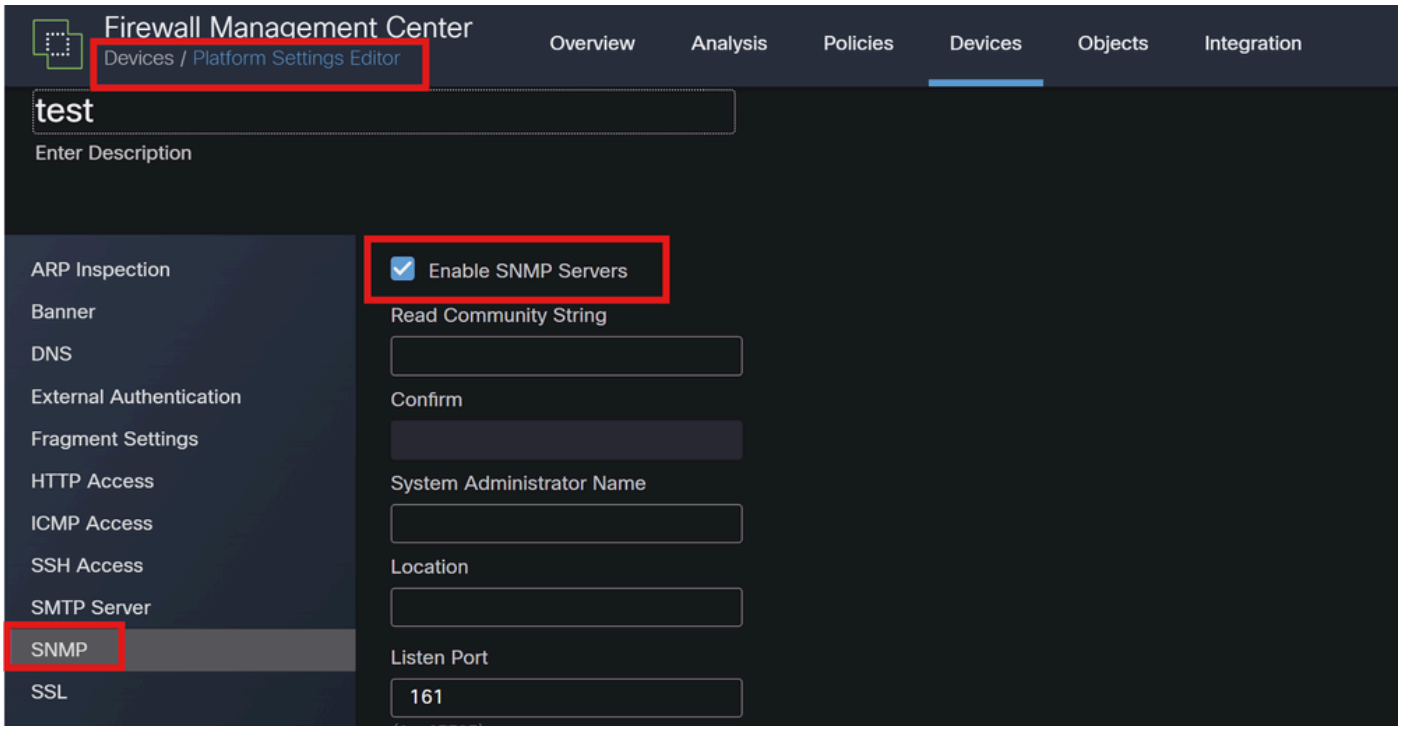


系统日志配置

- SNMP配置

SNMP设置：与syslog相似，请在**Devices** > **Platform Settings**下配置SNMP设置。

陷阱：确保为Snort实例统计信息启用必要的SNMP陷阱。



*SNMP*配置

4. 使用自定义脚本

对于高级用户，您可以编写使用FTD REST API收集有关Snort实例的统计信息的自定义脚本。此方法需要熟悉脚本编写和API用法。

- REST API

API访问：确保在FMC上启用API访问。

API调用：使用适当的API调用获取Snort统计信息和流量数据。

这会返回可以解析和分析的JSON数据，以确定由特定Snort实例处理的流量。

通过结合使用这些方法，您可以全面了解思科FTD部署中的每个Snort实例所处理的流量。

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）。