在安全FTD上使用Snort 3速率过滤器配置基于速率的攻击防御

问题

重点是如何构建覆盖多个子网的规则，了解实施的最佳实践，并确定适当的阈值（每秒计数）以用于警报或拦截，特别是在防御SYN泛洪攻击的环境中。

环境

- 运行FTD 7.4.2.4的思科安全防火墙Firepower
- Firepower 2110硬件平台
- 由Firepower管理中心(FMC)7.6.2.1管理
- 启用rate_filter检查器的Snort 3入侵防御系统
- 多个内部子网需要针对SYN泛洪进行保护
- 不存在活动故障；主动防御配置指南

分辨率

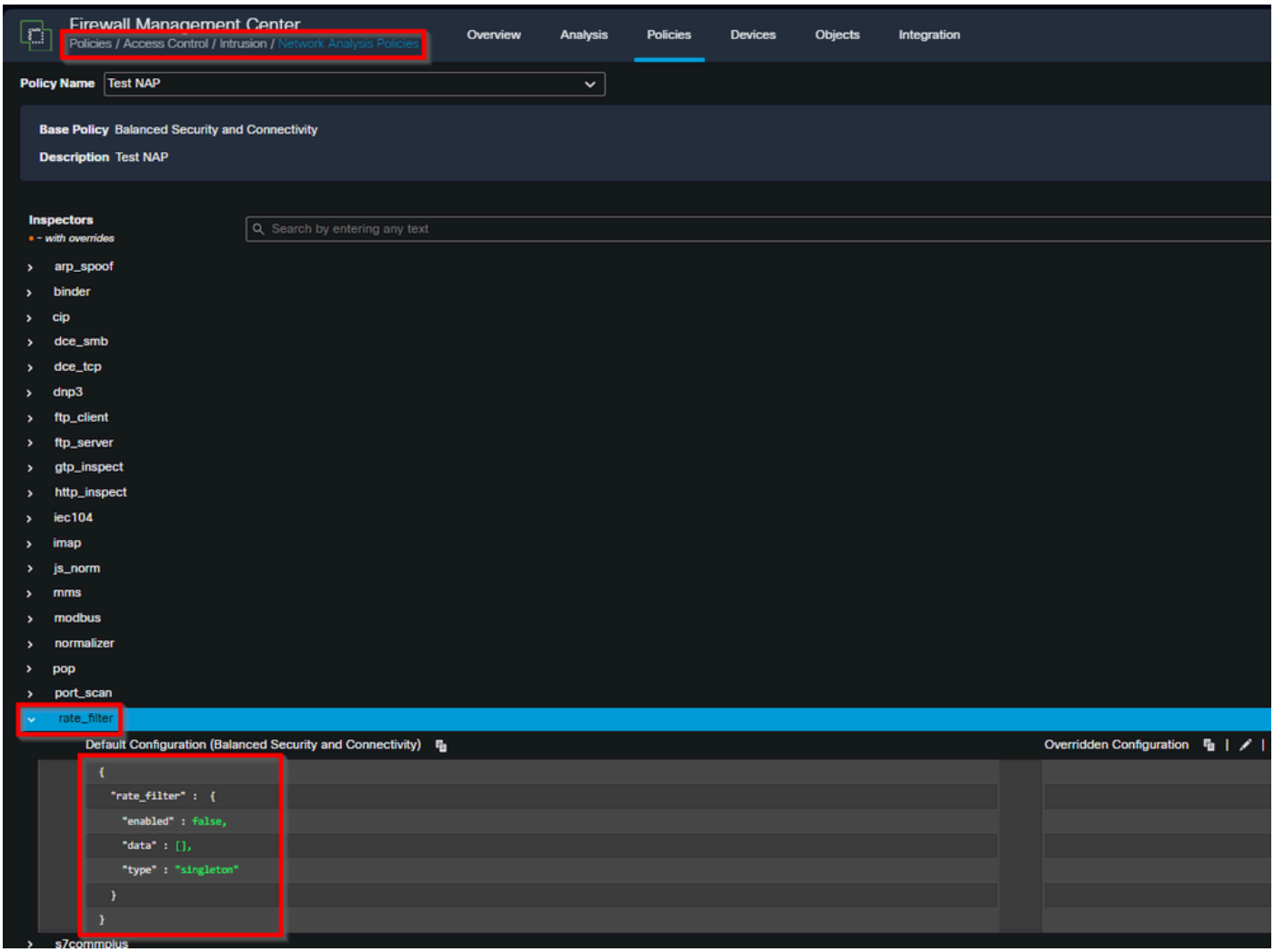
这些步骤详细介绍如何使用Cisco安全防火墙FTD上的Snort 3 rate_filter检查器来配置和实施基于速率的攻击防御，包括说明多个子网的规则结构和最佳实践建议。这些操作旨在帮助为正常流量建立基准，并启用有效检测或阻止SYN泛洪攻击。

注意：建议或建议这些规则过滤器的任何特定值不在TAC工作范围之内。每个环境都不同，需要对流量模式和网络设计进行深入分析，以确定这些过滤器的最佳值。

1：导航至Snort 3 rate_filter

在Policies > Access Control: Intrusion > Network Analysis Policies下配置这些过滤器，方法是点击

NAP策略的Snort 3 Version，然后点击左侧面板中的rate_filter下拉列表。



inline_image_0.png

2：了解Snort 3速率过滤器规则结构

Snort 3中的rate_filter检查器允许您定义规则，这些规则监控特定类型的流量（如SYN数据包），并在超过定义的阈值时采取操作（警报或丢弃）。这些规则可针对多个子网。

多个子网的rate_filter配置示例：

```
{
  "rate_filter": {
    "data": [
      {
        "apply_to": ["10.1.2.0/24", "10.1.3.0/24"],
        "count": 5,
        "gid": 135,
        "sid": 1,
        "new_action": "alert",
        "seconds": 10,
```

```
        "timeout": 15,
        "track": "by_src"
      }
    ],
    "enabled": true,
    "type": "singleton"
  }
}
```

参数说明：

- apply_to:过滤器应用的IP地址或子网的列表（支持多个子网）。
- count + seconds：事件的阈值（例如，10秒内有5个SYN数据包）。
- gid / sid：标识Snort事件（例如ss GID 135,SID 1用于SYN泛洪检测）。
- new_action:超过阈值时要执行的操作(例如，alert、drop)。
- timeout：针对相同条件触发新警报/操作之前的持续时间。
- track：跟踪模式(例如，by_src用于每个源IP，by_dst用于每个目标IP)。

3：阈值调整和策略部署的最佳实践

- 以警报模式开始：将new_action设置为alert，并使用保守阈值(例如更高计数和秒)来避免误报。
- 基线网络流量：监控生成的事件，以了解您的环境和子网的“正常”SYN速率是什么样的。
- 循环调整参数：根据观察的流量模式和操作需求调整计数、秒和超时。
- 移至阻止：一旦确定阈值准确反映异常行为，请将new_action从alert更改为drop或等效于主动阻止攻击。
- 根据需要独立过滤器：如果流量模式不同，请考虑不同网段或角色（例如，服务器与用户子网）的不同速率限制。
- 持续监控：保持对rate_filter事件的警报和监控，以快速确定调整问题或活动威胁。

原因

无。由于以前的SYN泛洪事件，请求配置是为了实现主动安全并作为指导。

相关内容

- Snort 3检查器参考：速率过滤器
- 思科安全防火墙管理中心设备配置指南7.4:基于速率的攻击防御
- 思科技术支持和下载

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）。