Firepower数据路径故障排除第8阶段：网络分析策略

目录

简介

本文是一系列文章的一部分，这些文章说明如何系统地排除Firepower系统上的数据路径故障，以确定Firepower的组件是否可能影响流量。有关Firepower平台架构的信息，以及指向其他数据路径故障排除文章的链接，请参阅概述文章。

本文介绍Firepower数据路径故障排除的第八阶段，即网络分析策略功能。

先决条件

- 本文适用于所有Firepower平台
  跟踪功能仅在软件版本6.2.0及更高版本中可用，仅适用于Firepower威胁防御(FTD)平台。
- 了解开源Snort很有帮助，但无需 有关开源Snort的信息，请访问https://www.snort.org/

排除网络分析策略功能故障

网络分析策略(NAP)包含根据所识别的应用对流量执行检测的snort预处理器设置。预处理器能够根据配置丢弃流量。本文介绍如何验证NAP配置并检查预处理器丢弃。

> **注意**：预处理器规则具有除“1”或“3”（即129、119、124）以外的生成器ID(GID)。 有关GID到预处理器映射的详细信息，请参阅《FMC配置指南》。

使用“跟踪”工具查找预处理器丢弃（仅FTD）

系统支持跟踪工具可用于检测在预处理器级别执行的丢包。

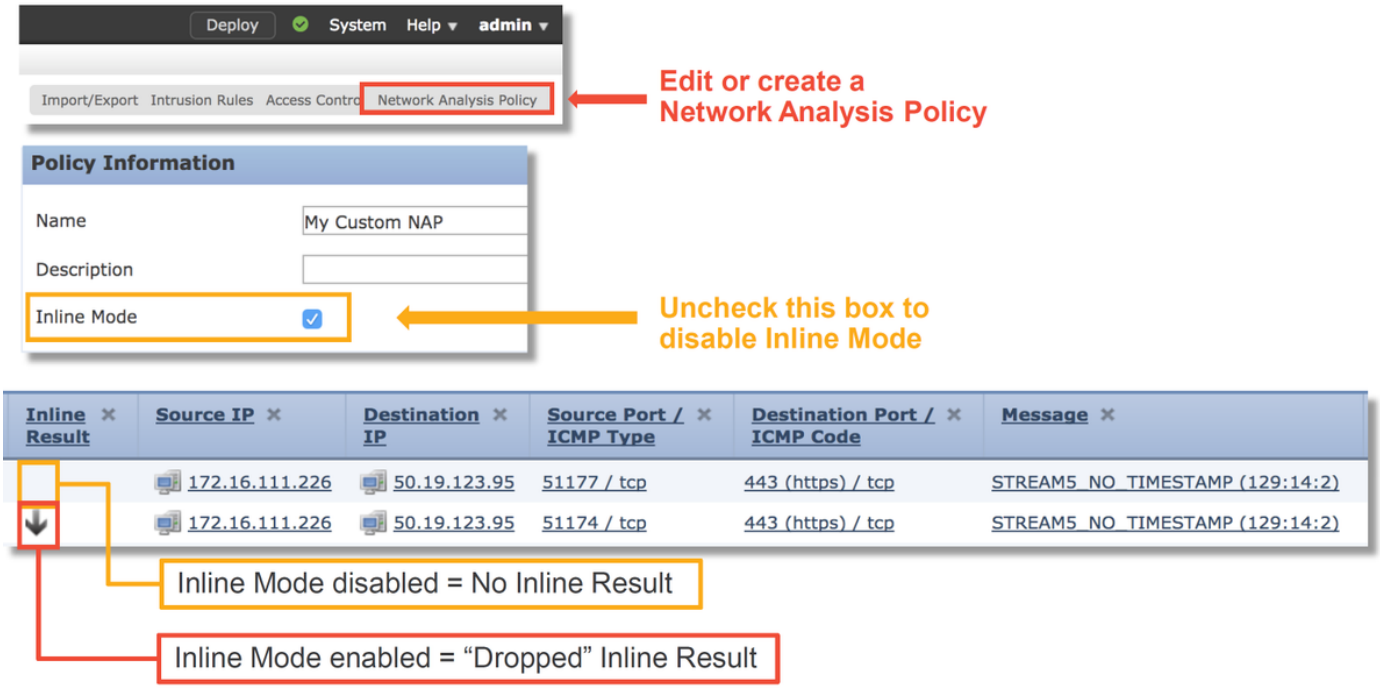
在以下示例中，TCP规范化预处理器检测到异常。因此，规则129:14会丢弃流量，该规则会查找TCP数据流中缺少的时间戳。

```
> system support trace

[omitted for brevity…]

172.16.111.226-51174 - 50.19.123.95-443 6 Packet: TCP, ACK, seq 3849839667, ack 1666843207
172.16.111.226-51174 - 50.19.123.95-443 6 Stream: TCP normalization error in timestamp, window, seq, ack, fin, flags, or
unexpected data, drop
172.16.111.226-51174 - 50.19.123.95-443 6 AppID: service unknown (0), application unknown (0)
172.16.111.226-51174 > 50.19.123.95-443 6 AS 4 I 0 Starting with minimum 3, 'block urls', and SrcZone first with zones -1 -> -1, geo 0 ->
0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
172.16.111.226-51174 > 50.19.123.95-443 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 0, icmpCode 0
172.16.111.226-51174 > 50.19.123.95-443 6 AS 4 I 0 pending rule order 3, 'block urls', URL
172.16.111.226-51174 > 50.19.123.95-443 6 Firewall: pending rule-matching, 'block urls', pending URL
172.16.111.226-51174 > 50.19.123.95-443 6 Snort: processed decoder alerts or actions queue, drop
172.16.111.226-51174 > 50.19.123.95-443 6 IPS Event: gid 129, sid 14, drop
172.16.111.226-51174 > 50.19.123.95-443 6 NAP id 1, IPS id 0, Verdict BLOCK
172.16.111.226-51174 > 50.19.123.95-443 6 ===> Blocked by Stream
```

> **注意**：虽然TCP流配置预处理器会丢弃流量，但由于内联规范化预处理器也处于启用状态，因此它能够这样做。有关内联规范化的详细信息，可以阅读此文章。

检验NAP配置

在Firepower管理中心(FMC)UI上，可在Policies > Access Control > Intrusion下查看NAP。然后，单击右上角的“网络分析策略”选项，之后可以查看NAP、创建新NAP和编辑现有NAP。



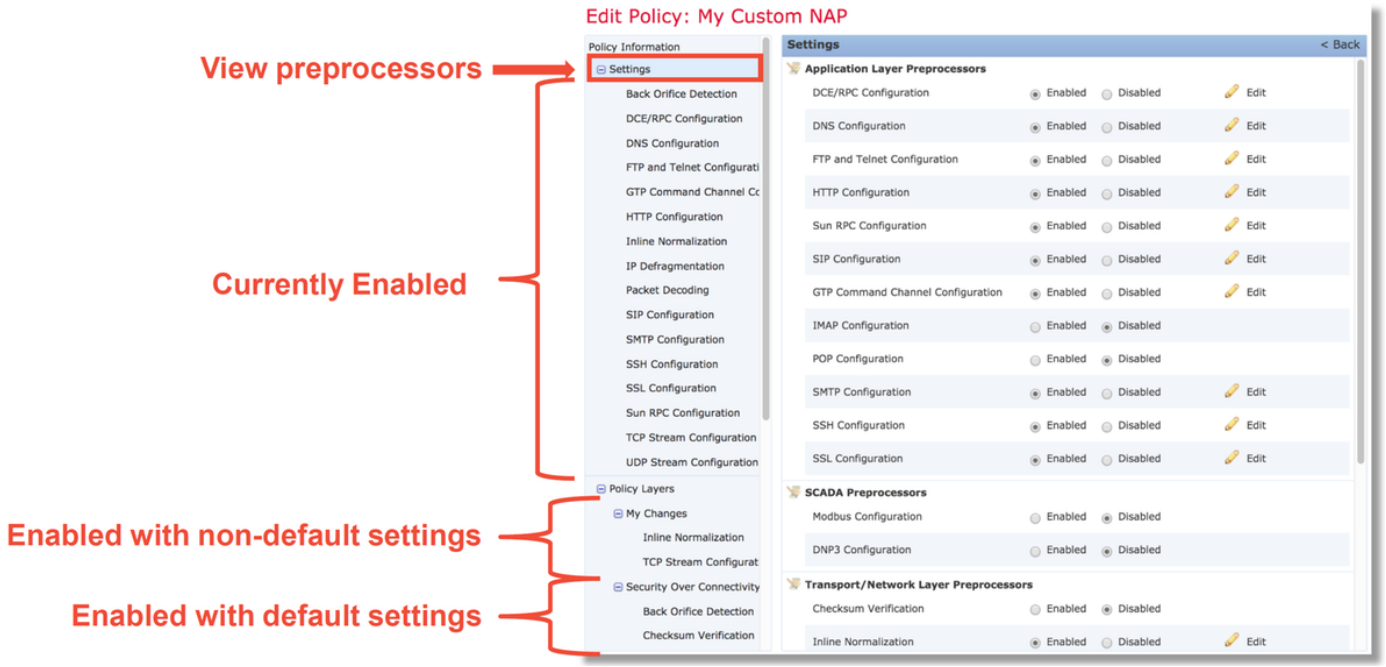
如上图所示，NAP包含“内联模式”功能，该功能相当于入侵策略中的“内联时丢弃”选项。防止NAP丢弃流量的快速缓解步骤是取消选中内联模式。NAP生成的入侵事件不显示内联模式禁用的内联结果

选项卡**中的任**何内容。

查看NAP设置

在NAP中，您可以查看当前设置。这包括启用的预处理器总数，后跟

已启用非默认设置的预处理器（手动调整的预处理器）和已启用默认设置的预处理器，如下图所示。

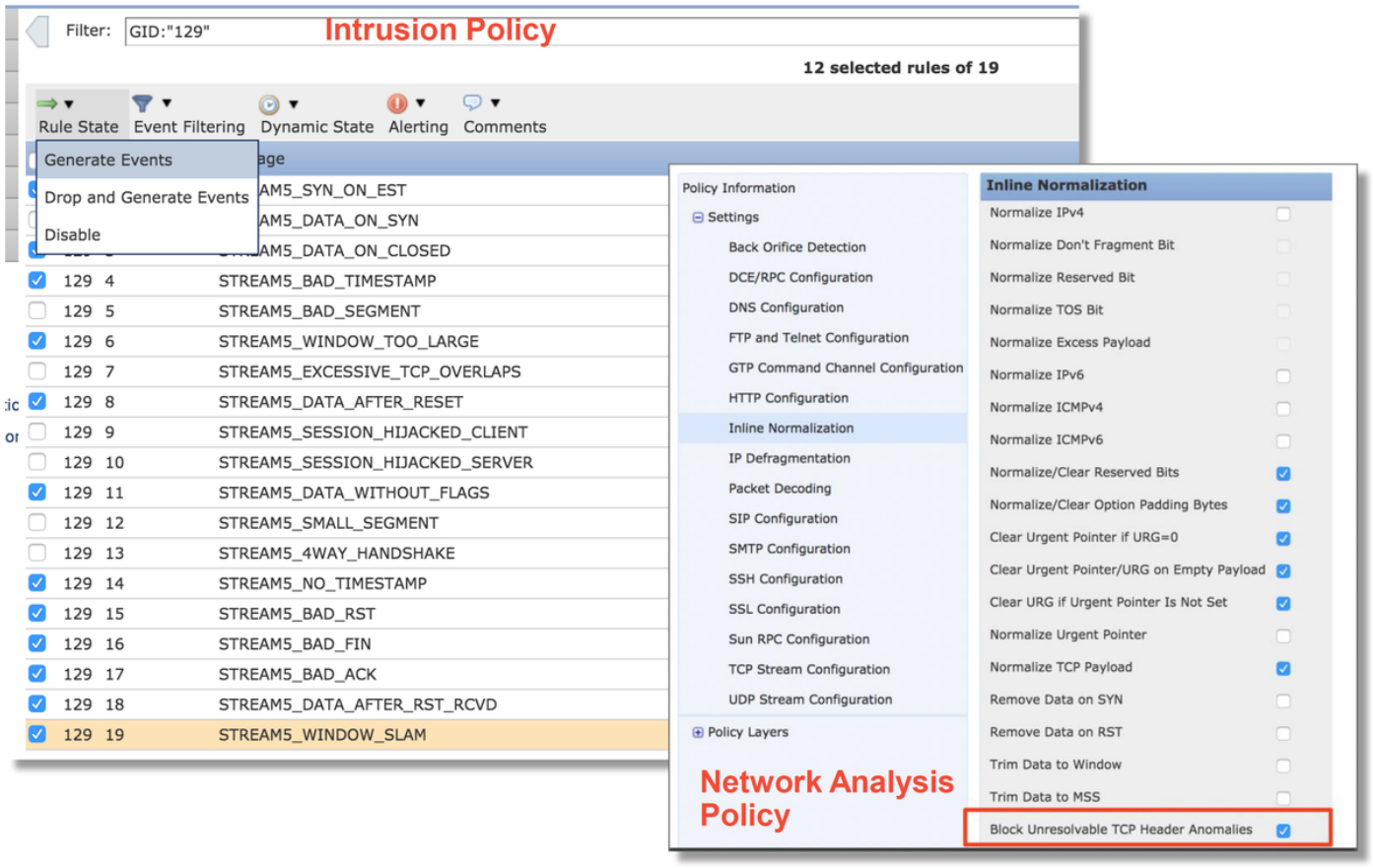


可能导致静默丢弃的NAP设置

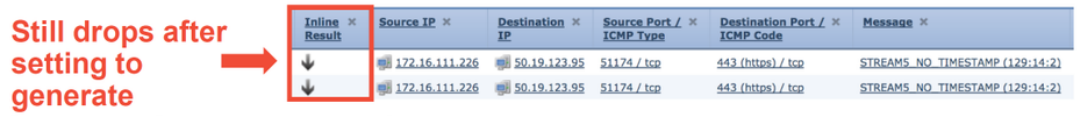
在跟踪部分提到的示例中，规则TCP流配置规则**129:14正在**丢弃流量。这通过查看系统支持跟**踪输出来**确定。但是，如果在各自的入侵策略中未启用上述规则，则不会向FMC发送入侵事件。

发生此情况的原因是内联规范化预处理器中**名为Block Unresolvable TCP Header Anomalies**的设**置**。此选项基本允许Snort在某些GID 129规则检测TCP数据流中的异常时执行阻止操作。

如果**启用了Block Unresolvable TCP Header Anomalies（阻止不可解析的TCP报头异常）**，则建议根据下图打开GID 129规则。



打开GID 129规则会导致入侵事件在对流量执行操作时发送到FMC。但是，只要启用**Block Unresolvable TCP Header Anomalies**，即使入侵策略中的**Rule State** 设置为仅**Generate Events**，它仍可以丢弃流量。此行为在FMC配置指南中进行了说明。



Check configuration guide for relative protocols/preprocessors:

Block Unresolvable TCP Header Anomalies

When you enable this option, the system blocks anomalous TCP packets that, if normalized, would be invalid and likely would be blocked by the receiving host. For example, the system blocks any SYN packet transmitted subsequent to an established session.

The system also drops any packet that matches any of the following TCP stream preprocessor rules, regardless of whether the rules are enabled:

- 129:1
- 129:3
- 129:4
- 129:6
- 129:8
- 129:11
- 129:14 through 129:19

The Total Blocked Packets performance graph tracks the number of packets blocked in inline deployments and, in passive deployments and inline deployments in tap mode, the number that would have been blocked in an inline deployment.

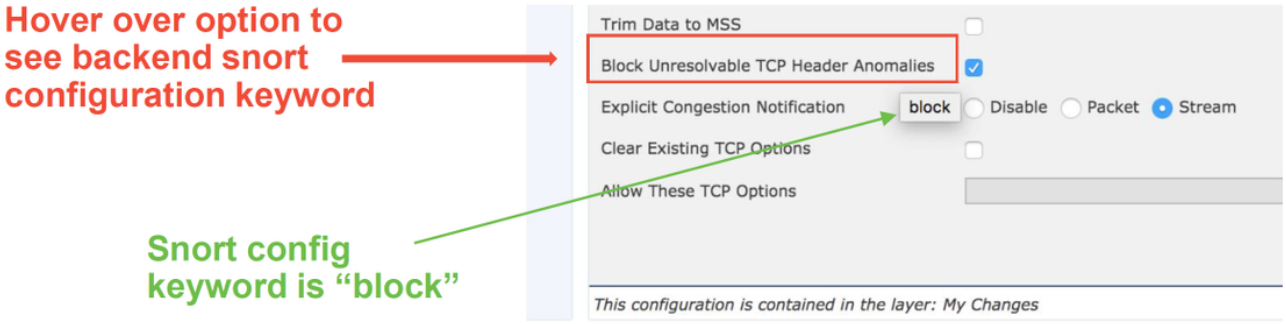
上述文档可在本文中找到（对于版本6.4，是本文发布时的最新版本）。

验证后端配置

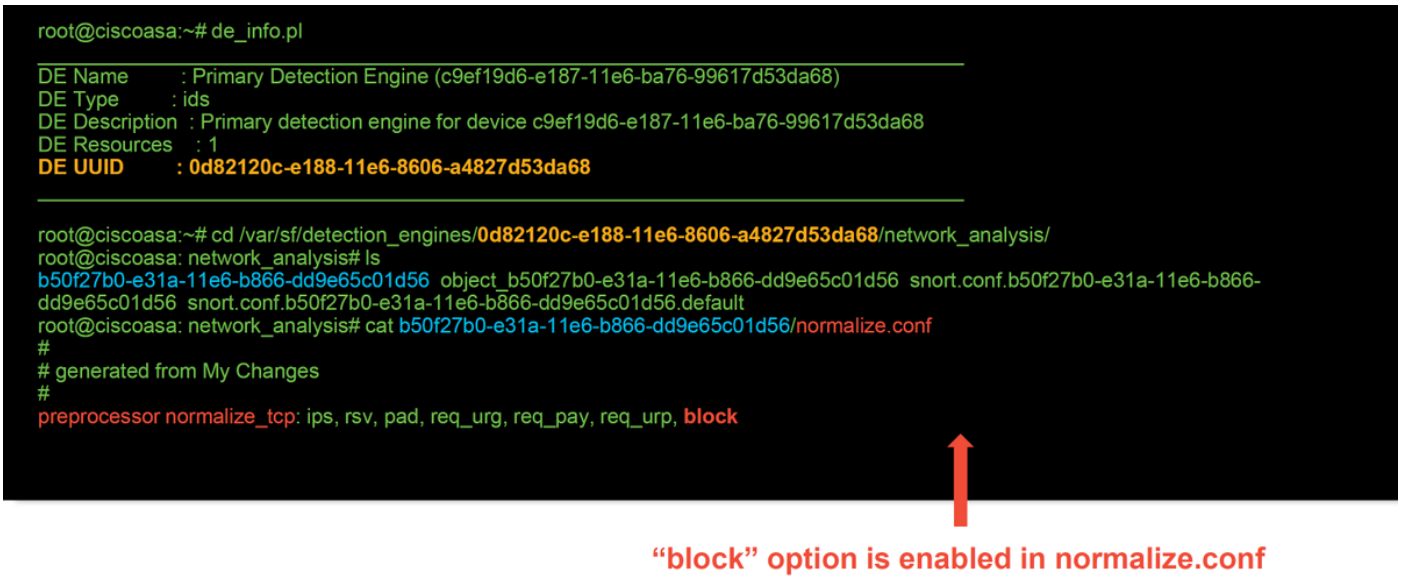
预处理器的行为增加了另一层复杂性，因为可以在后端启用某些设置，而不会反映在FMC中。这些是一些可能的原因。

- 其他已启用的功能可以强制启用预处理器设置（主要是文件策略）
- 某些入侵策略规则需要某些预处理器选项才能执行检测
- 缺陷可能导致行为 我们看到过一个实例： CSCuz50295 - “File policy with Malware block enables TCP normalization with block flag”

在查看后端配置之前，请注意，在后端Snort配置文件中使用的Snort关键字可以通过将鼠标悬停在NAP中的特定设置上来查看。请参阅下图。



NAP选项卡**中的Block Unresolvable TCP Header Anomalies选项**转换为后端上的**block**关键字。考虑到这些信息，可以从专家外壳检查后端配置。

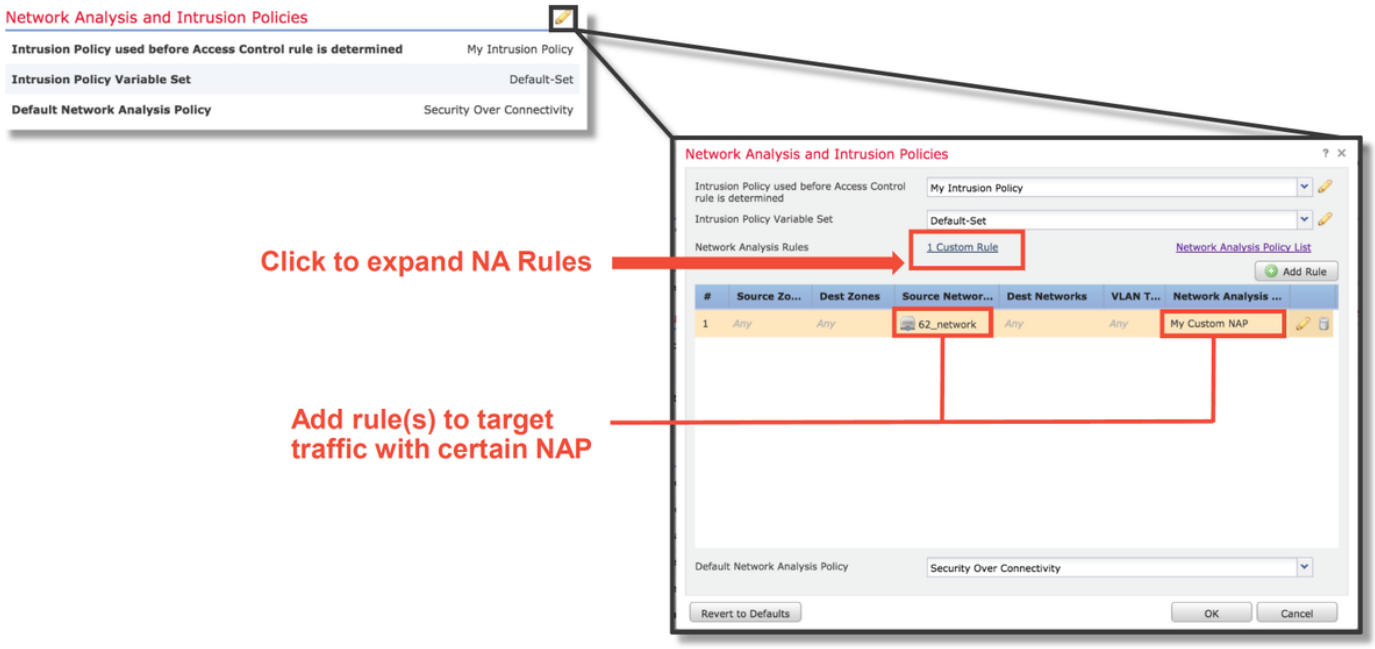


创建目标NAP

如果某些主机触发预处理器事件，则可以使用自定义NAP来检查进出这些主机的流量。在自定义NAP中，可禁用导致问题的设置。

这些是实施目标NAP的步骤。

1. 根据本文“验证NAP配置”一节中提到的说明创建NAP。
2. 在Access Control Policy**的Advanced**选项卡中，导航至Network Analysis and Intrusion Policies**部分。**单击**Add Rule(添**加规则)，使用目标主机创建规则，并在Network Analysis Policy（网络分析策略）部分**选择新创建的**NAP。

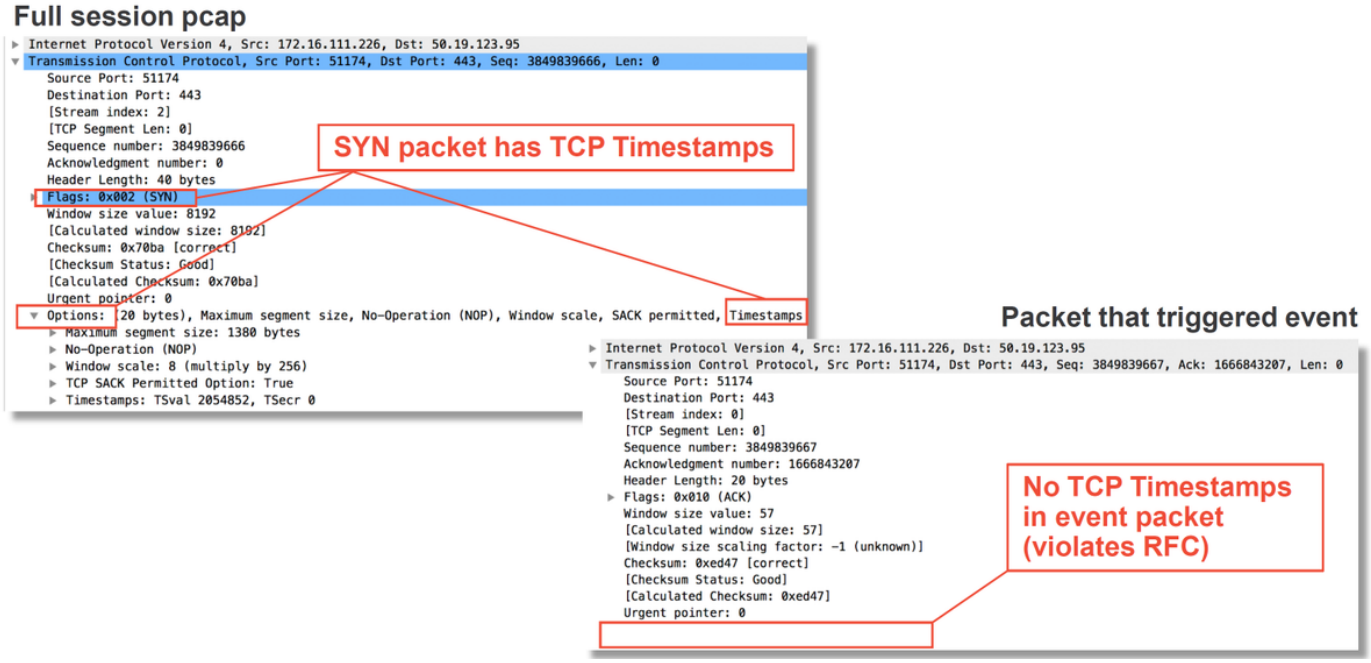


误报分析

在入侵事件中检查预处理器规则的误报与用于规则评估（包含GID 1和3）的Snort规则的误报非常不同。

为了对预处理器规则事件执行误报分析，需要执行完整会话捕获来查找TCP数据流中的异常。

在以下示例中，对规则129:14执行误报分析，**在**上例中显示该规则丢弃了流量。由于**129:14** 正在查找缺少时间戳的TCP流，因此您可以清楚地看到为什么根据下面所示的数据包捕获分析触发规则。

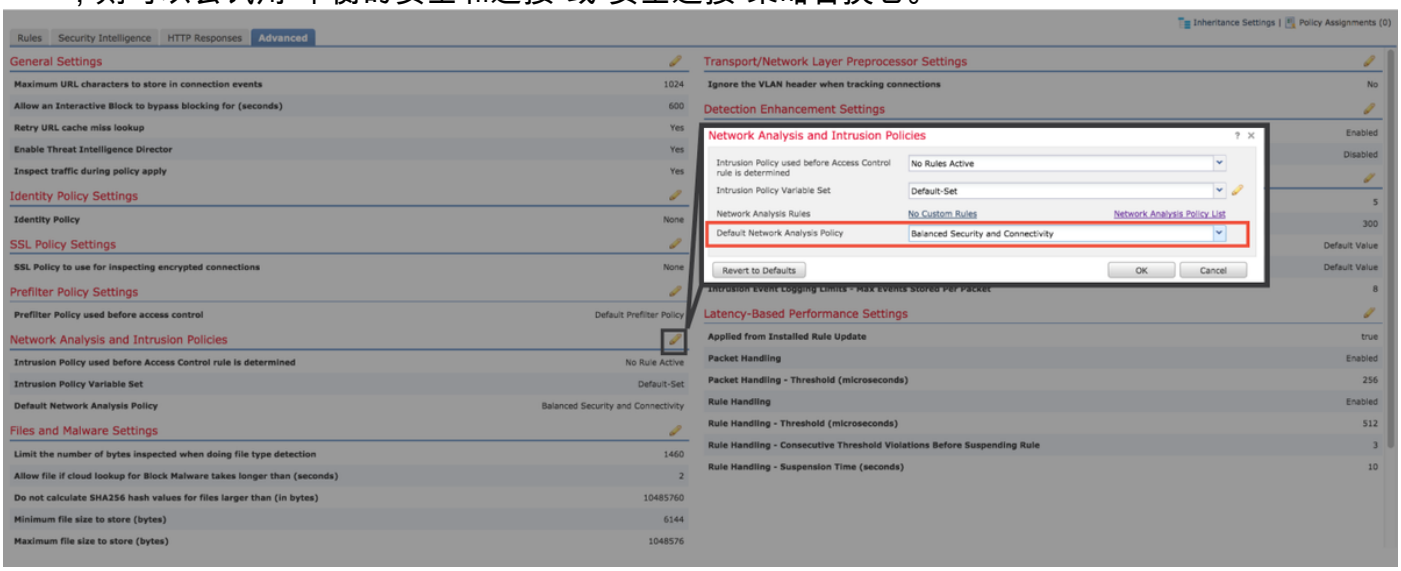


缓解步骤

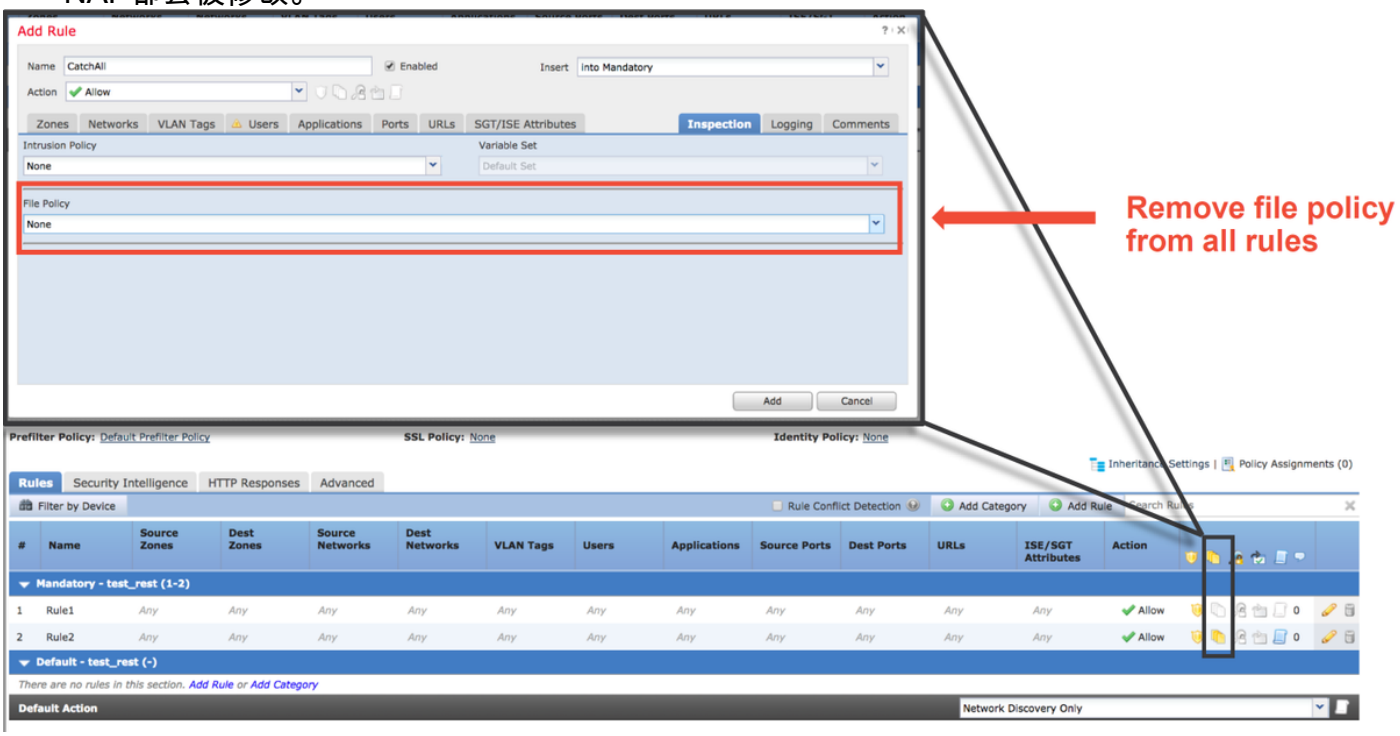
为快速缓解NAP可能出现的问题，可执行以下步骤。

- 如果正在使用自定义NAP，并且您不确定NAP设置是否正在丢弃流量，但您怀疑它可能会丢弃

，则可以尝试用“平衡的安全和连接”或“安全连接”策略替换它。



- 如果使用任何“自定义规则”，请确保将NAP设置为上述默认设置之一
- 如果任何访问控制规则使用文件策略，您可能需要尝试暂时删除它，因为文件策略可以在后端启用处理器前设置，这些设置不会反映在FMC中，而这会在“全局”级别发生，这意味着所有NAP都会被修改。



每种协议都有不同的预处理器，故障排除可能特定于预处理器。本文未介绍每种预处理器的所有设置和故障排除方法。

您可以检查每个预处理器的文档，以更好地了解每个选项的功能，这对于排除特定预处理器故障很有帮助。

向TAC提供的数据

数据	说明
从Firepower设备排除文件故障	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defen
从Firepower设备捕获完整会话数据包	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepo