Firepower数据路径故障排除：概述

目录

简介

本指南旨在帮助快速确定Firepower威胁防御(FTD)设备或具备FirePOWER服务的自适应安全设备(ASA)是否导致网络流量问题。此外，它还有助于缩小在与思科技术支持中心(TAC)接洽之前应调查哪些Firepower组件和应收集哪些数据的范围。

所有Firepower数据路径故障排除系列文章的列表。

Firepower数据路径故障排除第1阶段：数据包入口

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214574-firepower-data-path-troubleshooting-phas.html

Firepower数据路径故障排除第2阶段：DAQ层
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214575-firepower-data-path-troubleshooting-phas.html

Firepower数据路径故障排除第3阶段：安全情报
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214576-firepower-data-path-troubleshooting-phas.html

Firepower数据路径故障排除第4阶段：访问控制策略

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214577-firepower-data-path-troubleshooting-phas.html

Firepower数据路径故障排除第5阶段：SSL策略
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214581-firepower-data-path-troubleshooting-phas.html

Firepower数据路径故障排除第6阶段：主动身份验证
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/214608-firepower-data-path-troubleshooting-phas.html

Firepower数据路径故障排除第7阶段：入侵策略
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214609-firepower-data-path-troubleshooting-phas.html

Firepower数据路径故障排除第8阶段：网络分析策略

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214610-firepower-data-path-troubleshooting-phas.html

先决条件

- 本文假设您对FTD和ASA平台有基本的了解。
- 建议您了解开源snort，但不是必需的。

有关Firepower文档（包括安装和配置指南）的完整列表，请访问文档规划图页。

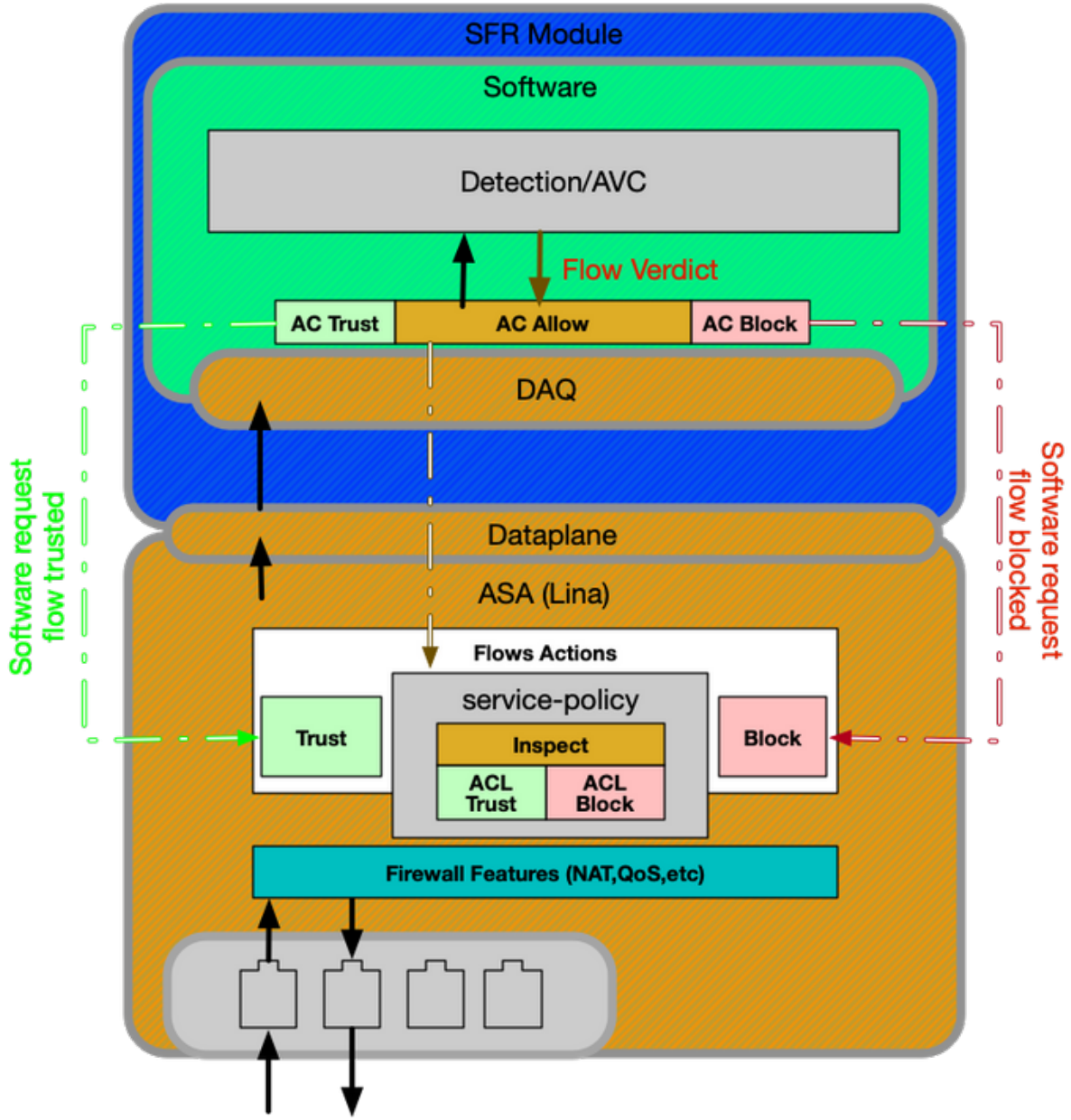
数据路径的架构概述

以下部分介绍各种Firepower平台的架构数据路径。在考虑架构的情况下，我们接下来将介绍如何快速确定Firepower设备是否正在阻止流量。

> **注意**：本文不涉及传统Firepower 7000和8000系列设备，也不涉及NGIPS（非FTD）虚拟平台。有关对这些平台进行故障排除的信息，请访问我们的TechNotes页面。

具备FirePOWER服务（SFR模块）的ASA平台

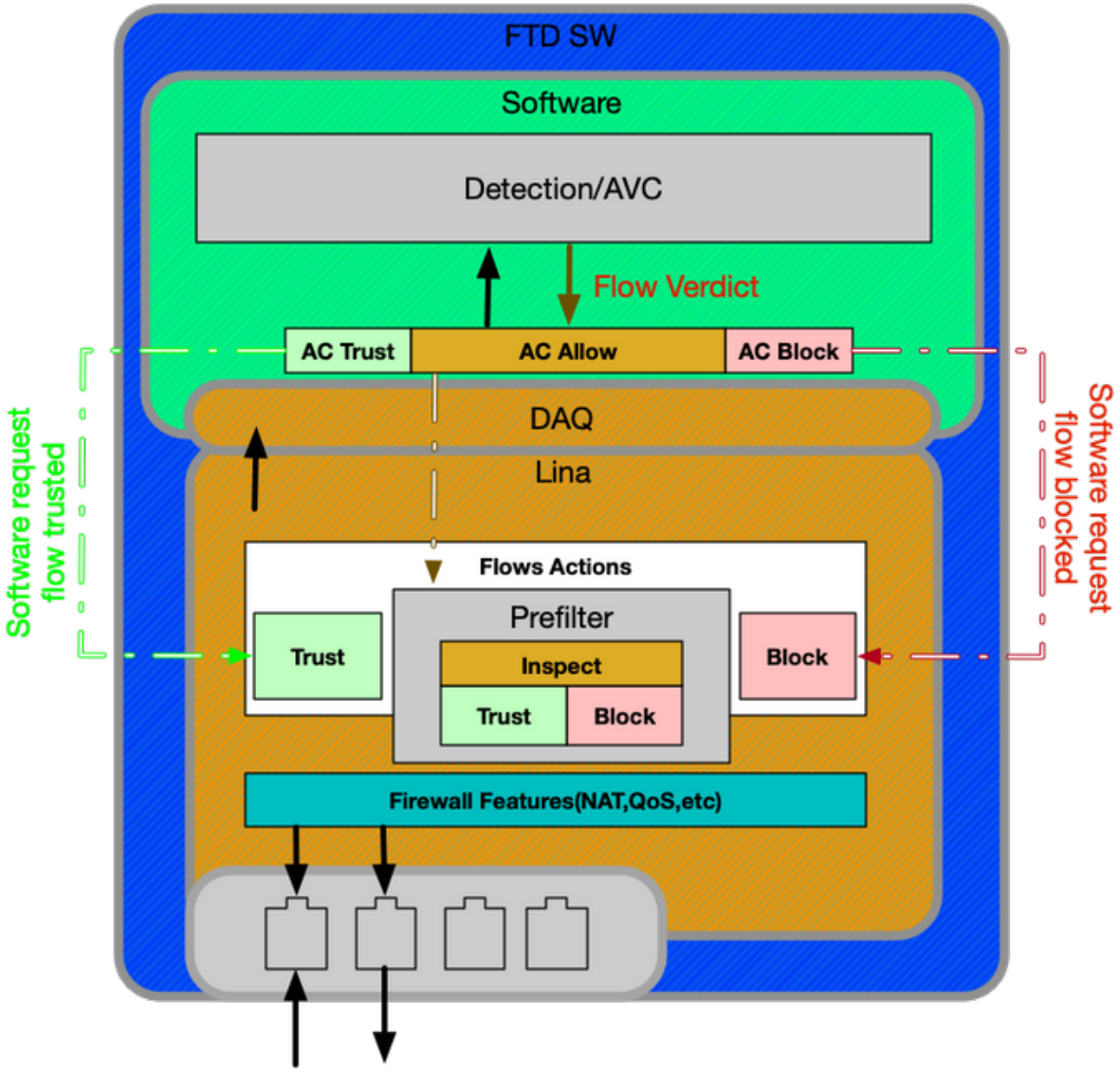
FirePOWER服务平台也称为SFR模块。这基本上是一个在5500-X ASA平台上运行的虚拟机。



ASA上的服务策略确定要向SFR模块发送的流量。数据平面层用于与Firepower数据采集(DAQ)引擎通信，该引擎用于以Snort能够理解的方式转换数据包。

ASA500-X和虚拟FTD平台上的Firepower威胁防御

FTD平台由包含Lina(ASA)和Firepower代码的单个映像组成。与带SFR模块平台的ASA相比，该模块的一个主要区别是Lina和Snort之间的通信效率更高。

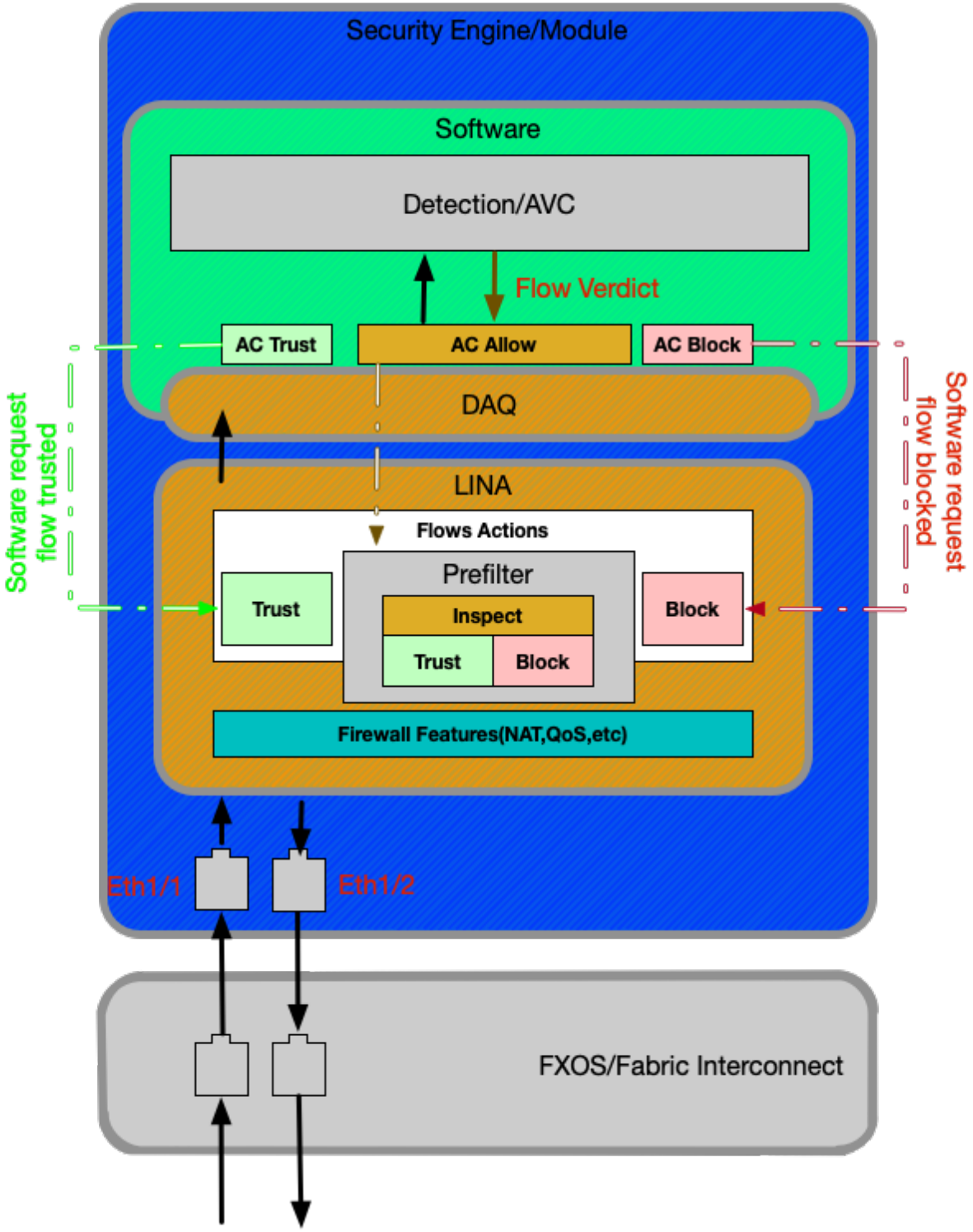


SSP平台上的FTD

在安全服务平台(SSP)型号上，FTD软件在Firepower可扩展操作系统(FXOS)平台上运行，该平台是用于管理机箱硬件和托管各种应用（称为逻辑设备）的底层操作系统(OS)。

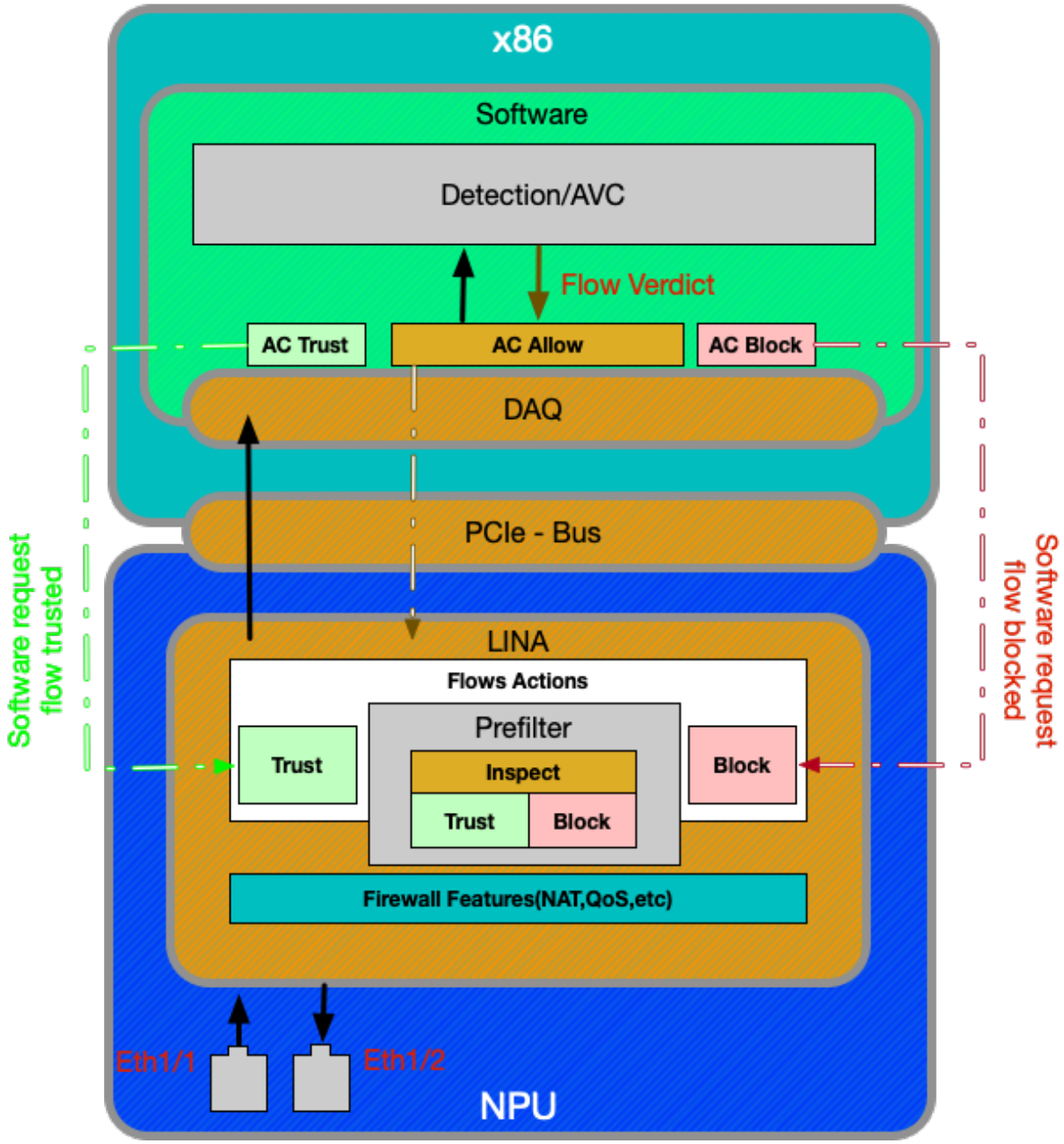
在SSP平台中，不同型号之间有一些差异，如下图和下面的说明所示。

Firepower 9300和4100设备



在Firepower 9300和4100平台上，由FXOS固件（交换矩阵互联）支持的交换机处理编写和编写数据包。 然后，数据包将发送到分配给逻辑设备（本例中为FTD）的接口。 之后，数据包处理与非SSP FTD平台上的处理相同。

Firepower 2100设备



Firepower 2100设备的功能与非SSP FTD平台非常相似。它不包含9300和4100型号上的交换矩阵互联层。但是，2100系列设备与其他设备相比有一个主要区别，即存在专用集成电路(ASIC)。 所有传统ASA功能(Lina)均在ASIC上运行，而所有下一代防火墙(NGFW)功能（snort、URL过滤等）均在传统x86架构上运行。Lina和Snort在此平台上通信的方式是通过外围组件互联快速(PCIe)通过数据包队列，而不是通过使用直接内存访问(DMA)将数据包排入snort队列的其他平台。

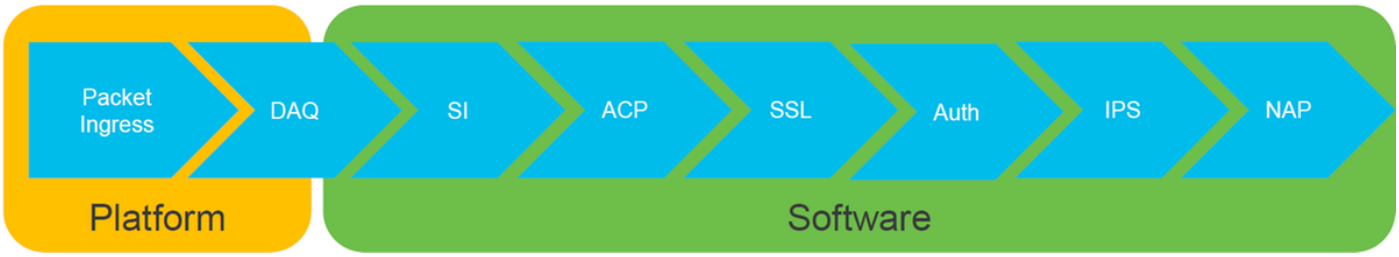
注意：在FPR-2100平台上，将遵循相同的FTD非SSP平台故障排除方法。

Firepower数据路径故障排除的推荐流程

现在，我们已经介绍了如何识别Firepower平台中的唯一流量以及基本数据路径架构，接下来我们将了解数据包可以丢弃的特定位置。数据路径文章包含八个基本组件，可以系统地进行故障排除以确定可能的丢包。这些新发展包括：

1. 数据包入口
2. Firepower数据获取层
3. 安全情报

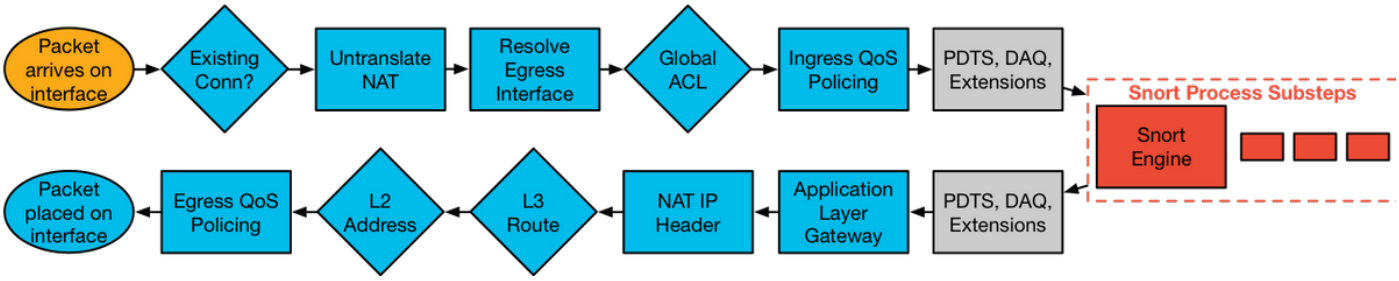
4. 访问控制策略
5. SSL策略
6. 主动身份验证功能
7. 入侵策略（IPS规则）
8. 网络分析策略（snort预处理器设置）



注意：这些组件未按Firepower处理中的确切操作顺序列出，而是根据我们推荐的故障排除工作流程进行排序。有关数据包图的实际路径，请参阅下图。

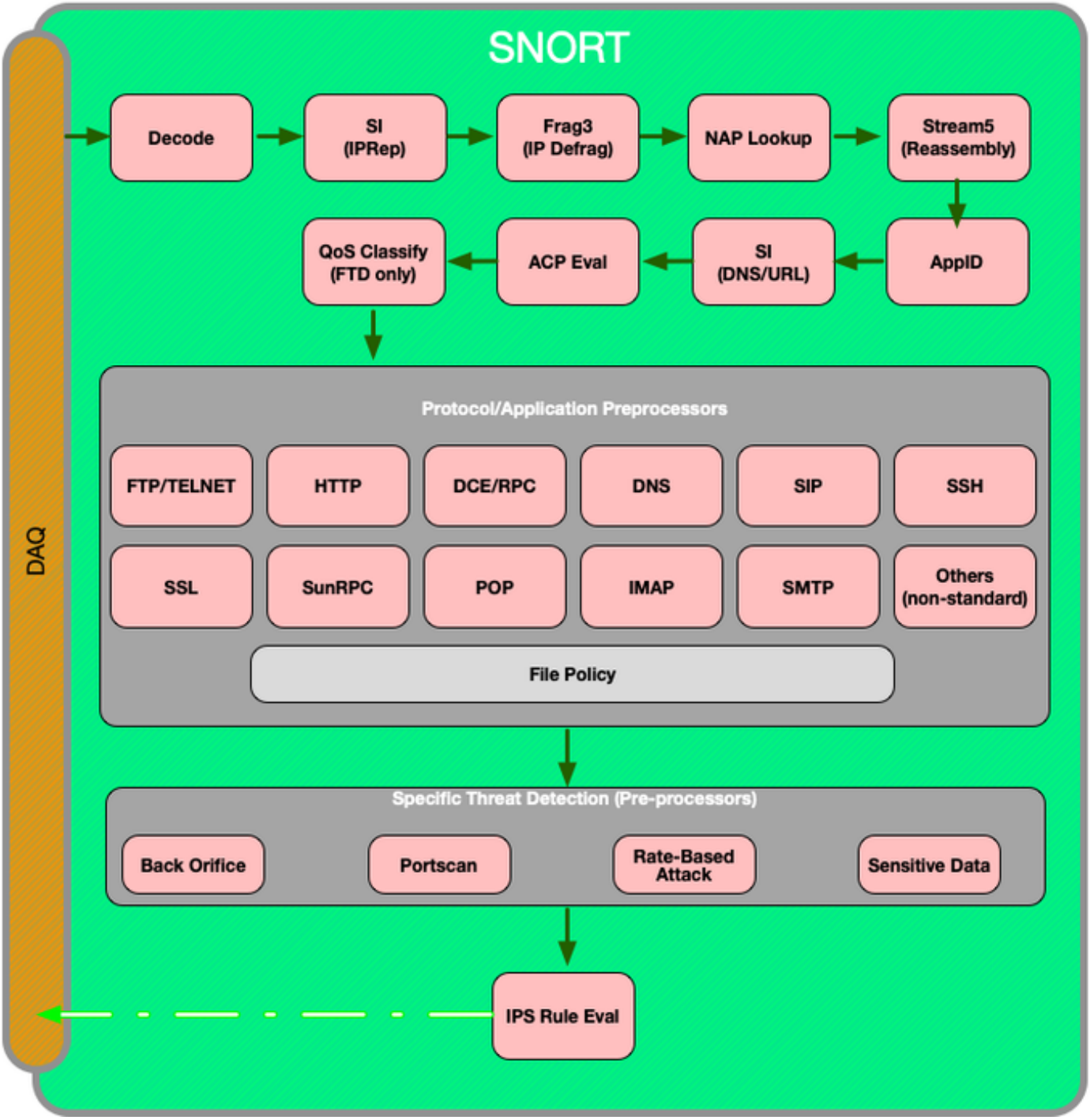
通过FTD的数据包的实际路径

下图显示了数据包在FTD中传输时的实际路径。



Snort数据包路径

下图显示数据包通过Snort引擎的路径。



数据包入口和出口

第一个数据路径故障排除步骤是确保数据包处理的入口或出口阶段不发生丢弃。如果数据包正在进入但未退出，则可以确定数据包正被设备丢弃在数据路径中的某个位置。

本文介绍如何对Firepower系统上的数据包入口和出口进行故障排除。

Firepower数据获取层

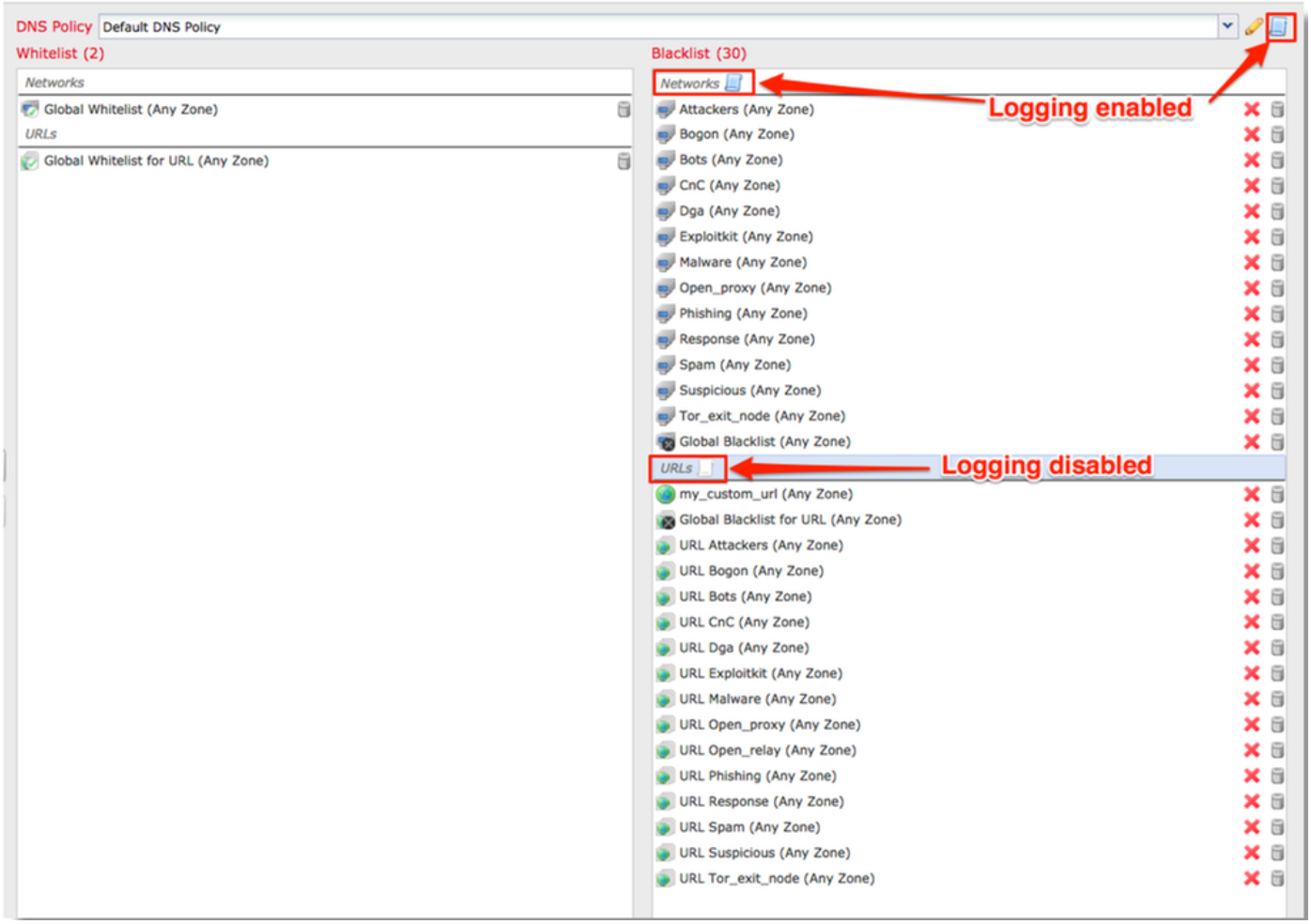
如果确定数据包正在进入但未退出，则数据路径故障排除的下一步应位于Firepower DAQ（数据获取）层，以确保相关流量正被发送到Firepower进行检查，如果是，则丢弃或修改。

本文介绍如何对Firepower对流量的初始处理以及流量在整个设备中所采用的路径进行故障排除。

它还介绍如何完全绕过Firepower设备，以确定Firepower组件是否对流量问题负责。

安全情报

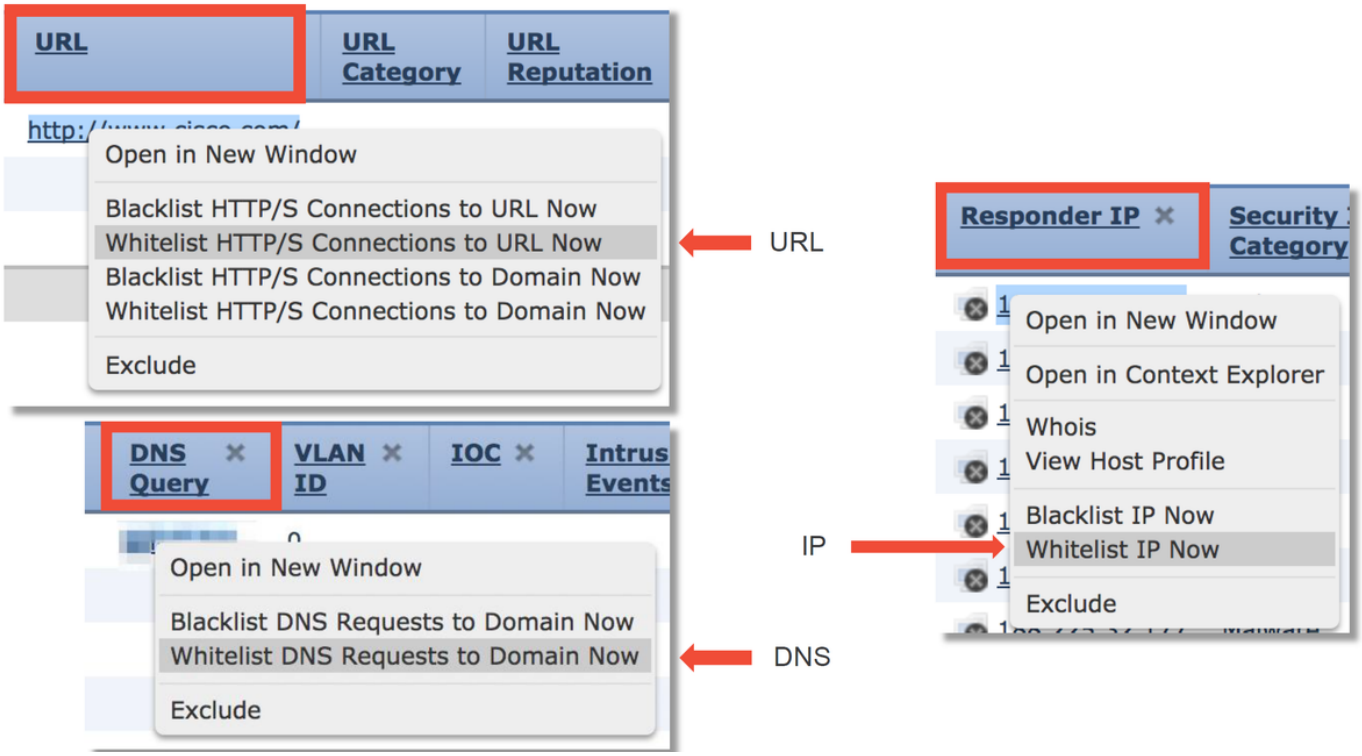
安全情报是Firepower中用于检查流量的第一个组件。只要启用日志记录，此级别的块就很容易确定。在FMC GUI上，可以通过导航到Policies > Access Control > Access Control Policy**来确定这一点**。点击所述策略旁边的编辑图标后，导航至安全情报**选项卡**。



启用日志记录后，可以在Analysis > Connections > Security Intelligence Events下查**看Security Intelligence Events**。应该清楚为什么流量被阻塞。

First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Security Intelligence Category
2017-05-16 17:00:16		Domain Not Found	DNS Block	192.168.1.95		DNS Response
2017-05-16 16:57:50	2017-05-16 16:57:50	Block	URL Block	192.168.1.95	10.83.48.40	my_custom_url
2017-05-16 16:50:05		Block	IP Block	192.168.1.95		Malware

作为快速缓解步骤，您可以右击安全情报功能阻止的IP、URL或DNS查询，并选择白名单选项。



如果您怀疑某些内容被错误地列入黑名单，或者您想请求更改信誉，可以通过以下链接直接与Cisco Talos打开票证：

https://www.talosintelligence.com/reputation_center/support

您还可以向TAC提供数据，以报告被阻止的内容，并且可能将条目从黑名单中删除。

有关安全情报组件的深入故障排除，请查看相关数据路径故障排除文章。

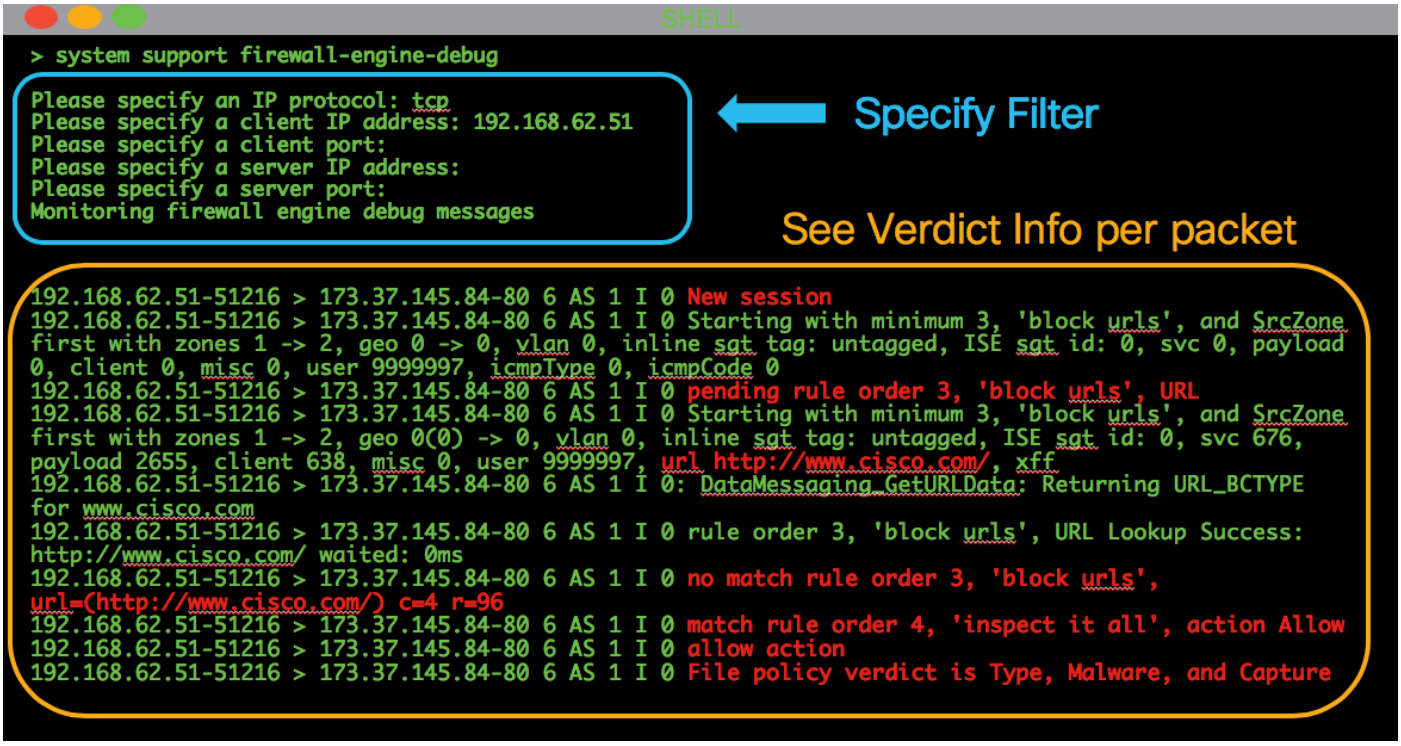
访问控制策略

如果已确定安全情报功能未阻止流量，则建议下一步是排除访问控制策略规则故障，以查看具有“阻止”(Block)操作的规则是否正在丢弃流量。

建议开始使用命令“firewall-engine-debug”或使用trace捕获。通常，这些工具可以立即为您提供答案，并告诉您流量的命中规则以及原因。

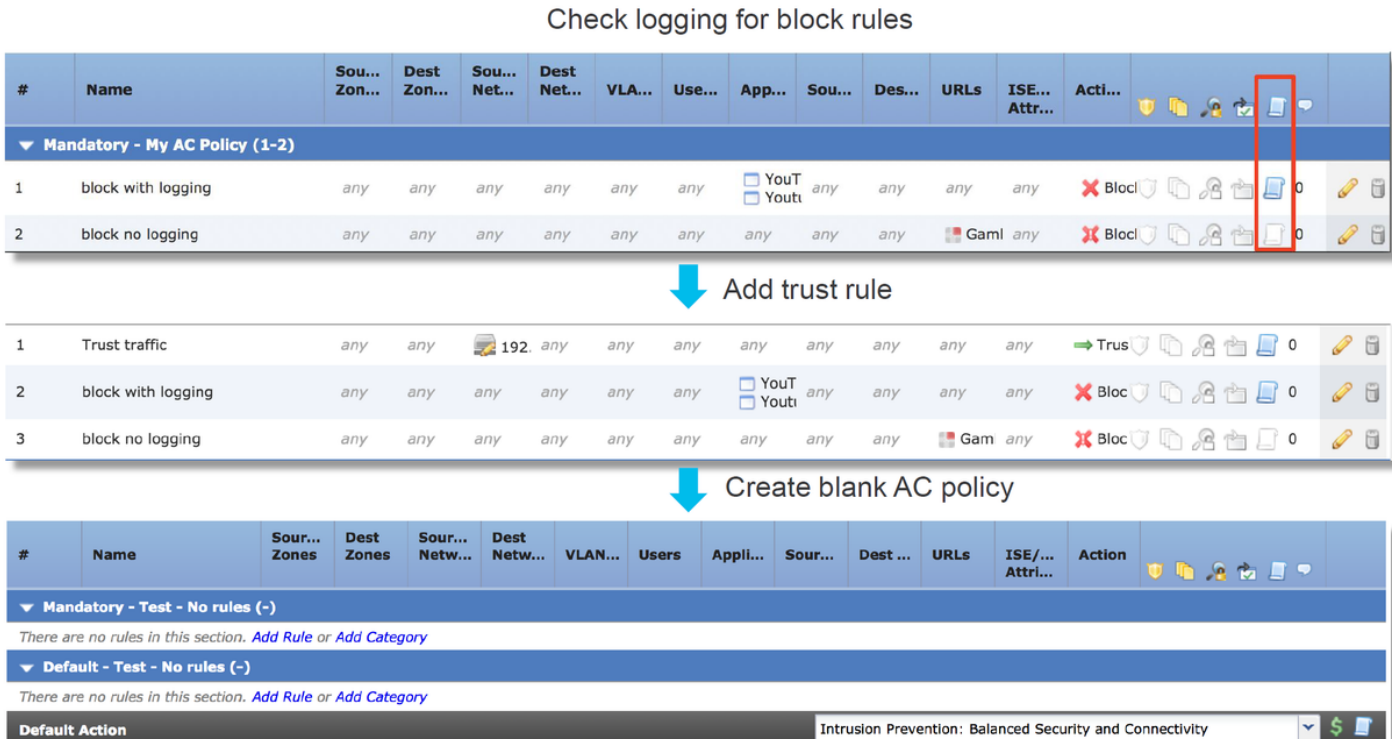
- 在Firepower CLI上运行调试，以通过以下命令查看阻止流量的规则（确保输入尽可能多的参数）：**> system support firewall-engine-debug**
- 调试输出可提供给TAC进行分析

以下是一些输出示例，描述与“允许”(Allow)操作匹配访问控制规则的流量的规则评估：



如果无法确定匹配哪个访问控制(AC)规则，或者无法使用上述工具确定AC策略是否存在问题，以下是排除访问控制策略故障的一些基本步骤（请注意，这些选项不是第一个选项，因为它们需要更改/部署策略）：

- 对具有“阻止”(Block)操作的任何规则启用日志记录
- 如果仍未看到流量的连接事件，且该流量被阻止，则接下来为有问题的流量创建信任规则作为缓解步骤
- 如果流量的信任规则仍无法解决问题，但您仍怀疑AC策略有故障，则接下来，如果可能，使用除“阻止所有流量”(Block All Traffic)之外的默认操作，创建一个新的空白访问控制策略

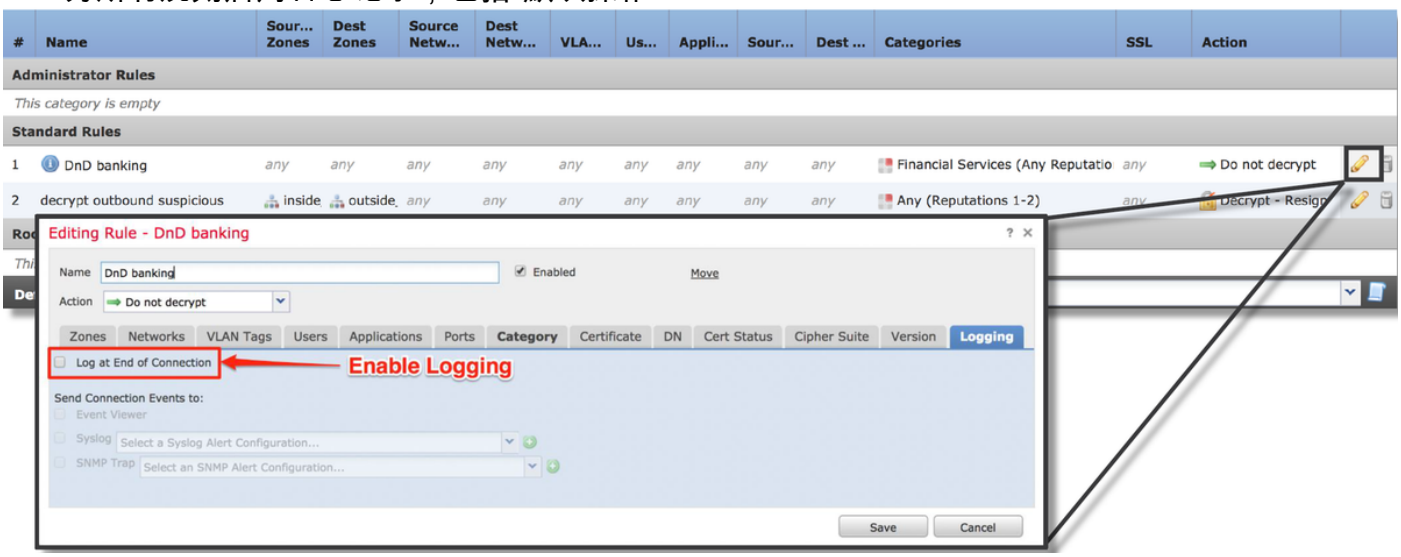


有关访问控制策略的深入故障排除，请查看相关数据路径故障排除文章。

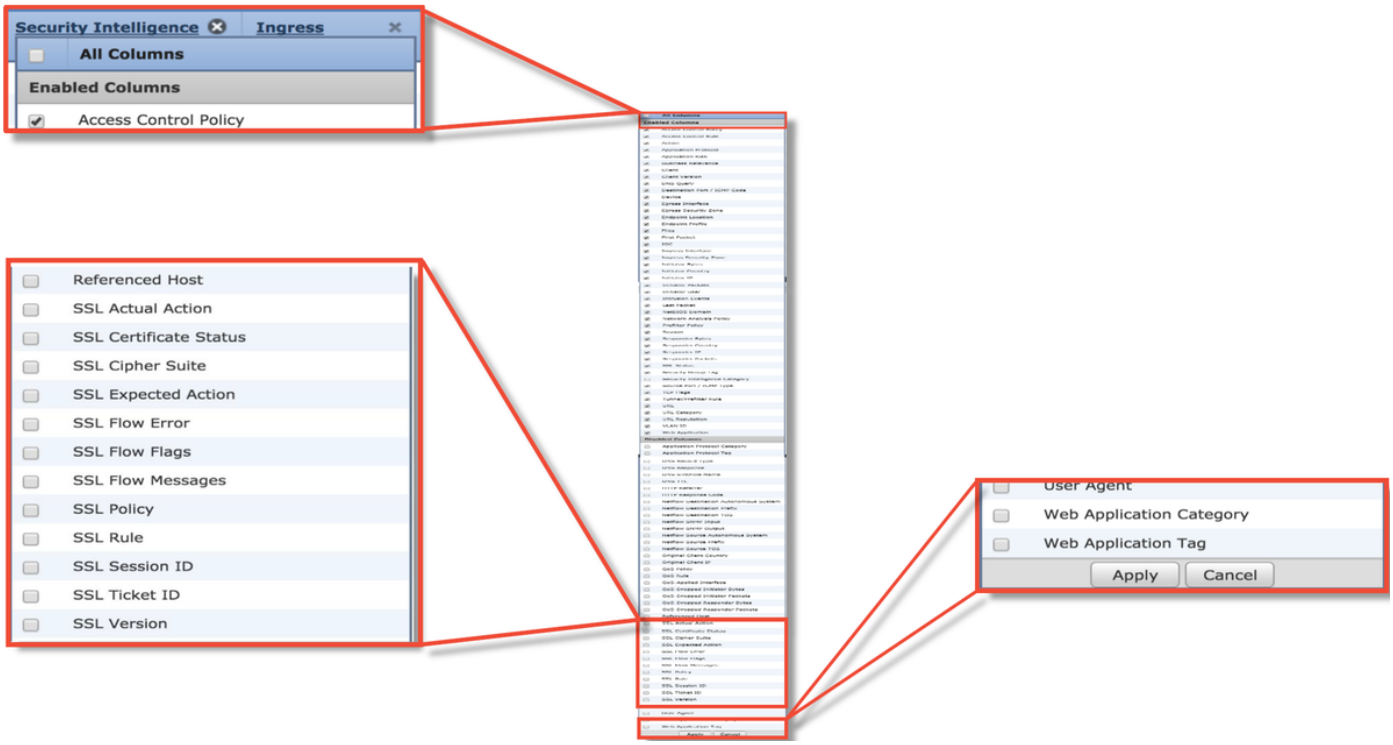
SSL策略

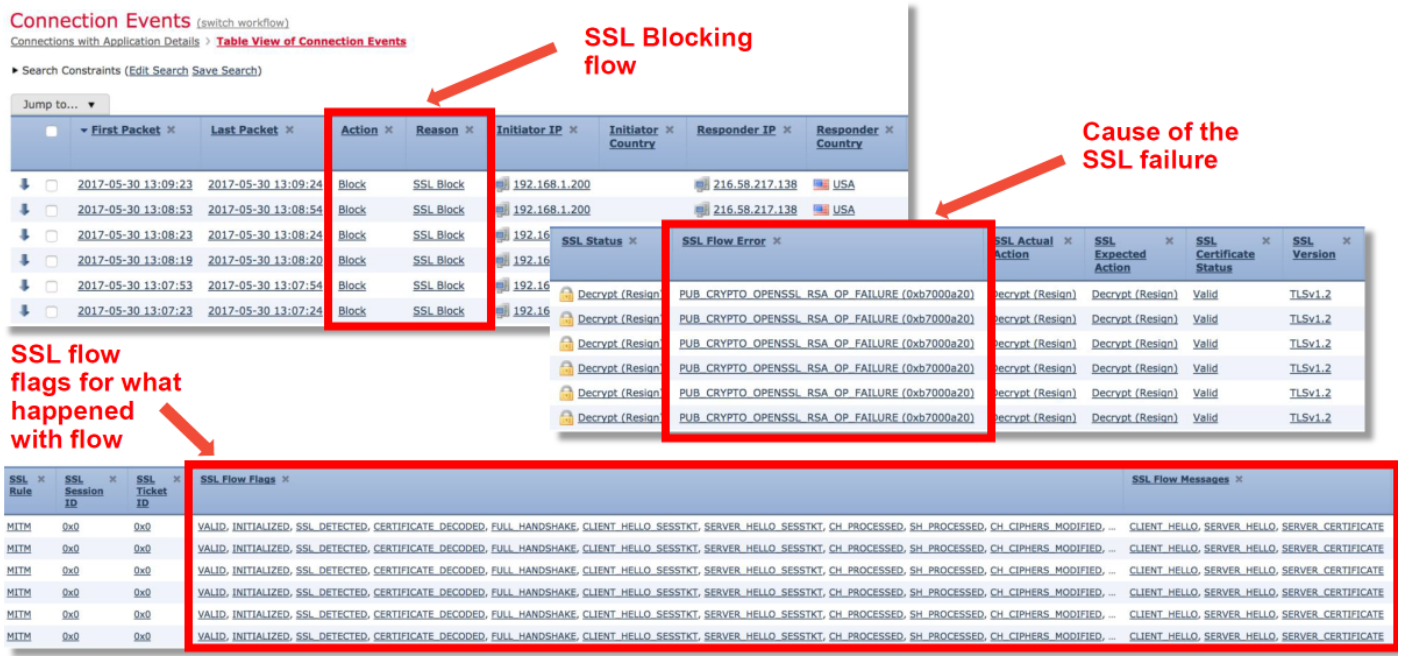
如果使用SSL策略，则可能会阻止流量。以下是排除SSL策略故障的一些基本步骤：

- 为所有规则启用日志记录，包括“默认操作”



- 选中Undecryptable Actions选项卡，查看是否将选项设置为阻止流量
- 在Connection events（连接事件）部分，检查名称中包含“SSL”的所有字段
  大多数默认为禁用状态，需要通过点击任何列名称旁边的交叉点在连接事件查看器中启用





- 创建空白SSL策略，将Do not Decrypt（不解密）作为默认操作作为缓解步骤
- 从访问控制策略中删除SSL策略作为缓解步骤
  这在“高级”选项卡中设置

SSL策略可能会丢弃流量，连接事件和策略配置可以发送到TAC。

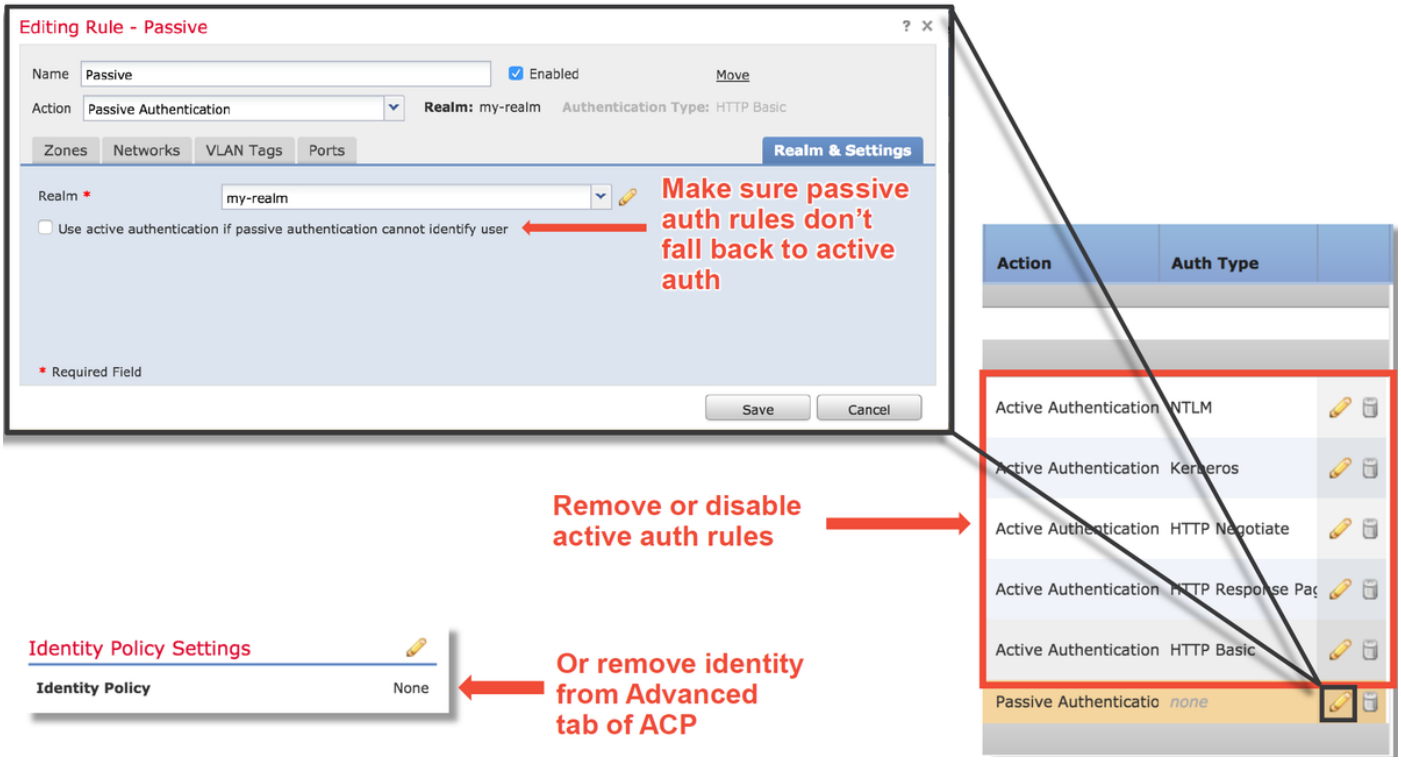
有关SSL策略的更深入故障排除，请查看相关数据路径故障排除文章。

主动身份验证

当在身份策略中使用时，主动身份验证能够丢弃在发生错误时应允许的流量。主动身份验证功能本身会直接影响所有HTTP/HTTPS流量，因为如果确定需要对用户进行身份验证，则所有这些都仅通过HTTP协议进行。这意味着主动身份验证不应影响其他网络服务（如DNS、ICMP等），除非您具有基于用户阻止的特定访问控制规则，并且用户无法通过FTD上的主动身份验证服务进行身份验证。但是，这不是主动身份验证功能的直接问题，而是用户无法进行身份验证并拥有阻止未经身份验证用户的策略的结果。

快速缓解步骤是使用“主动身份验证”(Active Authentication)操作禁用身份策略中的任何规则。

另外，请确保任何具有“被动身份验证”操作的规则都未选中“如果被动身份验证无法识别用户，则使用主动身份验证”选项。



有关主动身份验证的更深入故障排除，请参阅相关数据路径故障排除文章。

入侵策略

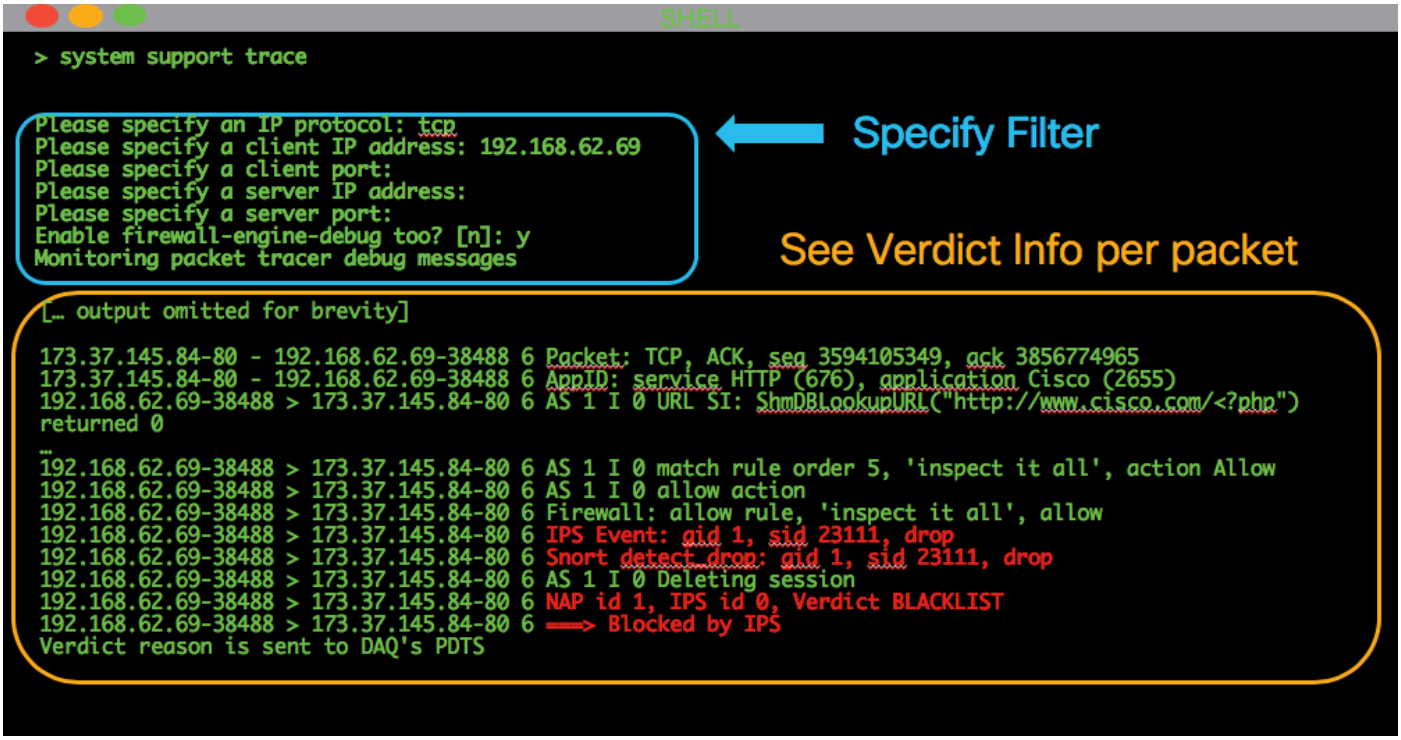
入侵策略可能正在丢弃流量或导致网络延迟。入侵策略可在访问控制策略中的以下三个位置之一使用：

- 在访问控制规则中，在“检查”选项卡中
- 在默认操作中
- 在“高级”(Advanced)选项卡中，在“**确定访问控制规则之**前使**用的网络分析和入侵策略”(Network Analysis and Intrusion Policies)>“入侵策略”(Intrusion Policy)**部分

要查看入侵策略规则是否正在阻止流量，请导航至FMC中的**Analysis > Intrusions > Events**页面。入侵**事件的表视图**提供有关事件中涉及的主机的信息。有关与事件分析相关的信息，请参阅相关数据路径故障排除文章。

确定入侵策略签名(IPS)是否阻止流量的第一个建议步骤是从FTD的CLI使用**>系统支**持跟踪功能。此debug命令的工作方式与firewall-engine-debug类似，它还提供了在跟踪的同时启用firewall-engine-debug的选项。

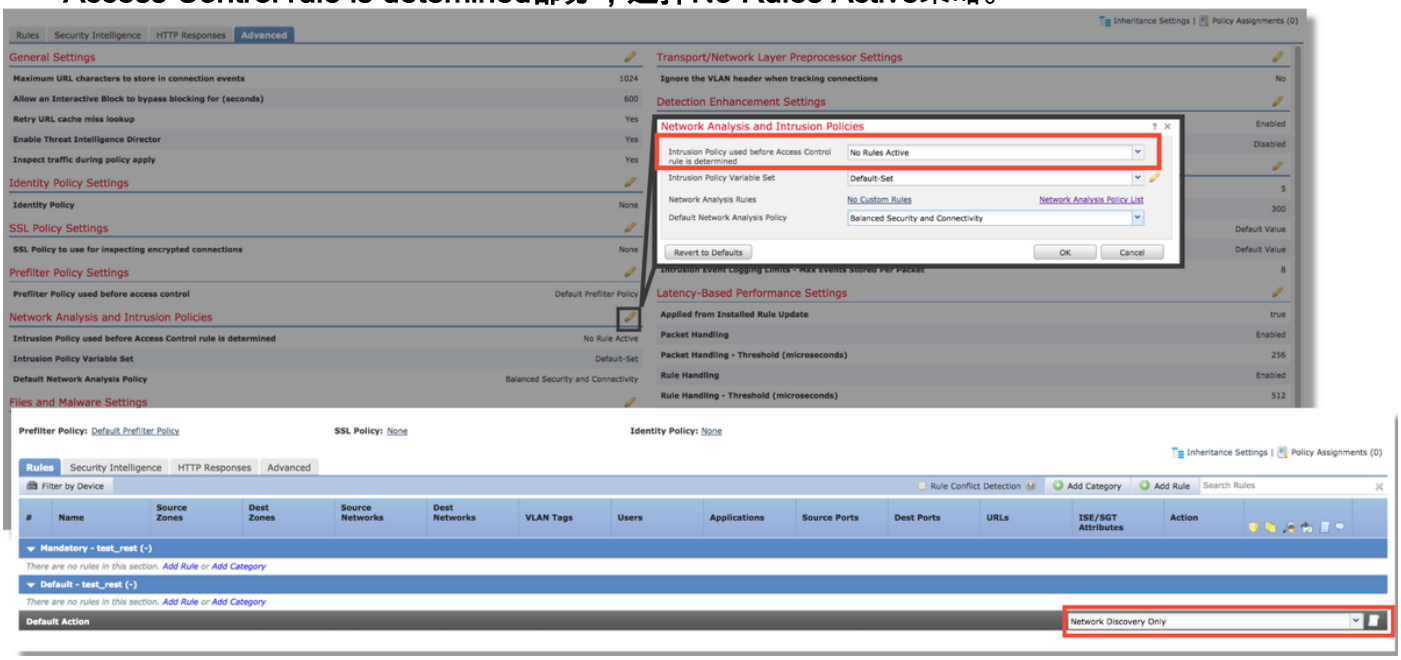
下图显示了使用系统支持跟踪工具的示例，其结果显示数据包因入侵规则而被阻止。这将为您提供所有详细信息，如GID（组标识符）、SID（签名标识符）、NAP（网络分析策略）ID和IPS ID，以便您确切地看到阻止此流量的策略/规则。



如果无法确定IPS正在阻止跟踪输出，但您怀疑由于自定义入侵策略而导致IPS丢弃，则可以用“平衡安全和连接”策略或“安全连接”策略替换入侵策略。这些是思科提供的入侵策略。如果进行更改，可解决问题，则TAC可以对之前使用的自定义入侵策略进行故障排除。如果已使用默认思科策略，您可以尝试将默认更改为安全性较低的策略，因为这些策略的规则较少，因此可能有助于缩小范围。例如，如果流量被阻止，并且您使用的是平衡策略，那么您切换到通过安全策略的连接，并且问题消失，则平衡策略中可能有一条规则丢弃未设置为通过安全策略的连接中丢弃的流量。

在访问控制策略中可以进行以下更改，以消除所有入侵策略检查块的可能性（建议尽可能少的更改，以便不更改安全效力，因此建议对相关流量制定目标AC规则，而不是在整个策略中禁用IPS）：

- 在所有访问控制规则（或仅特定流量匹配且受影响的规则）中，从Inspection（检查）选项卡中删除Intrusion Policy（入侵策略）
- 在Advanced选项卡的**Network Analysis and Intrusion Policies > Intrusion Policy used before Access Control rule is detemined部分，选择No Rules Active**策略。



如果仍无法解决问题，请继续排除网络分析策略故障。

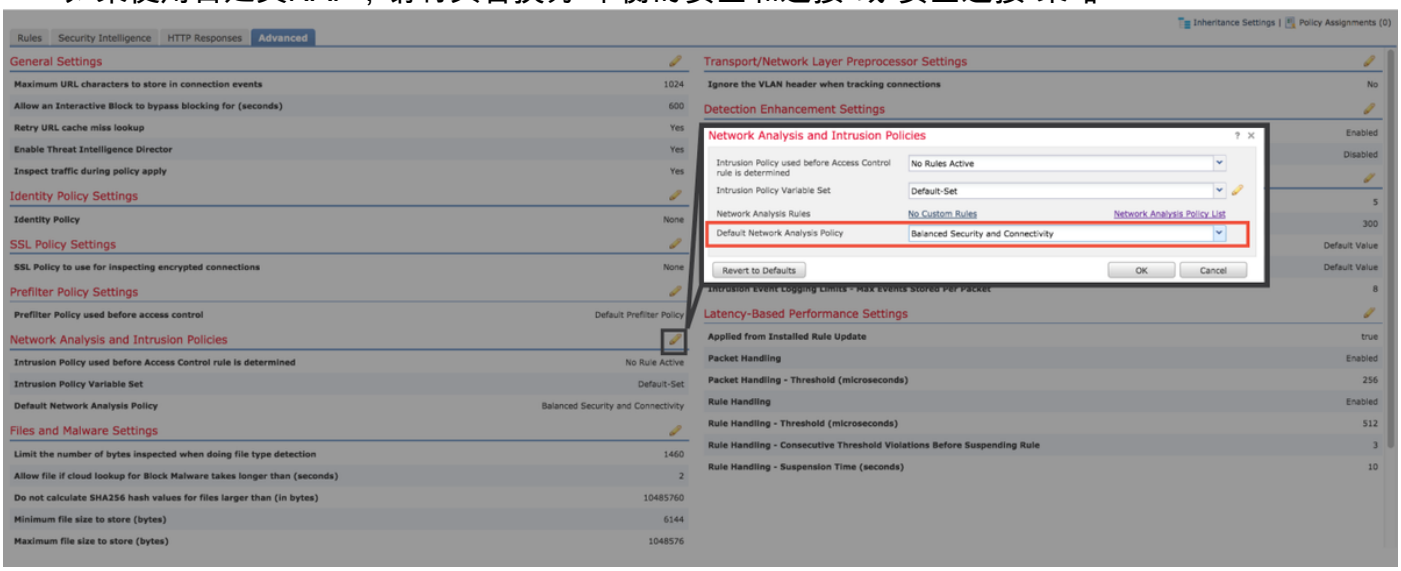
有关入侵策略功能的更深入故障排除，请参阅相关数据路径故障排除文章。

网络分析策略

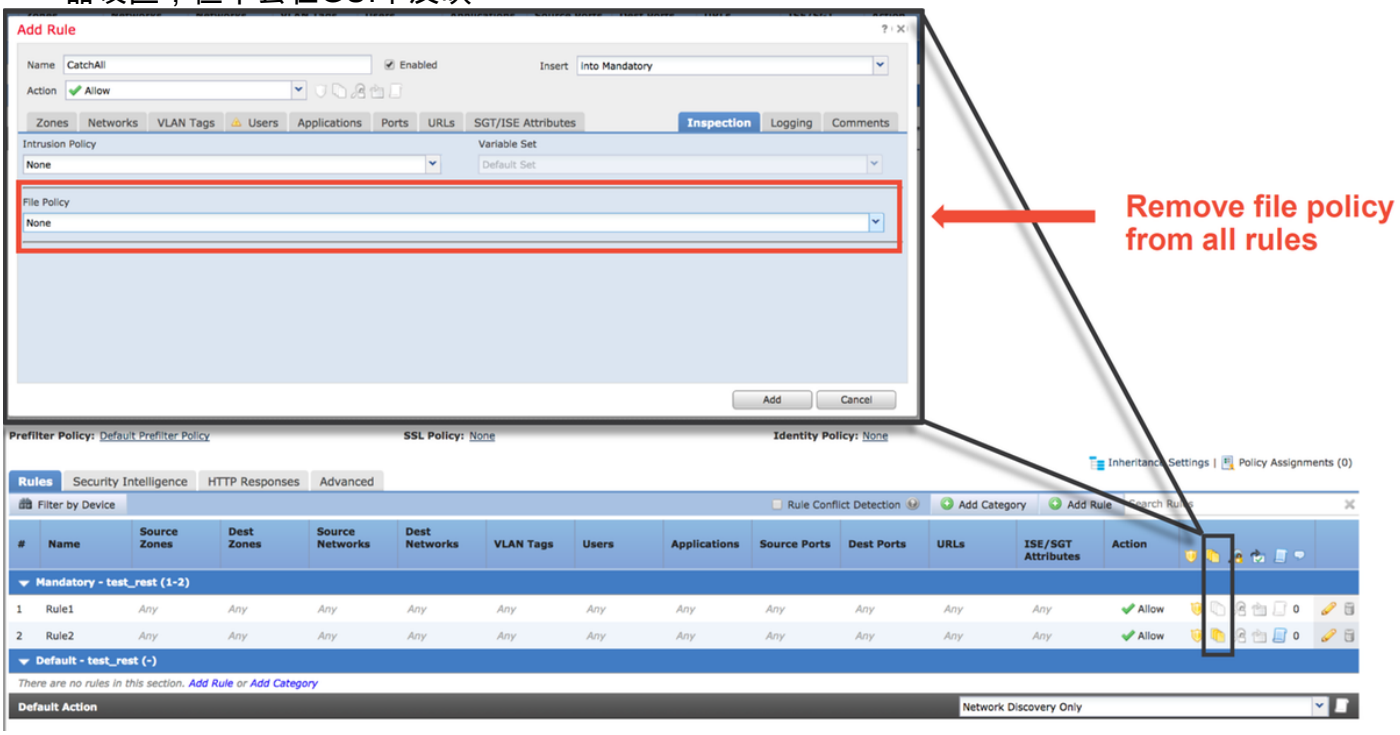
网络分析策略(NAP)包含Firepower预处理器设置，其中一些设置可以丢弃流量。故障排除的第一个建议步骤与IPS故障排除相同，即使用**>系统支持跟踪**工具尝试查找snort中阻止流量的内容。有关此工具和示例用法的详细信息，请参阅上面的“入侵策略”部分。

要快速缓解NAP可能出现的问题，可执行以下步骤：

- 如果使用自定义NAP，请将其替换为“平衡的安全和连接”或“安全连接”策略



- 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，则暂时将其删除，因为文件策略可以在后端启用预处理器设置，但不会在GUI中反映



本文将对网络分析策略功能进行更深入的故障排除。

相关信息

指向Firepower文档的链接

https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html