Firepower数据路径故障排除第3阶段：安全情报

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三阶段，即安全情报功能。

先决条件

- 本文涉及当前支持的所有Firepower平台
- URL和DNS的安全情报在版本6.0.0中引入

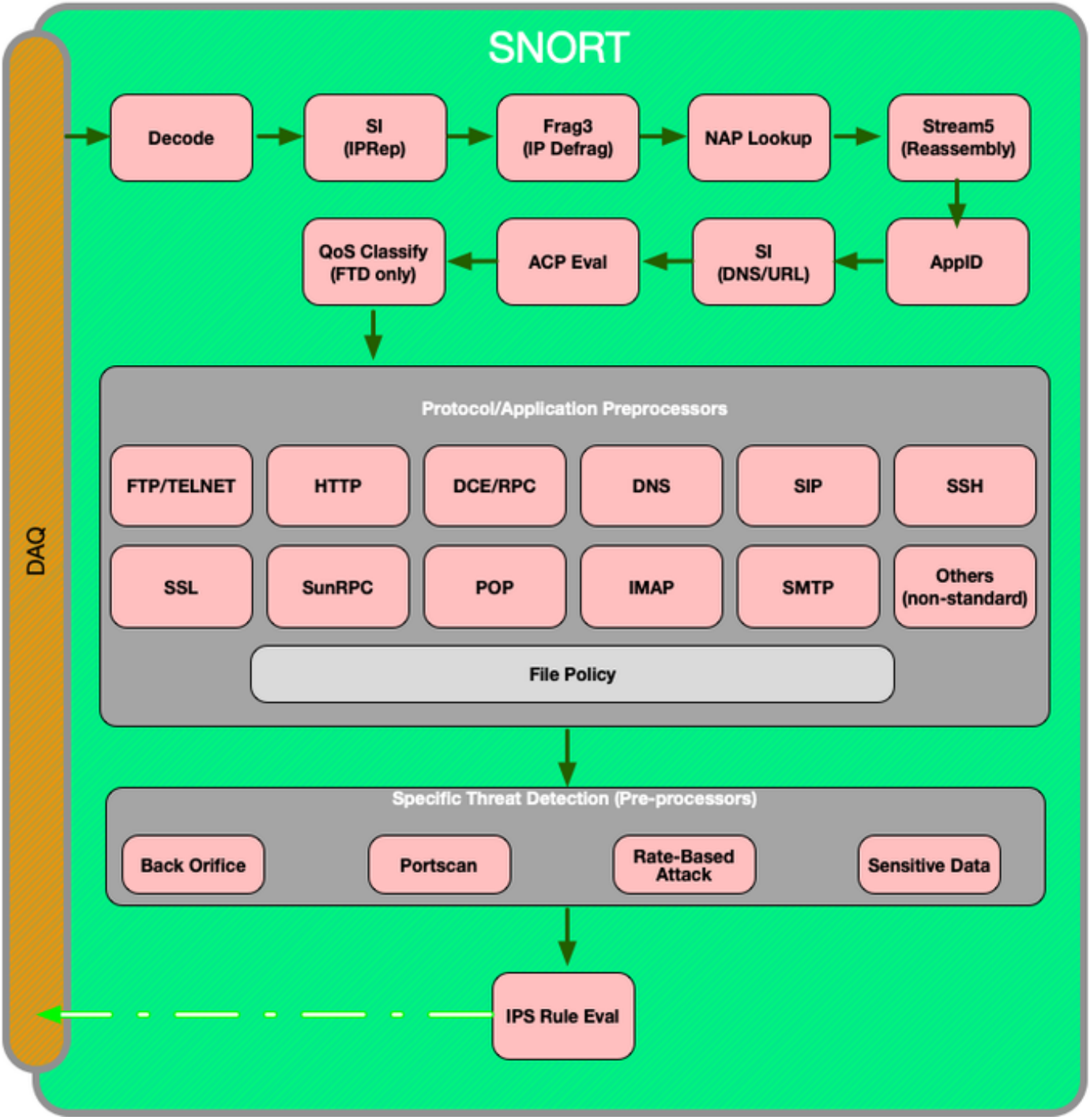
Firepower安全情报阶段故障排除

安全情报是一项功能，可对黑名单和白名单执行检查，以：

- IP地址（在UI的某些部分也称为“网络”）
- 统一资源定位器(URL)
- 域名系统(DNS)查询

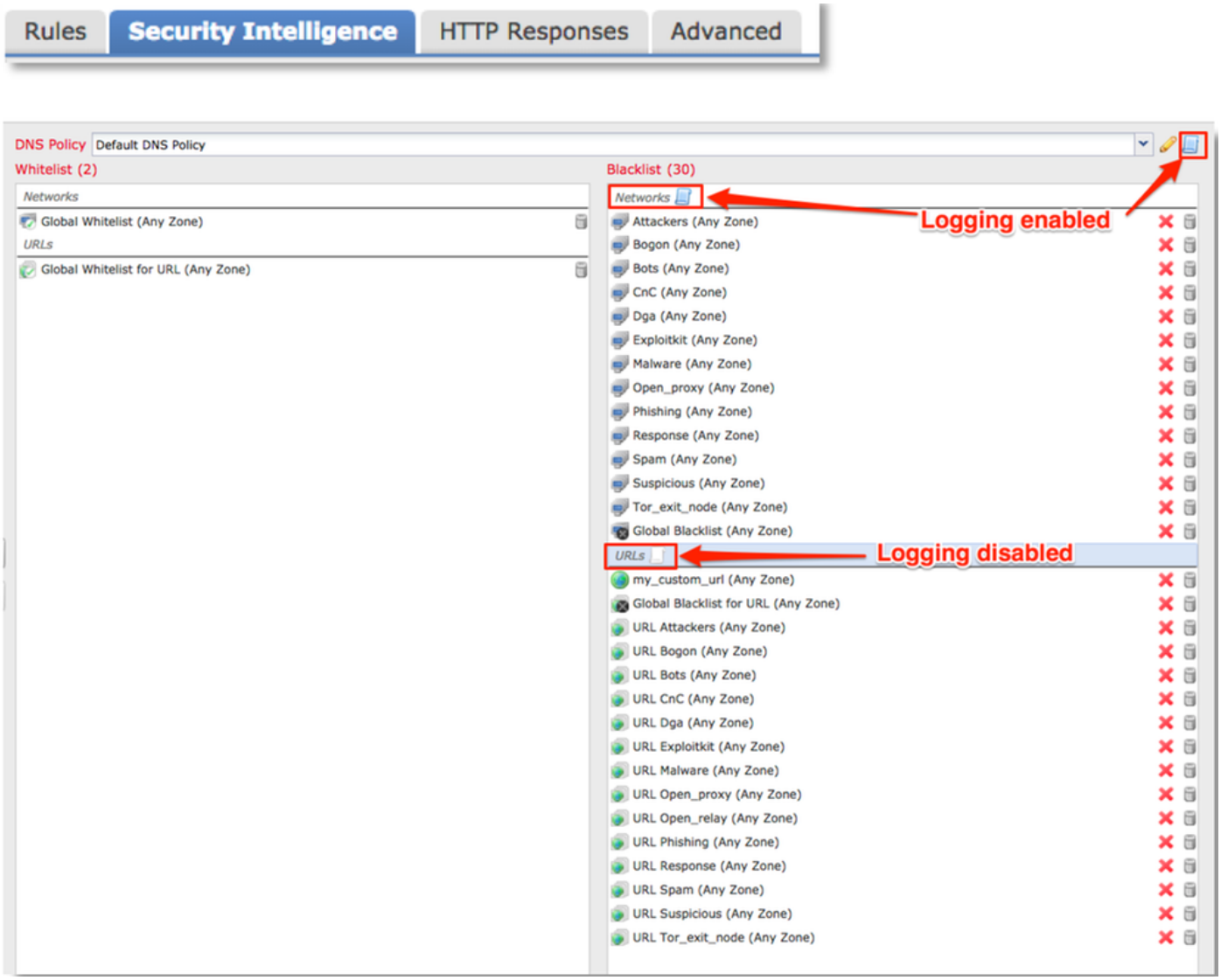
安全情报中的列表可以由思科提供的源和/或用户配置的列表和源填充。

基于IP地址的安全情报信誉是Firepower中用于检查流量的第一个组件。URL和DNS安全情报在发现相关应用协议后立即执行。下图概述了Firepower软件检查工作流程。



确定为安全情报事件启用日志记录

只要启用日志记录，安全情报级别的块就很容易确定。通过导航至策略>访问控制>访问控制策略，可以在Firepower管理中心(FMC)用户界面(UI)**上确定这一点**。点击所述策略旁边的编辑图标后，导航至安全情报**选项卡**。

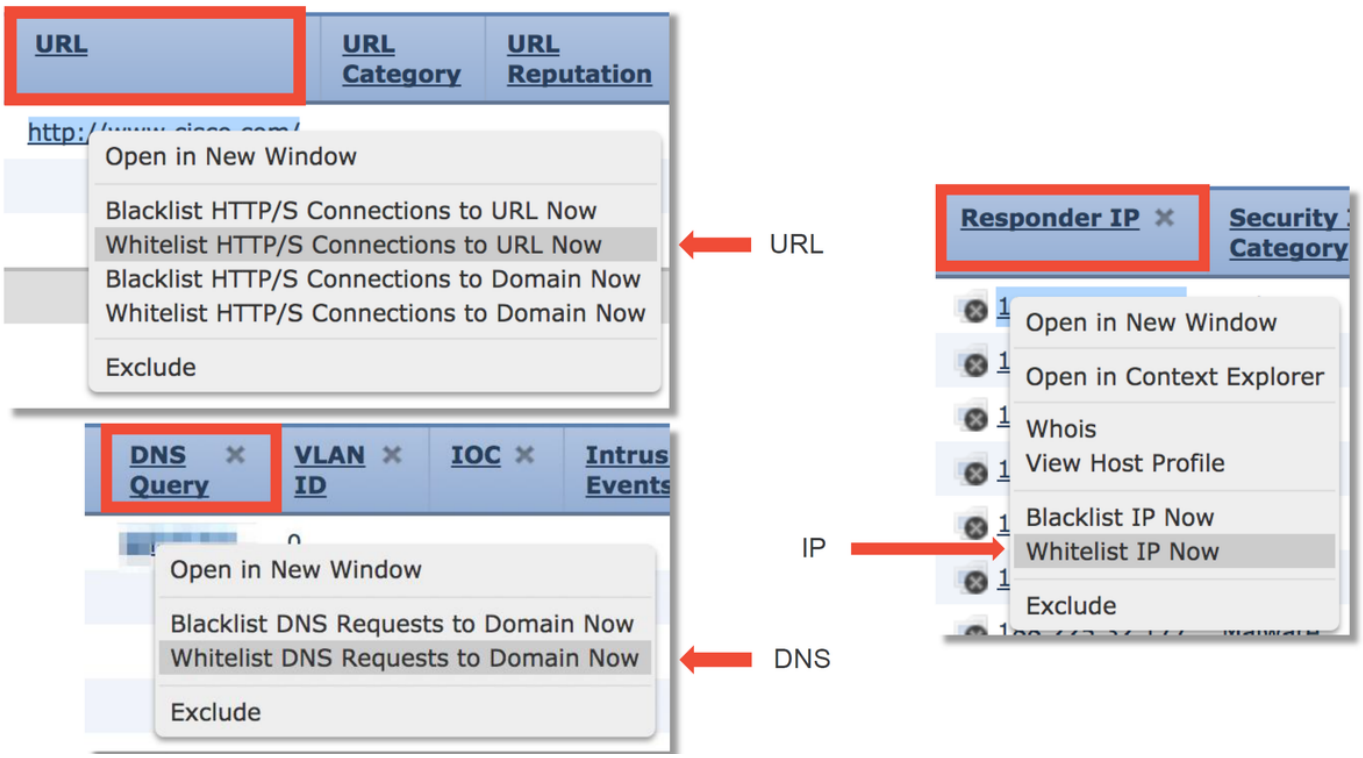


查看安全情报事件

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

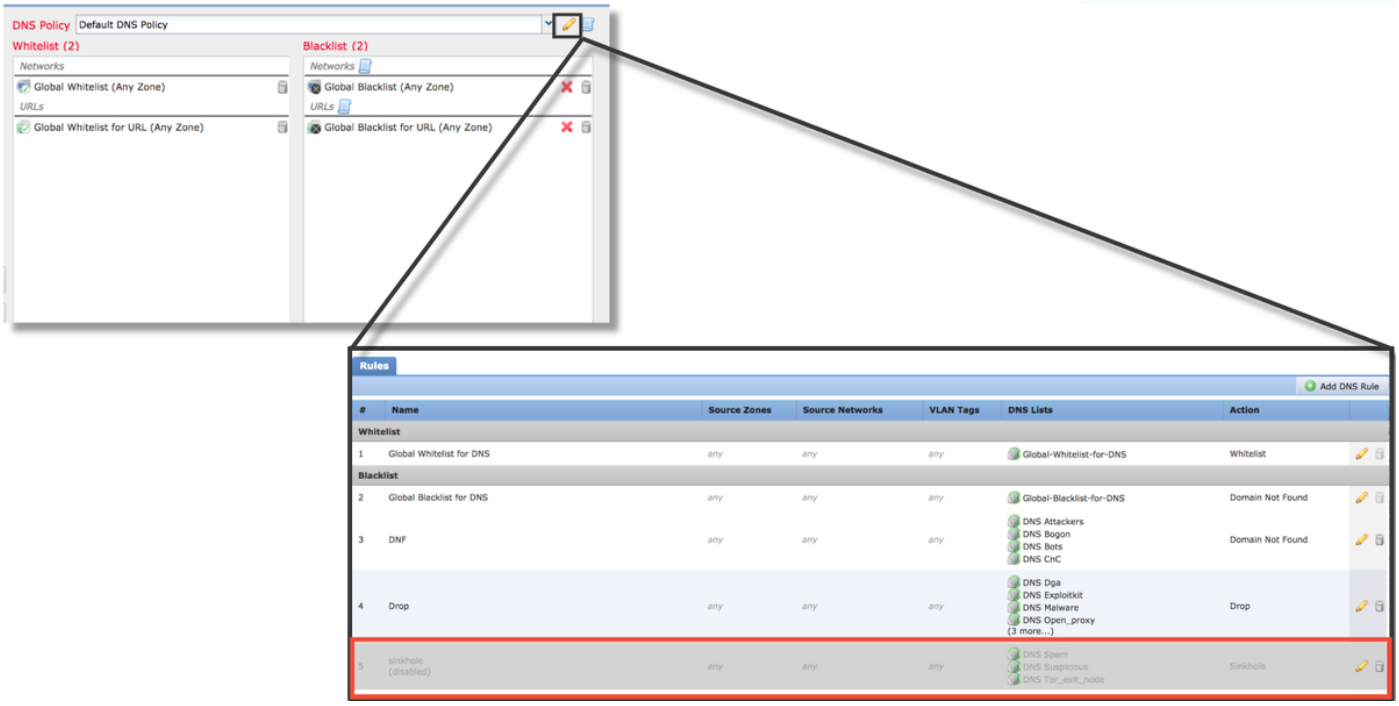
您还可以向思科技术支持中心(TAC)提供数据，以调查是否应从黑名单中删除项目。

> **注意**：添加到白名单仅向有关的安全情报白名单添加条目，这意味着允许该对象通过安全情报检查。但是，所有其他Firepower组件仍可以检查流量。

如何删除安全情报配置

要删除安全情报配置，请导航至安全情报**选项卡**，如上所述。分为三部分：一个用于网络、URL和DNS策略。

从中，点击垃圾桶符号可删除列表和源。



请注意，在上面的屏幕截图中，除全局黑名单和白名单外，所有IP和URL安全情报列表都已删除。

在存储DNS安全情报配置的DNS策略中，其中一个规则被禁用。

> **注意**：要查看全局黑名单和白名单的内容，请导航至“对象”(Objects)>“对象管理”(Object Management)>“安全情报”(Security Intelligence)。然后，点击感兴趣的部分（网络、URL、DNS）。 编辑列表后将显示内容，但配置必须在访问控制策略中执行。

验证后端的配置

安全情报配置可通过> show access-control-config命令在CLI上进行验证，该命令显示Firepower设备上运行的活动访问控制策略的内容。

```
> show access-control-config

==================[ My AC Policy ]==================
Description              :
Default Action            : Allow
Default Policy            : SOC
Logging Configuration
   DC                   : Enabled
   Beginning             : Disabled
   End                  : Enabled
Rule Hits                 : 0
Variable Set              : Default-Set

===[ Security Intelligence - Network Whitelist ]====
   Name                 : Global-Whitelist (List)
   IP Count             : 0
   Zone                 : any

===[ Security Intelligence - Network Blacklist ]====
Logging Configuration     : Enabled
   DC                   : Enabled


--------------------[ Block ]---------------------
   Name                 : Attackers (Feed)
   Zone                 : any

   Name                 : Bogon (Feed)
   Zone                 : any
…[omitted for brevity]
```

请注意，在上例中，为网络黑名单配置了日志记录，并且黑名单（攻击者和Bogon）中至少包含了两个源。

在专家模式下可确定单个项目是否在安全情报列表中。请参阅以下步骤：

每个安全情报列表都有一个具有唯一UUID的文件。上例显示如何使用head -n1命令标识列**表的名**称。

向TAC提供的数据

数据	说明
从FMC和Firepower设备检查流量的文件故障排除	http://www.cisco.com/c/en/us/support/docs/
事件截屏（包括时间戳）	有关说明，请参阅本文
CLI会话的文本输出	有关说明，请参阅本文
如果提交误报案例，请提供要争议的项目（IP、URL、域）。	提供应执行争议的原因和证据。

下一步

如果已确定安全情报组件不是问题的原因，则下一步是排除访问控制策略规则的故障。

单击此处继续下一篇文章。