Firepower数据路径故障排除第7阶段：入侵策略

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七阶段，即入侵策略功能。

先决条件

- 本文适用于运行入侵策略的所有Firepower平台 **跟踪**功能仅在版本6.2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/

入侵策略阶段故障排除

使用“跟踪”工具检测入侵策略丢弃（仅FTD）

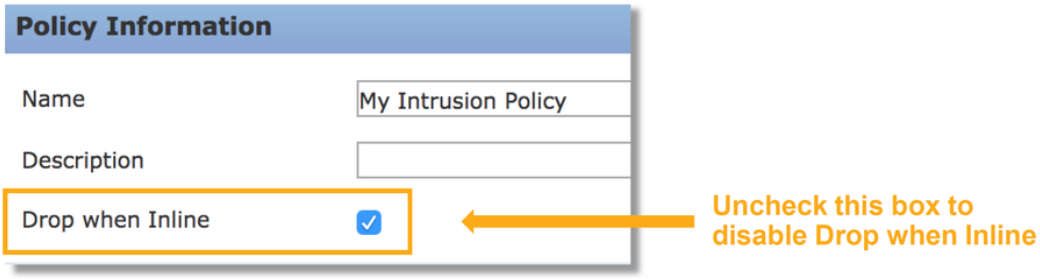
系统支持跟踪工具可从FTD命令行界面(CLI)运行。 这类似于访问控**制策略阶**段文章中提到的防火墙引擎调试工具，但它深入挖掘了Snort的内部工作原理。这对于查看相关流量是否触发任何入侵策略规则非常有用。

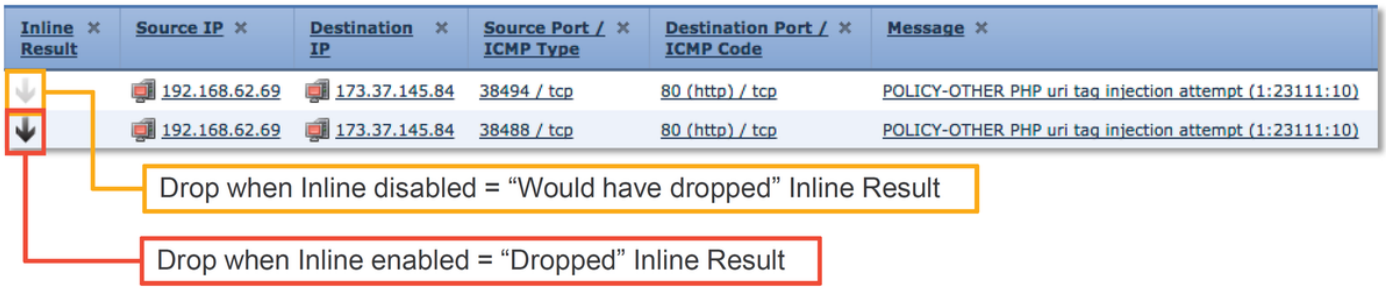
在以下示例中，来自IP地址为192.168.62.6的主机的流量被入侵策略规则阻止(在本例中为**1:23111**)

```
> system support trace

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.69
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

[… output omitted for brevity]

173.37.145.84-80 - 192.168.62.69-38488 6 Packet: TCP, ACK, seq 3594105349, ack 3856774965
173.37.145.84-80 - 192.168.62.69-38488 6 AppID: service HTTP (676), application Cisco (2655)
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://www.cisco.com/<?php") returned 0
…
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 match rule order 5, 'inspect it all', action Allow
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 allow action
192.168.62.69-38488 > 173.37.145.84-80 6 Firewall: allow rule, 'inspect it all', allow
192.168.62.69-38488 > 173.37.145.84-80 6 IPS Event: gid 1, sid 23111, drop
192.168.62.69-38488 > 173.37.145.84-80 6 Snort detect_drop: gid 1, sid 23111, drop
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 Deleting session
192.168.62.69-38488 > 173.37.145.84-80 6 NAP id 1, IPS id 0, Verdict BLACKLIST
192.168.62.69-38488 > 173.37.145.84-80 6 ===> Blocked by IPS
Verdict reason is sent to DAQ's PDTS
```

请注意，snort应用的操作已**删除**。当snort检测到丢弃时，该特定会话会被列入黑名单，以便也丢弃任何其他数据包。

Snort能够执行丢弃操作**的原**因是入侵策略中启用了“Drop when Inline”选项。这可在入侵策略的初始登录页中验证。在Firepower管理中心(FMC)中，导航至**策略>访问控制>入**侵，然后点击相关策略旁边的编辑图标。





如果禁用“Drop When Inline”，则snort不再丢弃违规数据包，但它仍会在入侵事件中以“Woul Have Dropped”的内联结果发出警报。

禁用“Drop When Inline”后，跟踪输出显示将丢弃**相关**流量会话的操作。

```
> system support trace


Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.69
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

[… output omitted for brevity]

173.37.145.84-80 - 192.168.62.69-38494 6 Packet: TCP, ACK, seq 2900935719, ack 691924600
173.37.145.84-80 - 192.168.62.69-38494 6 AppID: service HTTP (676), application Cisco (2655)
…
192.168.62.69-38494 > 173.37.145.84-80 6 AS 1 I 0 match rule order 5, 'inspect it all', action Allow
192.168.62.69-38494 > 173.37.145.84-80 6 AS 1 I 0 allow action
192.168.62.69-38494 > 173.37.145.84-80 6 Firewall: allow rule, 'inspect it all', allow
192.168.62.69-38494 > 173.37.145.84-80 6 IPS Event: gid 1, sid 23111, would drop
192.168.62.69-38494 > 173.37.145.84-80 6 Snort detect_drop: gid 1, sid 23111, would drop
192.168.62.69-38494 > 173.37.145.84-80 6 NAP id 1, IPS id 0, Verdict PASS
192.168.62.69-38494 > 173.37.145.84-80 6 ===> Blocked by IPS
Verdict reason is sent to DAQ's PDTS
```

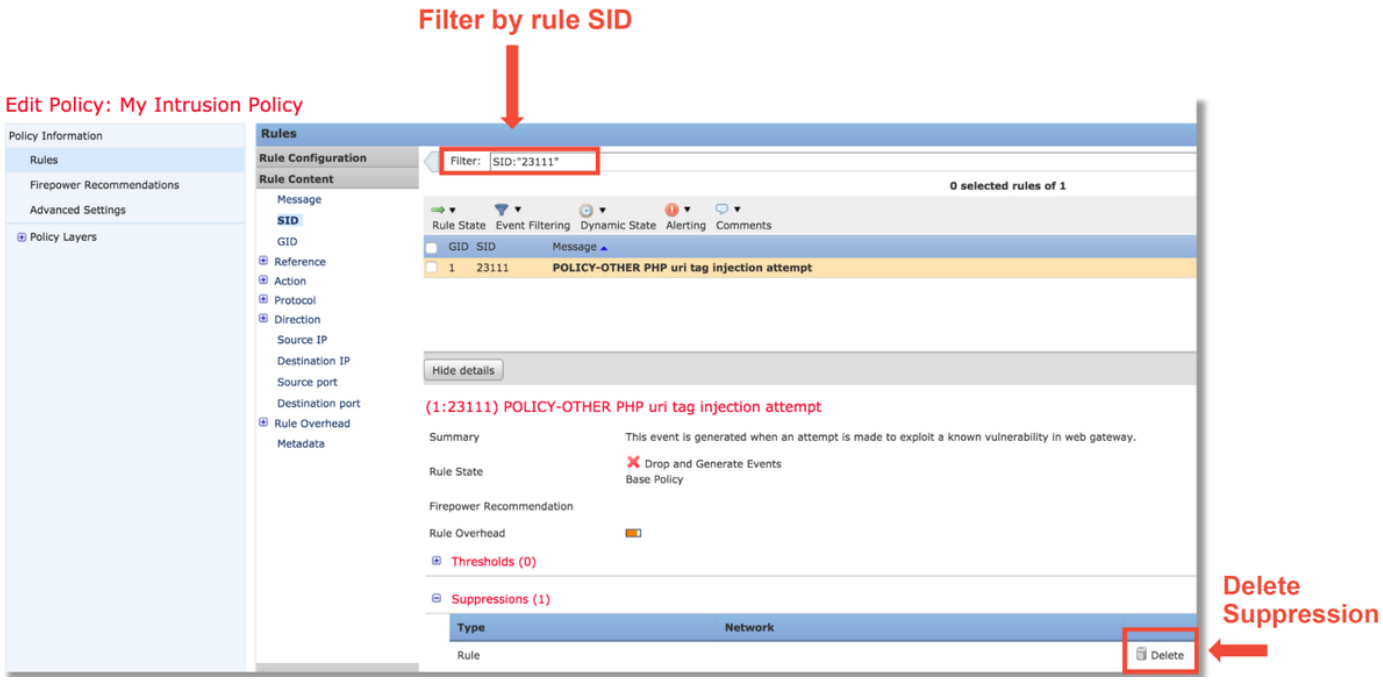
检查入侵策略中的抑制

Snort可以丢弃流量，而不将入侵事件发送到FMC（静默丢弃）。 这可通过配置抑制来**实现。**为了验证是否在入侵策略中配置了任何抑制，可以在后端检查专家外壳，如下所示。

```
[ Look for suppressions ]
> expert
$ cd /var/sf/detection_engines/*/
$ grep -H '^suppress' intrusion/*/snort_suppression.conf
intrusion/68acdfa2-e31a-11e6-b866-dd9e65c01d56/snort_suppression.conf:suppress gen_id 1, sig_id 23111

[ Get the policy name ]
$ grep Name intrusion/snort.conf.68acdfa2-e31a-11e6-b866-dd9e65c01d56
# Name        : My Intrusion Policy
```

请注意，名为“My Intrusion Policy”的入侵策略包含1:23111规则的抑制。因此，由于此规则，流量可以丢弃，而不会发生任何事件。这是跟踪实用程序可能有用的另一个原因，因为它仍显示发生的丢包。

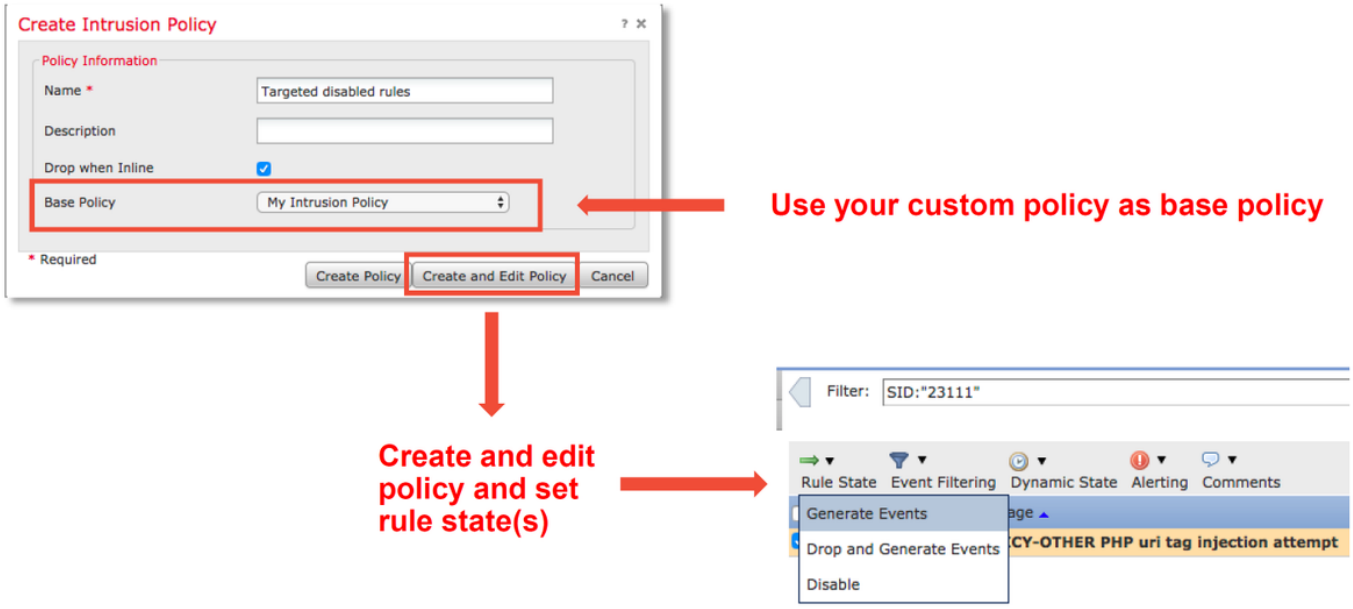
要删除抑制，可以在入侵策略规则视图中过滤相**关规**则。这将显示删除抑制的选项，如下所示。



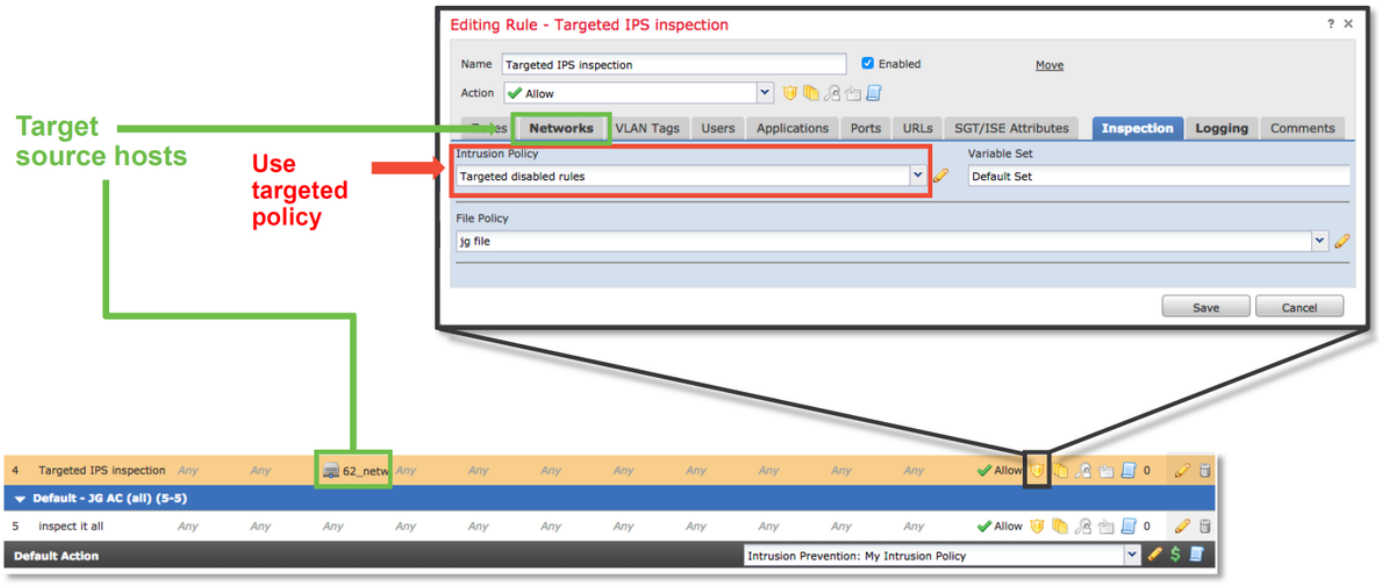
创建目标入侵策略

如果特定入侵策略规则丢弃了流量，则您可能不希望丢弃相关流量，但也不希望禁用该规则。解决方案是在禁用违规规则的情况下创建新的入侵策略，然后让其评估来自目标主机的流量。

下面是有关如何创建新入侵策略的图示(在“策略”(Policies)>“访问控制”(Access Control)>“入侵”(Intrusion)下)。



创建新入侵策略后，可在新的访问控制策略规则中使用该策略，该规则针对以前被原始入侵策略丢弃其流量的相关主机。



误报故障排除

常见案例场景是入侵事件误报分析。在打开误报案例之前，可以检查以下几项。

1.在“入侵事件的表视图”页中，单击相关事件的复选框

2.单击Download Packets(下载数据包)以获取Snort在触发入侵事件时捕获的数据包。

3.右键单击“消息”列中的规则名称，然后单击“规则文档”，查看规则语法和其他相关信息。

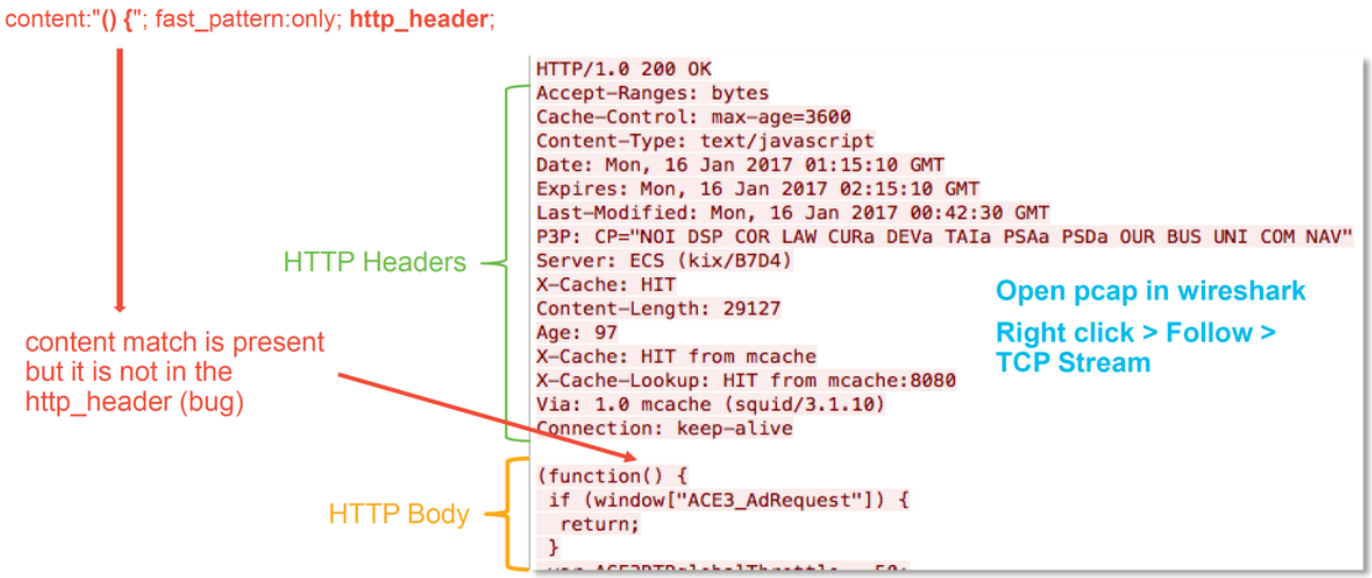
以下是触发上述示例中事件的规则的规则语法。可以根据从FMC下载的数据包捕获(PCAP)文件对此规则进行验证的规则部分以粗体显示。

alert **tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS** \
(msg：“OS-OTHER Bash CGI环境变量注入尝试";\
flow:to_server;established;\
内容："({";fast_pattern:only;http_header;\
元数据：policybalanced-ipsdrop、policy max-detect-ipsdrop、policy security-ipsdrop、ruleset community、service **http**;\
参考：cve，2014-6271;参考：cve，2014-6277;参考：cve，2014-6278;参考：cve，2014-7169;\
classtype:attemptedadmin;\
sid:31978;修订版5;)

然后，可以按照这些初始步骤执行分析过程，以查看流量是否应与触发的规则匹配。

1.检查流量匹配的访问控制规则。此信息作为Intrusion Events选项卡列的一部分找到。
2.查找在上述访问控制规则中使用的变量集。然后，可在“对象”(Objects)>“对象管理”(**Object Management)>“变量集”(Variable Sets)下查看变量集**
3.确保PCAP文件中的IP地址与变量匹配(在本例中，**包含在$EXTERNAL_NET变量**中的主机连接到包含在**$HOME_NET变量**配置中的主机)
4.对于**流**，可能需要捕获完整会话/连接。由于性能原因，Snort不会捕获完整的流。但是，在大多数情况下，可以放心地假设，如果具有flow:established触发的规则，则会话是在触发规则时建立的，因此在snort规则中验证此选项不需要完整的PCAP文件。但更好地理解触发它的原因可能是有用的。
5.对于**服务http**，请查看Wireshark中的PCAP文件，查看其是否类似于HTTP流量。如果已为主机启用网络发现，并且它以前看到过应用“HTTP”，则可能导致服务在会话上匹配。

考虑到这些信息，可以从FMC下载的数据包可以在Wireshark中进一步查看。可以评估PCAP文件以确定触发的事件是否为误报。



在上图中，规则检测到的内容存在于PCAP文件 — **"(){"**

但是，该规则指定应在数据包的HTTP报头 — http_header中检**测内容**

在本例中，内容在HTTP正文中找到。因此，这是误报。但是，从规则写错的意义上讲，它不是误报。规则正确，在这种情况下无法改进。此示例可能遇到Snort Bug，导致Snort出现缓冲区混淆。这意味着Snort错误地识别了http_headers。

在这种情况下，您可以检查设备运行的版本中是否存在任何Snort/IPS引擎的现有错误，如果没有，可以打开思科技术支持中心(TAC)的案例。要调查此类问题，需要完整的会话捕获，因为思科团队需要检查Snort如何进入该状态，而单个数据包无法完成。

真正的正面示例

下图显示了同一入侵事件的数据包分析。此时，事件为真正正正数，因为内容确实显示在HTTP报头中。

向TAC提供的数据

数据	说明
从Firepower设备检查流量的文件故障排除	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-
从FMC下载的数据包捕获	有关说明，请参阅本文
收集的任何相关CLI输出，如**跟踪输**出	有关说明，请参阅本文

后续步骤

如果已确定入侵策略组件不是问题的原因，则下一步是排除网络分析策略功能故障。

单击此处继续阅读上一篇文章。