Firepower数据路径故障排除第4阶段：访问控制策略

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四阶段，即访问控制策略(ACP)。 此信息适用于当前支持的所有Firepower平台和版本。

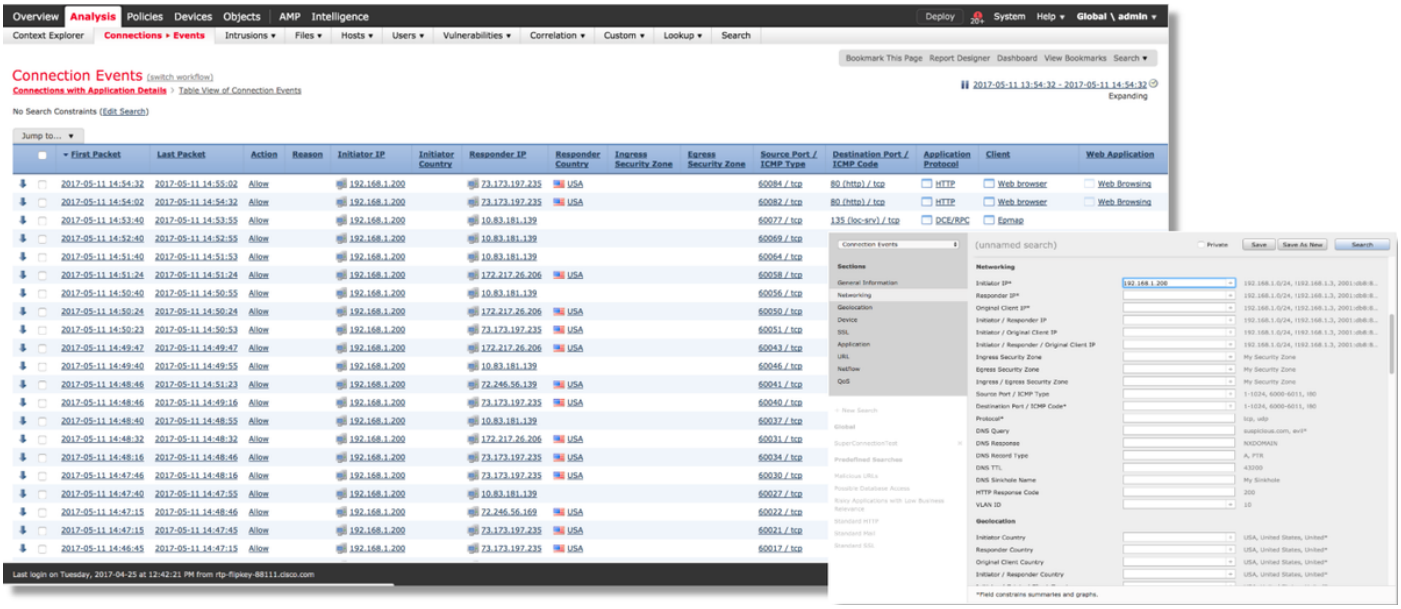
访问控制策略(ACP)阶段故障排除

一般来说，确定流匹配的ACP规则应该是相当直接的。可以查看Connection Events，以查看正在实施哪些规则/操作。如果这不能清楚地显示ACP对流量执行的操作，则可在Firepower命令行界面(CLI)上执行调试。

检查连接事件

在了解了入口和出口接口的流量应匹配以及流信息后，确定Firepower是否正在阻止流量的第一步是检查相关流量的连接事件。在Firepower管理中心的“分析”>“连接”>“事件”下可以**查看这些信息。**

> **注意：**在检查连接事件之前，请确保在ACP规则中启用日志记录。日志记录在每个Access Control Policy规则的“Logging”（记录）选项卡中以及Security Intelligence（安全情报）选项卡中配置。确保将可疑规则配置为将日志发送到“事件查看器”。 这也适用于默认操作。



通过点击“编辑搜索”(Edit Search)并按唯一源（发起方）IP过滤，您可以看到Firepower检测到的流。“操作”列显示此主机的流量的“允许”。

如果Firepower有意阻止流量，则操作将包含“阻止”一词。 单击“连接事件的表视图”可提供更多数据。如果操作为“阻止”，则可以查看连接事件中的以下字段：

— 原因

— 访问控制规则

快速缓解步骤

为了快速缓解据信由ACP规则引起的问题，可以执行以下操作：

- 为相关流量创建具有“信任”或“允许”操作的规则，并将其置于ACP的最顶部，或高于所有阻止规则。
- 使用包含“阻止”一词的操作临时禁用任何规则
- 如果Default Action（默认操作）设置为“Block All Traffic（阻止所有流量）”，请将其临时切换到“Network Discovery Only（仅网络发现）”

注意：这些快速缓解要求进行策略更改，而这些更改在所有环境中都可能实现。建议先尝试使用系统支持跟踪来确定流量匹配的规则，然后再进行策略更改。

调试ACP

可通过> system support firewall-engine-debug CLI实用程序对ACP操**作执行进一步的故障**排除。

注意：在Firepower 9300和4100平台上，可通过以下命令访问相关外壳：

```
# connect module 1 console
Firepower-module1> connect ftd
>
```

对于多实例，可使用以下命令访问逻辑设备CLI。

```
# connect module 1 telnet
Firepower-module1> connect ftd ftd1
正在连接到容器ftd(ftd1)控制台……输入“exit”以返回引导CLI
>
```

系统**支持防火墙引擎调试实**用程序为ACP评估的每个数据包都具有一个条目。它显示规则评估过程以及规则匹配或不匹配的原因。

> **注意**：在版本6.2及更高版本中，**系统支持跟**踪工具可以运行。它使用相同的参数，但包含更多详细信息。当出现“Enable firewall-engine-debug too?(**也启用防火墙引擎 — 调试？)”提示时，请务必**输入“y”。

示例 1：流量匹配信任规则

在以下示例中，使用system support firewall-engine-debug**评估SSH会话的建立**。

这是在Firepower设备上运行的ACP。

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN ...	Users	Applic...	Sourc...	Dest P...	URLs	ISE/S... Attrib...	Acti...
Mandatory - JG AC (all) (1-6)													
1	Trust ssh for host	Any	Any	192.168.0.7	Any	Any	Any	Any	Any	SSH	Any	Any	Trust
2	inspect	Any	Any	10.0.0.0/8	Any	Any	Any	Any	Any	Any	Any	Any	Allow
3	trust server backup	Any	Any	192.168.62.3	10.123.175.22	Any	Any	Any	Any	Any	Any	Any	Trust

ACP有三条规则。

1. 第一条规则是信任来自192.168.0.7的任何流量，并且SSH使用目标端口。
2. 第二条规则检查源自10.0.0.0/8的所有流量，其中网络条件基于XFF报头数据匹配（如网络对象旁的图标所示）
3. 第三条规则信任从192.168.62.3到10.123.175.22的所有流量

在故障排除场景中，分析从192.168.62.3到10.123.175.22的SSH连接。

期望会话与AC规则3“信任服务器备份”匹配。 问题是，此会话需要多少个数据包才能匹配此规则。是否需要第一个数据包中需要的所有信息来确定AC规则或多个数据包？如果是，需要多少？

在Firepower CLI上，输入以下命令以查看ACP规则评估流程。

```
>system support firewall-engine-debug

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.3
Please specify a client port:
Please specify a server IP address: 10.123.175.22
Please specify a server port: 22
Monitoring firewall engine debug messages
```

> **提示**：运行firewall-engine-debug时，最好尽可能多地填写**参数，以便仅将相关调试消息打印到屏幕。**

在下面的调试输出中，您将看到正在评估会话的前四个数据包。

SYN

SYN，ACK

确认

第一个SSH数据包（客户端到服务器）

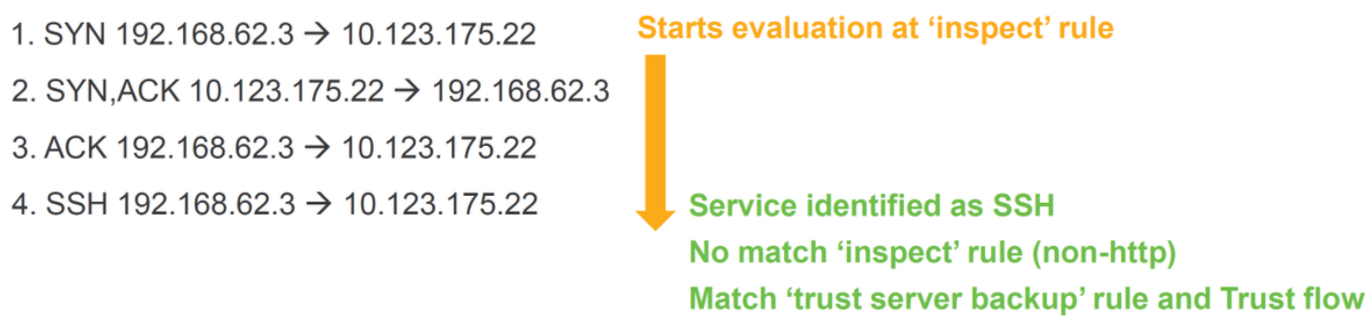
```
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, 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
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, 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
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 846, payload -1, client 2000000846, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust
```

此图进一步说明了调试逻辑。



对于此流，设备需要4个数据包才能匹配规则。

这是调试输出的详细说明。

- ACP评估过程从“inspect”规则开始，因为“trust ssh for host”规则不匹配，因为IP地址与要求不匹配。这是快速匹配，因为确定此规则是否匹配时需要的所有信息都存在于第一个数据包（IP和端口）中
- 在识别应用之前，无法确定该流量是否与“检查”规则匹配，因为在HTTP应用流量中找到X-Forwarded-For(XFF)信息，应用尚未知，因此这会将会话置于规则2的挂起状态，即挂起的应用数据。
- 在第四个数据包中确定应用后，“inspect”规则会导致不匹配，因为应用是SSH，而不是HTTP
- 然后根据IP地址匹配“信任服务器备份”规则。

总之，连接需要4个数据包才能匹配会话，因为它必须等待防火墙识别应用，因为规则2中包含应用约束。

如果规则2只有源网络，而不是XFF，则这将需要1个数据包来匹配会话。

如果可能，应始终将第1层至第4层规则置于策略中所有其他规则之上，因为这些规则通常需要1个

数据包才能做出决策。但是，您也可能注意到，即使仅使用第1-4层规则，也可能不止1个数据包与AC规则匹配，原因是URL/DNS安全情报。如果您启用了以上任一功能，则防火墙必须确定由AC策略评估的所有会话的应用，因为它必须确定这些会话是HTTP还是DNS。然后，它必须根据黑名单确定是否允许会话。

以下是firewall-engine-debug命令的截**断输出，该命令的相关字段以红色突出显示。**请注意用于获取已标识的应用名称的命令。

```
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, 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
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

[…omitted for brevity]

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 846, payload -1, client 2000000846, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust


[! How to map service/application ID to name]
> expert
$ grep "^846[^0-9]" /var/sf/appid/odp/appMapping.data
846 SSH 32 0 0 ssh
```

示例 2：与信任规则匹配的流量被阻止

在某些情况下，即使与ACP中的信任规则匹配，流量也可以被阻止。以下示例评估具有相同访问控制策略和主机的流量。

```
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, 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
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Deleting session

[!Session was deleted because we hit a drop IPS rule and blacklisted the flow.
This happened before AC rule was matched (Intrusion policy before AC rule match dropped).
Firewall engine will re-evaluate from top of AC policy to find a rule for logging decision]

192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 0, id 0 and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline
sgt tag: 0, ISE sgt id: 0, svc -1, payload -1, client -1, misc -1, user 9999997, icmpType 102, icmpCode 22
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 3, 'Trust ssh for host', src network and GEO
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust
```

Action	Reason	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Intrusion Events	Access Control Policy	Access Control Rule
Block	Intrusion Block	192.168.62.3	10.123.175.22	55654 / tcp	22 (ssh) / tcp				JG AC (all)	trust server backup

如上所示，**firewall-engine-debug**输出显示流量与“Trust”匹配，而Connection Events显示由于入侵策略规则(由于Reason列显示**Intrusion Block**而确定的**Block**操作。

出现此情况的原因是，在ACP的“高级”(Advanced)选**项卡中确定“访问控制”(Access Control)规则“设置”(Setting)之前使用的“入侵策略”(Intrusion Policy)。**在根据规则操作可以信任流量之前，相关的入侵策略会识别模式匹配并丢弃流量。但是，ACP规则评估结果与信任规则匹配，因为IP地址确实与“信任服务器备份”规则的条件匹配。

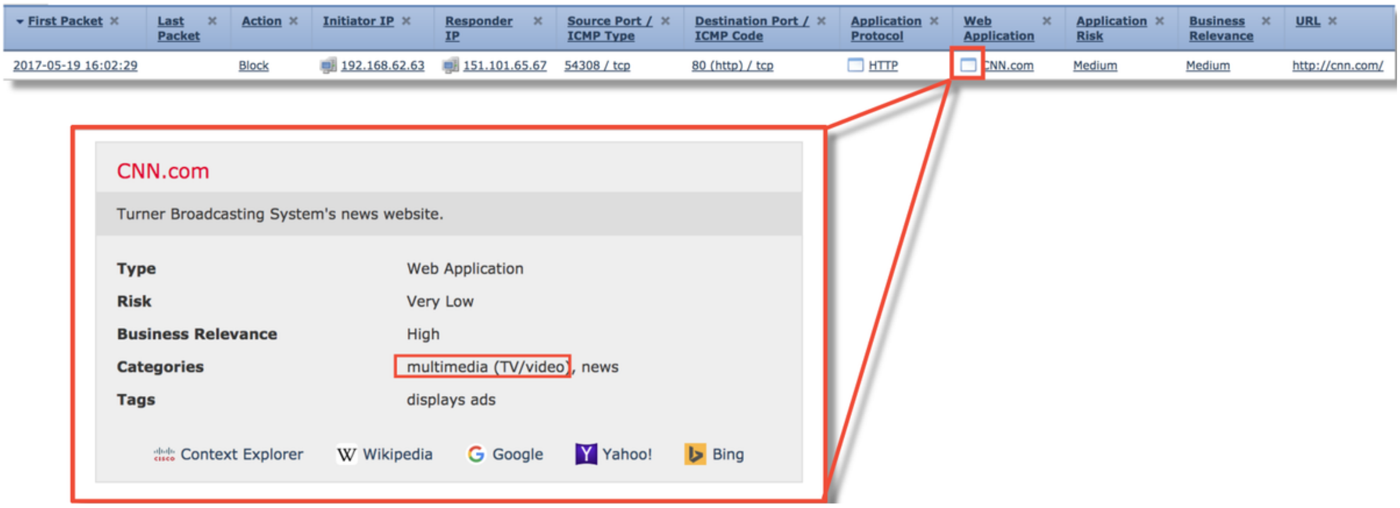
为了使流量不经受入侵策略检查，可将信任规则置于“检查”规则之上，这是两种情况下的最佳做法。由于“检查”规则的匹配和不匹配需要应用标识，因此在确定访问控制规则之前使用的**入侵策略**用于由相同规则评估的流量。将“信任服务器备份”规则置于“检查”规则之上会导致当发现第一个数据包时流量与规则匹配，因为该规则基于IP地址，可在第一个数据包中确定。因此，在确**定访问控制规**

则之前使用的入侵策略不需要使用。

情形 3：应用标记阻止的流量

在此场景中，用户报告cnn.com被阻止。但是，没有阻止CNN的具体规则。连接事件(Connection Events)与**firewall-engine-debug**输出一起显示阻止的原因。

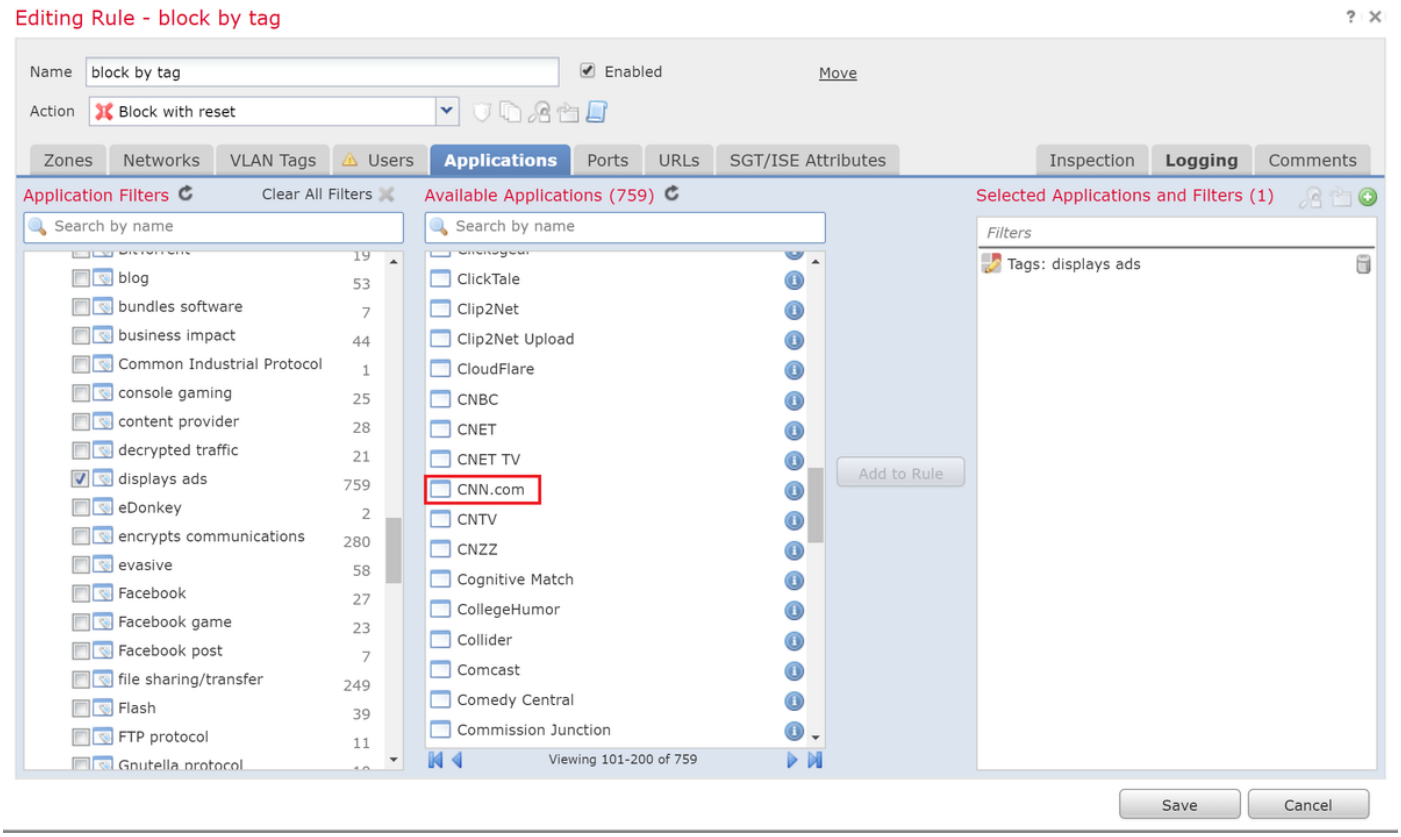
首先，连接事件在应用字段旁边有一个信息框，显示有关应用的信息以及Firepower如何对所述应用进行分类。



考虑到此信息，**将运行firewall-engine-debug**。在调试输出中，流量根据应用标记被阻止。

```
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 New session
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, 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
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, 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
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, 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
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://cnn.com/") returned 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0(0) -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 676, payload 1190, client 638, misc 0, user 9999997, url http://cnn.com/, xff
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 match rule order 4, 'block by tag', action Block
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 sending block response of 605 bytes
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Deleting session
```

即使没有明确阻止http://cnn.com的规则，标记**的**显示广告在ACP规则的“应**用**”选项卡内被阻止。



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-
系统支持firewall-engine-debug和system-support-trace输出	有关说明，请参阅本文
访问控制策略导出	导航至**系统>工具>导入/导**出，选择访问控制策略，然后单击**导**

警告：如果ACP包含SSL策略，请在导出之前从ACP中删除SSL策略，以避免泄露敏感PKI信息

下一步：排除SSL策略层故障

如果SSL策略正在使用，而访问控制策略故障排除未显示问题，则下一步是排除SSL策略故障。