Firepower数据路径故障排除第2阶段：DAQ层

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。

在本文中，我们将看到Firepower数据路径故障排除的第二阶段：DAQ（数据采集）层。

平台指南

下表介绍本文所涵盖的平台。

平台代码名称	描述	适用 Hardware 平台	备注
SFR	已安装带Firepower服务(SFR)模块的ASA。	ASA-5500-X系列	不适用
FTD（全部）	适用于所有Firepower威胁防御(FTD)平台	ASA-5500-X系列、虚拟NGFW平台、FPR-2100、FPR-9300、FPR-4100	不适用
FTD（非SSP和FPR-	安装在ASA或虚拟平台上的FTD映像	ASA-5500-X系列、虚拟NGFW平台、FPR-2100	不适用

2100）

FTD(SSP)	FTD作为逻辑设备安装在基于Firepower可扩展操作系统(FXOS)的机箱上	FPR-9300、FPR-4100	2100系列不使用FXOS机箱管理器

排除Firepower DAQ阶段故障

DAQ（数据获取）层是Firepower的组件，它将数据包转换为Snort能够理解的形式。它最初在数据包发送到snort时处理该数据包。因此，如果数据包正在进入但未退出Firepower设备，或数据包进入故障排除未产生有用结果，则DAQ故障排除可能非常有用。

在DAQ层捕获流量

要获得运行捕获的提示，必须首先使用SSH连接到SFR或FTD IP地址。

> **注意：**在FPR-9300和4100设备上，输入**connect ftd first**，最后出现第二个**>提示符**。您也可以通过SSH连接到FXOS机箱管理器IP，然后输入**connect module 1 console，**然后输入**connect ftd**。

本文介绍如何在Firepower DAQ级别收集数据包捕获。

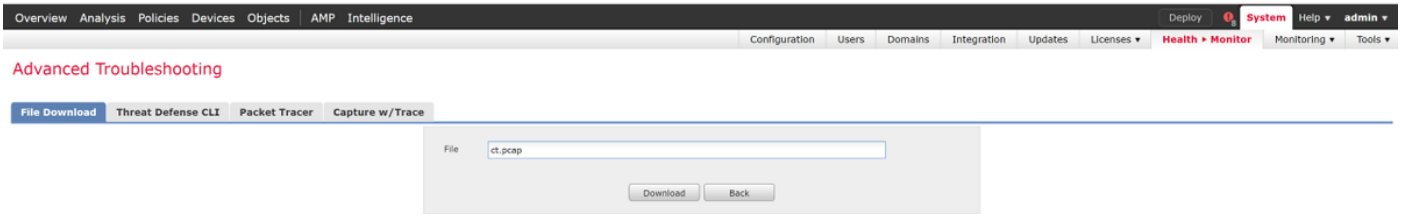
注意语法与ASA上使用的**capture**命令以及FTD平台的LINA端的语法不同。以下是从FTD设备运行的DAQ数据包捕获示例：

```
> system support capture-traffic

Please choose domain to capture traffic from:
  0 - br1
  1 - Router
  2 - my-inline inline set

Selection? 2

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: -s 1518 -w ct.pcap

> expert
admin@ciscoasa:~$ ls /ngfw/var/common/
ct.pcap
```

如上面的屏幕截图所示，PCAP格式ct.pcap的捕获被写入到**/ngfw/var/common目录(SFR平台上的**/var/common)。 这些捕获文件可以从>提示符中按照上述文章中的说明从Firepower设备中复制出来。

或者，在Firepower版本6.2.0及更高版本的Firepower管理中心(FMC)上，导航至“设备”>“设**备管理**”。然后，单击 图标，然后是高级故障排除>**文件下载**。

然后，可以输入捕获文件的名称，然后点击Download。



如何绕过Firepower

如果Firepower看到流量，但已确定数据包未离开设备或流量存在另一问题，则下一步是绕过Firepower检查阶段，确认其中一个Firepower组件正在丢弃流量。以下是在各种平台上使流量绕过Firepower的最快方法的细分。

SFR — 将Firepower模块置于仅监控模式

在托管SFR的ASA上，可以通过ASA命令行界面(CLI)或思科自适应安全设备管理器(ASDM)将

SFR模块置于仅监控模式。 这只会导致将实时数据包的副本发送到SFR模块。

要通过ASA CLI将SFR模块置于仅监控模式，必须首先通过运行**show service-policy sfr**命令确定用于SFR重定向的类映射和策略映射。

```
# show service-policy sfr

Global policy:
 Service-policy: global_policy
   Class-map: sfr
     SFR: card status Up, mode fail-open
       packet input 10000, packet output 9900, drop 100, reset-drop 0
```

输出显示global_policy策略映射正在“sfr”类映射上实施sfr fail-open操作。

> **注意**：“fail-close”也是SFR可以运行的模式，但并不常用，因为如果SFR模块关闭或无响应，它会阻止所有流量。

要将SFR模块置于仅监控模式，您可以发出以下命令来否定当前SFR配置并输入仅监控配置：

```
# configure terminal
(config)# policy-map global_policy
(config-pmap)# class sfr
(config-pmap-c)# no sfr fail-open
(config-pmap-c)# sfr fail-open monitor-only

INFO: The monitor-only mode prevents SFR from denying or altering traffic.

(config-pmap-c)# write memory
Building configuration...
```

将模块置于仅监控模式后，可以在show service-policy sfr输**出中验证该模**块。

```
# sh service-policy sfr

Global policy:
 Service-policy: global_policy
   Class-map: sfr
     SFR: card status Up, mode fail-open monitor-only
       packet input 0, packet output 100, drop 0, reset-drop 0
```

> **注意**：要将SFR模块重新置于内联模式，请在上面显示的**(config-pmap-c)#**提示符后发出**no sfr fail-open monitor-only**命令，然后发出**sfr {fail-open | fail-close}**命令。

或者，您也可以通过ASDM将模块置于仅监控模式，方法是导航到Configuration > **Firewall > Service Policy Rules。**然后，点击相关规则。然后，转到Rule Actions**页面**，并单击**ASA FirePOWER Inspection选**项卡。在此位置后，可**以选择“仅**监控”。

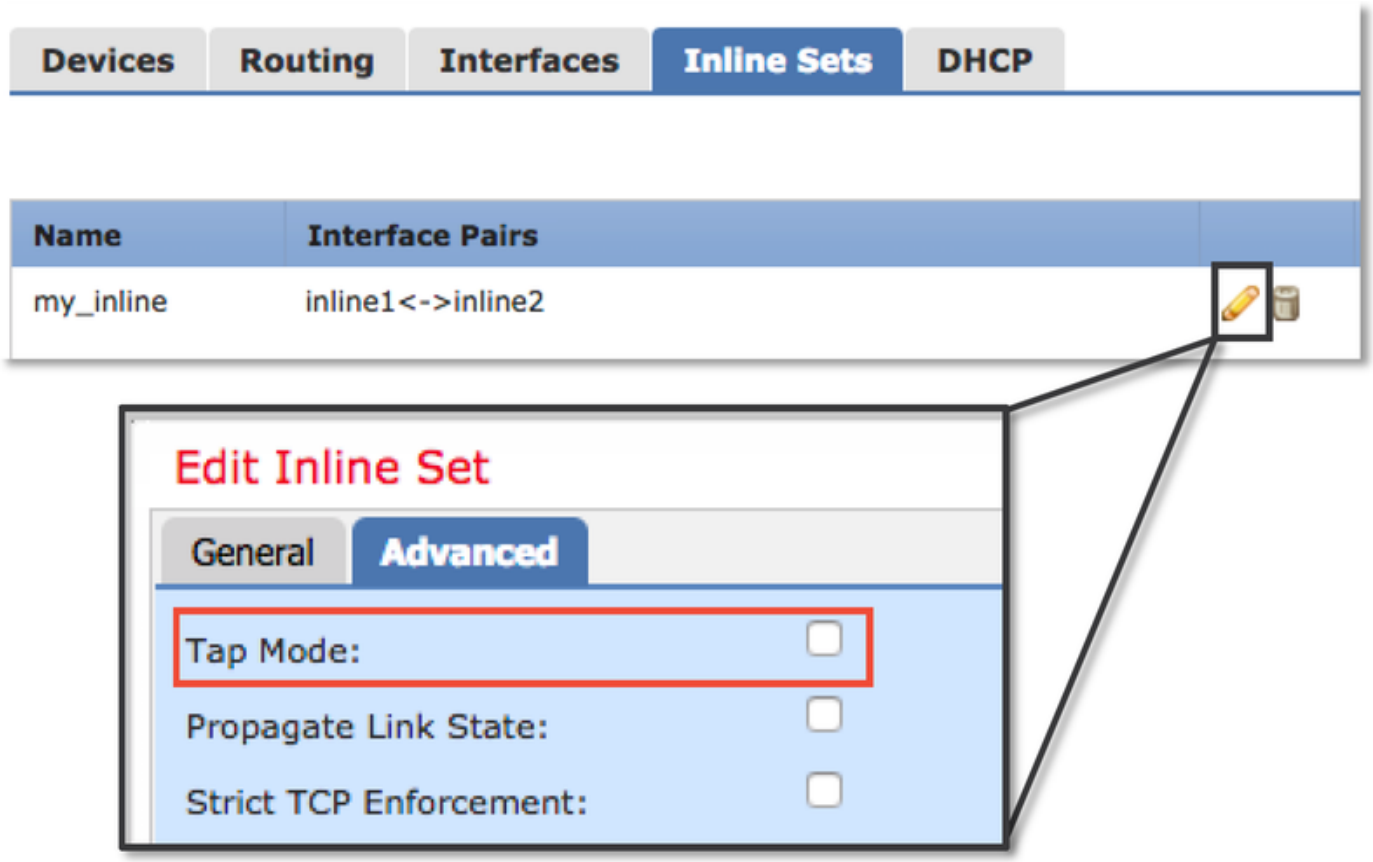
如果即使在SFR模块确认为处于仅监控模式后流量问题仍然存在，则Firepower模块不会导致问题。然后，可以运行Packet Tracer以进一步诊断ASA级别的问题。

如果问题不再存在，下一步是排除Firepower软件组件故障。

FTD（全部）— 将内联集置于TAP模式

如果流量通过内联集中配置的接口对传输，内联集可以置于TAP模式。这实际上会导致Firepower不对实时数据包采取操作。它不适用于没有内联集的路由器或透明模式，因为设备必须在将数据包发送到下一跳之前修改数据包，并且不能在不丢弃流量的情况下将其置于旁路模式。对于没有内联集的路由和透明模式，请继续执行packet tracer步骤。

要从FMC用户界面(UI)配置TAP模式，请导航至“设备”**>“设备管理”**，然后编辑相关设备。在内联**集选**项卡下，选中TAP模**式选项**。



如果TAP模式解决了问题，下一步是排除Firepower软件组件故障。

如果TAP模式无法解决问题，则问题将不在Firepower软件之外。然后，Packet Tracer可用于进一步诊断问题。

使用Packet Tracer排除模拟流量故障

Packet Tracer是一种实用程序，可帮助确定丢包的位置。它是一个模拟器，因此它执行人工数据包的跟踪。

SFR — 在ASA CLI上运行Packet Tracer

以下是如何在ASA CLI上为SSH流量运行packet-tracer的示例。有关packet tracer命令语法的更多详细信息，请参阅《ASA系列命令参考指南》中的此部分。

```
asa# packet-tracer input inside tcp 192.168.62.60 10000 10.10.10.10 ssh

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.151.37.1 using egress ifc  outside

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: SFR
Subtype:
Result: ALLOW
Config:
class-map inspection_default
 match any
policy-map global_policy
 class inspection_default
  sfr fail-open
service-policy global_policy global
Additional Information:
```

```
Phase: 6
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
class-map inspection_default
 match any
policy-map global_policy
 class inspection_default
  inspect icmp
service-policy global_policy global
Additional Information:

Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 756, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

在上例中，我们看到ASA和SFR模块都允许数据包，以及有关ASA如何处理数据包流的有用信息。

FTD（全部）— 在FTD CLI上运行Packet Tracer

在所有FTD平台上，可以从FTD CLI运行packet tracer命令。

```
> packet-tracer input inside tcp 192.168.62.60 10000 10.10.10.10 ssh

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.100.1 using egress ifc  outside
```

```
Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434433
access-list CSM_FW_ACL_ remark rule-id 268434433: ACCESS POLICY:
My_AC_Policy - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268434433: L7 RULE: Block urls
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will
be reached

Phase: 4
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Config:
class-map class-default
 match any
policy-map global_policy
 class class-default
  set connection advanced-options UM_STATIC_TCP_MAP
service-policy global_policy global
Additional Information:
```

```
Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
object network 62_network
 nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 192.168.62.60/10000 to 192.168.100.51/10000

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 8
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 10
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 612016, packet dispatched to next module
```

```
Phase: 11
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 12
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: TCP, SYN, seq 1821549761
Reputation: packet blacklisted, drop
Snort: processed decoder alerts or actions queue, drop
IPS Event: gid 136, sid 1, drop
Snort detect_drop: gid 136, sid 1, drop
NAP id 1, IPS id 0, Verdict BLACKLIST, Blocked by Reputation
Snort Verdict: (black-list) black list this flow
```

在本例中，Packet Tracer确实显示丢弃的原因。在这种情况下，它是Firepower中安全情报功能中阻止数据包的IP黑名单。下一步是对导致丢弃的单个Firepower软件组件进行故障排除。

使用捕获和跟踪对实时流量进行故障排除

实时流量也可以通过带跟踪功能的捕获进行跟踪，该功能可通过CLI在所有平台上使用。以下是对SSH流量运行带跟踪的捕获的示例。

```
> capture ssh_traffic trace interface inside match tcp any any eq 22
> show capture ssh_traffic

7 packets captured

   1: 01:17:38.498906       192.168.62.70.48560 > 10.83.180.173.22: S 4250994241:4250994241(0) win 29200 <mss 1460,sackOK,timestamp 1045829951
0,nop,wscale 7>
   2: 01:17:38.510898       10.83.180.173.22 > 192.168.62.70.48560: S 903999422:903999422(0) ack 4250994242 win 17896 <mss 1380,sackOK,timestamp
513898266 1045829951,nop,wscale 7>
   3: 01:17:38.511402       192.168.62.70.48560 > 10.83.180.173.22: . ack 903999423 win 229 <nop,nop,timestamp 1045829956 513898266>
   4: 01:17:38.511982       192.168.62.70.48560 > 10.83.180.173.22: P 4250994242:4250994283(41) ack 903999423 win 229 <nop,nop,timestamp
1045829957 513898266>
   5: 01:17:38.513294       10.83.180.173.22 > 192.168.62.70.48560: . ack 4250994283 win 140 <nop,nop,timestamp 513898268 1045829957>
   6: 01:17:38.528125       10.83.180.173.22 > 192.168.62.70.48560: P 903999423:903999444(21) ack 4250994283 win 140 <nop,nop,timestamp 513898282
1045829957>
   7: 01:17:38.528613       192.168.62.70.48560 > 10.83.180.173.22: . ack 903999444 win 229 <nop,nop,timestamp 1045829961 513898282>
```

```
> show capture ssh_traffic packet-number 4 trace

7 packets captured

   4: 01:17:38.511982       192.168.62.70.48560 > 10.83.180.173.22: P
4250994242:4250994283(41) ack 903999423 win 229 <nop,nop,timestamp
1045829957 513898266>
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
```

```
Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found flow with id 626406, using existing flow

Phase: 4
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'
```

```
Phase: 5
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: TCP, ACK, seq 4250994242, ack 903999423
AppID: service SSH (846), application unknown (0)
Firewall: starting rule matching, zone 1 -> 2, geo 0 -> 0, vlan 0, sgt 65535, user 2, icmpType 0, icmpCode 0
Firewall: trust/fastpath rule, id 268435458, allow
NAP id 1, IPS id 0, Verdict WHITELIST
Snort Verdict: (fast-forward) fast forward this flow

Result:
input-interface: inside
input-status: up
input-line-status: up
Action: allow
```

在本示例中，跟踪捕获中的第四个数据包，因为这是定义了应用数据的第一个数据包。如图所示，数据包最终被snort列入白名单，这意味着无需对流进行进一步的snort检测，并且总体允许。

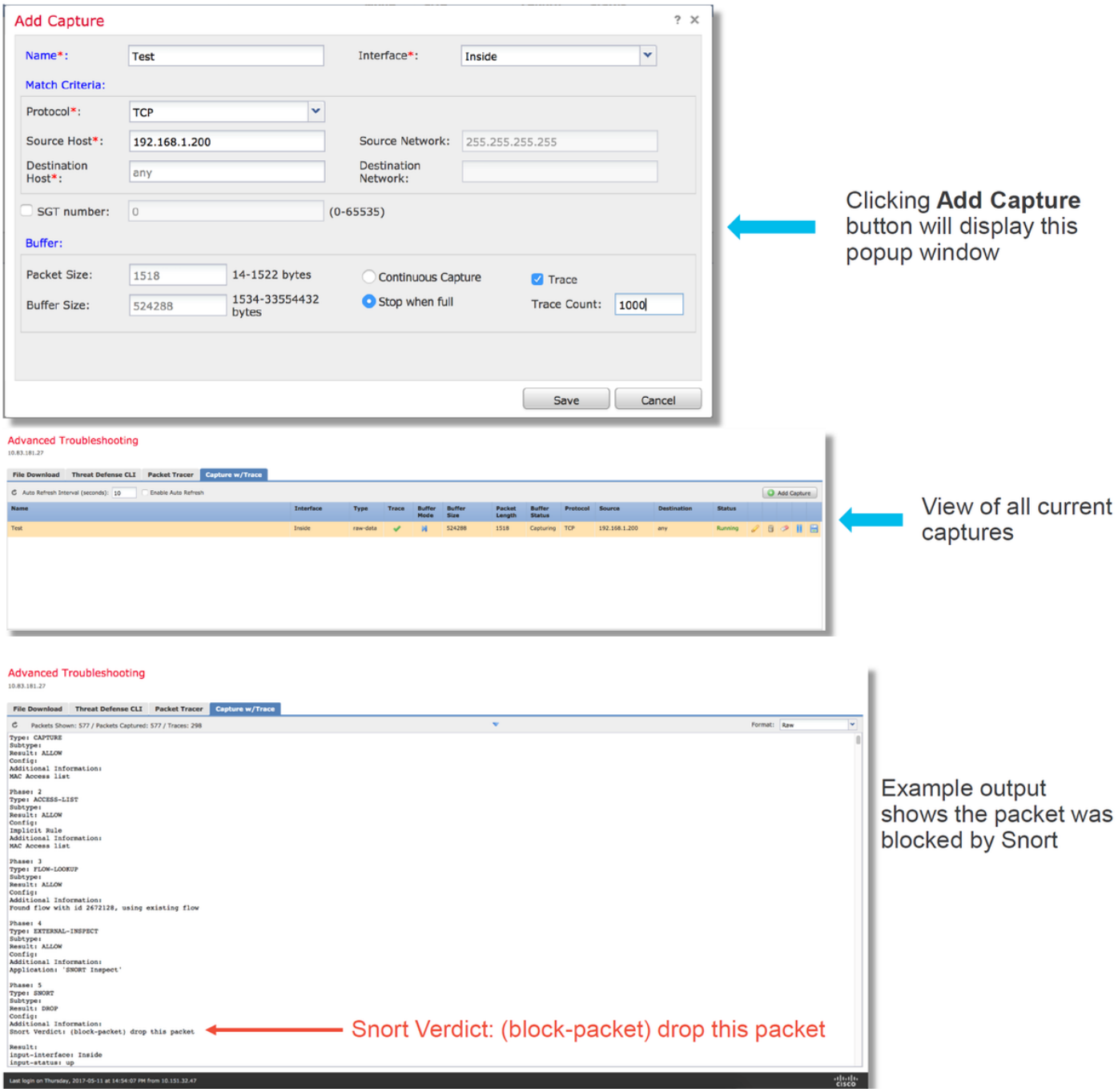
有关使用跟踪语法捕获的详细信息，请参阅《ASA系列命令参考指南》中的此部分。

FTD（全部）— 在FMC GUI上运行带跟踪的捕获

在FTD平台上，可在FMC UI上运行带跟踪的捕获。要访问该实用程序，请导航至**Devices > Device Management**。

然后，单击  图标，然后是高级故障排除**>捕获，带跟踪。**

以下是如何通过GUI运行带跟踪的捕获的示例。



如果带跟踪的捕获显示丢包的原因，则下一步是对各个软件组件进行故障排除。

如果它不清楚显示问题的原因，则下一步是快速通过流量。

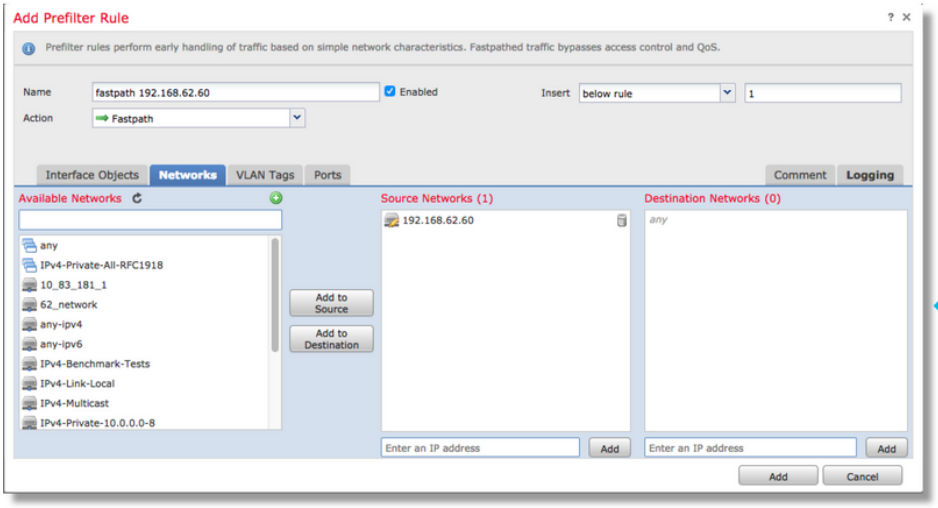
在FTD中创建PreFilter快速路径规则

在所有FTD平台上，都有预过滤器策略，可用于转移来自Firepower(snort)检测的流量。

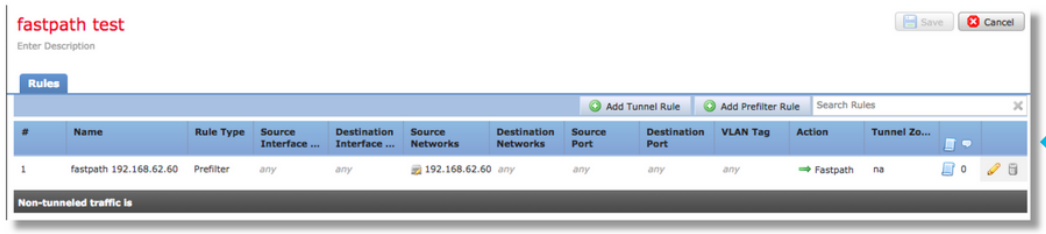
在FMC上，此字段位于**Policies > Access Control > Prefilter**下。无法编辑默认预过滤器策略，因此需要创建自定义策略。

之后，新创建的预过滤器策略需要与访问控制策略关联。这在“预过滤器策略设置”(Prefilter Policy Settings)部分的访问控制策略(Access Control Policy)的“高级”(Advanced)选**项卡中进行**配置。

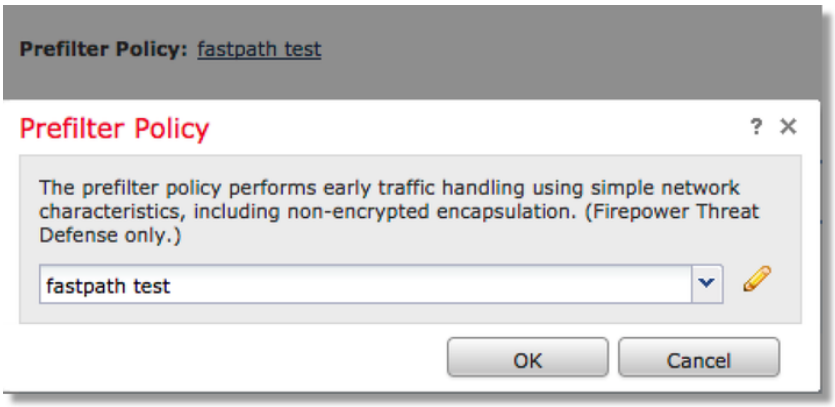
以下是如何在预过滤器策略中创建快速路径规则并验证命中计数的示例。



Clicking **Add Prefilter Rule** button will display this popup window.



View of all rules in the **fastpath test** Prefilter policy



From AC policy make sure the Prefilter Policy is set to the custom Prefilter Policy

View of connection events matching prefilter rule

First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Prefilter Policy	Tunnel/Prefilter Rule
2017-05-15 16:05:14	2017-05-15 16:05:14	Fastpath		192.168.62.60	10.83.180.173	48480 / tcp	22 (ssh) / tcp	fastpath test	fastpath 192.168.62.60

单击此处了解有关预过滤器策略的操作和配置的更多详细信息。

如果添加预过滤器策略可解决流量问题，则可根据需要保留规则。但是，没有对该流进行进一步检查。需要对Firepower软件进行进一步的故障排除。

如果添加预过滤器策略无法解决问题，则可以再次运行带跟踪步骤的数据包以跟踪数据包的新路径。

向TAC提供的数据

数据	说明
命令输出	有关说明，请参阅本文

数据包捕获	对于ASA/LINA:https://www.cisco.com/c/en/us/support/docs/sec asa-00.html 对于Firepower:http://www.cisco.com/c/en/us/support/docs/secu sourcefire-00.html
ASA“show tech”输出	登录ASA CLI并将终端会话保存到日志中。输入**show** techcomm 此文件可使用此命令保存到磁盘或外部存储系统。 show tech | redirect disk0:/show_tech.log
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-

下一步

如果已确定Firepower软件组件是问题的原因，则下一步是从安全情报开始系统地排除每个组件。

单击此处继续阅读下一个指南。