Firepower数据路径故障排除第1阶段：数据包入口

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，我们将了解Firepower数据路径故障排除的第一阶段，即数据包入口阶段。

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（非SSP和FPR-2100）	安装在自适应安全设备(ASA)或虚拟平台上的Firepower威胁防御(FTD)映像	ASA-5500-X系列，虚拟NGFW平台	不适用
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

数据包入口阶段故障排除

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，或者设备无法创建出口数据包（例如，缺少ARP条目）。

确定相关流量

排除数据包入口阶段故障的第一步是隔离流量和问题流量所涉及的接口。包括：

流信息	接口信息
协议 源 IP 地址 源端口 目的 IP 目标端口	Ingress 接口 Egress 接口

例如：

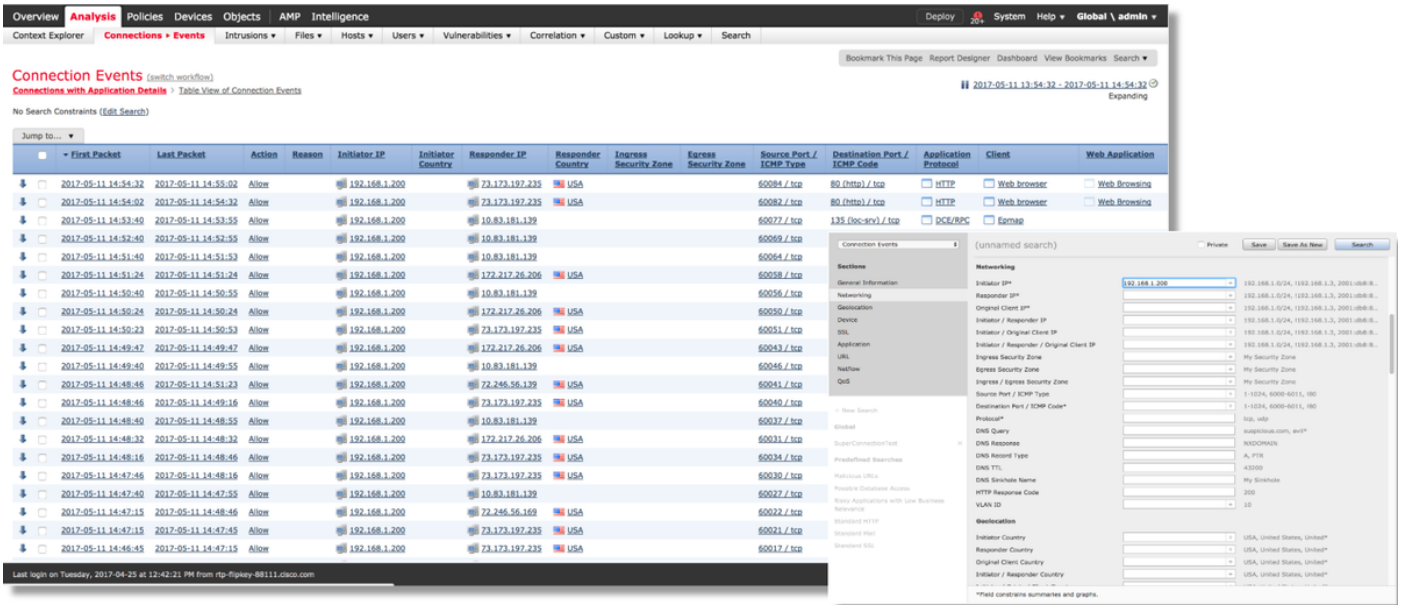
```
TCP inside 172.16.100.101:38974 outside 192.168.1.10:80
```

> **提示：**由于每个流中的源端口通常不同，因此您可能无法确定确切的源端口，但目标（服务器）端口应该足够。

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是否阻止流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，请确保在访问控制策略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”。



在上例中，点击“编辑搜索”，并添加唯一源（发起方）IP作为过滤器，以查看Firepower检测到的流。“操作”列显示此主机流量的“允许”。

如果Firepower有意阻止流量，则操作包含“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“Block”，则可以记录连接事件中的以下字段：

— 原因

— 访问控制规则

这与相关事件中的其他字段相结合，有助于缩小阻止流量的组件范围。

有关排除访问控制规则故障的详细信息，请单击此处。

在入口和出口接口上捕获数据包

如果没有事件，或尽管连接事件显示规则操作“允许”或“信任”，但仍怀疑Firepower被阻止，则数据路径故障排除将继续。

以下是有关如何在上述各种平台上运行入口和出口数据包捕获的说明：

SFR — 在ASA接口上捕获

由于SFR模块只是运行在ASA防火墙上的模块，因此最好先捕获ASA的入口和出口接口，以确保入口也正在流出的相同数据包。

本文包含有关如何在ASA上执行捕获的说明。

如果确定正在输入ASA的数据包未退出，请继续进入故障排除的下一阶段（DAQ阶段）。

> **注意**：如果在ASA入口接口上看到数据包，则可能需要检查连接的设备。

FTD（非SSP和FPR-2100）— 在入口和出口接口上捕获

在非SSP FTD设备上捕获与在ASA上捕获类似。但是，您可以直接从CLI初始提示符运行capture命令。排除丢包故障时，建议在捕获中添加“trace”选项。

以下是在端口22上为TCP流量配置入口捕获的示例：

```
> 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>
```

如果添加“trace”选项，则可以选择单个数据包以在系统中跟踪，以查看它如何得出最终判定。它还有助于确保对数据包(如网络地址转换(NAT)IP修改)进行适当修改，并且已选择适当的出口接口。

```
> 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
```

在上面的示例中，我们看到流量进入Snort检测，并且最终达到允许判定，并且总体通过设备。由于流量可以双向查看，因此您可以确保流量流经此会话的设备，因此可能不需要出口捕获，但您也可以在此捕获出口捕获，以确保流量正确流出，如跟踪输出所示。

> **注意：**如果设备无法创建出口数据包，则跟踪操作仍为“允许”，但在出口接口捕获上未创建或看到该数据包。这是FTD没有下一跳或目的IP的ARP条目（如果最后一个条目直接连接）的非常常见的场景。

FTD(SSP) — 在逻辑FTD接口上捕获

在SSP平台上可以执行上述在FTD上生成数据包捕获的相同步骤。您可以使用SSH连接到FTD逻辑接口的IP地址，并输入以下命令：

```
Firepower-module1> connect ftd
>
```

您还可以使用以下命令从FXOS命令提示符导航到FTD逻辑设备外壳：

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

如果使用Firepower 9300，则模块编号可能因使用的安全模块而异。这些模块最多可支持3个逻辑设备。

如果使用多实例，则“connect”命令中必须包含实例ID。Telnet命令可用于同时连接到不同的实例。

```
# connect module 1 telnet
Firepower-module1>connect ftd ftd1
Connecting to container ftd(ftd1) console... enter "exit" to return to Boot CLI
>
```

检查接口错误

在此阶段，还可以检查接口级别问题。如果入口接口捕获中丢失了数据包，则这特别有用。如果发现接口错误，检查连接的设备会很有帮助。

SFR — 检查ASA接口

由于FirePOWER(SFR)模块基本上是运行在ASA上的虚拟机，因此会检查实际ASA接口是否存在错误。有关检查ASA上接口统计信息的详细信息，请参阅本ASA系列命令参考指南部分。

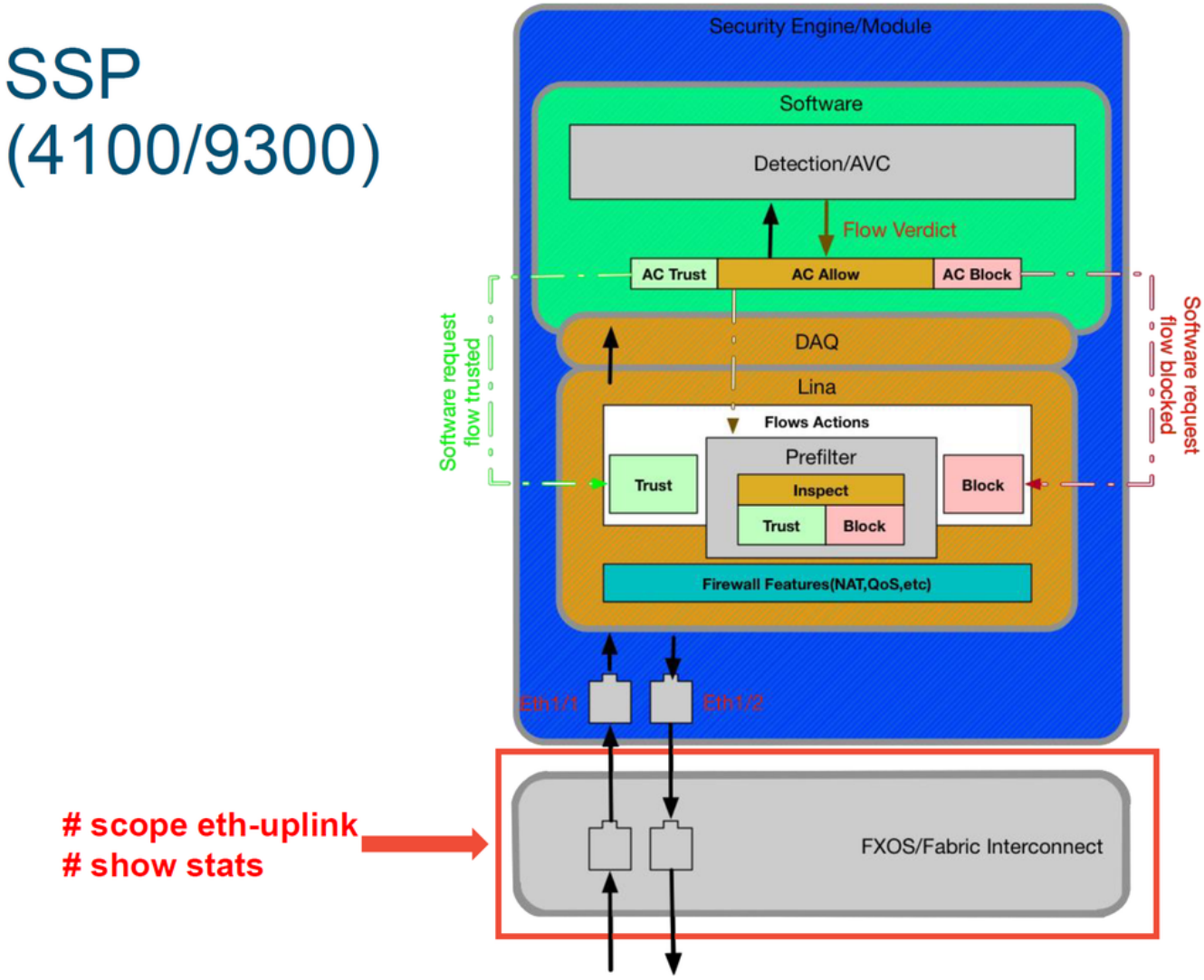
FTD（非SSP和FPR-2100）— 检查接口错误

在非SSP FTD设备上，**> show interface**命令可以从初始命令提示符运行。相关输出以红色突出显示。

```
> show interface
InterfaceGigabitEthernet0/0 "outside", is up, line protocol is up
    Hardware is i82545EM rev01, BW 1000 Mbps, DLY 10 usec
            Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
             Input flow control is unsupported, output flow control is off
             MAC address 000c.2961.f78b, MTU 1500
             IPS Interface-Mode: inline, Inline-Set: InlineSet
             IP address unassigned
             20686130 packets input, 8859847035 bytes, 0 no buffer
             Received 0 broadcasts, 0 runts, 0 giants
             2312 input errors, 0 CRC, 0 frame, 12313 overrun, 0 ignored, 0 abort
             0 pause input, 0 resume input
             0 L2 decode drops
             6485096 packets output, 1480276815 bytes, 0 underruns
             0 pause output, 0 resume output
             1341 output errors, 45635 collisions, 1 interface resets
             0 late collisions, 0 deferred
             0 input reset drops, 0 output reset drops
             input queue (blocks free curr/low): hardware (509/362)
             output queue (blocks free curr/low): hardware (511/415)
  Traffic Statistics for "outside":
             20686131 packets input, 8485139715 bytes
             6485096 packets output, 1375761699 bytes
             4702172 packets dropped
        1 minute input rate 2 pkts/sec,  999 bytes/sec
        1 minute output rate 0 pkts/sec,  78 bytes/sec
        1 minute drop rate, 0 pkts/sec
        5 minute input rate 3 pkts/sec,  1222 bytes/sec
        5 minute output rate 1 pkts/sec,  319 bytes/sec
        5 minute drop rate, 1 pkts/sec
```

FTD(SSP) — 导航数据路径以查找接口错误

9300和4100 SSP平台具有内部交换矩阵互联，该互联首先处理数据包。



值得检查初始数据包入口是否存在任何接口问题。这些命令要在FXOS系统CLI上运行，以便获取此信息。

```
ssp# scope eth-uplink
ssp /et-uplink # show stats
```

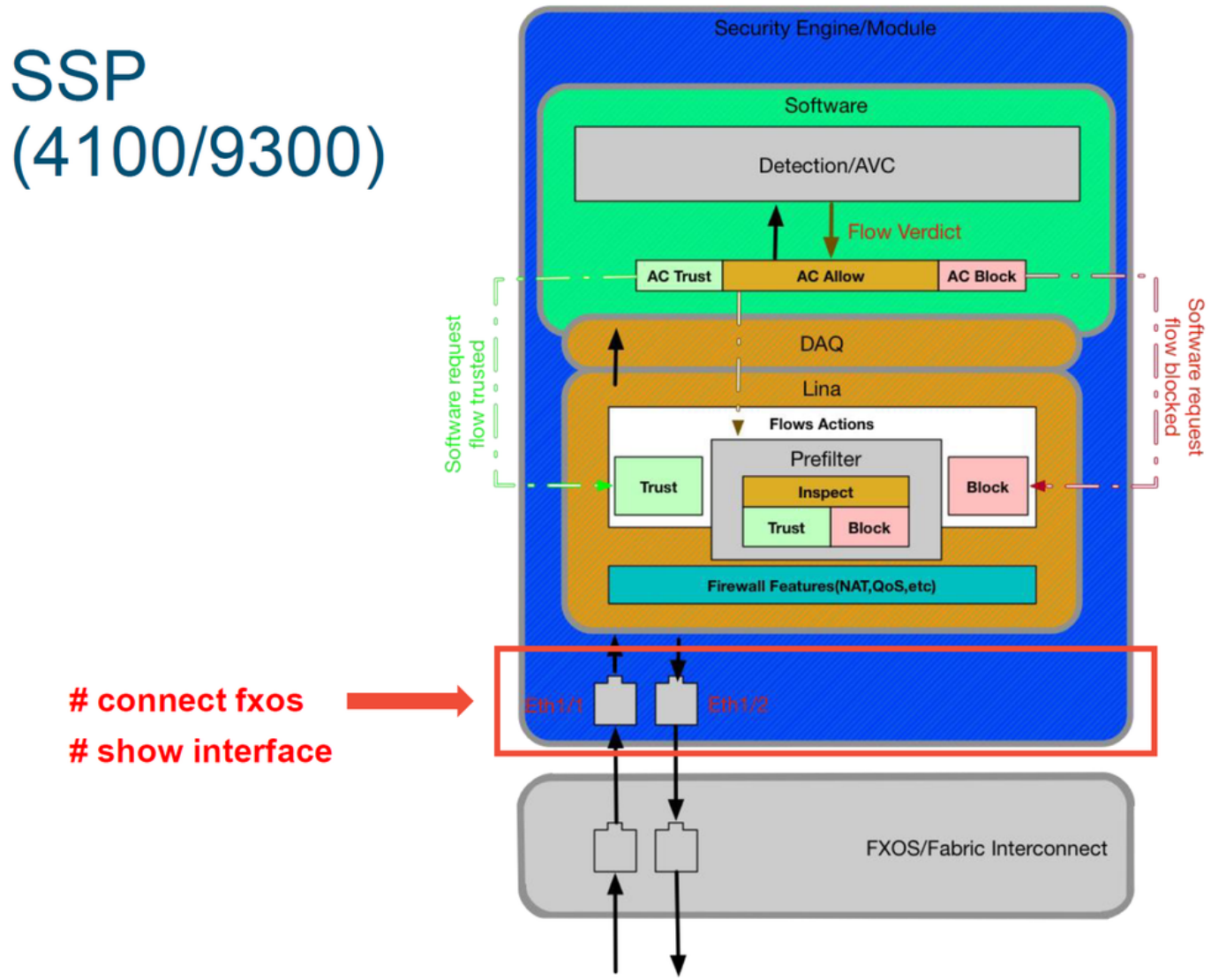
这是输出示例。

```
ssp# scope eth-uplink

ssp /eth-uplink # show stats

Ether Error Stats:
    Time Collected: 2017-05-15T14:13:46.032
    Monitored Object: fabric/lan/A/pc-44/err-stats
    Suspect: No
    Rcv (errors): 0
    Align (errors): 0
    Fcs (errors): 0
    Xmit (errors): 0
    Under Size (errors): 0
    Out Discard (errors): 0
    Int Mac Tx (errors): 0
    Int Mac Rx (errors): 0
    Deferred Tx (errors): 0
    Thresholded: Xmit Delta Min

Time Collected: 2017-05-15T14:13:46.032
    Monitored Object: fabric/lan/A/pc-48/err-stats
    Suspect: No
    Rcv (errors): 0
    Align (errors): 0
    Fcs (errors): 0
    Xmit (errors): 0
    Under Size (errors): 0
    Out Discard (errors): 0
    Int Mac Tx (errors): 0
    Int Mac Rx (errors): 0
    Deferred Tx (errors): 0
    Thresholded: Xmit Delta Min
```

```
Ether Loss Stats:
    Time Collected: 2017-05-15T14:13:46.032
    Monitored Object: fabric/lan/A/pc-44/loss-stats
    Suspect: No    Single Collision (errors): 0
    Multi Collision (errors): 0
    Late Collision (errors): 0
    Carrier Sense (errors): 0
    Giants (errors): 0
    Symbol (errors): 0
    SQE Test (errors): 0
    Excess Collision (errors): 0
    Thresholded: 0

    Time Collected: 2017-05-15T14:13:46.032
    Monitored Object: fabric/lan/A/pc-48/loss-stats
    Suspect: No    Single Collision (errors): 0
    Multi Collision (errors): 0
    Late Collision (errors): 0
    Carrier Sense (errors): 0
    Giants (errors): 0
    Symbol (errors): 0
    SQE Test (errors): 0
    Excess Collision (errors): 0
    Thresholded: 0
```

在交换矩阵互联在入口时处理数据包后，会将其发送到接口，这些接口分配给托管FTD设备的逻辑设备。

以下是供参考的图：



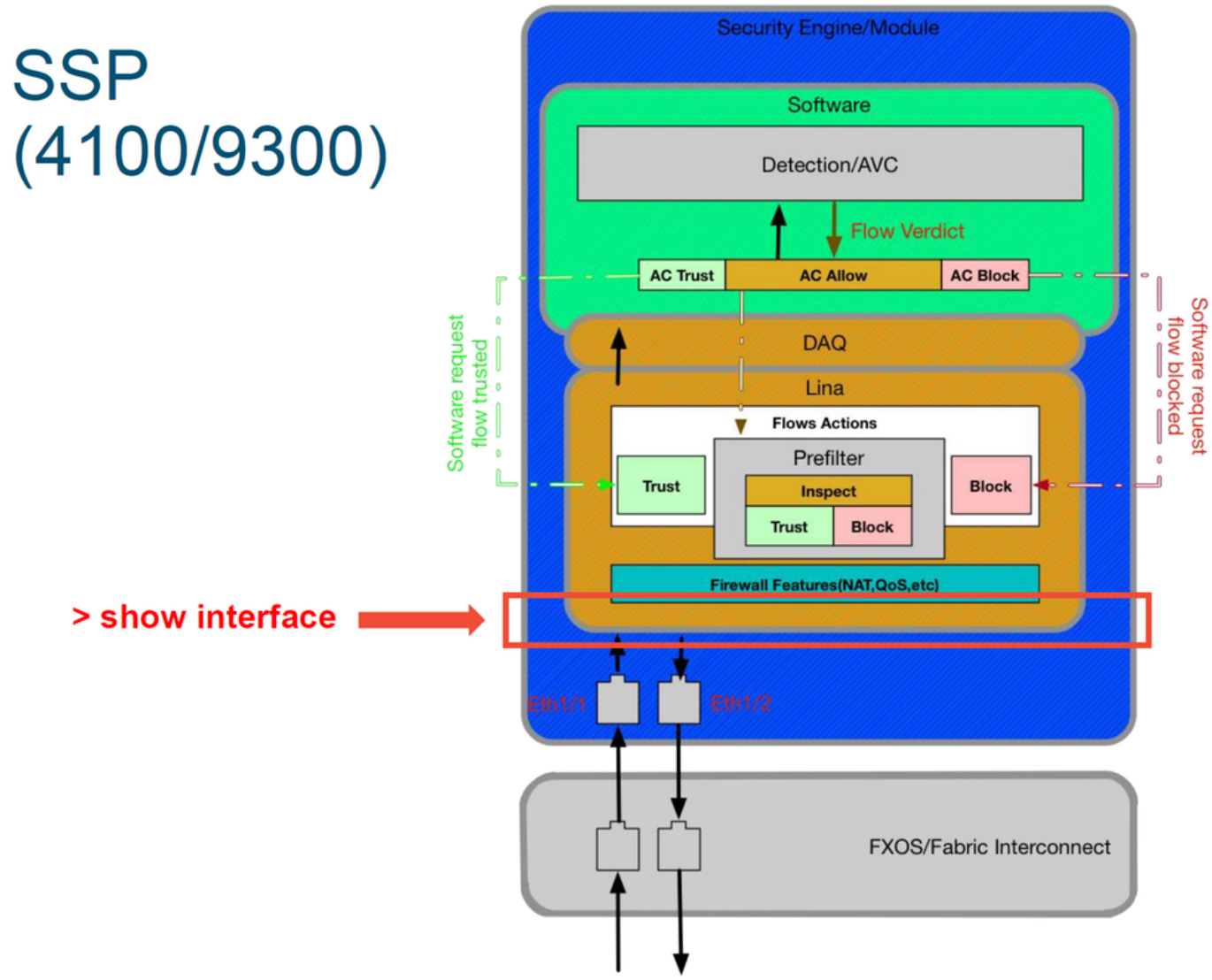
要检查接口级别问题，请输入以下命令：

```
ssp# connect fxos
ssp(fxos)# show interface Ethernet 1/7
```

以下是输出示例（以红色突出显示的可能问题）：

```
ssp# connect fxos

ssp(fxos)# show interface Ethernet 1/7
Ethernet1/7 is up
 Dedicated Interface
  Hardware: 1000/10000 Ethernet, address: 5897.bdb9.4080 (bia 5897.bdb9.4080)
  Description: U: Uplink
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec
  reliability 254/255, txload 1/255, rxload 1/255
  […Omitted for brevity]
  Last link flapped 14week(s) 4day(s)
  Last clearing of "show interface" counters never
  2 interface resets
  30 seconds input rate 1352 bits/sec, 1 packets/sec
  30 seconds output rate 776 bits/sec, 1 packets/sec
  Load-Interval #2: 5 minute (300 seconds)
    input rate 728 bps, 0 pps; output rate 608 bps, 0 pps
  RX
    3178795 unicast packets  490503 multicast packets  1142652 broadcast packets
    4811950 input packets  3354211696 bytes
    0 jumbo packets  0 storm suppression bytes
    0 runts  0 giants  0 CRC  0 no buffer
    44288 input error  0 short frame  44288 overrun   0 underrun  0 ignored
    0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
    0 input with dribble  306404 input discard
    0 Rx pause
  TX
    1974109 unicast packets  296078 multicast packets  818 broadcast packets
    2271005 output packets  696237525 bytes
    0 jumbo packets
    0 output errors  0 collision  0 deferred  0 late collision
    0 lost carrier  0 no carrier  0 babble 0 output discard
    0 Tx pause
```

如果发现任何错误，也可以检查实际的FTD软件是否存在接口错误。



要进入FTD提示符，首先需要导航到FTD CLI提示符。

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

对于多实例：

```
# connect module 1 telnet
Firepower-module1>connect ftd ftd1
Connecting to container ftd(ftd1) console... enter "exit" to return to Boot CLI
>
```

这是输出示例。

```
# connect module 1 console

Firepower-module1> connect ftd

> show interface
InterfaceGigabitEthernet0/0 "outside", is up, line protocol is up
     Hardware is i82545EM rev01, BW 1000 Mbps, DLY 10 usec
                Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
                 Input flow control is unsupported, output flow control is off
                 MAC address 000c.2961.f78b, MTU 1500
                 IPS Interface-Mode: inline, Inline-Set: InlineSet
                 IP address unassigned
                 20686130 packets input, 8859847035 bytes, 0 no buffer
                 Received 0 broadcasts, 0 runts, 0 giants
                 2312 input errors, 0 CRC, 0 frame, 12313 overrun, 0 ignored, 0 abort
                 0 pause input, 0 resume input
                 0 L2 decode drops
                 6485096 packets output, 1480276815 bytes, 0 underruns
                 0 pause output, 0 resume output
                 1341 output errors, 45635 collisions, 1 interface resets
                 0 late collisions, 0 deferred
                 0 input reset drops, 0 output reset drops
                 input queue (blocks free curr/low): hardware (509/362)
                 output queue (blocks free curr/low): hardware (511/415)
    Traffic Statistics for "outside":
                 20686131 packets input, 8485139715 bytes
                 6485096 packets output, 1375761699 bytes
                 4702172 packets dropped
            1 minute input rate 2 pkts/sec,  999 bytes/sec
            1 minute output rate 0 pkts/sec,  78 bytes/sec
            1 minute drop rate, 0 pkts/sec
            5 minute input rate 3 pkts/sec,  1222 bytes/sec
            5 minute output rate 1 pkts/sec,  319 bytes/sec
            5 minute drop rate, 1 pkts/sec
```

向思科技术支持中心(TAC)提供的数据

数据	说明
连接事件屏幕截图	有关说明，请参阅本文
'show interface'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 firewalls/1180..。 对于Firepower:http://www.cisco.com/c/en/us/support/docs/secu appliances/11777..。
ASA“show tech”输出	登录ASA CLI并将终端会话保存到日志中。输入**show tech**命令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：排除Firepower DAQ层故障

如果不清楚Firepower设备是否正在丢弃数据包，则可以绕过Firepower设备本身，一次性排除所有Firepower组件。如果相关流量正在吞入Firepower设备，但未退出，这对缓解问题特别有帮助。

要继续，请复习Firepower数据路径故障排除的下一阶段；Firepower数据获取。单击此处继续。