Firepower Data Path Troubleshooting Phase 1: Packet Ingress

Contents

Introduction

This article is part of a series of articles which explain how to systematically troubleshoot the data path on Firepower systems to determine whether components of Firepower may be affecting traffic. Please refer to the [Overview article](#) for information about the architecture of Firepower platforms and links to the other Data Path Troubleshooting articles.

In this article, we will look at the first stage of the Firepower data path troubleshooting, the Packet Ingress stage.

Platform Guide

The following table describes the platforms covered by this article.

Platform Code Name	Description	Applicable Hardware Platforms	Notes
SFR	ASA with FirePOWER Services (SFR) module installed.	ASA-5500-X series	N/A
FTD (non-SSP and	Firepower Threat Defense (FTD) image installed on an Adaptive Security Appliance	ASA-5500-X series, virtual	N/A

FPR-2100)	(ASA) or a Virtual Platform	NGFW platforms	
FTD (SSP)	FTD installed as a logical device on a Firepower eXtensible Operative System (FXOS) based chassis	FPR-9300, FPR-4100, FPR-2100	The 2100 series does not use the FXOS Chassis Manager

Troubleshooting the Packet Ingress Phase

The first data path troubleshooting step is to make sure that there are no drops occurring at the ingress or egress stage of packet processing. If a packet is ingressing but not egressing, then you can be sure that the packet is being dropped by the device at some place within the data-path or that the device is unable to create the egress packet (for example, a missing ARP entry).

Identify the Traffic in Question

The first step in troubleshooting the packet ingress stage is to isolate the flow and the interfaces involved in the problem traffic. This includes:

Flow Information	Interface Information
Protocol	
Source IP Address	Ingress Interface
Source Port	Egress Interface
Destination IP	
Destination Port	

For example:

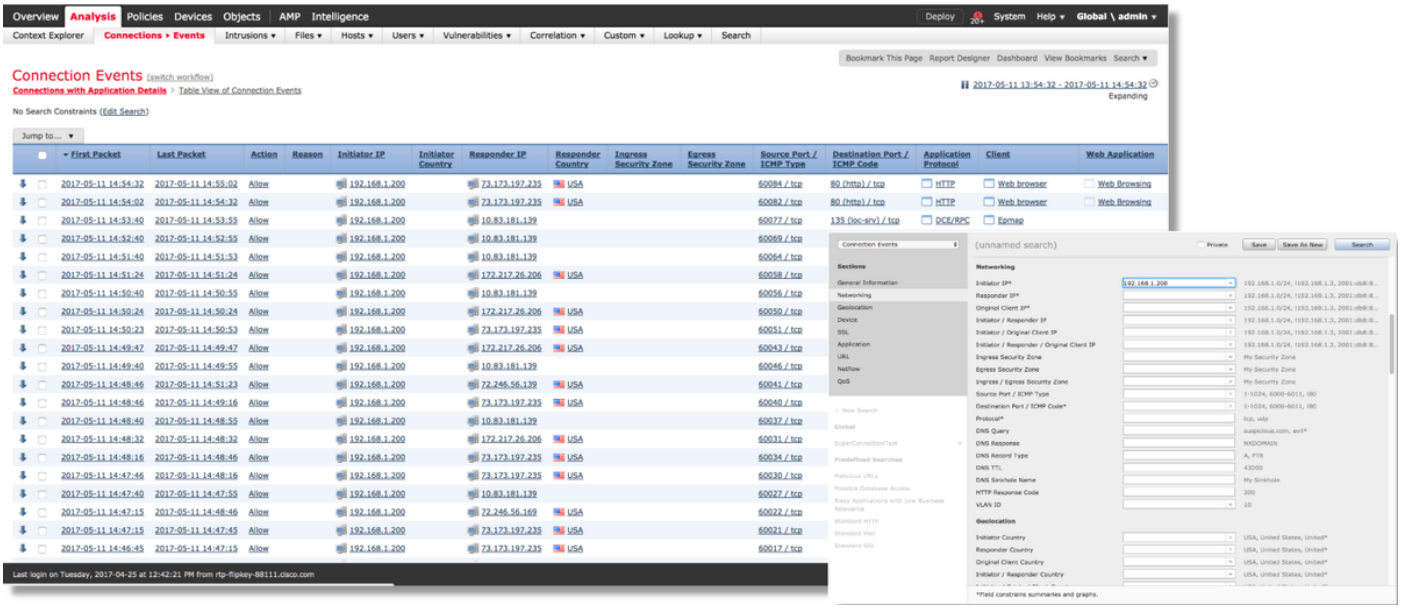
```
TCP inside 172.16.100.101:38974 outside 192.168.1.10:80
```

> **Tip**: You may not be able to identify the exact source port since it is often different in each flow, but the destination (server) port should suffice.

Check for Connection Events

After getting an idea of the ingress and egress interface the traffic should be matching as well as the flow information, the first step to identify whether Firepower is blocking the flow is to check the Connection Events for the traffic in question. These can be viewed in the Firepower Management Center under **Analysis > Connections > Events**

> **Note**: Prior to checking Connection Events, ensure that logging is enabled in your Access Control Policy rules. Logging is configured in the "Logging" tab within each Access Control Policy rule as well as the Security Intelligence tab. Make sure the suspect rules are configured to send the logs to the "Event Viewer".



In the example above, "Edit Search" is clicked and a unique source (Initiator) IP is added as a filter to see the flows which were being detected by Firepower. The Action column shows "Allow" for this host traffic.

If Firepower is intentionally blocking traffic, the Action contains the word "Block". Clicking on "Table View of Connection Events" provides more data. The following fields in the Connection Events can be noted if the action is "Block":

- Reason

- Access Control Rule

This, combined with the other fields in the event in question, can help to narrow down which component is blocking the traffic.

For more information about troubleshooting Access Control Rules, you can click here.

Capturing Packets on the Ingress and Egress Interfaces

If there are no events or the Firepower is still suspected of blocking despite the Connection Events displaying a rule action of "Allow" or "Trust", the data path troubleshooting continues.

Here are instructions on how to run an ingress and egress packet capture on the various platforms mentioned above:

SFR - Capture on the ASA Interfaces

Since the SFR module is simply a module running on the ASA Firewall, it is best to first capture on the ingress and egress interfaces of the ASA to make sure that the same packets which ingress are also egressing.

This article contains instructions on how to perform the captures on the ASA.

If it has been determined that the packets which are ingressing the ASA are not egressing, continue to the next phase in troubleshooting (the DAQ phase).

Note: If packets are seen on the ASA ingress interface, it may be worth checking the connected devices.

FTD (non-SSP and FPR-2100) - Capture on the Ingress and Egress Interfaces

Capturing on a non-SSP FTD device is similar to capturing on the ASA. However, you can run the capture commands directly from the CLI initial prompt. When troubleshooting dropped packets it is advised to add the "trace" option to the capture.

Here is an example of configuring an ingress capture for TCP traffic on port 22:

```
> 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>
```

If you add the "trace" option, you can then select an individual packet to trace through the system to see how it came to the final verdict. It also helps to make sure that the proper modifications are done to the packet such as Network Address Translation (NAT) IP modification and that the proper egress interface has been chosen.

```
> 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
```

In the example above, we see that the traffic make it to Snort inspection and that it finally reached an allow verdict and overall was passed through the device. Since the traffic can be seen in both directions you can be sure traffic is flowing through the device for this session, so an egress capture may not be needed, but you can take one there as well to make sure the traffic is egressing properly as shown in the trace output.

> **Note**: If the device is unable to create the egress packet, the trace action is still "allow" but the packet is not created or seen on the egress interface capture. This is a very common scenario where the FTD doesn't have an ARP entry for the next hop or destination IP (if this last one is directly connected).

FTD (SSP) - Capture on the Logical FTD Interfaces

The same steps to generate a packet capture on FTD as mentioned above can be followed on an SSP platform. You can connect using SSH into the IP address of the FTD logical interface and enter the following command:

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

You can also navigate to the FTD logical device shell from the FXOS command prompt with the following commands:

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

If a Firepower 9300 is used, the module number can vary depending on which Security Module is being used. These modules can support up to 3 logical devices.

If multi-instances are being used, the instance ID must be included on the "connect" command. Telnet command can be used to connect to different instances at the same time.

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

Check for Interface Errors

Interface level issues can also be checked during this phase. This is especially helpful if packets are missing in the ingress interface capture. If interface errors are seen, checking the connected devices can be helpful.

SFR - Check ASA Interfaces

Since the FirePOWER (SFR) module is basically a virtual machine running on an ASA, the actual ASA interfaces are checked for errors. For detailed information on checking the interface statistics on the ASA, see this ASA Series Command Reference guide section.

FTD (non-SSP and FPR-2100) - Check for Interface Errors

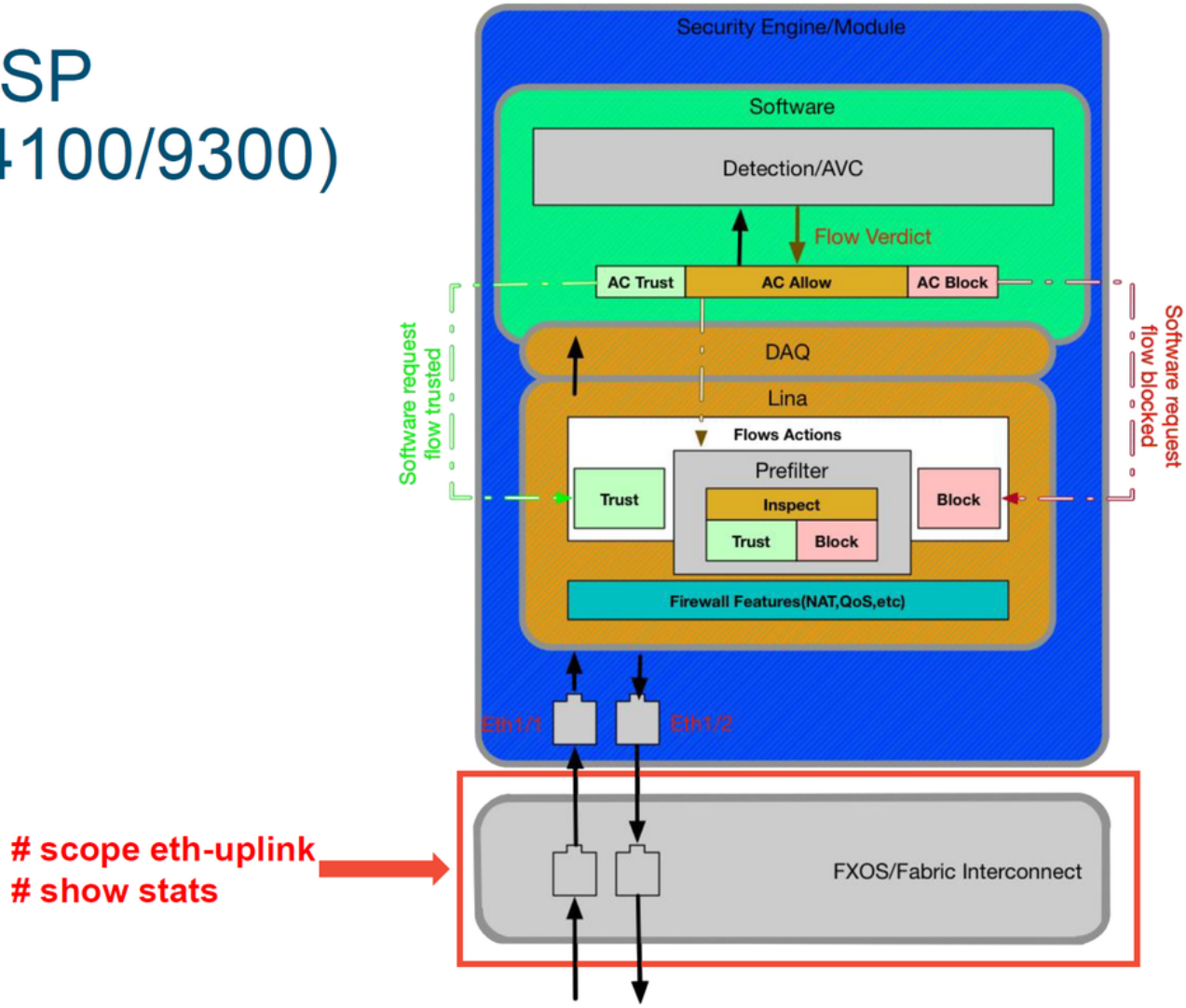
On non-SSP FTD devices, the **> show interface** command can be run from the initial command prompt. The interesting output is highlighted in red.

```
> 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) - Navigating the Data Path to Look for Interface Errors

The 9300 and 4100 SSP platforms have an internal fabric interconnect which first handles the packets.

SSP (4100/9300)



It is worth to check if there are any interface issues at the initial packet ingress. These are the commands to run on the FXOS system CLI in order to get this information.

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

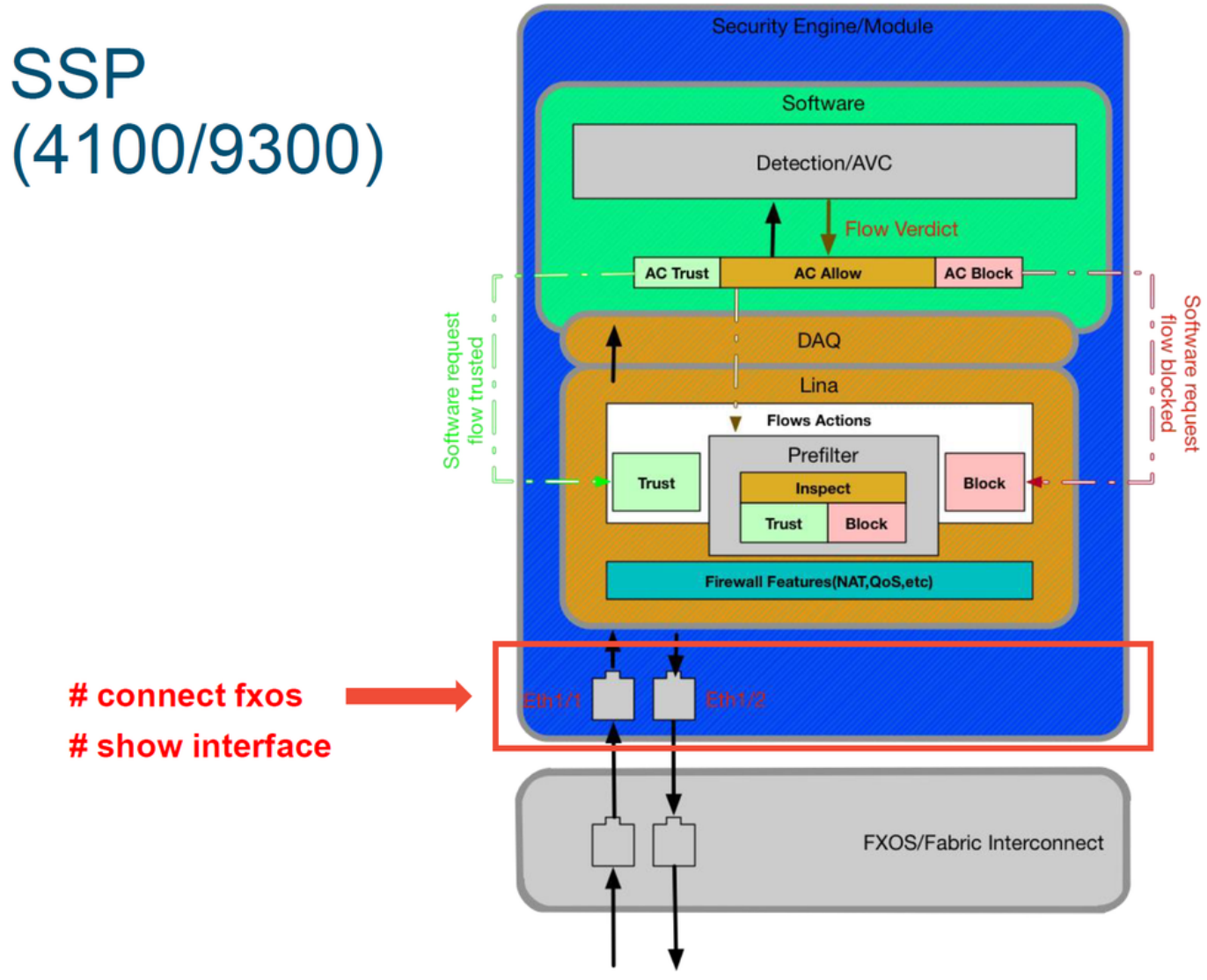
This is a sample output.

```
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
```

After the fabric interconnect handles the packet upon ingress, it is then sent to the interfaces which are assigned to the logical device hosting the FTD device.

Here is a diagram for reference:



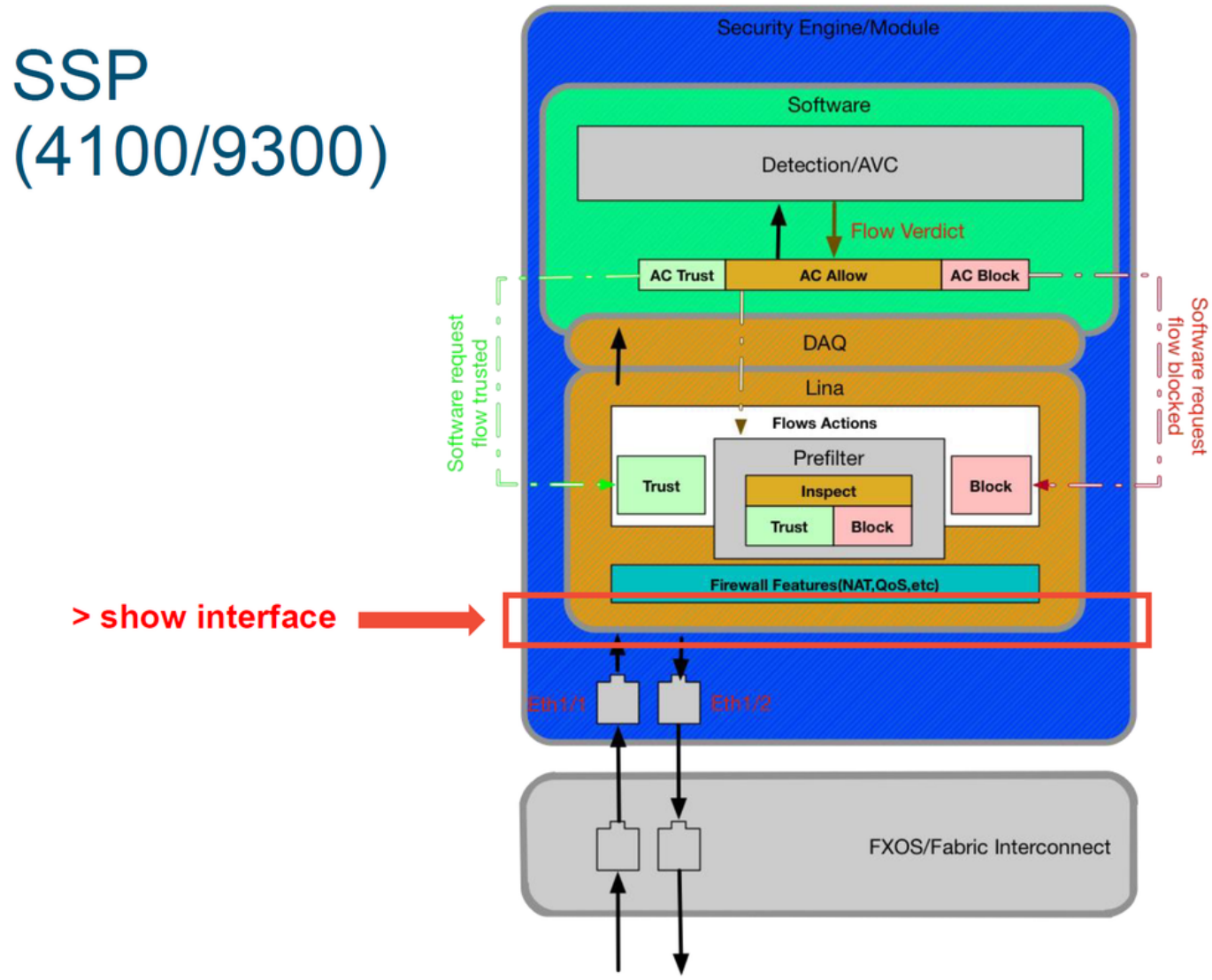
In order to check for any interface level issues, enter the following commands:

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

This is an output example (possible issues highlighted in red):

```
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
```

If any errors are seen, the actual FTD software can be checked for interface errors as well.



In order to get to the FTD prompt, it is first necessary to navigate to the FTD CLI prompt.

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

For multi-instances:

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

This is an output example.

```
# 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
```

Data to Provide to Cisco Technical Assistance Center (TAC)

Data	Instructions
Connection Event screenshots	See this article for instructions
'show interface' output	See this article for instructions
Packet captures	For ASA/LINA: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next firewalls/1180... For Firepower: http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-800 appliances/11777...
ASA 'show tech' output	Log into ASA CLI and have the terminal session saved to a log. Enter the **show tech** comm the terminal session output file to TAC. This file can be saved to disk or an external storage system with this command. show tech | redirect disk0:/show_tech.log
Troubleshoot file from the Firepower device inspecting the traffic	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-techn

Next Step: Troubleshoot the Firepower DAQ Layer

If it is unclear as to whether the Firepower device is dropping packets, the Firepower device itself can be bypassed to rule out all of the Firepower components at once. This is especially helpful in mitigating an issue if the traffic in question is ingressing the Firepower device but not egressing.

To proceed, please review the next phase of Firepower data path troubleshooting; The Firepower DAQ. Click here to continue.