Firepowerデータパスのトラブルシューティング フェーズ1:パケット入力

内容

概要
プラットフォームガイド
パケット入力フェーズのトラブルシューティング
問題のトラフィックの特定
接続イベントの確認
入力および出力インターフェイスでのパケットのキャプチャ
SFR:ASAインターフェイスでのキャプチャ
FTD（非SSPおよびFPR-2100）：入力および出力インターフェイスでのキャプチャ
FTD(SSP)：論理FTDインターフェイスでのキャプチャ
インターフェイスエラーのチェック
SFR:ASAインターフェイスの確認
FTD（非SSPおよびFPR-2100）：インターフェイスエラーの確認
FTD(SSP) – インターフェイスエラーを検索するためのデータパスの移動
Cisco Technical Assistance Center(TAC)に提供するデータ
次の手順：Firepower DAQレイヤのトラブルシューティング

概要

この記事は、Firepowerシステムのデータパスを体系的にトラブルシューティングし、Firepowerのコンポーネントがトラフィックに影響を与えているかどうかを判断する方法を説明する一連の記事の一部です。Firepowerプラットフォームのアーキテクチャに関する情報や、その他のデータパスのトラブルシューティングに関する記事へのリンクについては、概要記事を参照してください。

この記事では、Firepowerのデータパスのトラブルシューティングの最初の段階であるパケット入力の段階について説明します。

プラットフォームガイド

次の表では、この記事で扱うプラットフォームについて説明します。

プラットフォームコード名	説明	該当 ハードウェア プラットフォーム	注意事項
SFR	ASA with FirePOWER Services(SFR)モジュールがインストールされている。	ASA-5500-Xシリーズ	N/A
FTD（非	適応型セキュリティアプライアンス(ASA)ま	ASA-5500-Xシリ	N/A

SSPおよびFPR-2100）	たは仮想プラットフォームにインストールされたFirepower Threat Defense(FTD)イメージ	ーズ、仮想NGFWプラットフォーム	
FTD(SSP)	Firepower eXtensible Operational System(FXOS)ベースのシャーシに論理デバイスとしてインストールされるFTD	FPR-9300、FPR-4100、FPR-2100	2100シリーズでは、FXOS Chassis Managerは使用されません

パケット入力フェーズのトラブルシューティング

最初のデータパスのトラブルシューティング手順は、パケット処理の入力または出力ステージでドロップが発生していないことを確認することです。パケットが入力されていても出力されない場合は、パケットがデータパス内の任意の場所でデバイスによってドロップされているか、またはデバイスが出力パケットを作成できないことが確認できます（ARPエントリの欠落など）。

問題のトラフィックの特定

パケット入力段階のトラブルシューティングの最初のステップは、問題のトラフィックに関係するフローとインターフェイスを切り分けることです。これには、次のような特徴があります。

フロー情報	インターフェイス情報
プロトコル	
送信元 IP アドレス	入力インターフェイス
送信元ポート	出力インターフェイス
宛先 IP	
宛先ポート	

以下に、いくつかの例を示します。

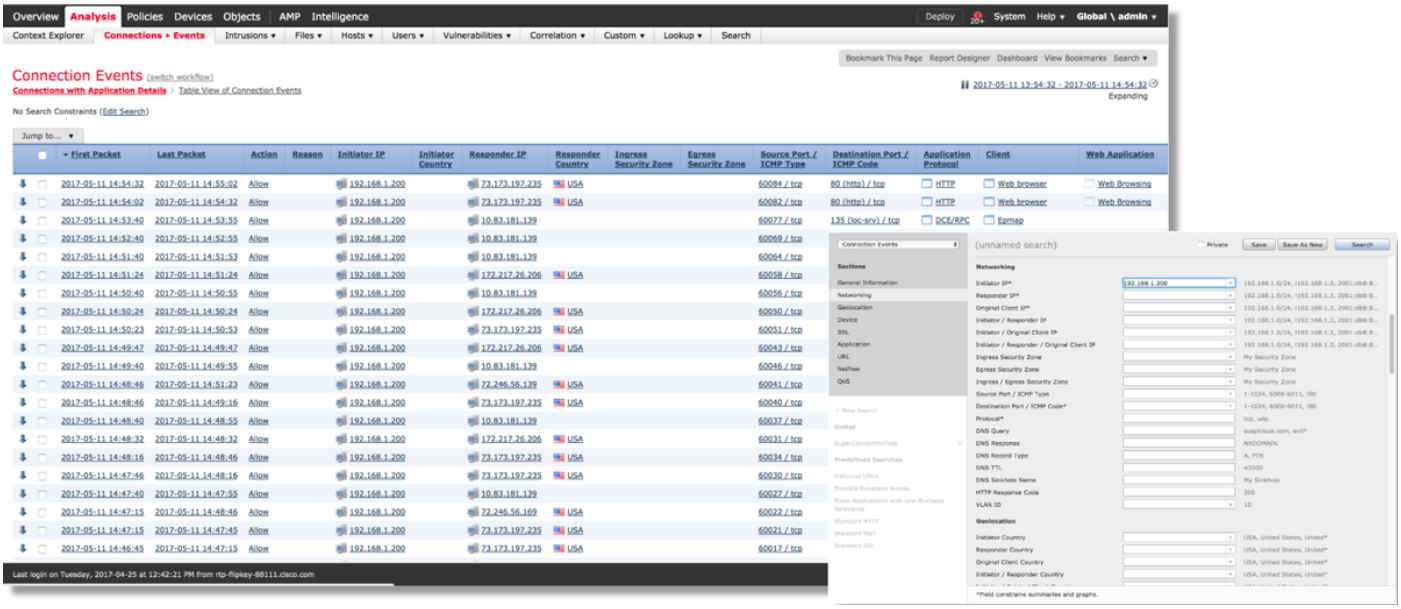
```
TCP inside 172.16.100.101:38974 outside 192.168.1.10:80
```

> **ヒント**：送信元ポートは各フローで異なることが多いため、正確な送信元ポートを特定できない場合がありますが、宛先（サーバ）ポートで十分です。

接続イベントの確認

トラフィックが一致する必要がある入力および出力インターフェイスとフロー情報を確認した後、Firepowerがフローをブロックしているかどうかを確認する最初のステップは、該当するトラフィックの接続イベントを確認することです。これらはFirepower Management Centerの[**Analysis**] > [**Connections**] > [**Events**]で表示できます

> **注**：接続イベントを確認する前に、アクセスコントロールポリシールールでロギングが有効になっていることを確認してください。ロギングは、各アクセスコントロールポリシールールの[Logging]タブおよび[Security Intelligence]タブで設定します。疑わしいルールが「イベントビューア」にログを送信するように設定されていることを確認します。



上の例では、[Edit Search]をクリックし、一意のソース（イニシエータ）IPをフィルタとして追加して、Firepowerによって検出されたフローを確認します。[Action]列には、このホストトラフィックの[Allow]が表示されます。

Firepowerが意図的にトラフィックをブロックしている場合、アクションには「ブロック」という単語が含まれます。 [接続イベントのテーブルビュー]をクリックすると、さらに多くのデータが表示されます。アクションが「ブロック」の場合、接続イベントの次のフィールドに注意してください。

-原因

– アクセスコントロールルール

このフィールドは、問題のイベントの他のフィールドと組み合わされて、トラフィックをブロックしているコンポーネントを絞り込むのに役立ちます。

アクセスコントロールルールのトラブルシューティングの詳細については、ここをクリックしてください。

入力および出力インターフェイスでのパケットのキャプチャ

接続イベントで「許可」または「信頼」のルールアクションが表示されているにもかかわらず、イベントが存在しない場合やFirepowerがブロックの疑いがある場合は、データパスのトラブルシューティングが続行されます。

上記のさまざまなプラットフォームで入力および出力パケットキャプチャを実行する方法を次に示します。

SFR:ASAインターフェイスでのキャプチャ

SFRモジュールは単にASAファイアウォールで実行されるモジュールであるため、最初にASAの入力インターフェイスと出力インターフェイスでキャプチャし、入力と同じパケットが出力されていることを確認することをお勧めします。

この記事では、ASAでキャプチャを実行する方法について説明します。

ASAに着信しているパケットが出力されていないと判断された場合は、トラブルシューティングの次のフェーズ（DAQフェーズ）に進みます。

> **注**：ASA入力インターフェイスでパケットが見られる場合は、接続されたデバイスを確認する価値があります。

FTD（非SSPおよびFPR-2100）：入力および出力インターフェイスでのキャプチャ

非SSP FTDデバイスでのキャプチャは、ASAでのキャプチャと同様です。ただし、CLIの初期プロンプトからcaptureコマンドを直接実行できます。ドロップされたパケットのトラブルシューティングを行う場合は、キャプチャに「trace」オプションを追加することを推奨します。

次に、ポート22でTCPトラフィックの入力キャプチャを設定する例を示します。

```
> 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>
```

"trace"オプションを追加すると、システムをトレースする個々のパケットを選択して、最終的な判定がどのように行われたかを確認できます。また、ネットワークアドレス変換(NAT)のIP変更などのパケットに対して適切な変更が行われ、適切な出力インターフェイスが選択されていることを確認することもできます。

```
> 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
```

上記の例では、トラフィックがSnort検査に到達し、最終的に許可の判定に達し、デバイス全体が通過していることがわかります。トラフィックは両方向で確認できるため、このセッションのデバイスを通過するトラフィックを確認できます。そのため、出力キャプチャは必要ない可能性がありますが、トレース出力に示すように、トラフィックが正しく出力されていることを確認することもできます。

> **注**：デバイスが出力パケットを作成できない場合、トレースアクションは「allow」のままですが、パケットは出力インターフェイスキャプチャで作成または表示されません。これは、FTDにネクストホップまたは宛先IPのARPエントリがない（この最後のエントリが直接接続されている場合）非常によく見られるシナリオです。

FTD(SSP)：論理FTDインターフェイスでのキャプチャ

上記と同じ手順で、FTDでパケットキャプチャを生成できます。この手順は、SSPプラットフォームでも実行できます。SSHを使用してFTD論理インターフェイスのIPアドレスに接続し、次のコマンドを入力できます。

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

次のコマンドを使用して、FXOSコマンドプロンプトからFTD論理デバイスシェルに移動することもできます。

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

Firepower 9300が使用されている場合、使用されているセキュリティモジュールによってモジュール番号が異なる場合があります。これらのモジュールは、最大3つの論理デバイスをサポートできます。

マルチインスタンスを使用する場合は、「connect」コマンドにインスタンスIDを含める必要があります。Telnetコマンドを使用すると、異なるインスタンスに同時に接続できます。

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

インターフェイスエラーのチェック

このフェーズでは、インターフェイスレベルの問題も確認できます。これは、入力インターフェイスキャプチャでパケットが欠落している場合に特に役立ちます。インターフェイスエラーが表示される場合は、接続されているデバイスを確認すると便利です。

SFR:ASAインターフェイスの確認

FirePOWER(SFR)モジュールは基本的にASAで実行される仮想マシンであるため、実際のASAインターフェイスでエラーがチェックされます。ASAのインターフェイス統計情報の確認の詳細については、次の「ASAシリーズコマンドリファレンスガイド」セクションを参照してください。

FTD（非SSPおよびFPR-2100）：インターフェイスエラーの確認

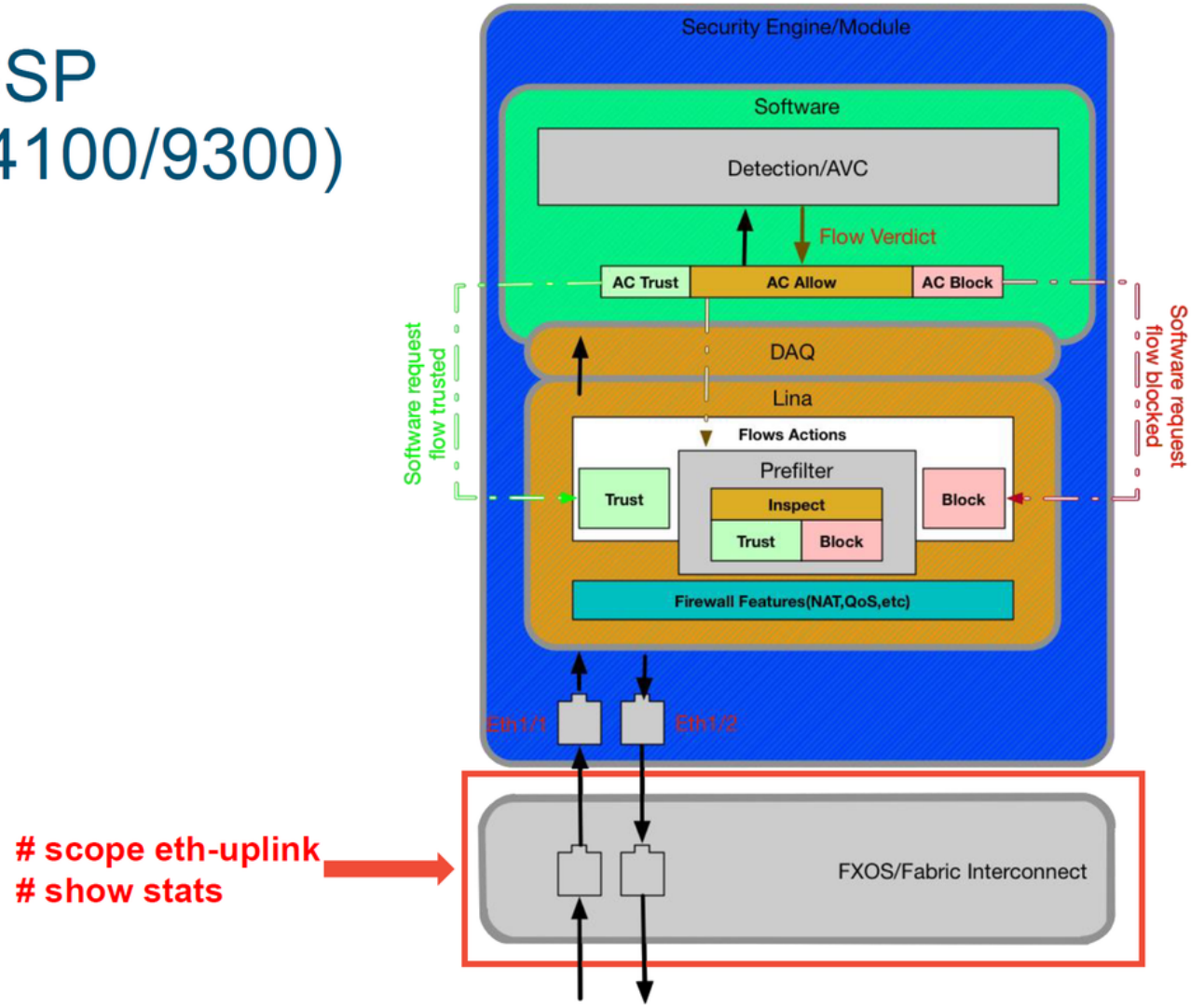
SSP以外のFTDデバイスでは、**> show interfaceコマンド**を初期コマンドプロンプトから実行できます。対象となる出力は赤で強調表示されています。

```
> 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) – インターフェイスエラーを検索するためのデータパスの移動

9300および4100 SSPプラットフォームには、最初にパケットを処理する内部ファブリックインターコネクトがあります。

SSP (4100/9300)



最初のパケット入力にインターフェイスの問題があるかどうかを確認する価値があります。この情報を取得するには、FXOSシステムCLIで実行するコマンドを次に示します。

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

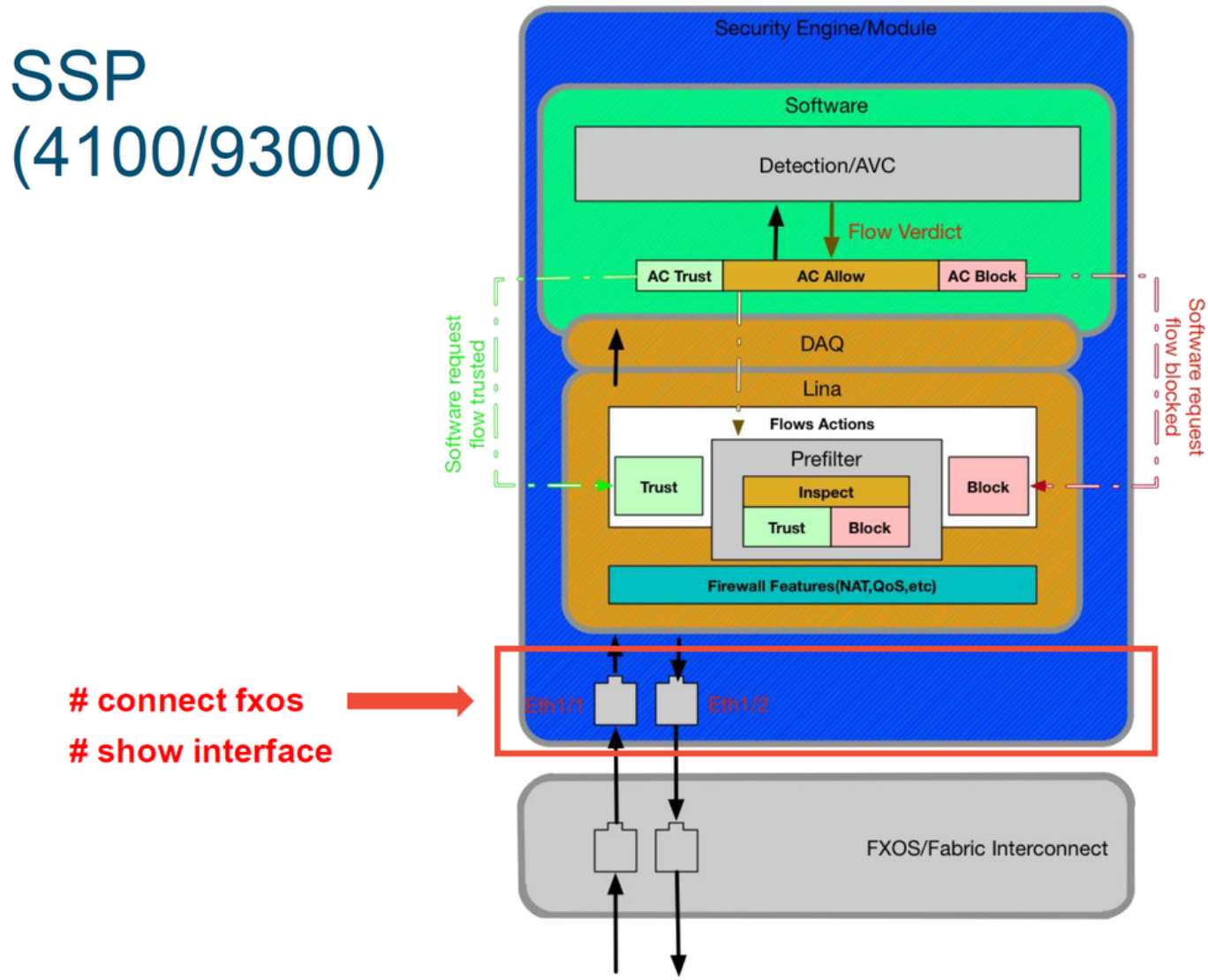
次に出力例を示します。

```
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
```

ファブリックインターコネクトは、入力時にパケットを処理した後、FTDデバイスをホストする論理デバイスに割り当てられたインターフェイスに送信されます。

次の図を参照してください。



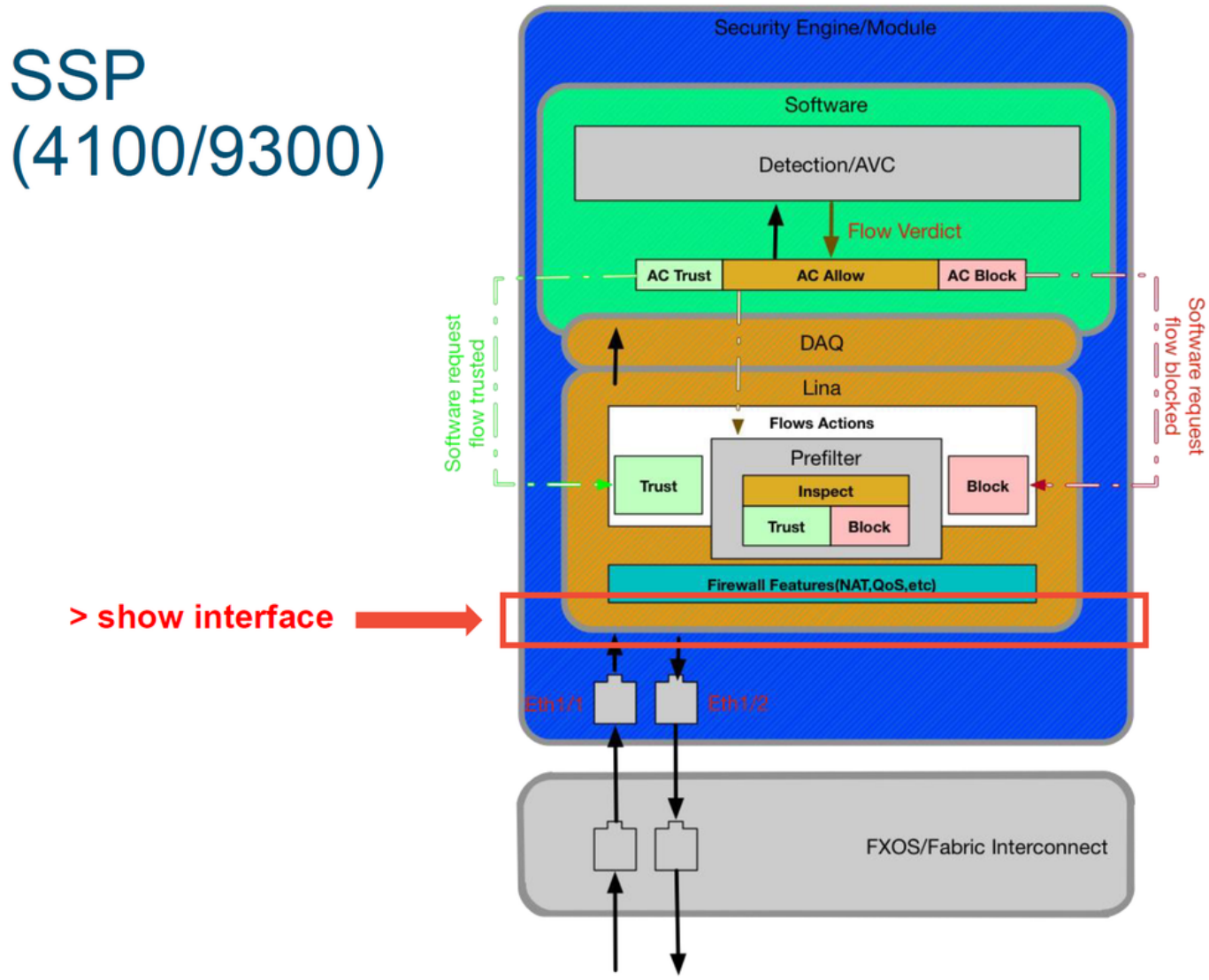
インターフェイスレベルの問題を確認するには、次のコマンドを入力します。

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

次に出力例を示します（赤で強調表示されている問題の可能性があります）。

```
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
```

エラーが見つかった場合は、実際のFTDソフトウェアでもインターフェイスエラーをチェックできます。



FTDプロンプトに移動するには、まずFTD CLIプロンプトに移動する必要があります。

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

マルチインスタンスの場合：

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

次に出力例を示します。

```
# 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
```

Cisco Technical Assistance Center(TAC)に提供するデータ

Data	手順
接続イベントのスクリーンショット	手順については、
「show interface」出力	手順については、
パケット キャプチャ	ASA/LINAの場合 firewalls/1180.. に Firepowerの場合 appliances/11777
ASAの「show tech」出力	ASA CLIにログイ ナルセッション出 このファイルは、 show tech | redire
トラフィックを検査するFirepowerデバイスからのファイルのトラブルシューティング	http://www.cisco.c

次の手順：Firepower DAQレイヤのトラブルシューティング

Firepowerデバイスがパケットをドロップしているかどうかがわからない場合は、Firepowerデバイス自体をバイパスして、すべてのFirepowerコンポーネントを一度に除外できます。これは、問題のトラフィックがFirepowerデバイスに入り込んで出てこない場合の問題を軽減するのに特に役立ちます。

続行するには、Firepowerデータパスのトラブルシューティングの次のフェーズを確認してください。Firepower DAQ。続行するにはここをクリックします。