Firepowerデータパスのトラブルシューティング フェーズ2:DAQレイヤ

内容

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データパスのトラブルシューティングの2番目の段階について説明します。DAQ（データ収集）レイヤ

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	ASA-5500-Xシリーズ	N/A

	されている。		
FTD（すべて）	すべてのFirepower Threat Defense(FTD)プラットフォームに適用	ASA-5500-Xシリーズ、仮想NGFWプラットフォーム、FPR-2100、FPR-9300、FPR-4100	N/A
FTD（非SSPおよびFPR-2100）	ASAまたは仮想プラットフォームにインストールされたFTDイメージ	ASA-5500-Xシリーズ、仮想NGFWプラットフォーム、FPR-2100	N/A
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	2100シリーズでは、FXOS Chassis Managerは使用されません

Firepower DAQフェーズのトラブルシューティング

DAQ（データ収集）レイヤは、パケットをSnortが理解できる形式に変換するFirepowerのコンポーネントです。Snortに送信されると、最初にパケットが処理されます。したがって、パケットが入力されていてもFirepowerアプライアンスから出力されていない場合、またはパケット入力のトラブルシューティングで有用な結果が得られなかった場合は、DAQのトラブルシューティングが役立ちます。

DAQレイヤでのトラフィックのキャプチャ

キャプチャを実行するプロンプトを表示するには、まずSSHを使用してSFRまたはFTDのIPアドレスに接続する必要があります。

> **注：**FPR-9300および4100デバイスで、**connect ftd**を最初に入力し、2番目の>プロンプトで終了します。また、FXOS Chassis Manager IPにSSH接続し、**connect module 1 console**、**connect ftdの順**に入力することもできます。

この記事では、Firepower DAQレベルでパケットキャプチャを収集する方法について説明します。

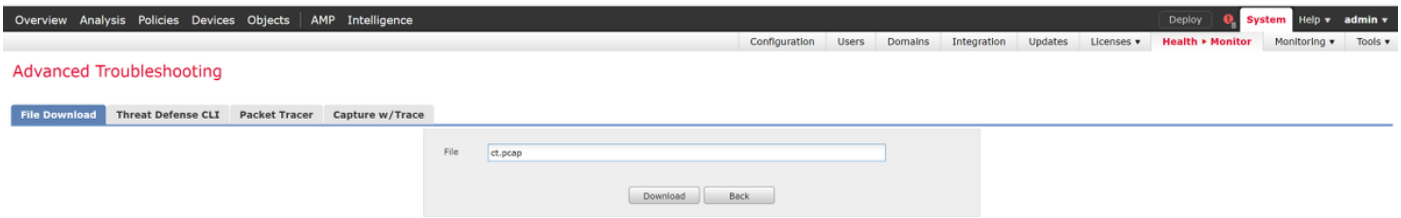
構文は、FTDプラットフォームのLINA側だけでなく、ASAで使用される**captureコマンドと同じ**ではないことに注意してください。FTDデバイスから実行されるDAQパケットキャプチャの例を次に示します。

```
> 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
```

上のスクリーンショットに示すように、ct.pcapというPCAPフォーマットのキャプチャが**/ngfw/var/commonディレクトリ**(SFRプラットフォームで**/var/common)に書き込まれ**ました。 これらのキャプチャファイルは、上記の記事の指示に従って、>プロンプトからFirepowerデバイスからコピー[すること](#)ができます。

または、Firepowerバージョン6.2.0以降のFirepower Management Center(FMC)で、[デバイス(**Devices)] > [デバイス管理(Device Management)]に移動します**。次に、 アイコンをクリックし、その後に[**Advanced Troubleshooting**] > [**File Download**]をクリックします。

キャプチャファイルの名前を入力し、[Download]をクリックします。



Firepowerをバイパスする方法

Firepowerがトラフィックを検出しているものの、パケットがデバイスから出ていないか、トラフィックに別の問題があると判断された場合は、次のステップとしてFirepower検査フェーズをバイパスし、Firepowerコンポーネントの1つがトラフィックをドロップしていることを確認します。次に、さまざまなプラットフォームでFirepowerをバイパスするトラフィックの最も高速な方法の内訳を示します。

SFR:Firepowerモジュールをモニタ専用モードにします

SFRをホストするASAで、SFRモジュールをモニタ専用モードにするには、ASAコマンドラインインターフェイス(CLI)またはCisco Adaptive Security Device Manager(ASDM)を使用します。 これにより、ライブパケットのコピーだけがSFRモジュールに送信されます。

ASA CLIを使用してSFRモジュールをモニタ専用モードにするには、**show service-policy sfr**コマンドを実行して、SFRリダイレクトに使用するクラスマップとポリシーマップを最初に決定する必要があります。

```
# 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
```

この出力は、global_policyポリシーマップが「sfr」クラスマップに対してsfr fail-openアクションを実行していることを示しています。

> **注**：「fail-close」はSFRを実行できるモードですが、SFRモジュールがダウンしたり応答しなくなると、すべてのトラフィックがブロックされるため、一般的には使用されません。

SFRモジュールをモニタ専用モードにするには、次のコマンドを発行して、現在のSFR設定を無効にし、モニタ専用の設定を入力します。

```
# 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...
```

モジュールがモニタ専用モードになると、**show service-policy sfrの出力で確認できます。**

```
# 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**：SFRモジュールをインラインモードに戻すには、上に示す**(config-pmap-c)#プロンプトからno sfr fail-open monitor-onlyコマンドを発行し、その後にsfr {fail-open | fail-close}コマンドを使用します。**

または、[Configuration] > [Firewall] > [Service Policy Rules]の順に移動して、ASDMを介してモジュールをモニタ専用に配置**することもできます。**次に、対象のルールをクリックします。次に、

[Rule Actions]ページに移動し、[ASA FirePOWER Inspection]タブをクリックします。その後、[Monitor-only]を選択できます。

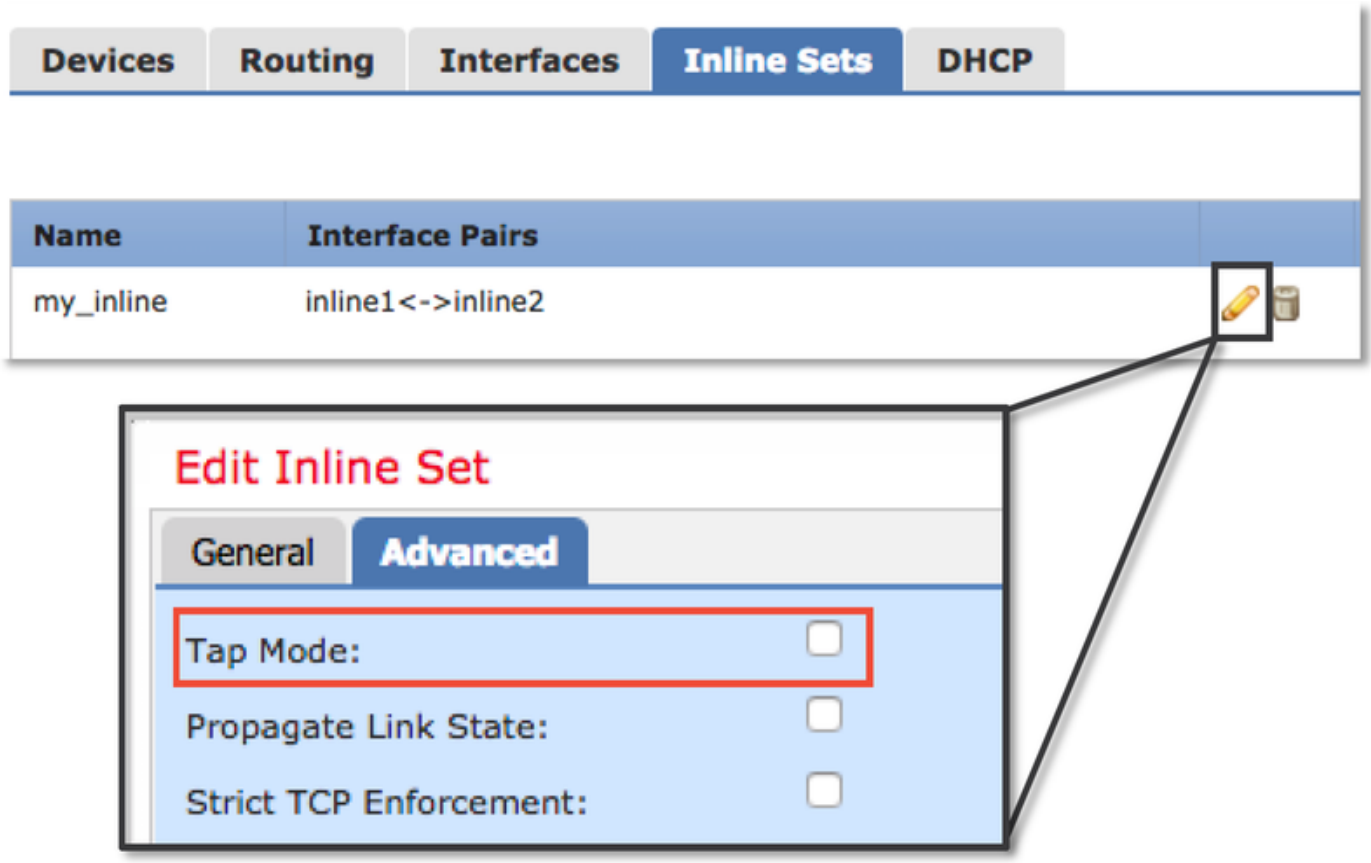
SFRモジュールがモニタ専用モードであることが確認された後もトラフィックの問題が解決しない場合は、Firepowerモジュールが問題の原因ではありません。その後、Packet Tracerを実行して、ASAレベルでさらに問題を診断できます。

問題が解決しない場合は、次のステップとして、Firepowerソフトウェアコンポーネントのトラブルシューティングを行います。

FTD（すべて）：インラインセットをTAPモードに配置

トラフィックがインラインセットで設定されたインターフェイスペアを通過する場合は、インラインセットをTAPモードにすることができます。これにより、Firepowerはライブパケットに対してアクションを実行しなくなります。デバイスはパケットをネクストホップに送信する前にパケットを変更する必要があり、トラフィックをドロップせずにバイパスモードに設定することはできないため、インラインセットのないルータや透過モードには適用されません。インラインセットのないルーテッドモードおよびトランスペアレントモードの場合は、パケットトレーサの手順に進みます。

FMCユーザインターフェイス(UI)からTAPモードを設定するには、[デバイス] > [デバイス管理]に移動し、該当するデバイスを編集します。[インラインセット]タブで、[TAPモード]オプションをオフにします。



TAPモードで問題が解決した場合、次のステップはFirepowerソフトウェアコンポーネントのトラブルシューティングです。

TAPモードで問題が解決しない場合、問題はFirepowerソフトウェアの対象外になります。その後、パケットトレーサを使用して、問題をさらに診断できます。

Packet Tracerを使用したシミュレーショントラフィックのトラブルシューティング

Packet Tracerは、パケットドロップの場所を特定するのに役立つユーティリティです。シミュレータであるため、人工パケットのトレースを実行します。

SFR:ASA CLIでのPacket Tracerの実行

SSHトラフィック用にASA CLIでパケットトレーサを実行する方法の例を次に示します。packet tracerコマンドの構文の詳細については、『ASA Series Command Reference guide』のこの項を参照してください。

```
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
```

上記の例では、ASAとSFRモジュールの両方がパケットを許可し、ASAによるパケットフローの処理方法に関する有用な情報が表示されています。

FTD（すべて）:FTD CLIでパケットトレーサを実行します。

すべてのFTDプラットフォームで、packet tracerコマンドはFTD CLIから実行できます。

```
> 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
```

この例では、パケットトレーサはドロップの理由を示しています。この場合、これはFirepowerのセキュリティインテリジェンス機能のIPブラックリストであり、パケットをブロックしています。次のステップは、ドロップの原因となる個々のFirepowerソフトウェアコンポーネントのトラブルシューティングです。

トレースによるキャプチャを使用したライブトラフィックのトラブルシューティング

ライブトラフィックは、トレース機能を使用してキャプチャをトレースすることもできます。この機能は、CLIですべてのプラットフォームで使用できます。次に、SSHトラフィックに対するトレースを使用してキャプチャを実行する例を示します。

```
> 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>
```

```
> 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
```

この例では、アプリケーションデータが定義された最初のパケットであるため、キャプチャの4番目のパケットがトレースされました。図に示すように、パケットはsnortによってホワイトリストに表示されます。つまり、フローに対してこれ以上snort検査が必要なく、全体が許可されます。

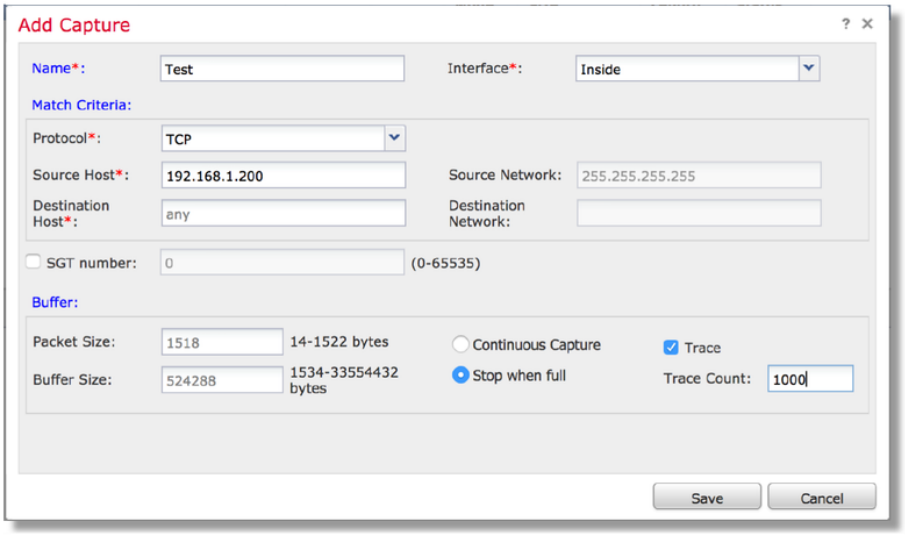
トレース構文を使用したキャプチャの詳細については、『ASA Series Command Reference guide』のこのセクションを参照してください。

FTD（すべて）:FMC GUIでのトレースによるキャプチャの実行

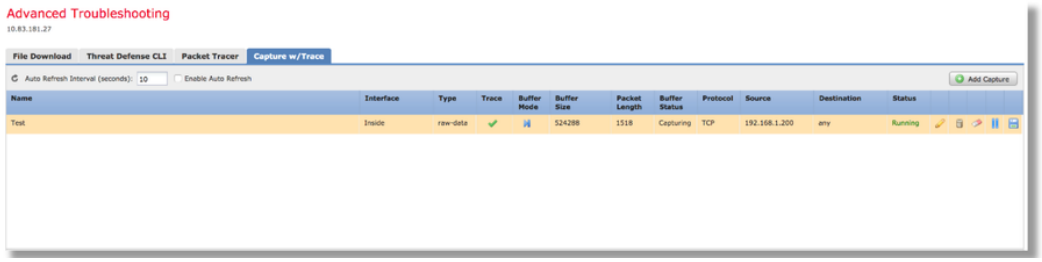
FTDプラットフォームでは、トレースによるキャプチャをFMC UIで実行できます。このユーティリティにアクセスするには、**[Devices] > [Device Management]に移動します。**

次に、 アイコンをクリックし、次に**[Advanced Troubleshooting] > [Capture w/Trace]をクリックします。**

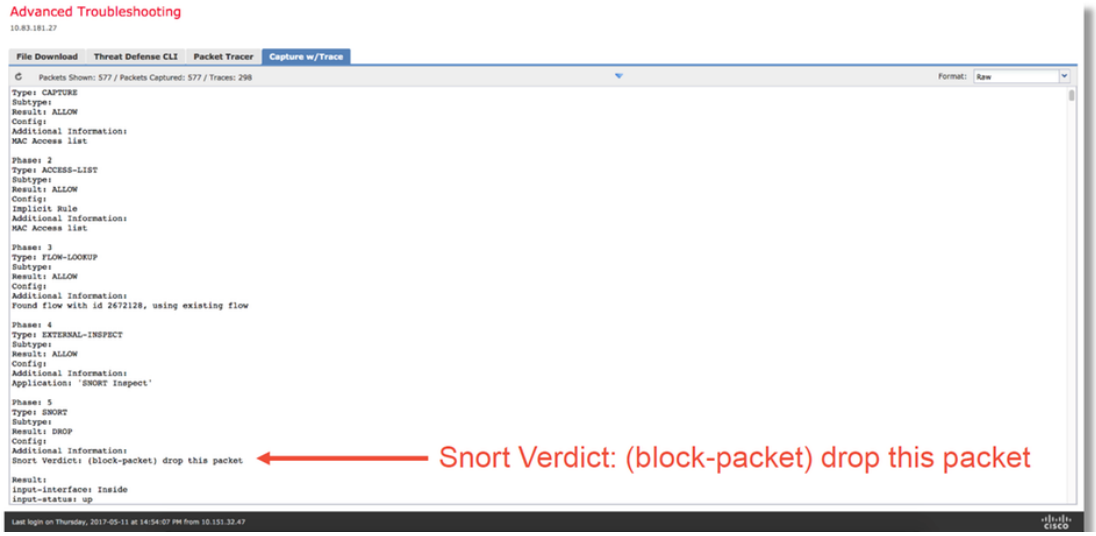
次に、GUIを介してトレースを使用してキャプチャを実行する方法の例を示します。



Clicking **Add Capture** button will display this popup window



View of all current captures



Example output shows the packet was blocked by Snort

トレースを使用したキャプチャがパケット廃棄の原因を示している場合は、次のステップとして個々のソフトウェアコンポーネントのトラブルシューティングを行います。

問題の原因が明確に示されていない場合は、次のステップとしてトラフィックの高速パスを設定します。

FTDでのPreFilter Fastpathルールの作成

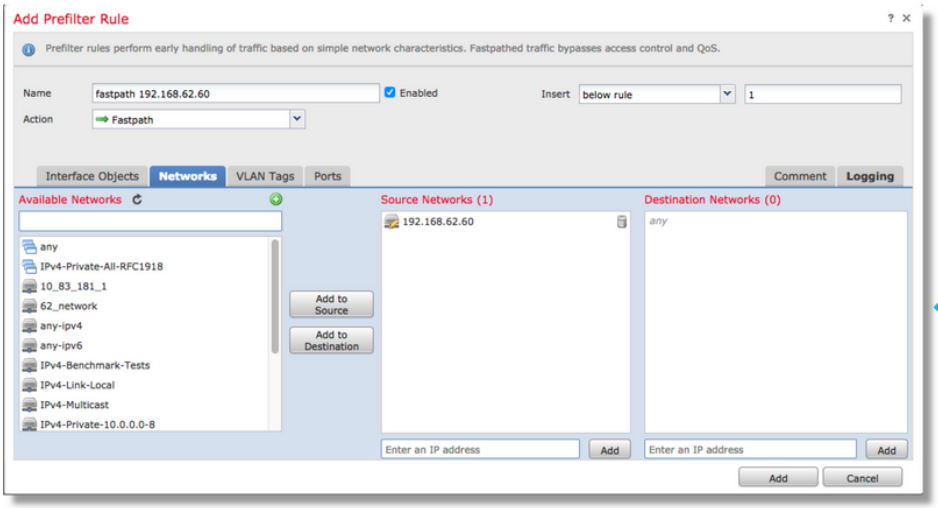
すべてのFTDプラットフォームには、Pre-Filter Policyがあり、Firepower(snort)インスペクションからトラフィックを転送するために使用できます。

FMCでは、[Policies] > [Access Control] > [**Prefilter**]の**下にあります**。デフォルトのプレフィルタポリシーは編集できないため、カスタムポリシーを作成する必要があります。

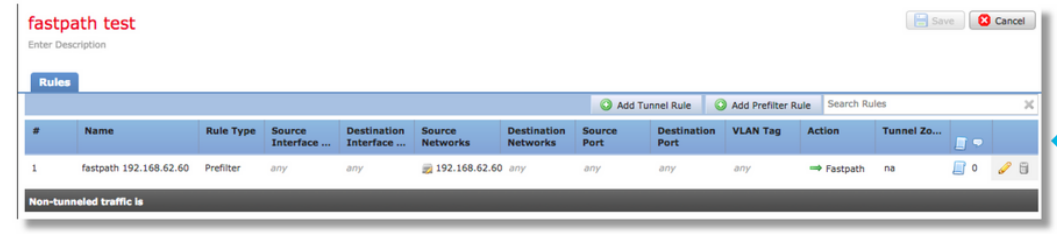
その後、新しく作成したPrefilter Policyをアクセスコントロールポリシーに関連付ける必要があります。これは、[プレフィルタポリシーの設定]セクションの[アクセスコントロールポリシー]の[**詳**

細設定]タブで設定します。

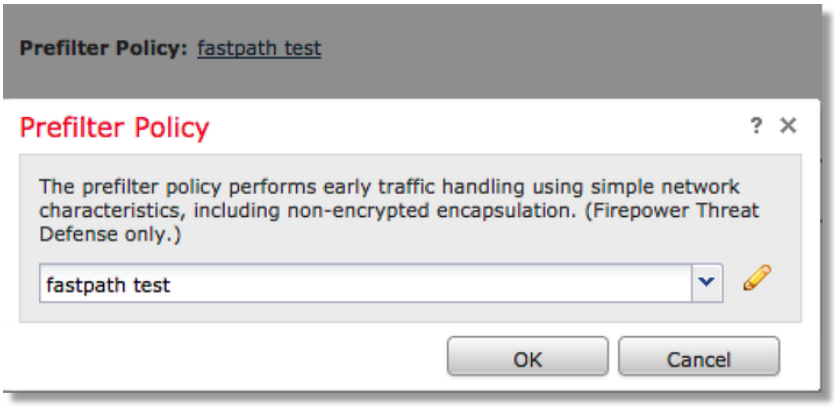
次に、プレフィルタポリシー内でFastpathルールを作成し、ヒットカウントを確認する方法の例を示します。



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

プレフィルタポリシーの操作と構成の詳細については、ここをクリックしてください。

PreFilterポリシーを追加してトラフィックの問題を解決した場合は、必要に応じてルールを残すことができます。ただし、そのフローに対する検査は行われません。Firepowerソフトウェアの詳細なトラブルシューティングを実行する必要があります。

Prefilter Policyを追加しても問題が解決しない場合は、トレースステップを含むパケットを再度実行して、パケットの新しいパスをトレースできます。

TACに提供するデータ

Data	手順
コマンド出力	手順については、
パケット キャプチャ	ASA/LINAの場合 configure-asa-00. Firepowerの場合 technote-sourcefi
ASAの「show tech」出力	ASA CLIにログイ 出力ファイルを提 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

次のステップ

Firepowerソフトウェアコンポーネントが問題の原因であると判断された場合は、次のステップとして、セキュリティインテリジェンスから始めて、各コンポーネントを体系的に除外します。

ここをクリックして、次のガイドに進みます。