

Fehlerbehebung für FirePOWER Data Path 2: DAQ-Schicht

Inhalt

[Einführung](#)

[Plattform-Leitfaden](#)

[Fehlerbehebung in der FirePOWER-DAQ-Phase](#)

[Erfassen von Datenverkehr auf der DAQ-Ebene](#)

[Umgehung der FirePOWER](#)

[SFR - Aktivieren Sie den Modus "Monitor Only" \(Nur Überwachung\) für das FirePOWER-Modul.](#)

[FTD \(alle\) - Inline-Sets in TAP-Modus schalten](#)

[Verwenden von Packet Tracer zur Fehlerbehebung bei simuliertem Datenverkehr](#)

[SFR - Ausführen von Packet Tracer auf ASA CLI](#)

[FTD \(alle\) - Packet Tracker auf der FTD-CLI ausführen](#)

[Beheben von Live-Datenverkehr mit Trace mithilfe von Capture with Trace](#)

[FTD \(alle\) - Erfassung mit Trace auf der FMC-GUI ausführen](#)

[Erstellen einer PreFilter Fastpath-Regel in FTD](#)

[Daten für TAC](#)

[Nächster Schritt](#)

Einführung

Dieser Artikel ist Teil einer Reihe von Artikeln, in denen erläutert wird, wie der Datenpfad auf FirePOWER-Systemen systematisch behoben wird, um festzustellen, ob Komponenten von FirePOWER den Datenverkehr beeinträchtigen können. Weitere Informationen zur Architektur von FirePOWER-Plattformen und Links zu anderen Artikeln zur Fehlerbehebung für Datenpfade finden Sie im [Übersichtsartikel](#).

In diesem Artikel betrachten wir die zweite Phase der Fehlerbehebung für den FirePOWER-Datenpfad: die Datenerfassungs-Schicht (DAQ).



Plattform-Leitfaden

Die folgende Tabelle beschreibt die in diesem Artikel behandelten Plattformen.

Plattformcode-Name	Beschreibung	Anwendbar Hardware Plattformen	Hinweise
SFR	Installiertes ASA mit FirePOWER Services (SFR)-Modul.	Serie ASA-5500-X	K/A

FTD (alle)	Gilt für alle Firepower Threat Defense (FTD)-Plattformen	ASA-5500-X-Serie, virtuelle NGFW-Plattformen, FPR-2100, FPR-9300, FPR-4100	K/A
FTD (nicht SSP und FPR-2100)	FTD-Image auf einer ASA oder virtuellen Plattform installiert	ASA-5500-X-Serie, virtuelle NGFW-Plattformen, FPR-2100	K/A
FTD (SSP)	FTD als logisches Gerät auf einem FXOS-basierten Chassis (FirePOWER eXtensible Operative System) installiert	FPR-9300, FPR-4100	Die Serie 2100 verwendet den FXOS Chassis Manager nicht.

Fehlerbehebung in der FirePOWER-DAQ-Phase

Die Datenerfassungs-Schicht (DAQ) ist eine Komponente von FirePOWER, die Pakete in eine Form übersetzt, die leicht verständlich ist. Es behandelt das Paket zunächst, wenn es an Snort gesendet wird. Wenn die Pakete die FirePOWER-Appliance empfangen, aber nicht auslaufen, oder die Fehlerbehebung für den Paketeingang keine nützlichen Ergebnisse erbracht hat, kann die Fehlerbehebung für die Datenerfassung nützlich sein.

Erfassen von Datenverkehr auf der DAQ-Ebene

Um eine Eingabeaufforderung zu erhalten, von der aus die Erfassung ausgeführt werden soll, müssen Sie zuerst über SSH eine Verbindung zur SFR- oder FTD-IP-Adresse herstellen.

Hinweis: Geben Sie auf den FPR-9300- und 4100-Geräten **connect ftd** zuerst ein, um an der zweiten > Eingabeaufforderung zu enden. Sie können auch SSH in die IP-Adresse des FXOS-Chassis-Managers eingeben und dann **die Konsole des Verbindungsmoduls 1** eingeben, gefolgt von **Verbinden mit ftd**.

In diesem [Artikel](#) wird beschrieben, wie Paketerfassungen auf der FirePOWER-DAQ-Ebene erfasst werden.

Beachten Sie, dass die Syntax nicht mit dem auf ASA verwendeten **Capture**-Befehl identisch ist, ebenso wie mit dem LINA-Teil der FTD-Plattform. Hier ein Beispiel für eine Datenerfassung über ein FTD-Gerät:

```
> 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
```

Wie im obigen Screenshot gezeigt, wurde eine Aufnahme im PCAP-Format namens ct.pcap in das `/ngfw/var/common` Verzeichnis (`/var/common` auf der SFR-Plattform) geschrieben. Diese Erfassungsdateien können aus dem FirePOWER-Gerät von der Eingabeaufforderung `>` kopiert werden, indem Sie die Anweisungen in dem oben genannten [Artikel](#) verwenden.

Alternativ können Sie im FirePOWER Management Center (FMC) in FirePOWER 6.2.0 und höher zu **Devices > Device Management (Geräte > Gerätemanagement)** navigieren. Klicken Sie anschließend auf die Schaltfläche  neben dem betreffenden Gerät, gefolgt von **Advanced Troubleshooting > File Download**.

Sie können dann den Namen der Erfassungsdatei eingeben und auf Herunterladen klicken.



Umgehung der FirePOWER

Wenn FirePOWER den Datenverkehr sieht, aber festgestellt wurde, dass die Pakete das Gerät nicht aussenden oder ein anderes Problem mit dem Datenverkehr besteht, besteht der nächste Schritt darin, die FirePOWER-Prüfphase zu umgehen, um zu bestätigen, dass eine der FirePOWER-Komponenten den Datenverkehr verwirft. Im Folgenden wird die schnellste Methode

zur Umgehung der FirePOWER-Datenverkehr auf den verschiedenen Plattformen dargestellt.

SFR - Aktivieren Sie den Modus "Monitor Only" (Nur Überwachung) für das FirePOWER-Modul.

Auf der ASA, die das SFR hostet, können Sie das SFR-Modul über die ASA Command Line Interface (CLI) oder den Cisco Adaptive Security Device Manager (ASDM) im Modus "Monitor Only" platzieren. Dadurch wird nur eine Kopie der Live-Pakete an das SFR-Modul gesendet.

Um das SFR-Modul über die ASA CLI in den Modus "Monitor Only" (Nur Überwachung) zu versetzen, müssen die für die SFR-Umleitung verwendete Klassenzuordnung und Richtlinienzuordnung zunächst mithilfe des Befehls **show service-policy sfr** bestimmt werden.

```
# 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
```

Die Ausgabe zeigt, dass die global_policy-Map die sfr fail-open-Aktion in der "sfr"-Klassenzuordnung erzwingt.

Hinweis: "Fail-Close" ist auch ein Modus, in dem die SFR ausgeführt werden kann. Er wird jedoch nicht so häufig verwendet, da er den gesamten Datenverkehr blockiert, wenn das SFR-Modul ausgefallen ist oder nicht reagiert.

Um das SFR-Modul in den Nur-Monitor-Modus zu versetzen, können Sie die folgenden Befehle ausführen, um die aktuelle SFR-Konfiguration zu vernachlässigen und die Konfiguration nur für den Monitor einzugeben:

```
# 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...
```

Nachdem das Modul in den Modus "Monitor-only" (Nur Monitor) versetzt wurde, kann es in der Ausgabe **"show service-policy sfr"** überprüft werden.

```
# 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
```

Hinweis: Um das SFR-Modul wieder in den Inline-Modus zu versetzen, führen Sie den Befehl **no sfr fail-open monitor-only** über die oben dargestellte **(config-pmap-c)#**-Eingabeaufforderung aus, gefolgt vom Befehl **sfr {fail-open | fail-close}**-Befehl, der ursprünglich vorhanden war.

Alternativ können Sie das Modul auch über das ASDM nur auf Monitor aufstellen, indem Sie zu **Configuration > Firewall > Service Policy Rules** (Konfiguration > Firewall > Service Policy Rules) navigieren. Klicken Sie dann auf die entsprechende Regel. Wechseln Sie anschließend zur Seite **Regelaktionen**, und klicken Sie auf die Registerkarte **ASA FirePOWER-Inspektion**. Danach kann **Monitor only (Nur Monitor)** ausgewählt werden.

Wenn das Datenverkehrsproblem auch dann besteht, wenn bestätigt wurde, dass sich das SFR-Modul nur im Überwachungsmodus befindet, verursacht das FirePOWER-Modul das Problem nicht. Der Packet Tracer kann dann ausgeführt werden, um weitere Probleme auf ASA-Ebene zu diagnostizieren.

Wenn das Problem nicht mehr besteht, besteht der nächste Schritt in der Fehlerbehebung für die FirePOWER-Softwarekomponenten.

FTD (alle) - Inline-Sets in TAP-Modus schalten

Wenn der Datenverkehr durch Schnittstellenpaare geleitet wird, die in Inline-Sets konfiguriert wurden, kann der Inline-Satz in den TAP-Modus versetzt werden. Dies bewirkt im Wesentlichen, dass FirePOWER keine Maßnahmen für das Live-Paket ergreift. Sie gilt nicht für den Router- oder transparenten Modus ohne Inline-Sätze, da das Gerät die Pakete ändern muss, bevor sie an den nächsten Hop gesendet werden, und nicht in einen Umgehungsmodus versetzt werden kann, ohne den Datenverkehr zu verwerfen. Bei Routing- und transparentem Modus ohne Inline-Sätze fahren Sie mit dem Schritt Packet Tracer fort.

Um den TAP-Modus über die FMC-Benutzeroberfläche zu konfigurieren, navigieren Sie zu **Devices > Device Management (Geräte > Gerätemanagement)**, und bearbeiten Sie dann das betreffende Gerät. Deaktivieren Sie auf der Registerkarte **Inline Sets** die Option für **TAP Mode**.

The screenshot shows the configuration page for 'Inline Sets' in a network management interface. The top navigation bar includes 'Devices', 'Routing', 'Interfaces', 'Inline Sets', and 'DHCP'. Below is a table with the following data:

Name	Interface Pairs
my_inline	inline1<->inline2

A callout box titled 'Edit Inline Set' is shown, with the 'Advanced' tab selected. It contains three options, each with a checkbox:

- Tap Mode:
- Propagate Link State:
- Strict TCP Enforcement:

The 'Tap Mode' checkbox is highlighted with a red rectangular box.

Wenn der TAP-Modus das Problem löst, besteht der nächste Schritt in der Fehlerbehebung für die FirePOWER-Softwarekomponenten.

Wenn der TAP-Modus das Problem nicht behebt, liegt das Problem außerhalb der FirePOWER-Software. Der Packet Tracer kann dann zur weiteren Diagnose des Problems verwendet werden.

Verwenden von Packet Tracer zur Fehlerbehebung bei simuliertem Datenverkehr

Packet Tracer ist ein Dienstprogramm, mit dem der Speicherort eines Paketverlusts ermittelt werden kann. Es ist ein Simulator, also führt er eine Spur eines künstlichen Pakets durch.

SFR - Ausführen von Packet Tracer auf ASA CLI

Nachfolgend finden Sie ein Beispiel für die Ausführung von Packet-Tracer auf der ASA-CLI für SSH-Datenverkehr. Ausführlichere Informationen zur Syntax des Befehls Packet Tracer finden Sie in diesem [Abschnitt](#) im Leitfaden zur ASA-Serie.

```
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
```

Im obigen Beispiel sehen wir sowohl das ASA- als auch das SFR-Modul, das die Pakete erlaubt, als auch nützliche Informationen darüber, wie die ASA den Paketfluss handhaben würde.

FTD (alle) - Packet Tracker auf der FTD-CLI ausführen

Auf allen FTD-Plattformen kann der Befehl Packet Tracer über die FTD-CLI ausgeführt werden.

```
> 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
```

In diesem Beispiel zeigt Packet Tracer den Grund für das Verwerfen an. In diesem Fall ist es die IP-Blacklist innerhalb der Security Intelligence-Funktion in Firepower, die das Paket blockiert. Der nächste Schritt wäre die Fehlerbehebung für die einzelne FirePOWER-Softwarekomponente, die den Ausfall verursacht.

Beheben von Live-Datenverkehr mit Trace mithilfe von Capture with Trace

Der Live-Datenverkehr kann auch über die Trace-Funktion verfolgt werden, die auf allen Plattformen über die CLI verfügbar ist. Im Folgenden finden Sie ein Beispiel für das Ausführen einer Erfassung mit Ablaufverfolgung für SSH-Datenverkehr.

```
> 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
```

In diesem Beispiel wurde das vierte Paket in der Erfassung verfolgt, da es das erste Paket mit definierten Anwendungsdaten ist. Wie gezeigt, wird das Paket schließlich durch Snort Whitelist dargestellt, d. h., für den Fluss ist keine weitere Snort-Überprüfung erforderlich und insgesamt zulässig.

Weitere Informationen zur Erfassung mit Ablaufverfolgungssyntax finden Sie in diesem [Abschnitt](#) im Leitfaden zur ASA-Serie-Befehlsreferenz.

FTD (alle) - Erfassung mit Trace auf der FMC-GUI ausführen

Auf den FTD-Plattformen kann die Erfassung mit Trace auf der FMC-Benutzeroberfläche ausgeführt werden. Um auf das Dienstprogramm zuzugreifen, wählen Sie **Geräte > Gerätemanagement** aus.

Klicken Sie anschließend auf die Schaltfläche  neben dem betreffenden Gerät, gefolgt von **Advanced Troubleshooting > Capture with Trace**.

Im Folgenden finden Sie ein Beispiel, wie eine Erfassung mit trace über die GUI ausgeführt wird.

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

Name	Interface	Type	Trace	Buffer Mode	Buffer Size	Packet Length	Buffer Status	Protocol	Source	Destination	Status
Test	Inside	raw-data	✓	🔄	524288	1518	Capturing	TCP	192.168.1.200	any	Running

View of all current captures

```

Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

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

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found flow with id 2672128, using existing flow

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

Phase: 5
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Verdict: (block-packet) drop this packet
Result:
input-interfaces: Inside
input-status: up

```

Example output shows the packet was blocked by Snort

Wenn die Erfassung mit Ablaufverfolgung die Ursache für den Paketverlust anzeigt, besteht der nächste Schritt darin, die Fehler für die einzelnen Softwarekomponenten zu beheben.

Wenn die Ursache des Problems nicht eindeutig angezeigt wird, besteht der nächste Schritt darin, den Datenverkehr schnell zu leiten.

Erstellen einer PreFilter Fastpath-Regel in FTD

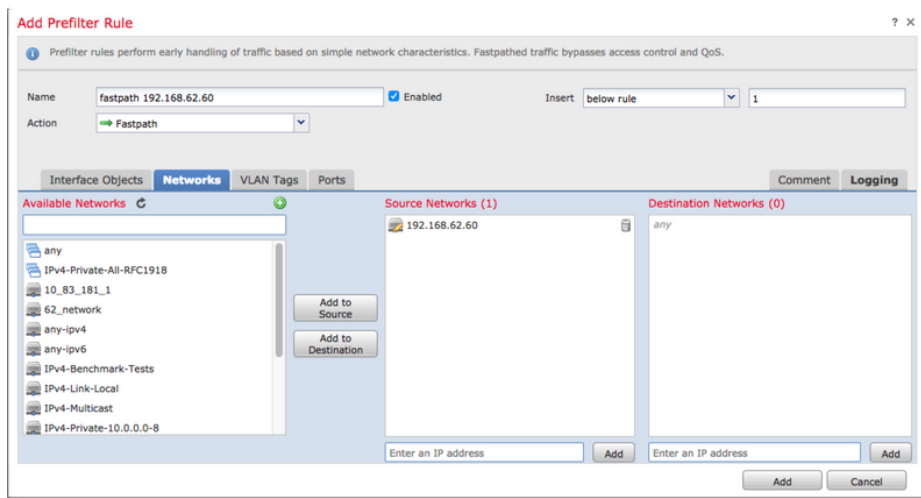
Auf allen FTD-Plattformen gibt es eine Richtlinie vor dem Filtern, mit der der Datenverkehr von der FirePOWER-(Snort-)Inspektion umgeleitet werden kann.

Im FMC finden Sie diese Informationen unter **Richtlinien > Zugriffskontrolle > Vorfilter**. Die Standard-Policy vor dem Filter kann nicht bearbeitet werden. Daher muss eine benutzerdefinierte Richtlinie erstellt werden.

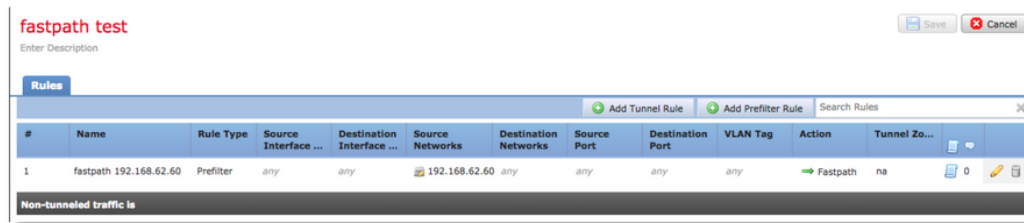
Danach muss die neu erstellte Vorfilterrichtlinie der Zugriffskontrollrichtlinie zugeordnet werden.

Dies wird auf der Registerkarte Erweitert der Zugriffskontrollrichtlinie im Abschnitt **Voreingestellte** Richtlinieneinstellungen konfiguriert.

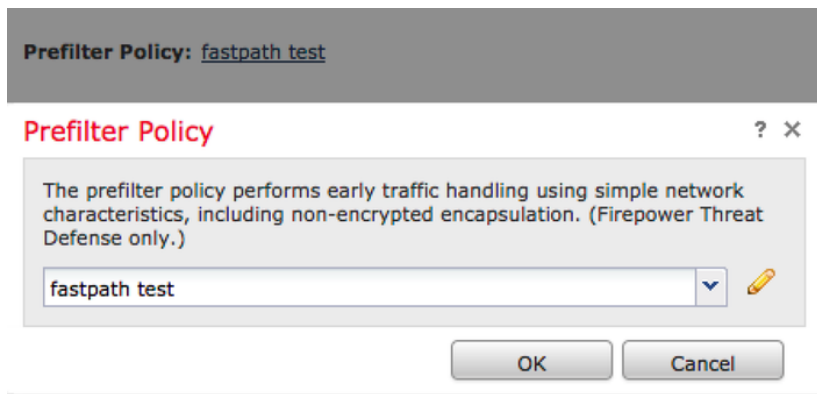
Im Folgenden finden Sie ein Beispiel für das Erstellen einer Fastpath-Regel in einer Vorfilterrichtlinie und das Überprüfen der Trefferanzahl.



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

[Klicken Sie hier](#), um weitere Informationen über den Betrieb und die Konfiguration von Prefilter Policies zu erhalten.

Wenn das Problem mit dem Datenverkehr durch Hinzufügen einer PreFilter Policy gelöst wird, kann die Regel bei Bedarf an der richtigen Stelle belassen werden. Dieser Fluss wird jedoch nicht erneut überprüft. Weitere Fehlerbehebungen für die FirePOWER-Software müssen durchgeführt werden.

Wenn das Problem durch Hinzufügen der Vorfilterrichtlinie nicht behoben wird, kann das Paket mit

dem Ablaufverfolgungsschritt erneut ausgeführt werden, um den neuen Pfad des Pakets zu verfolgen.

Daten für TAC

Daten	Anweisungen
Befehlsausgaben	Anweisungen hierzu finden Sie in diesem Artikel Für ASA/LINA: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-s
Paketerfassung	asa-00.html Für FirePOWER: http://www.cisco.com/c/en/us/support/docs/security/sourcefire-fir sourcefire-00.html
ASA-Ausgabe "show tech"	Melden Sie sich bei der ASA CLI an, und lassen Sie die Terminalsitzung in einem techcommand ein, und stellen Sie dann die Ausgabedatei für die Terminalsitzung Diese Datei kann mit diesem Befehl auf der Festplatte oder einem externen Speicher Showtechnik Redirect disk0:/show_tech.log
Fehlerbehebungsdatei vom FirePOWER-Gerät, die den Datenverkehr prüft	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117

Nächster Schritt

Wenn festgestellt wurde, dass eine FirePOWER-Softwarekomponente die Ursache des Problems ist, besteht der nächste Schritt darin, jede Komponente systematisch auszuschließen, angefangen mit Security Intelligence.

Klicken Sie [hier](#), um mit dem nächsten Leitfaden fortzufahren.