

Firepower 데이터 경로 문제 해결 2단계: DAQ 레이어

목차

- [소개](#)
- [플랫폼 가이드](#)
- [Firepower DAQ 문제 해결 단계](#)
- [DAQ 레이어에서 트래픽 캡처](#)
- [Firepower를 우회하는 방법](#)
- [SFR - Firepower 모듈을 모니터링 전용 모드로 설정](#)
- [FTD\(모두\) - 인라인 집합을 TAP 모드로 설정](#)
- [패킷 트레이서를 사용하여 시뮬레이션된 트래픽 문제 해결](#)
- [SFR - ASA CLI에서 패킷 트레이서 실행](#)
- [FTD\(모두\) - FTD CLI에서 패킷 트레이서 실행](#)
- [추적을 사용한 캡처를 활용하여 라이브 트래픽 문제 해결](#)
- [FTD\(모두\) - FMC GUI에서 추적을 사용한 캡처 실행](#)
- [FTD에서 사전 필터 단축경로\(Fastpath\) 규칙 생성](#)
- [TAC에 제공할 데이터](#)
- [다음 단계](#)

소개

이 문서는 Firepower 시스템의 데이터 경로 문제를 체계적으로 해결하여 Firepower의 구성 요소가 트래픽에 영향을 미치는지 여부를 확인하는 방법을 설명하는 일련의 문서 중 일부입니다. Firepower 플랫폼의 아키텍처에 대한 자세한 내용은 [개요 문서](#)를 참조하고 다른 데이터 경로 문제 해결 문서에 대한 링크를 참조하십시오.

이 문서에서는 Firepower 데이터 경로 문제 해결의 2단계인 DAQ(Data Acquisition) 레이어를 살펴봅니다.



플랫폼 가이드

다음 표에서는 이 문서에서 다루는 플랫폼에 대해 설명합니다.

플랫폼 코드 이름	설명	적용 가능 하드웨어 플랫폼	참고
SFR	FirePOWER 서비스 (SFR) 모듈이 설치된 ASA	ASA 5500-X 시리즈	해당 없음
FTD(모두)	모든 FTD(Firepower Threat Defense) 플랫폼	ASA-5500-X 시리즈, 가상 NGFW 플랫폼, FPR-2100,	해당 없음

	폼에 적용	FPR-9300, FPR-4100	
FTD(비 SSP 및 FPR-2100)	ASA 또는 가상 플랫폼에 설치된 FTD 이미지	ASA-5500-X 시리즈, 가상 NGFW 플랫폼, FPR-2100	해당 없음
FTD(SSP)	FXOS(Firepower eXtensible Operative System) 기반 새시에 논리적 디바이스로 설치된 FTD	FPR-9300, FPR-4100	2100 시리즈는 FXOS 새시 관리자를 사용하지 않음

Firepower DAQ 문제 해결 단계

DAQ(Data Aquisition) 레이어는 패킷을 Snort가 이해할 수 있는 형식으로 변환하는 Firepower의 구성 요소입니다. 처음에 패킷이 Snort로 전송되면 처리합니다. 따라서 패킷이 Firepower 어플라이언스에 인그레스되지만 이그레스되지 않는 경우 또는 패킷 인그레스 문제 해결에서 유용한 결과를 얻지 못한 경우 DAQ 문제 해결이 유용할 수 있습니다.

DAQ 레이어에서 트래픽 캡처

캡처를 실행할 프롬프트를 표시하려면 먼저 SSH를 사용하여 SFR 또는 FTD IP 주소에 연결해야 합니다.

참고: FPR-9300 및 4100 디바이스에서 먼저 **connect ftd**를 입력하여 두 번째 > 프롬프트에서 종료합니다. SSH를 통해 FXOS 새시 관리자 IP에 연결한 다음 **connect module 1 console**과 **connect ftd**를 차례로 입력할 수도 있습니다.

이 [문서](#)에서는 Firepower DAQ 레벨에서 패킷 캡처를 수집하는 방법을 설명합니다.

구문이 FTD 플랫폼의 LINA 측뿐만 아니라 ASA에서 사용되는 **capture** 명령과 어떻게 다른지 확인하십시오. 다음은 FTD 디바이스에서 실행되는 DAQ 패킷 캡처의 예입니다.

```
> 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
```

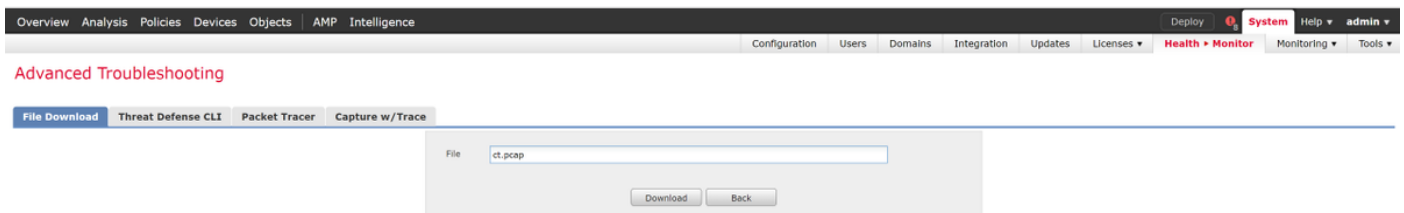
```
admin@ciscoasa:~$ ls /ngfw/var/common/
```

```
ct.pcap
```

위의 스크린샷에서 볼 수 있듯이 ct.pcap이라는 PCAP 형식의 캡처가 /ngfw/var/common 디렉토리 (SFR 플랫폼의 /var/common)에 작성되었습니다. 위에서 언급한 [문서](#)의 지침을 사용하여 > 프롬프트에서 Firepower 디바이스 외부로 이러한 캡처 파일을 복사할 수 있습니다.

또는 Firepower 버전 6.2.0 이상의 FMC(Firepower Management Center)에서 디바이스 > 디바이스 관리로 이동합니다. 그런 다음  해당 디바이스 옆의 아이콘과 **Advanced Troubleshooting(고급 문제 해결)** > **File Download(파일 다운로드)**가 차례로 나타납니다.

그런 다음 캡처 파일의 이름을 입력하고 다운로드를 클릭할 수 있습니다.



Firepower를 우회하는 방법

Firepower에서 트래픽이 확인되지만, 패킷이 디바이스를 이그레스하지 않는 것으로 확인되었거나 트래픽에 또 다른 문제가 있는 경우, 다음 단계로 Firepower 검사 단계를 우회하여 Firepower 구성 요소 중 하나가 트래픽을 삭제 중인지 확인합니다. 다음은 다양한 플랫폼에서 트래픽이 Firepower를 우회하도록 하는 가장 빠른 방법에 대한 자세한 설명입니다.

SFR - Firepower 모듈을 모니터링 전용 모드로 설정

SFR을 호스팅하는 ASA에서는 ASA CLI(Command Line Interface) 또는 Cisco ASDM(Adaptive Security Device Manager)을 통해 SFR 모듈을 모니터링 전용 모드로 설정할 수 있습니다. 이렇게 하면 라이브 패킷의 복사본만 SFR 모듈로 전송됩니다.

ASA CLI를 통해 SFR 모듈을 모니터링 전용 모드로 설정하려면 먼저 **show service-policy sfr** 명령을 실행하여 SFR 리디렉션에 사용되는 class-map 및 policy-map을 확인해야 합니다.

```
# 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
```

출력은 global_policy 정책 맵이 "sfr" class-map에서 sfr fail-open 작업을 적용하고 있음을 보여줍니다.

참고: "fail-close"도 SFR을 실행할 수 있는 모드이지만, SFR 모듈이 다운되거나 응답하지 않는 경우 모든 트래픽을 차단하므로 일반적으로 사용되지 않습니다.

SFR 모듈을 모니터링 전용 모드로 설정하려면 다음 명령을 실행하여 현재 SFR 설정을 무효화하고 모니터링 전용 설정을 입력할 수 있습니다.

```
# 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...
```

모듈을 모니터링 전용 모드로 설정하면 **show service-policy sfr** 출력에서 확인할 수 있습니다.

```
# 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
```

참고: SFR 모듈을 다시 인라인 모드로 설정하려면 위에 표시된 (config-pmap-c)# 프롬프트에서 **no sfr fail-open monitor-only** 명령을 실행한 다음 원래 거기에 있었던 **sfr {fail-open | fail-close}** 명령을 실행하십시오.

또는 ASDM을 통해 **설정 > 방화벽 > 서비스 정책 규칙**으로 이동하여 모듈을 모니터링 전용으로 설정할 수 있습니다. 그런 다음 해당 규칙을 클릭합니다. 다음으로, 규칙 작업 페이지로 이동하여 **ASA Firepower 검사** 탭을 클릭합니다. 그런 다음 **모니터링 전용**을 선택할 수 있습니다.

SFR 모듈이 모니터링 전용 모드인 것을 확인한 후에도 트래픽 문제가 계속되면 Firepower 모듈이 문제를 일으키는 것이 아닙니다. 그러면 패킷 트레이서를 실행하여 ASA 레벨에서 문제를 추가 진단

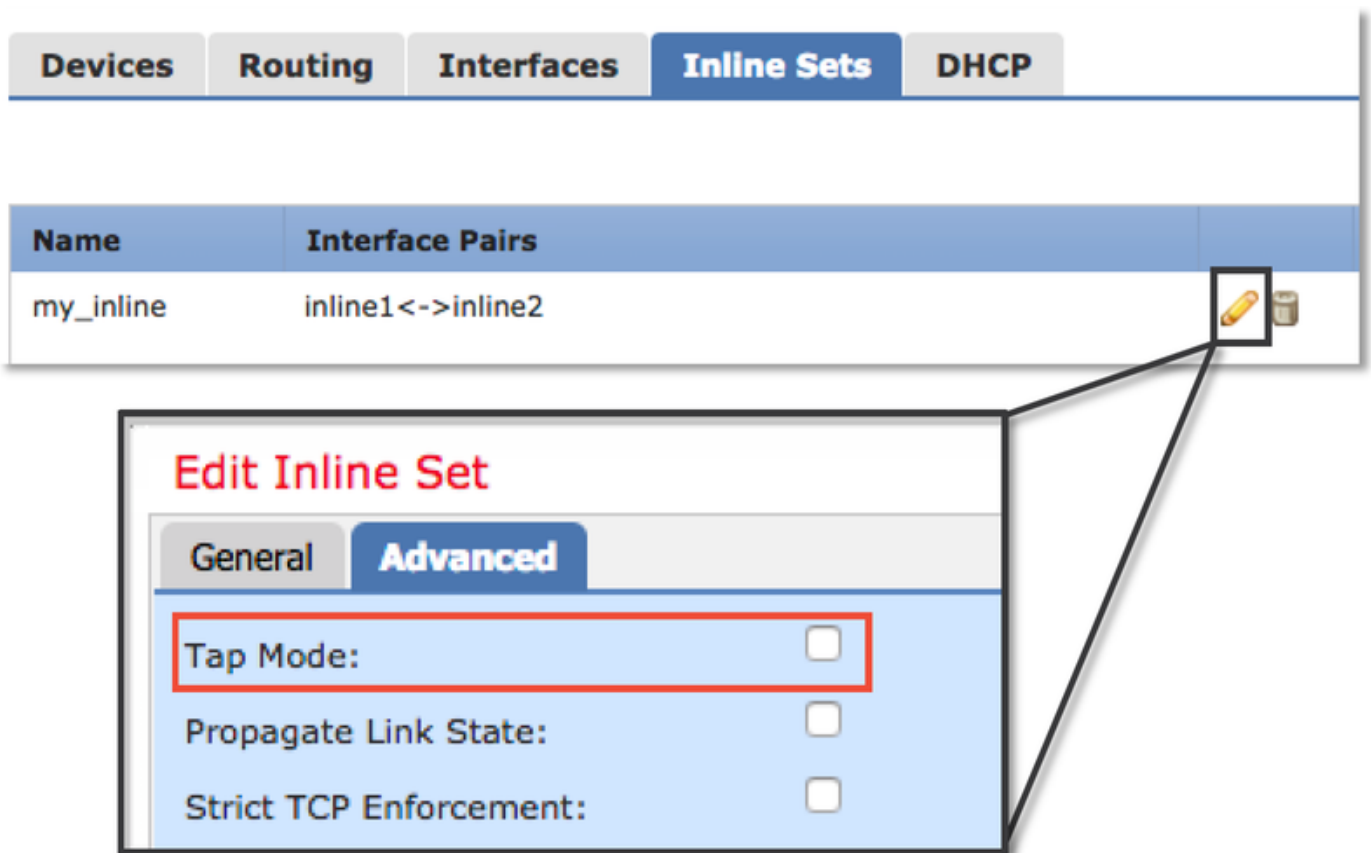
단할 수 있습니다.

문제가 더 이상 지속되지 않는 경우 다음 단계는 Firepower 소프트웨어 구성 요소의 문제 해결을 수행하는 것입니다.

FTD(모두) - 인라인 집합을 TAP 모드로 설정

트래픽이 인라인 집합에 구성된 인터페이스 쌍을 통과하는 경우 인라인 집합을 TAP 모드로 설정할 수 있습니다. 그러면 Firepower에서 라이브 패킷에 대해 작업을 수행하지 않습니다. 이는 인라인 집합이 없는 라우터 또는 투명 모드에는 적용되지 않습니다. 디바이스에서는 다음 홉으로 전송하기 전에 패킷을 수정해야 하며 트래픽을 삭제하지 않고는 우회 모드로 디바이스를 설정할 수 없기 때문입니다. 인라인 집합이 없는 라우팅 및 투명 모드의 경우 패킷 트레이서 단계를 진행합니다.

FMC UI(사용자 인터페이스)에서 TAP 모드를 설정하려면 **디바이스 > 디바이스 관리**로 이동한 다음 해당 디바이스를 편집합니다. **인라인 집합** 탭에서 **TAP 모드** 옵션을 선택합니다.



TAP 모드에서 문제가 해결되면 다음 단계는 Firepower 소프트웨어 구성 요소의 문제 해결을 수행하는 것입니다.

TAP 모드에서 문제가 해결되지 않으면 Firepower 소프트웨어 외부의 문제일 수 있습니다. 그러면 패킷 트레이서를 사용하여 문제를 추가 진단할 수 있습니다.

패킷 트레이서를 사용하여 시뮬레이션된 트래픽 문제 해결

패킷 트레이서는 패킷 삭제 위치를 식별하는 데 도움이 되는 유틸리티입니다. 이는 시뮬레이터이므로 인공 패킷의 추적을 수행합니다.

SFR - ASA CLI에서 패킷 트레이서 실행

다음은 SSH 트래픽에 대해 ASA CLI에서 패킷 트레이서를 실행하는 방법의 예입니다. 패킷 트레이서 명령의 구문에 대한 보다 자세한 내용은 ASA 시리즈 명령 참조 가이드의 이 [섹션](#)을 참조하십시오.

```

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

```

위의 예에서는 패킷을 허용하는 ASA 및 SFR 모듈과 ASA에서 패킷 플로우를 처리하는 방법에 대한 유용한 정보를 확인할 수 있습니다.

FTD(모두) - FTD CLI에서 패킷 트레이서 실행

모든 FTD 플랫폼에서 FTD CLI를 통해 패킷 트레이서 명령을 실행할 수 있습니다.

```
> 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
```

이 예에서 패킷 트레이서는 삭제 이유를 보여줍니다. 이 경우, 패킷을 차단하는 Firepower의 보안 인텔리전스 기능 내 IP 블랙리스트가 이유입니다. 다음 단계로, 삭제를 유발하는 개별 Firepower 소프트웨어 구성 요소의 문제 해결을 수행합니다.

추적을 사용한 캡처를 활용하여 라이브 트래픽 문제 해결

추적 기능을 사용한 캡처를 통해 라이브 트래픽을 추적할 수도 있으며 이는 CLI를 통해 모든 플랫폼에서 사용할 수 있습니다. 다음은 SSH 트래픽에 대해 추적을 사용한 캡처를 실행하는 예입니다.

```
> 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
```

이 예에서는 캡처의 네 번째 패킷이 추적되었는데, 이 패킷이 애플리케이션 데이터가 정의된 첫 번째 패킷이기 때문입니다. 표시된 대로 패킷은 Snort에 의해 화이트리스트에 추가됩니다. 즉, 플로우에 대해 추가 Snort 검사가 필요하지 않으며 전체적으로 허용됩니다.

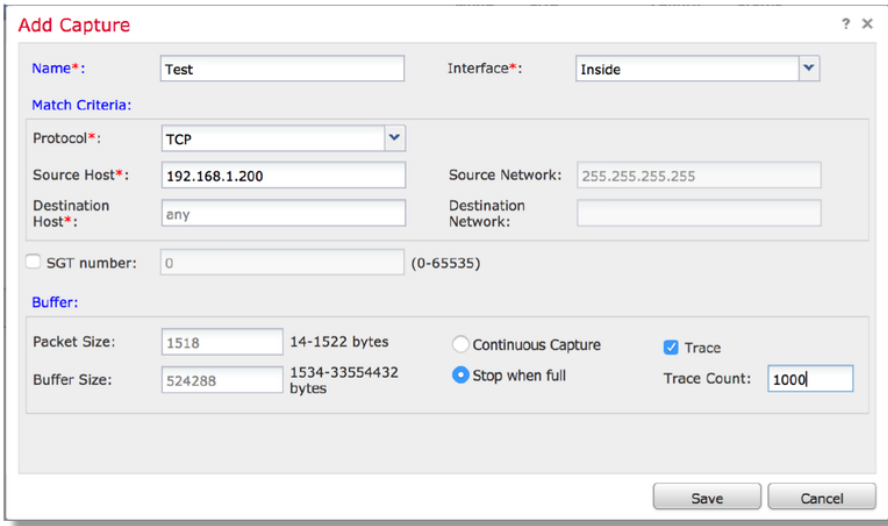
추적을 사용한 캡처 구문에 대한 자세한 내용은 ASA 시리즈 명령 참조 가이드의 이 [섹션](#)을 참조하십시오.

FTD(모두) - FMC GUI에서 추적을 사용한 캡처 실행

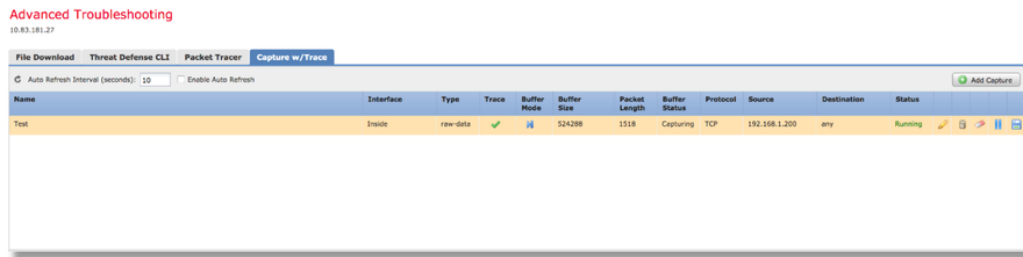
FTD 플랫폼에서 추적을 사용한 캡처는 FMC UI에서 실행할 수 있습니다. 유틸리티에 액세스하기 위해 **디바이스 > 디바이스 관리**로 이동합니다.

그런 다음  해당 디바이스 옆의 아이콘과 **Advanced Troubleshooting(고급 트러블슈팅) > Capture w/Trace(추적을 통한 캡처)** 옆의 아이콘을 클릭합니다.

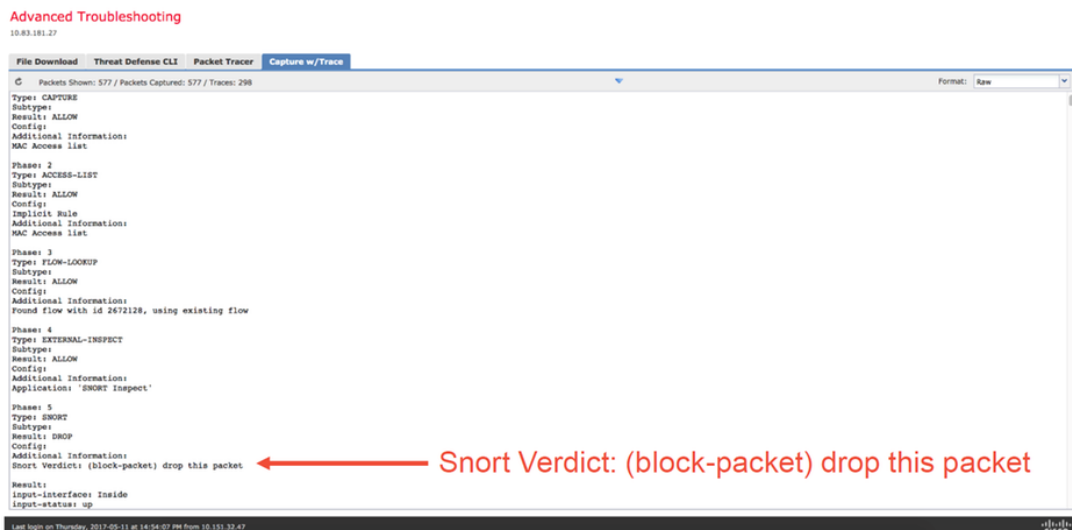
다음은 GUI를 통해 추적을 사용한 캡처를 실행하는 방법의 예입니다.



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



View of all current captures



Example output shows the packet was blocked by Snort

추적을 사용한 캡처에서 패킷 삭제의 원인이 표시되면 다음 단계로 개별 소프트웨어 구성 요소의 문제 해결을 수행합니다.

문제의 원인을 명확하게 표시하지 않는 경우 다음 단계로 트래픽의 단축경로(fastpath)를 지정합니다.

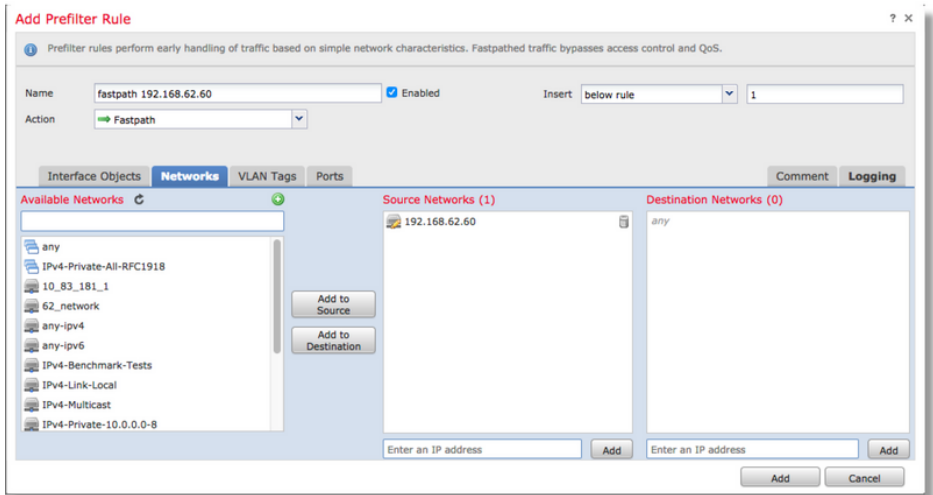
FTD에서 사전 필터 단축경로(Fastpath) 규칙 생성

모든 FTD 플랫폼에는 Firepower(Snort) 검사에서 트래픽을 전환하는 데 사용할 수 있는 사전 필터 정책이 있습니다.

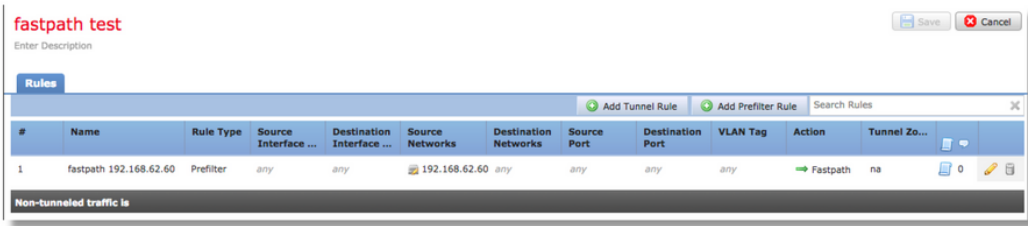
FMC에서는 **정책 > 액세스 제어 > 사전 필터** 아래에 있습니다. 기본 사전 필터 정책은 수정할 수 없으므로 맞춤형 정책을 생성해야 합니다.

그런 다음 새로 생성된 사전 필터 정책을 액세스 제어 정책과 연결해야 합니다. 이는 액세스 제어 정책의 고급 탭에 있는 **사전 필터 정책 설정** 섹션에서 설정합니다.

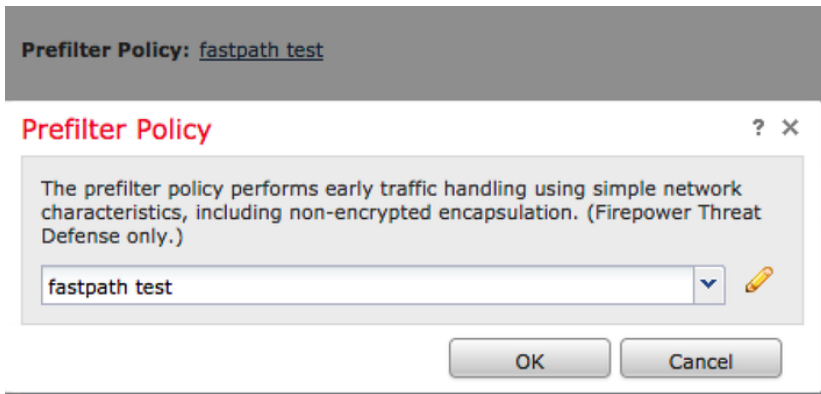
다음은 사전 필터 정책 내에서 단축경로(Fastpath) 규칙을 생성하고 적중 횟수를 확인하는 방법의 예입니다.



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

[사전 필터 정책의 작동 및 설정에 대한 자세한 내용을 보려면 여기를 클릭](#)하십시오.

사전 필터 정책을 추가하여 트래픽 문제가 해결되면, 원하는 경우 규칙을 그대로 둘 수 있습니다. 그러나 해당 플로우에 대한 추가 검사는 수행되지 않습니다. Firepower 소프트웨어의 추가 문제 해결을 수행해야 합니다.

사전 필터 정책을 추가해도 문제가 해결되지 않으면 패킷 추적 단계를 다시 실행하여 패킷의 새 경로를 추적할 수 있습니다.

TAC에 제공할 데이터

데이터
명령 출력

지침

지침은 이 문서를 참조하십시오.

ASA/LINA: <https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-gen/00.html>

패킷 캡처

Firepower: <http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-8000-sourcefire-00.html>

ASA 'show
tech' 출력

ASA CLI에 로그인하여 터미널 세션을 로그에 저장합니다. **show tech** 명령을 입력한 다음, T

다.

이 명령을 사용하여 이 파일을 디스크 또는 외부 스토리지 시스템에 저장할 수 있습니다.

```
show tech | redirect disk0:/show_tech.log
```

트래픽을 검
사하는

Firepower 디
바이스에서

파일 문제 해
결

<http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-tech>

다음 단계

Firepower 소프트웨어 구성 요소가 문제의 원인인 것으로 확인된 경우, 다음 단계로 보안 인텔리전스부터 시작하여 각 구성 요소를 체계적으로 배제합니다.

다음 가이드를 진행하려면 [여기](#)를 클릭하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.