firepower Threat Defense 캡처 및 패킷 추적기 사용

목차

소개

이 문서에서는 FTD(Firepower Threat Defense) 캡처 및 패킷 추적기 유틸리티를 사용하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

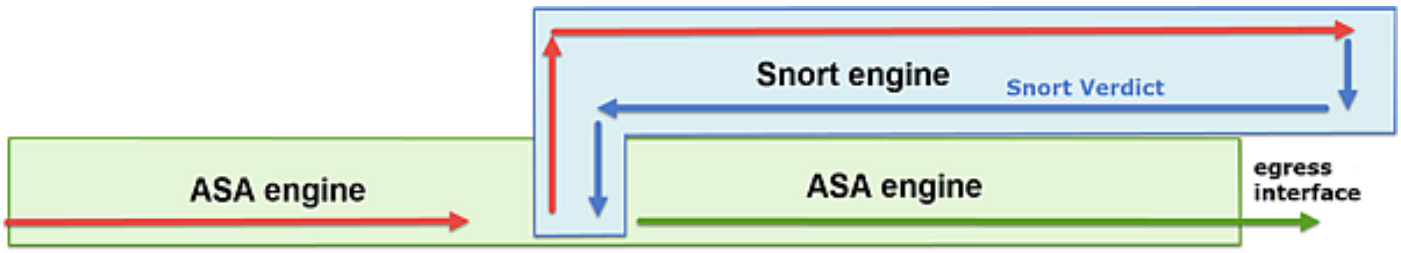
- FTD 소프트웨어 6.1.0을 실행하는 ASA5515-X
- FTD 소프트웨어 6.2.2를 실행하는 FPR4110
- FMC(Firepower Management Center) 소프트웨어 6.2.2를 실행하는 FS4000

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

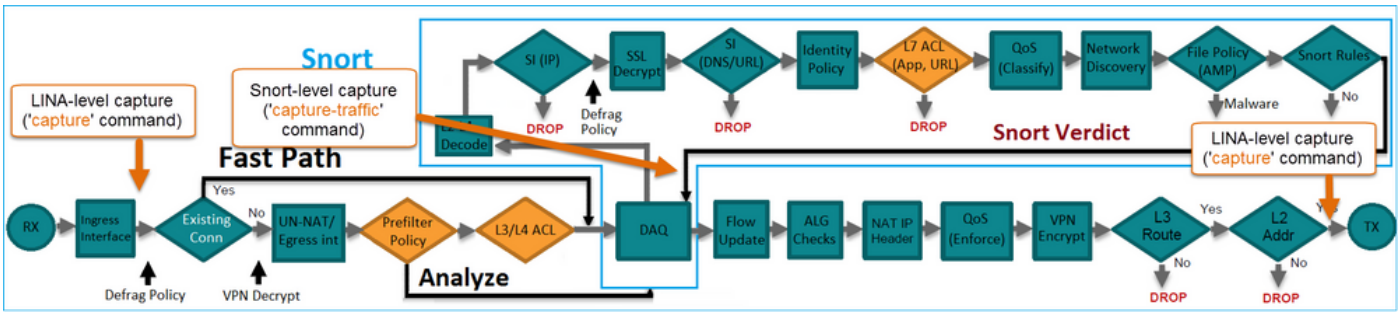
FTD 패킷 처리

FTD 패킷 처리는 다음과 같이 시각화됩니다.



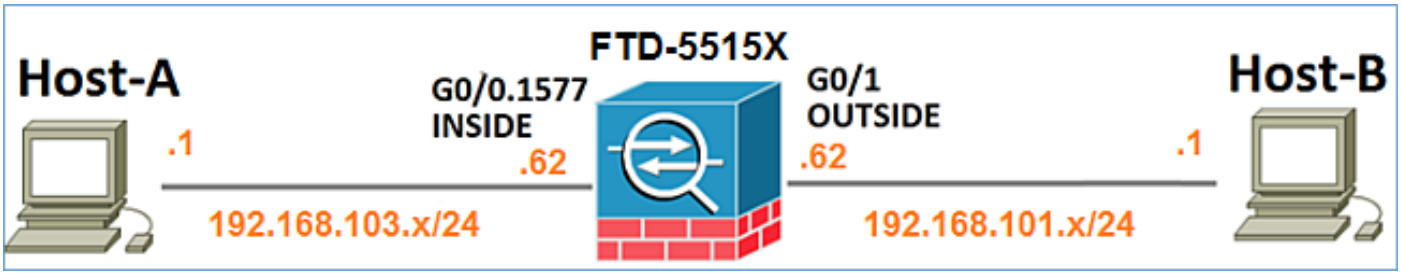
1. 패킷은 인그레스 인터페이스로 들어가며 LINA 엔진에서 처리됩니다.
2. 정책에 따라 Snort 엔진에서 패킷을 검사해야 하는 경우.
3. Snort 엔진이 패킷에 대한 판정을 반환합니다.
4. LINA 엔진은 Snort 판정을 기반으로 패킷을 삭제하거나 전달합니다.

아키텍처를 기반으로 FTD 캡처를 다음 위치에서 수행할 수 있습니다.



구성

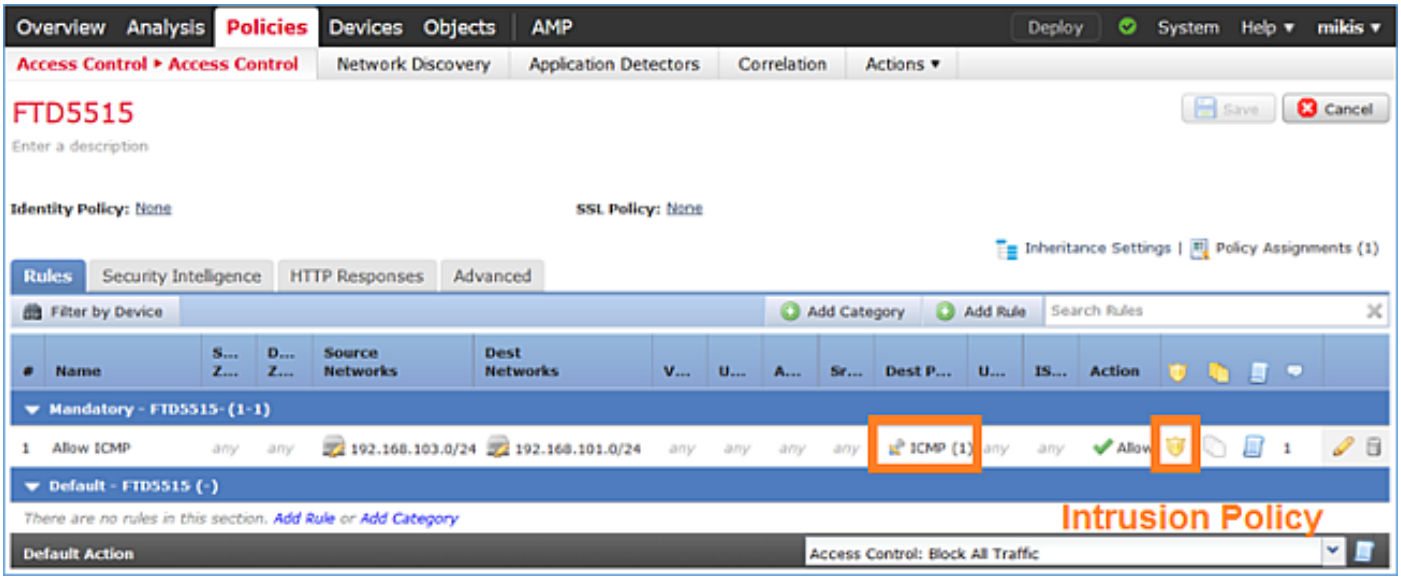
네트워크 다이어그램



Snort 엔진 캡처 작업

사전 요구 사항

FTD에 ICMP(Internet Control Message Protocol) 트래픽이 통과하도록 허용하는 ACP(Access Control Policy)가 적용됩니다. 정책에 침입 정책도 적용되어 있습니다.



요구 사항

1. 필터 없이 FTD CLISH 모드에서 캡처를 활성화합니다.

2. FTD를 ping하여 캡처된 출력을 확인합니다.

솔루션

1단계. FTD 콘솔 또는 SSH를 br1 인터페이스에 로그인하고 필터 없이 FTD CLISH 모드에서 캡처를 활성화합니다.

<#root>

>

capture-traffic

Please choose domain to capture traffic from:
  0 - br1
  1 - Router

Selection?

1

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:

FTD 6.0.x에서 명령은 다음과 같습니다.

<#root>

>

system support

capture-traffic

2단계. FTD를 통해 Ping하고 캡처된 출력을 확인합니다.

<#root>

>

capture-traffic

Please choose domain to capture traffic from:
  0 - br1
  1 - Router

Selection?

1

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
```

```
12:52:34.749945 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 1, le
12:52:34.749945 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq 1, leng
12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 2, le
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq 2, leng
12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 3, le
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq 3, leng
12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 4, le
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq 4, leng
^C    <- to exit press CTRL + C
```

Snort 엔진 캡처 작업

요구 사항

1. IP 192.168.101.1용 필터를 사용하여 FTD CLISH 모드에서 캡처를 활성화합니다.
2. FTD를 통해 Ping하고 캡처된 출력을 확인합니다.

솔루션

1단계. IP 192.168.101.1용 필터를 사용하여 FTD CLISH 모드에서 캡처를 활성화합니다.

<#root>

```
>
```

```
capture-traffic
```

```
Please choose domain to capture traffic from:
  0 - br1
  1 - Router

Selection?
```

```
1
```

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
```

```
host 192.168.101.1
```

2단계. FTD를 통해 Ping하고 캡처된 출력을 확인합니다.

```
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 0, leng
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 1, leng
```

```
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 2, len
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 3, len
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 4, len
```

-n 옵션을 사용하여 호스트와 포트 번호를 숫자 형식으로 볼 수 있습니다. 예를 들어, 이전 캡처는 다음과 같이 표시됩니다.

```
<#root>

>

capture-traffic


Please choose domain to capture traffic from:
  0 - br1
  1 - Router

Selection?

1


Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:

-n host 192.168.101.1

13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 0, length 80
13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 1, length 80
13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 2, length 80
13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 3, length 80
13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 4, length 80
```

Tcpdump 필터 예

예 1:

Src IP 또는 Dst IP = 192.168.101.1 및 Src 포트 또는 Dst 포트 = TCP/UDP 23을 캡처하려면 다음 명령을 입력합니다.

```
<#root>

Options:

-n host 192.168.101.1 and port 23
```

예 2:

소스 IP = 192.168.101.1 및 소스 포트 = TCP/UDP 23을 캡처하려면 다음 명령을 입력합니다.

<#root>

Options:

-n src 192.168.101.1 and src port 23

예 3:

소스 IP = 192.168.101.1 및 소스 포트 = TCP 23을 캡처하려면 다음 명령을 입력합니다.

<#root>

Options:

-n src 192.168.101.1 and tcp and src port 23

예 4:

소스 IP = 192.168.101.1을 캡처하고 패킷의 MAC 주소를 보려면 'e' 옵션을 추가하고 다음 명령을 입력합니다.

<#root>

Options:

-ne

src 192.168.101.1

17:57:48.709954

6c:41:6a:a1:2b:f6 > a8:9d:21:93:22:90,

ethertype IPv4 (0x0800), length 58: 192.168.101.1.23 > 192.168.103.1.25420:
Flags [S.], seq 3694888749, ack 1562083610, win 8192, options [mss 1380], length 0

예 5:

10개의 패킷을 캡처한 후 종료하려면 다음 명령을 입력합니다.

<#root>

Options:

-n -c 10 src 192.168.101.1

```
18:03:12.749945 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 3758037348, win 32768, length
18:03:12.749945 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 1, win 32768, length 2
18:03:12.949932 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 1, win 32768, length 10
18:03:13.249971 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 3, win 32768, length 0
18:03:13.249971 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 3, win 32768, length 2
18:03:13.279969 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 5, win 32768, length 0
18:03:13.279969 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 5, win 32768, length 10
18:03:13.309966 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 7, win 32768, length 0
18:03:13.309966 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 7, win 32768, length 12
18:03:13.349972 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 9, win 32768, length 0
```

예 6:

capture.pcap라는 이름의 파일에 캡처를 쓰고 FTP를 통해 원격 서버에 복사하려면 다음 명령을 입력합니다.

<#root>

```
Options:

-w capture.pcap host 192.168.101.1
CTRL + C <- to stop the capture
> file copy 10.229.22.136 ftp / capture.pcap

Enter password for ftp@10.229.22.136:
Copying capture.pcap

Copy successful.


>
```

FTD LINA 엔진 캡처 작업

요구 사항

1. 다음 필터를 사용하여 FTD에서 두 개의 캡처를 활성화합니다.

소스 IP	192.168.103.1
대상 IP	192.168.101.1
프로토콜	ICMP
인터페이스	내부

소스 IP	192.168.103.1
대상 IP	192.168.101.1
프로토콜	ICMP
인터페이스	외부

2. Host-A(192.168.103.1)에서 Host-B(192.168.101.1)로 Ping하고 캡처를 확인합니다.

솔루션

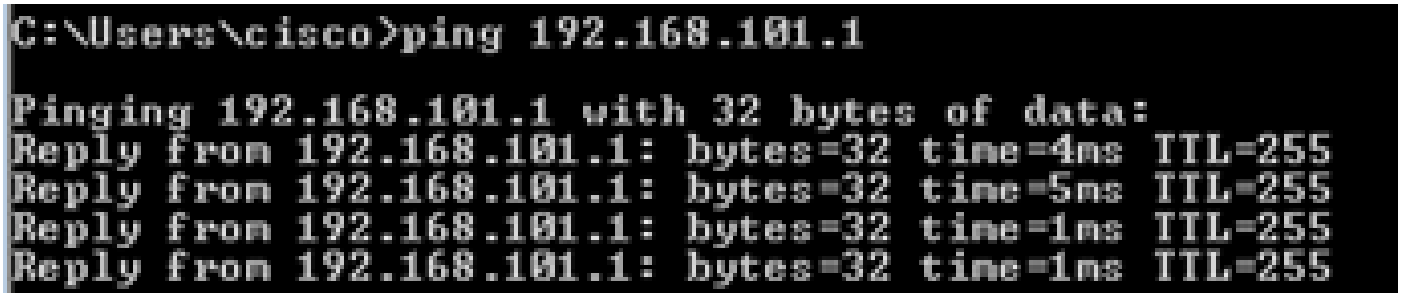
1단계. 캡처를 활성화합니다.

<#root>

```
> capture CAPI interface INSIDE match icmp host 192.168.103.1 host 192.168.101.1
> capture CAPO interface OUTSIDE match icmp host 192.168.101.1 host 192.168.103.1
```

2단계. CLI에서 캡처를 확인합니다.

Host-A에서 Host-B로 Ping:



<#root>

```
> show capture

capture CAPI type raw-data interface INSIDE [Capturing

- 752 bytes

]
  match icmp host 192.168.103.1 host 192.168.101.1
capture CAPO type raw-data interface OUTSIDE [Capturing

- 720 bytes

]
  match icmp host 192.168.101.1 host 192.168.103.1
```

다음 출력 예와 같이 INSIDE 인터페이스의 Dot1Q 헤더로 인해 두 캡처의 크기가 서로 다릅니다.

<#root>

```
> show capture CAPI

8 packets captured
   1: 17:24:09.122338

802.1Q vlan#1577

 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   2: 17:24:09.123071 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
   3: 17:24:10.121392 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   4: 17:24:10.122018 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
   5: 17:24:11.119714 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   6: 17:24:11.120324 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
   7: 17:24:12.133660 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   8: 17:24:12.134239 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
8 packets shown
```

<#root>

```
> show capture CAPO

8 packets captured
   1: 17:24:09.122765  192.168.103.1 > 192.168.101.1: icmp: echo request
   2: 17:24:09.122994  192.168.101.1 > 192.168.103.1: icmp: echo reply
   3: 17:24:10.121728  192.168.103.1 > 192.168.101.1: icmp: echo request
   4: 17:24:10.121957  192.168.101.1 > 192.168.103.1: icmp: echo reply
   5: 17:24:11.120034  192.168.103.1 > 192.168.101.1: icmp: echo request
   6: 17:24:11.120263  192.168.101.1 > 192.168.103.1: icmp: echo reply
   7: 17:24:12.133980  192.168.103.1 > 192.168.101.1: icmp: echo request
   8: 17:24:12.134194  192.168.101.1 > 192.168.103.1: icmp: echo reply
8 packets shown
```

FTD LINA 엔진 캡처 작업 - HTTP를 통해 캡처 내보내기

요구 사항

이전 시나리오에서 찍은 캡처를 브라우저로 내보냅니다.

솔루션

브라우저에서 캡처를 내보내려면 다음을 수행해야 합니다.

1. HTTPS 서버 활성화
2. HTTPS 액세스 허용

기본적으로 HTTPS 서버는 비활성화되며 액세스가 허용되지 않습니다.

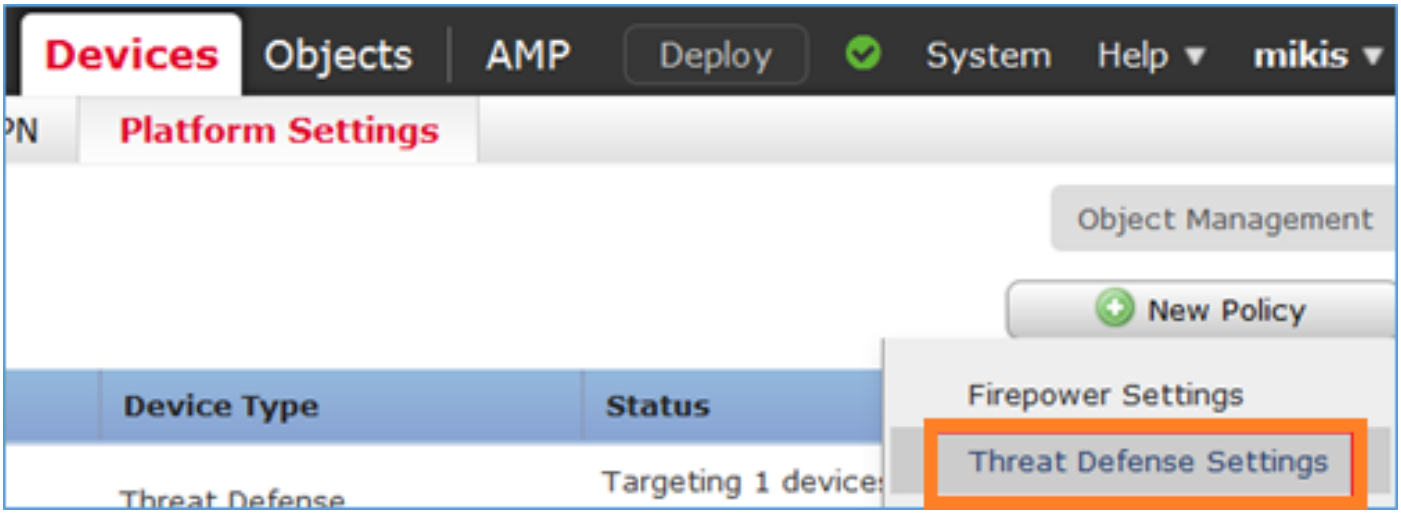
<#root>

>

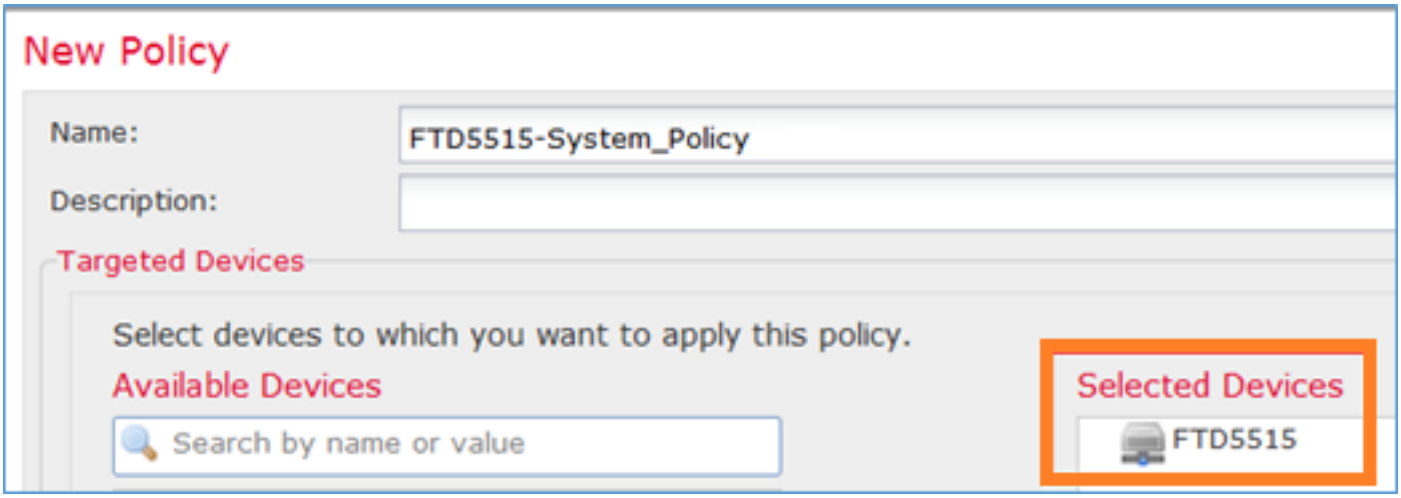
show running-config http

>

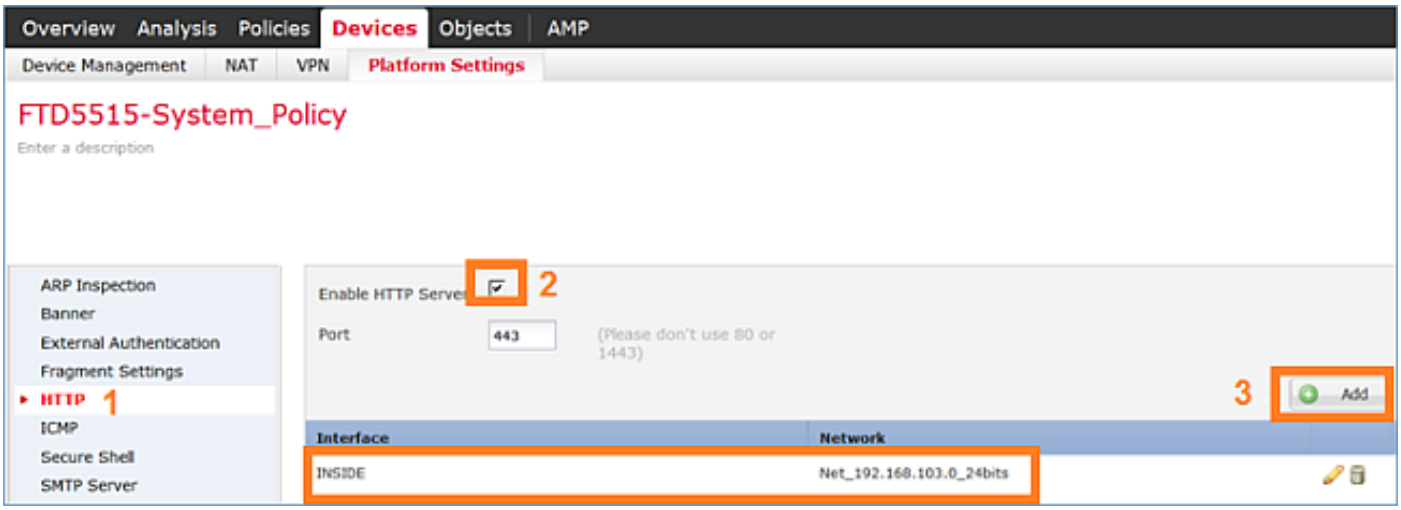
1단계. Devices(디바이스) > Platform Settings(플랫폼 설정)로 이동하고 New Policy(새 정책)를 클릭한 다음 Threat Defense Settings(Threat Defense 설정)를 선택합니다.



정책 이름 및 장치 대상 지정:



2단계. HTTPS 서버를 활성화하고 HTTPS를 통해 FTD 디바이스에 액세스하도록 허용하려는 네트워크를 추가합니다.



저장 및 구축.

정책 구축 시 HTTP 서비스의 시작을 확인하기 위해 debug http를 활성화할 수 있습니다.

<#root>

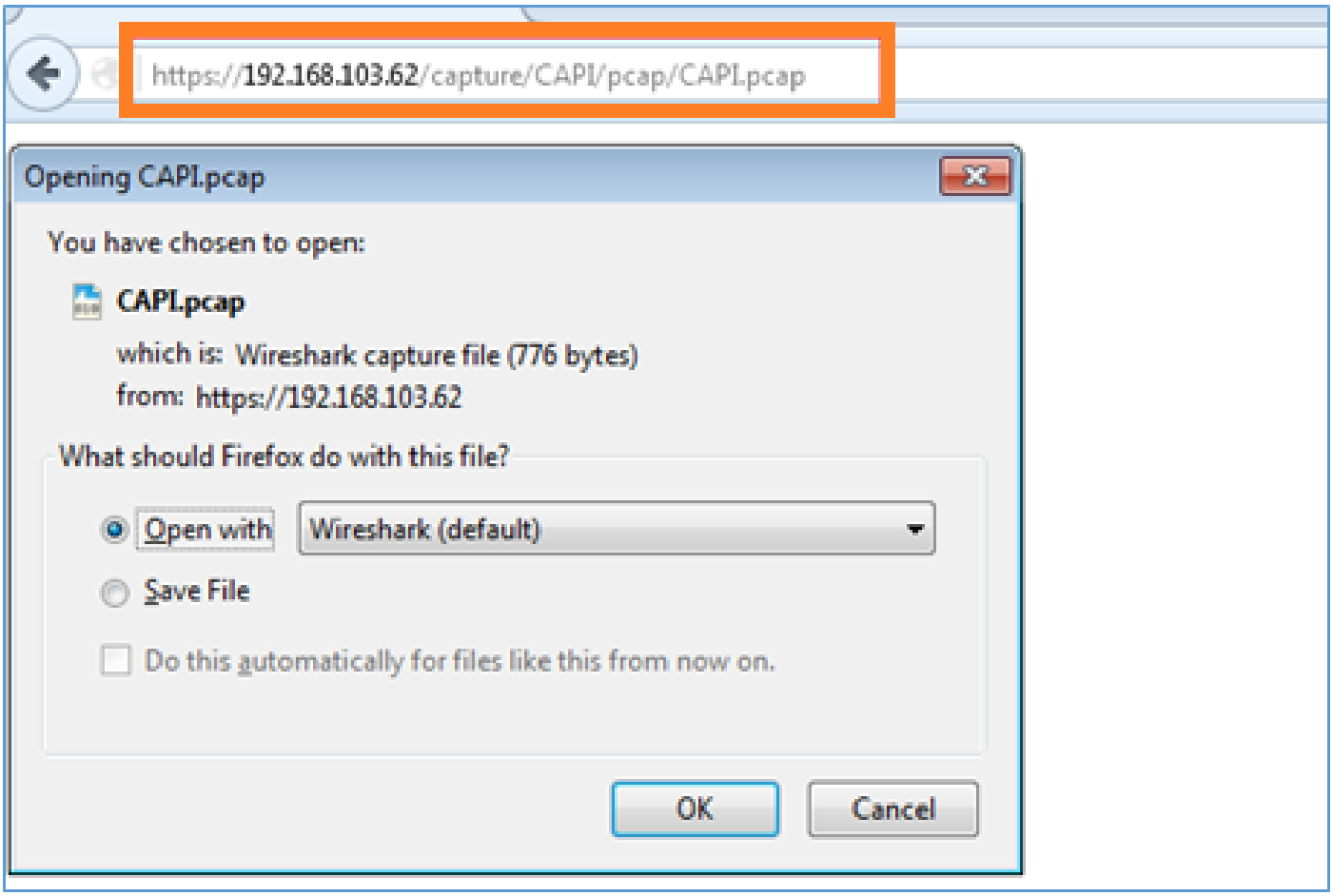
```
> debug http 255

debug http enabled at level 255.

http_enable: Enabling HTTP server
HTTP server starting.
```

FTD CLI의 결과는 다음과 같습니다.

<#root>

```
> unebug all

> show run http
http server enable
http 192.168.103.0 255.255.255.0 INSIDE
```

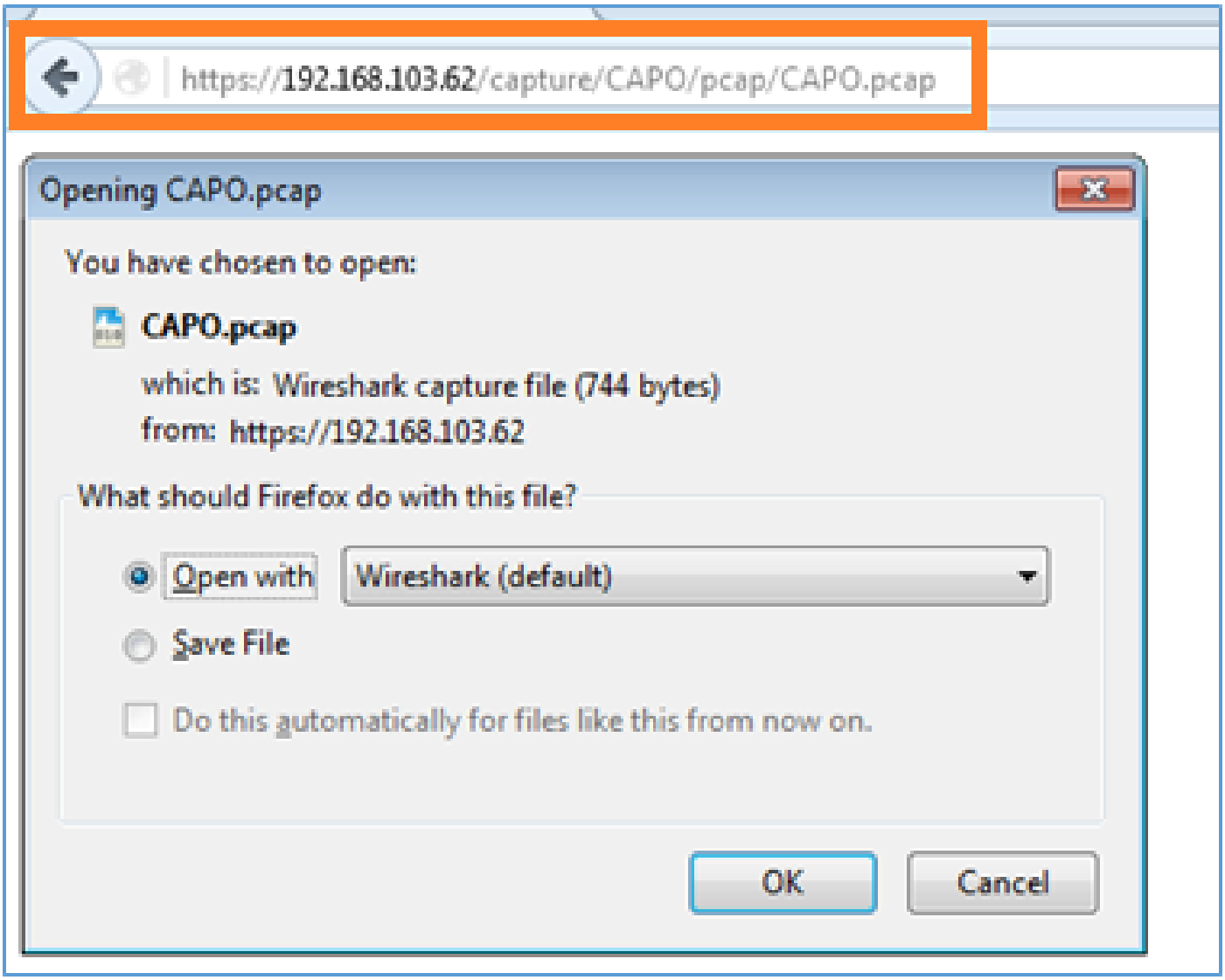
Host-A(192.168.103.1)에서 브라우저를 열고 이 URL을 사용하여 첫 번째 캡처를 다운로드합니다. https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap.



참조:

https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	HTTP 서버가 활성화된 FTD 데이터 인터페이스의 IP
https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	FTD 캡처의 이름
https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	다운로드된 파일의 이름

두 번째 캡처에서는 https://192.168.103.62/capture/CAPO/pcap/CAPO.pcap을 사용합니다.



FTD LINA 엔진 캡처 작업 - FTP/TFTP/SCP를 통해 캡처 내보내기

요구 사항

FTP/TFTP/SCP 프로토콜로 이전 시나리오에서 가져온 캡처를 내보냅니다.

솔루션

FTP 서버로 캡처 내보내기:

<#root>

```
firepower
# copy /pcap capture:CAPI ftp://ftp_username:ftp_password@192.168.78.73/CAPI.pcap
Source capture name [CAPI]?
Address or name of remote host [192.168.78.73]?
Destination username [ftp_username]?
```

Destination password [ftp_password]?

Destination filename [CAPI.pcap]?
!!!!!!

114 packets copied in 0.170 secs

firepower#

TFTP 서버로 캡처 내보내기:

<#root>

firepower

copy /pcap capture:CAPI tftp://192.168.78.73

Source capture name [CAPI]?

Address or name of remote host [192.168.78.73]?

Destination filename [CAPI]?
!!!!!!!!!!!!!!!!

346 packets copied in 0.90 secs

firepower#

SCP 서버로 캡처 내보내기:

<#root>

firepower#

copy /pcap capture:CAPI scp://scp_username:scp_password@192.168.78.55

Source capture name [CAPI]?

Address or name of remote host [192.168.78.55]?

Destination username [scp_username]?

Destination filename [CAPI]?
The authenticity of host '192.168.78.55 (192.168.78.55)' can't be established.
RSA key fingerprint is <cb:ca:9f:e9:3c:ef:e2:4f:20:f5:60:21:81:0a:85:f9:02:0d:0e:98:d0:9b:6c:dc:f9:af:4
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.78.55' (SHA256) to the list of known hosts.

!!!
454 packets copied in 3.950 secs (151 packets/sec)

```
firepower#
```

FTD의 오프로드 캡처. 현재 FTD에서 캡처를 오프로드해야 하는 경우 가장 쉬운 방법은 다음 단계를 수행하는 것입니다.

1. Lina - copy /pcap capture:<cap_name> disk0:

2. FPR 루트에서 mv /ngfw/mnt/disk0/<cap_name> /ngfw/var/common/

3. FMC UI - System > Health > Monitor > Device > Advanced Troubleshooting에서 <cap_name> 필드에 입력하고 다운로드합니다.

FTD LINA 엔진 캡처 작업 - 실제 트래픽 패킷 추적

요구 사항

다음 필터를 사용하여 FTD에서 캡처를 활성화합니다.

소스 IP	192.168.103.1
대상 IP	192.168.101.1
프로토콜	ICMP
인터페이스	내부
패킷 추적	예
추적 패킷 수	100

Host-A(192.168.103.1)에서 Host-B(192.168.101.1)로 Ping하고 캡처를 확인합니다.

솔루션

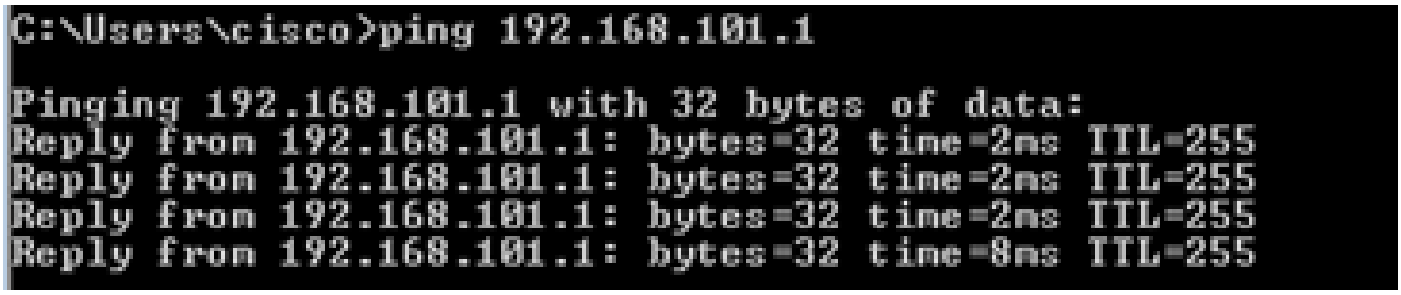
실제 패킷을 추적하는 것은 연결 문제를 해결하는 데 매우 유용합니다. 패킷이 통과하는 모든 내부 검사를 볼 수 있습니다. trace detail 키워드를 추가하고 추적하고자 하는 패킷 수를 지정합니다. 기본적으로 FTD는 처음 50개의 인그레스 패킷을 추적합니다.

이 경우 FTD가 INSIDE 인터페이스에서 수신하는 처음 100개 패킷에 대해 추적 세부사항이 포함된 캡처를 활성화합니다.

<#root>

```
> capture CAPI2 interface INSIDE trace detail trace-count 100 match icmp host 192.168.103.1 host 192.168
```

Host-A에서 Host-B로 Ping하고 결과를 확인합니다.



캡처된 패킷은 다음과 같습니다.

<#root>

```
> show capture CAPI2

8 packets captured
   1: 18:08:04.232989  802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   2: 18:08:04.234622  802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
   3: 18:08:05.223941  802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   4: 18:08:05.224872  802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
   5: 18:08:06.222309  802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   6: 18:08:06.223148  802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
   7: 18:08:07.220752  802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   8: 18:08:07.221561  802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
8 packets shown
```

이 출력은 첫 번째 패킷의 추적을 표시합니다. 관심 있는 부품:

- 12단계에서는 '전진 흐름'이 보입니다. LINA 엔진 디스패치 어레이입니다(사실상 내부 작업 순서).
- 13단계에서는 FTD가 Snort 인스턴스로 패킷을 전송합니다.
- 14단계에서는 Snort 판정을 볼 수 있습니다.

<#root>

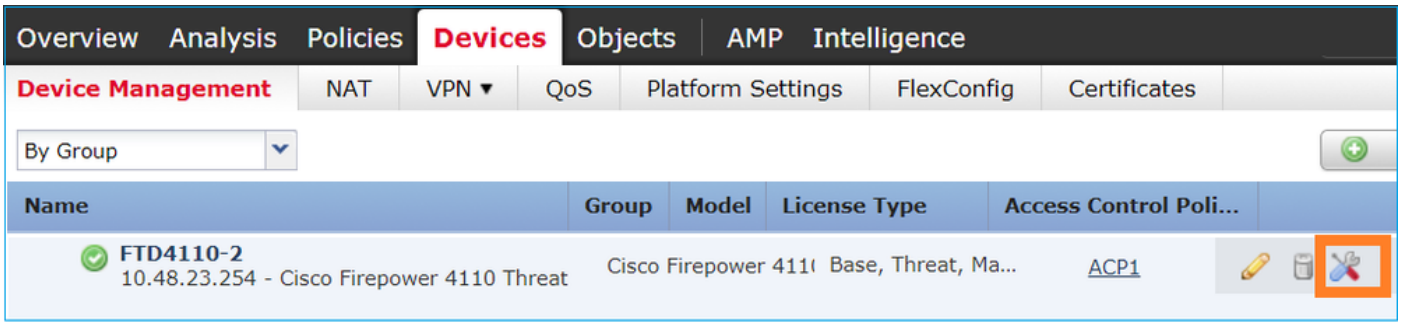
```
> show capture CAPI2 packet-number 1 trace detail

8 packets captured
   1: 18:08:04.232989 000c.2998.3fec a89d.2193.2293 0x8100 Length: 78
      802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request (ttl 128, id 3346)
Phase: 1
Type: CAPTURE
... output omitted ...

Phase: 12
Type: FLOW-CREATION
Subtype:
```

```
Result: ALLOW
Config:
Additional Information:
New flow created with id 195, packet dispatched to next module
Module information for forward flow ...

snp_fp_inspect_ip_options
snp_fp_snort
snp_fp_inspect_icmp
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat


Module information for reverse flow ...

snp_fp_inspect_ip_options
snp_fp_inspect_icmp
snp_fp_snort
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat



Phase: 13
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 14
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet


... output omitted ...

Result:
input-interface: OUTSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow

1 packet shown
>
```

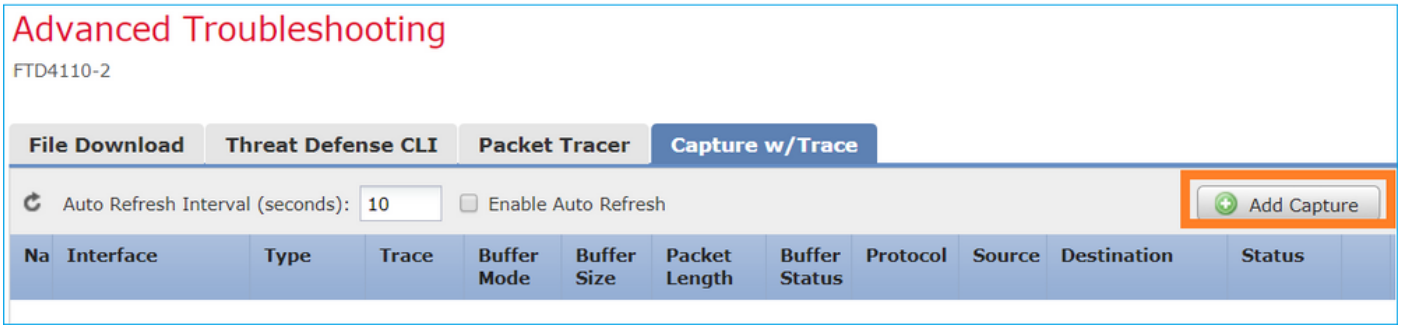
Post-6.2 FMC 소프트웨어 버전의 캡처 툴

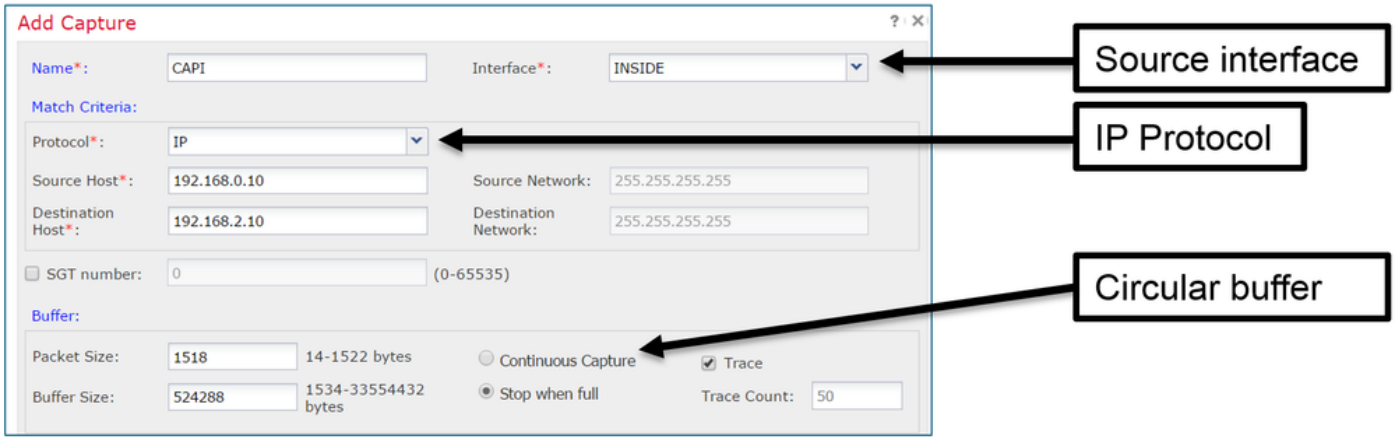
FMC 버전 6.2.x에는 새로운 패킷 캡처 마법사가 도입되었습니다. Devices(디바이스) > Device Management(디바이스 관리)로 이동하고 Troubleshoot(문제 해결) 아이콘을 클릭합니다. 그런 다음

Advanced Troubleshooting(고급 문제 해결)을 선택하고 마지막으로 Capture w/Trace(추적 포함 캡처)를 선택합니다.



Add Capture(캡처 추가)를 선택하여 FTD 캡처를 생성합니다.



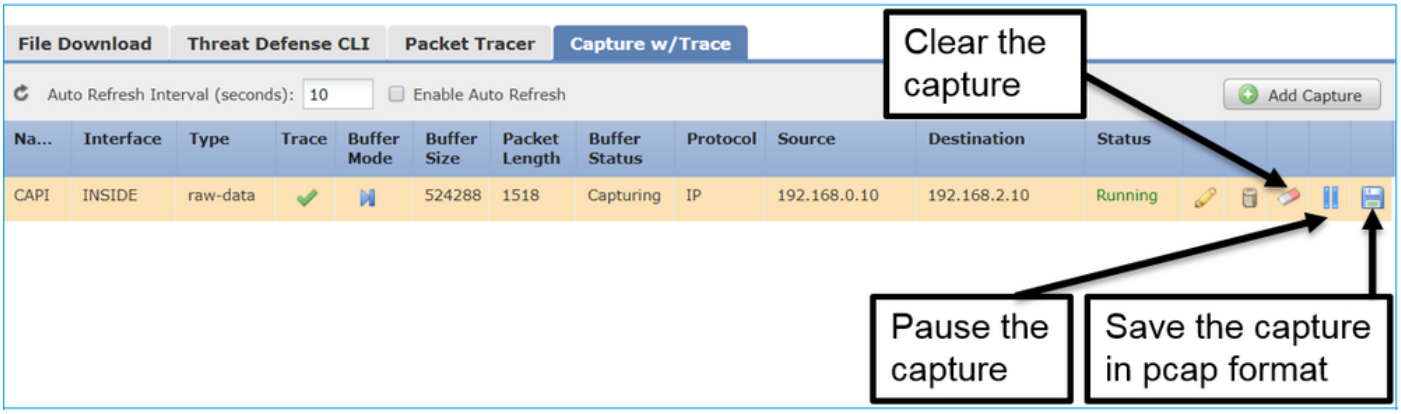


현재 FMC UI 제한은 다음과 같습니다.

- Src 및 Dst 포트를 지정할 수 없습니다.
- 기본 IP 프로토콜만 일치 가능
- LINA 엔진 ASP 삭제에 대한 캡처를 사용하도록 설정할 수 없습니다.

해결 방법 - FTD CLI 사용

FMC UI에서 캡처를 적용하는 즉시 캡처가 실행됩니다.



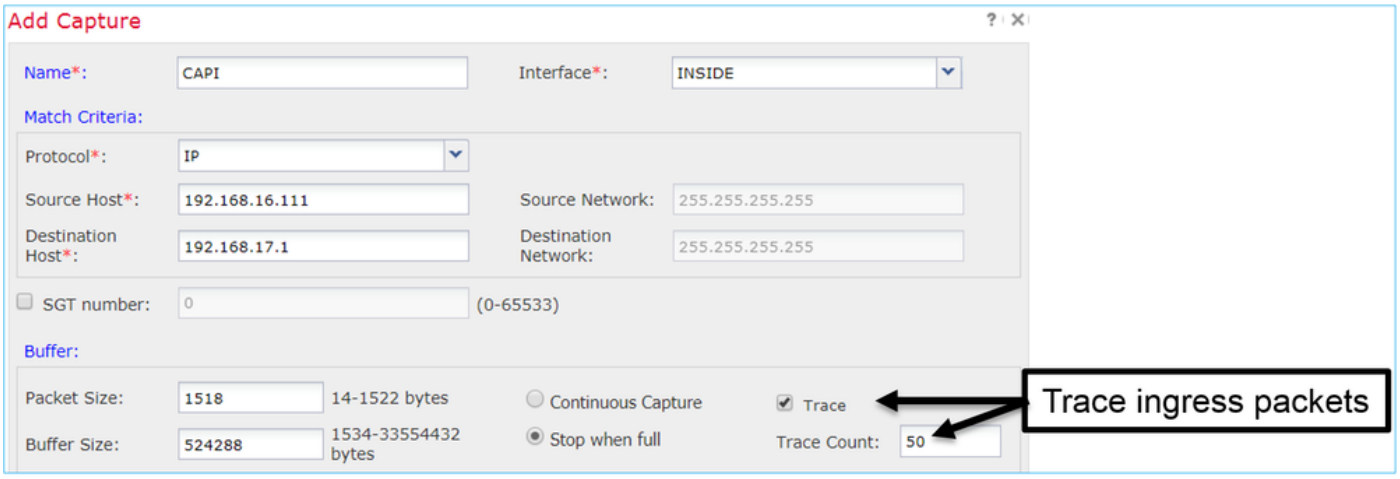
FTD CLI의 캡처:

<#root>

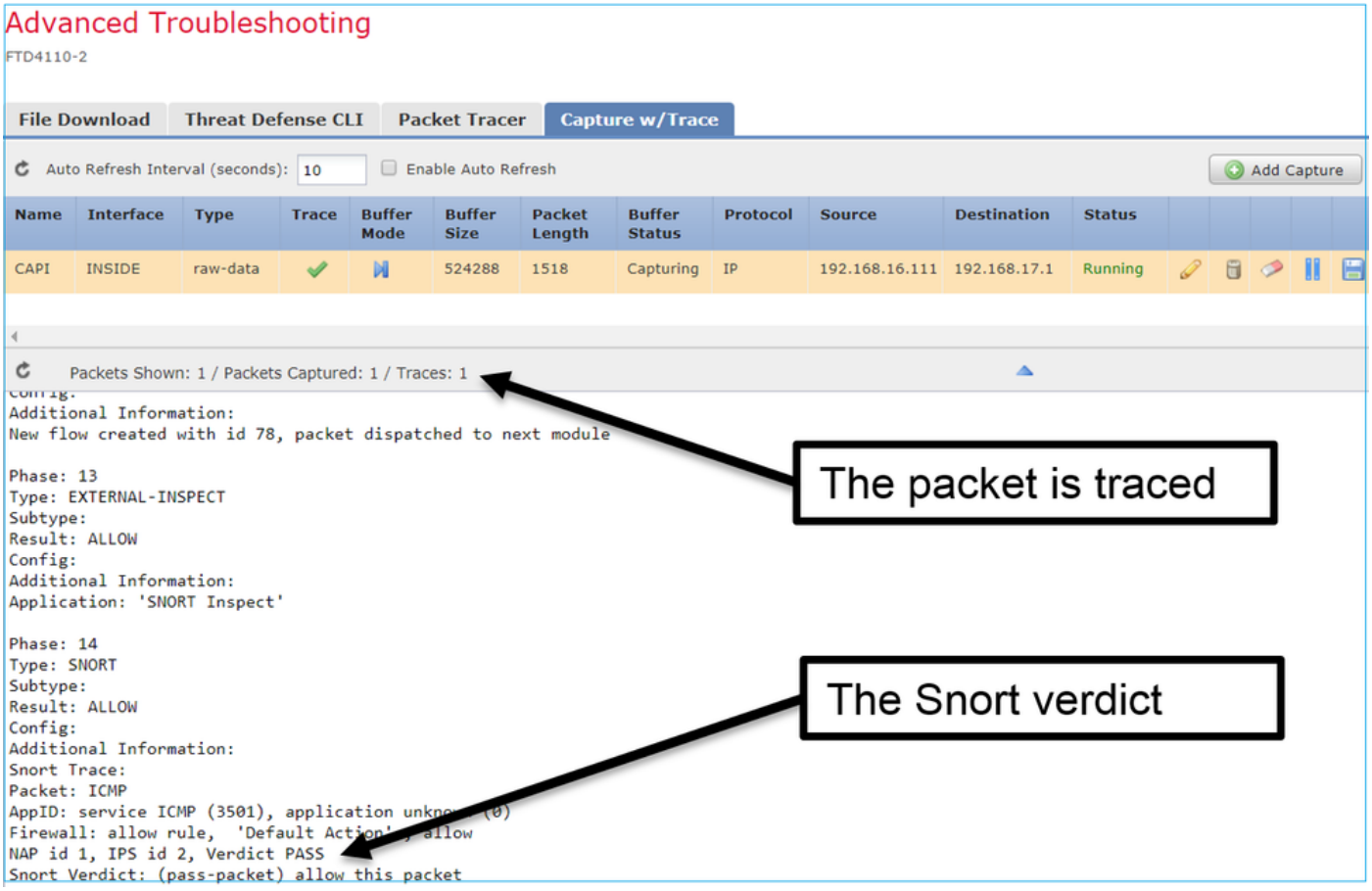
```
> show capture

capture CAPI%intf=INSIDE% type raw-data trace interface INSIDE [Capturing - 0 bytes]
  match ip host 192.168.0.10 host 192.168.2.10
>
```

Post-6.2 FMC에서 실제 패킷 추적

FMC 6.2.x에서 Capture w/Trace(추적 포함 캡처) 마법사를 사용하면 FTD에서 실제 패킷을 캡처하고 추적할 수 있습니다.



FMC UI에서 추적된 패킷을 확인할 수 있습니다.



FTD 패킷 추적기 유틸리티

요구 사항

이 흐름에 대해 Packet Tracer 유틸리티를 사용하여 패킷이 내부에서 처리되는 방식을 확인합니다.

인그레스 인터페이스	내부
프로토콜	ICMP 에코 요청
소스 IP	192.168.103.1
대상 IP	192.168.101.1

솔루션

Packet Tracer는 가상 패킷을 생성합니다. 이 예에서 보여주는 것처럼 패킷은 Snort 검사의 대상이 됩니다. Snort-level(capture-traffic)에서 동시에 캡처한 캡처는 ICMP 에코 요청을 보여줍니다.

> packet-tracer input INSIDE icmp 192.168.103.1 8 0 192.168.101.1

```
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: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.101.1 using egress ifc  OUTSIDE

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip 192.168.103.0 255.255.255.0 192.168.101.0 255.255.255.0 rule
access-list CSM_FW_ACL_ remark rule-id 268436482: ACCESS POLICY: FTD5515 - Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 268436482: L4 RULE: Allow ICMP
```

Additional Information:
This packet is sent to snort for additional processing where a verdict is reached

```
... output omitted ...

Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 203, packet dispatched to next module

Phase: 13
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: ICMP
AppID: service ICMP (3501), application unknown (0)
Firewall: allow rule, id 268440225, allow
NAP id 2, IPS id 0, Verdict PASS
```

```
Snort Verdict: (pass-packet) allow this packet


Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow

>
```

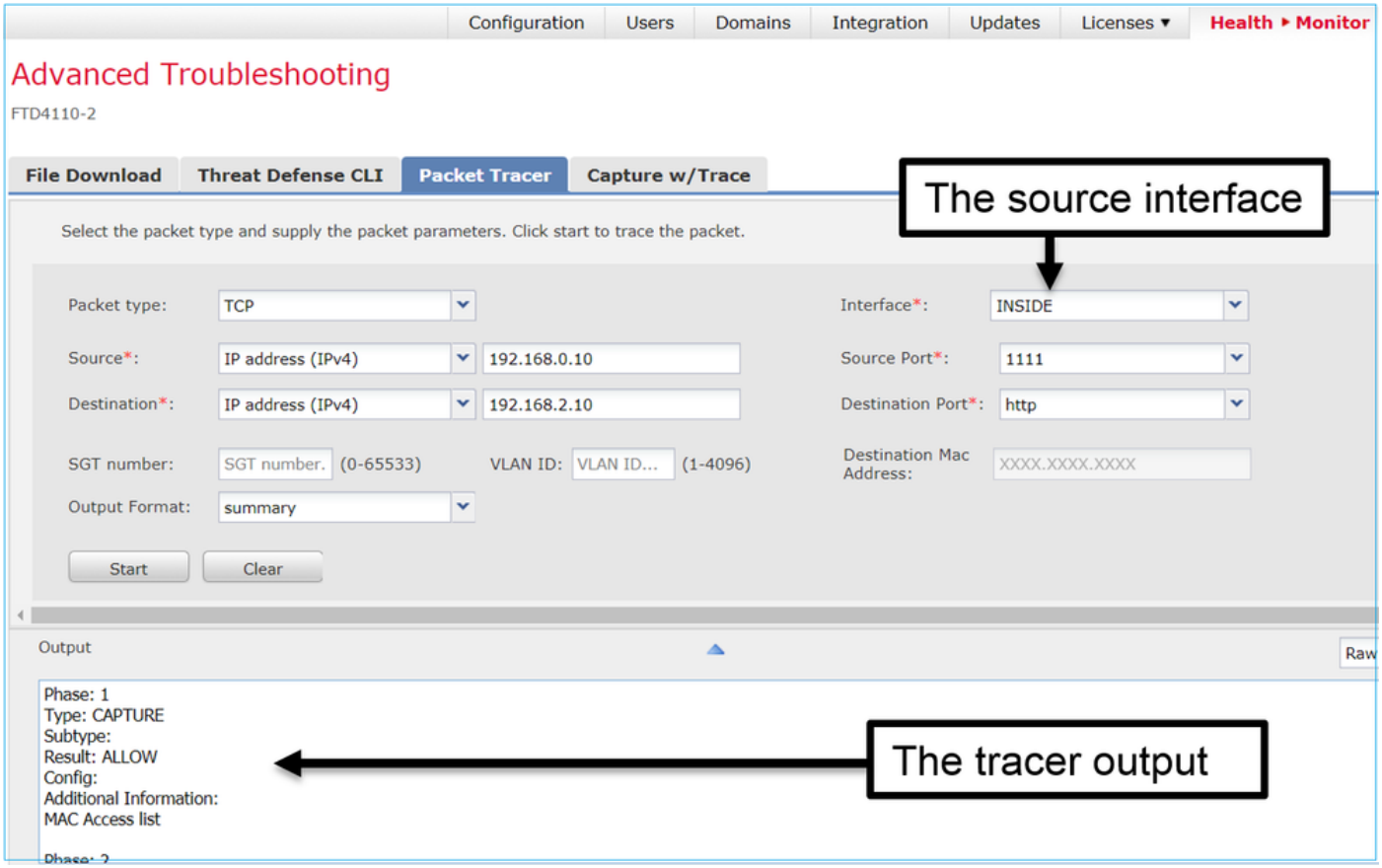
패킷 추적기 테스트 시점의 Snort 레벨 캡처에서는 가상 패킷을 보여줍니다.

<#root>

```
>

capture-traffic


Please choose domain to capture traffic from:
  0 - management0
  1 - Router

Selection? 1

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:

-n
13:27:11.939755 IP 192.168.103.1 > 192.168.101.1: ICMP echo request, id 0, seq 0, length 8
```

Post-6.2 FMC 소프트웨어 버전의 Packet Tracer UI 툴

FMC 버전 6.2.x에는 Packet Tracer UI 툴이 도입되었습니다. 이 툴은 캡처 툴과 동일한 방식으로 액세스할 수 있으며 FMC UI에서 FTD에서 Packet Tracer를 실행할 수 있습니다.



관련 정보

- Firepower 위협 방어 명령 참조 설명서
- Firepower 시스템 릴리스 정보, 버전 6.1.0
- firepower 디바이스 관리자용 Cisco Firepower Threat Defense 컨피그레이션 가이드, 버전 6.1
- 기술 지원 및 문서 – Cisco Systems

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.