

보안 방화벽 및 Firepower 내부 스위치 캡처 구성 및 확인

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[시스템 아키텍처의 개괄적 개요](#)

[내부 스위치 운영에 대한 개괄적 개요](#)

[패킷 흐름 및 캡처 포인트](#)

[Firepower 4100/9300의 컨피그레이션 및 확인](#)

[물리적 또는 포트 채널 인터페이스의 패킷 캡처](#)

[백플레인 인터페이스의 패킷 캡처](#)

[애플리케이션 및 애플리케이션 포트의 패킷 캡처](#)

[물리적 또는 포트 채널 인터페이스의 하위 인터페이스에서 패킷 캡처](#)

[패킷 캡처 필터](#)

[Firepower 4100/9300 내부 스위치 캡처 파일 수집](#)

[내부 스위치 패킷 캡처에 대한 지침, 제한 및 모범 사례](#)

[Secure Firewall 3100의 컨피그레이션 및 확인](#)

[물리적 또는 포트 채널 인터페이스의 패킷 캡처](#)

[물리적 또는 포트 채널 인터페이스의 하위 인터페이스에서 패킷 캡처](#)

[내부 인터페이스의 패킷 캡처](#)

[패킷 캡처 필터](#)

[Secure Firewall 3100 내부 스위치 캡처 파일 수집](#)

[내부 스위치 패킷 캡처에 대한 지침, 제한 및 모범 사례](#)

[관련 정보](#)

소개

이 문서에서는 Firepower 및 Secure Firewall 내부 스위치의 컨피그레이션 및 검증에 대해 설명합니다.

사전 요구 사항

요구 사항

기본 제품 지식, 캡처 분석

사용되는 구성 요소

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.

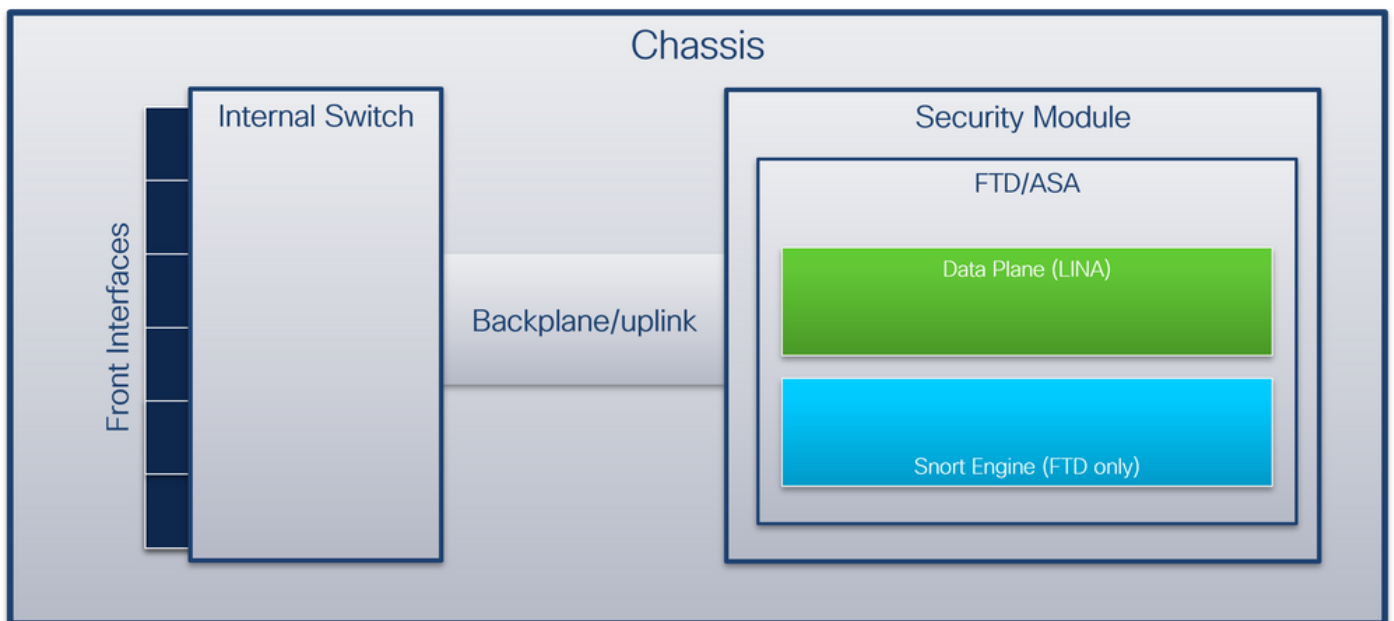
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 보안 방화벽 31xx
- Firepower 41xx
- Firepower 93xx
- Cisco FXOS(Secure eXtensible Operating System) 2.12.0.x
- Cisco FTD(Secure Firewall Threat Defense) 7.2.0.x
- Cisco FMC(Secure Firewall Management Center) 7.2.0.x
- Cisco FDM(Secure Firewall Device Manager) 7.2.0.x
- ASA(Adaptive Security Appliance) 9.18(1)x
- ASDM(Adaptive Security Appliance Device Manager) 7.18.1.x
- Wireshark 3.6.7(<https://www.wireshark.org/download.html>)

배경 정보

시스템 아키텍처의 개괄적 개요

패킷 흐름의 관점에서 Firepower 4100/9300 및 Secure Firewall 3100의 아키텍처는 다음 그림과 같이 시각화할 수 있습니다.



샤페에는 다음 구성 요소가 포함됩니다.

- **내부 스위치** - 네트워크에서 애플리케이션으로 패킷을 전달하며, 그 반대의 경우도 마찬가지입니다. 내부 스위치는 내장된 인터페이스 모듈 또는 외부 네트워크 모듈에 있는 **전면 인터페이스**에 연결되어 외부 장치(예: 스위치)에 연결됩니다. 전면 인터페이스의 예로는 Ethernet 1/1, Ethernet 2/4 등이 있습니다. "전면"은 강력한 기술적 정의가 아닙니다. 이 문서에서는 외부 디바이스에 연결된 인터페이스를 백플레인 또는 업링크 인터페이스와 구분하는 데 사용됩니다.
- **백플레인 또는 업링크** - 보안 모듈(SM)을 내부 스위치에 연결하는 내부 인터페이스입니다. 다

음 표는 Firepower 4100/9300의 백플레인 인터페이스와 Secure Firewall 3100의 업링크 인터페이스를 보여줍니다.

플랫폼	지원되는 보안 모듈 수	백플레인/업링크 인터페이스	매핑된 애플리케이션 인터페이스
Firepower 4100(Firepower 4110/4112 제외)	1	SM1: 이더넷1/9 이더넷1/10	내부 데이터0/0 내부 데이터0/1
Firepower 4110/4112	1	이더넷1/9	내부 데이터0/0 내부 데이터0/0 내부 데이터0/1
Firepower 9300	3	SM1: 이더넷1/9 이더넷1/10 SM2: 이더넷1/11 이더넷1/12 SM3: 이더넷1/13 이더넷1/14	내부 데이터0/0 내부 데이터0/1 내부 데이터0/0 내부 데이터0/1
보안 방화벽 3100	1	SM1: in_data_uplink1	내부 데이터0/1

모듈당 2개의 백플레인 인터페이스의 경우, 내부 스위치와 모듈의 애플리케이션이 2개의 인터페이스를 통해 트래픽 로드 밸런싱을 수행합니다.

- **보안 모듈, 보안 엔진 또는 블레이드** - FTD 또는 ASA와 같은 애플리케이션이 설치되는 모듈입니다. Firepower 9300은 최대 3개의 보안 모듈을 지원합니다.
- **매핑된 애플리케이션 인터페이스** - FTD 또는 ASA와 같은 애플리케이션은 백플레인 또는 업링크 인터페이스를 내부 인터페이스에 매핑합니다. 즉, 백플레인 또는 업링크 인터페이스는 애플리케이션에서 내부 인터페이스로 표시됩니다.

내부 인터페이스를 확인하려면 **show interface detail** 명령을 사용합니다.

```
> show interface detail | grep Interface
Interface Internal-Control0/0 "ha_ctl_nlp_int_tap", is up, line protocol is up
Control Point Interface States:
  Interface number is 6
  Interface config status is active
  Interface state is active
Interface Internal-Data0/0 "", is up, line protocol is up
Control Point Interface States:
  Interface number is 2
  Interface config status is active
  Interface state is active
Interface Internal-Data0/1 "", is up, line protocol is up
Control Point Interface States:
  Interface number is 3
  Interface config status is active
  Interface state is active
Interface Internal-Data0/2 "nlp_int_tap", is up, line protocol is up
Control Point Interface States:
  Interface number is 4
  Interface config status is active
  Interface state is active
Interface Internal-Data0/3 "ccl_ha_nlp_int_tap", is up, line protocol is up
```

```
Control Point Interface States:
  Interface number is 5
  Interface config status is active
  Interface state is active
Interface Internal-Data0/4 "cmi_mgmt_int_tap", is up, line protocol is up
Control Point Interface States:
  Interface number is 7
  Interface config status is active
  Interface state is active
Interface Port-channel6.666 "", is up, line protocol is up
Interface Ethernet1/1 "diagnostic", is up, line protocol is up
Control Point Interface States:
  Interface number is 8
  Interface config status is active
  Interface state is active
```

내부 스위치 운영에 대한 개괄적 개요

Firepower 4100/9300

전달 결정을 내리기 위해 내부 스위치는 인터페이스 VLAN 태그, 즉 포트 VLAN 태그와 가상 네트워크 태그(VN-tag)를 사용합니다.

포트 VLAN 태그는 내부 스위치에서 인터페이스를 식별하는 데 사용됩니다. 스위치는 전면 인터페이스에 제공된 각 이그레스 패킷에 포트 VLAN 태그를 삽입합니다. VLAN 태그는 시스템에서 자동으로 구성되며 수동으로 변경할 수 없습니다. 태그 값은 fxos 명령 셸에서 확인할 수 있습니다.

```
firepower# connect fxos
...
firepower(fxos)# show run int e1/2
!Command: show running-config interface Ethernet1/2
!Time: Tue Jul 12 22:32:11 2022
```

```
version 5.0(3)N2(4.120)
```

```
interface Ethernet1/2
description U: Uplink
no lldp transmit
no lldp receive
no cdp enable
switchport mode dot1q-tunnel
switchport trunk native vlan 102
speed 1000
duplex full
udld disable
no shutdown
```

VN-tag도 내부 스위치에 의해 삽입되어 패킷을 애플리케이션에 전달하는 데 사용된다. 자동으로 구성되며 수동으로 변경할 수 없습니다.

포트 VLAN 태그 및 VN 태그는 애플리케이션과 공유됩니다. 애플리케이션은 각 패킷에 각 이그레스 인터페이스 VLAN 태그와 VN 태그를 삽입합니다. 애플리케이션의 패킷이 백플레인 인터페이스의 내부 스위치에 수신되면 스위치는 이그레스 인터페이스 VLAN 태그와 VN-태그를 읽고 애플리케이션과 이그레스 인터페이스를 식별하고 포트 VLAN 태그와 VN-태그를 스트리핑한 다음 패킷을 네트워크에 전달합니다.

보안 방화벽 3100

Firepower 4100/9300에서와 마찬가지로, 내부 스위치에서 인터페이스를 식별하는 데 포트 VLAN

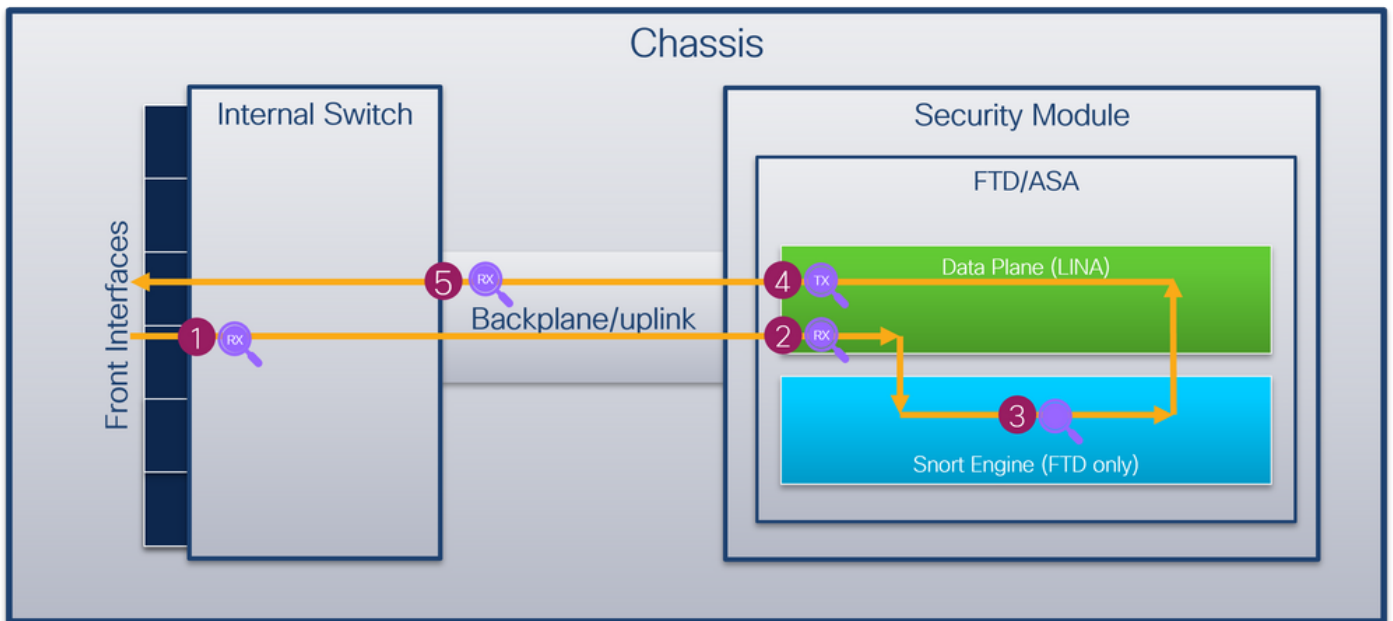
태그를 사용합니다.

포트 VLAN 태그는 애플리케이션과 공유됩니다. 애플리케이션은 각 패킷에 각 이그레스 인터페이스 VLAN 태그를 삽입합니다. 애플리케이션의 패킷이 업링크 인터페이스의 내부 스위치에 수신되면 스위치는 이그레스 인터페이스 VLAN 태그를 읽고 이그레스 인터페이스를 식별하고 포트 VLAN 태그를 스트립한 다음 패킷을 네트워크로 전달합니다.

패킷 흐름 및 캡처 포인트

Firepower 4100/9300 및 Secure Firewall 3100 방화벽은 내부 스위치의 인터페이스에서 패킷 캡처를 지원합니다.

이 그림에서는 샤페이 및 애플리케이션 내의 패킷 경로를 따라 패킷 캡처 지점을 보여줍니다.



캡처 포인트는 다음과 같습니다.

1. 내부 스위치 전면 인터페이스 인그레스 캡처 포인트 전면 인터페이스는 스위치와 같은 피어 디바이스에 연결된 인터페이스입니다.
2. 데이터 플레인 인터페이스 인그레스 캡처 지점
3. Snort 캡처 포인트
4. 데이터 플레인 인터페이스 이그레스 캡처 지점
5. 내부 스위치 백플레인 또는 업링크 인그레스 캡처 포인트 백플레인 또는 업링크 인터페이스가 내부 스위치를 애플리케이션에 연결합니다.

내부 스위치는 인그레스 인터페이스 캡처만 지원합니다. 즉, 네트워크 또는 ASA/FTD 애플리케이션에서 수신된 패킷만 캡처할 수 있습니다. 이그레스 패킷 캡처는 지원되지 않습니다.

구성 및 확인 Firepower 4100/9300

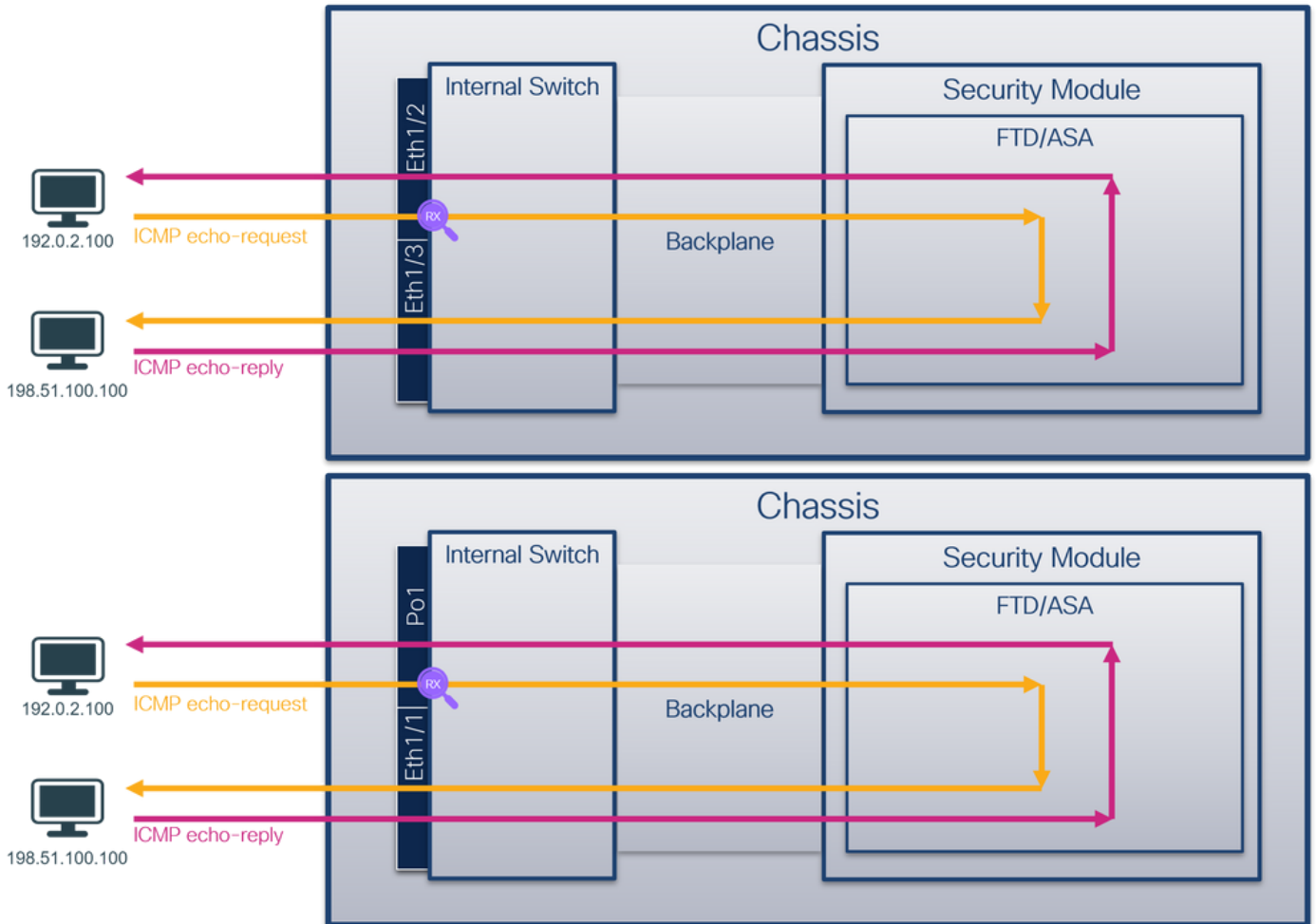
Firepower 4100/9300 내부 스위치 캡처는 FCM의 **Tools > Packet Capture** 또는 FXOS CLI의 **scope packet-capture**에서 구성할 수 있습니다. 패킷 캡처 옵션에 대한 설명은 *Cisco Firepower 4100/9300 FXOS Chassis Manager 컨피그레이션 가이드* 또는 *Cisco Firepower 4100/9300 FXOS CLI 컨피그레이션 가이드*, **문제 해결**, **패킷 캡처** 섹션을 참조하십시오.

이러한 시나리오에서는 Firepower 4100/9300 내부 스위치 캡처의 일반적인 활용 사례를 다룹니다.

물리적 또는 포트 채널 인터페이스의 패킷 캡처

FCM 및 CLI를 사용하여 인터페이스 Ethernet1/2 또는 Portchannel1 인터페이스에서 패킷 캡처를 구성하고 확인합니다. 포트 채널 인터페이스의 경우 모든 물리적 멤버 인터페이스를 선택해야 합니다.

토폴로지, 패킷 흐름 및 캡처 포인트

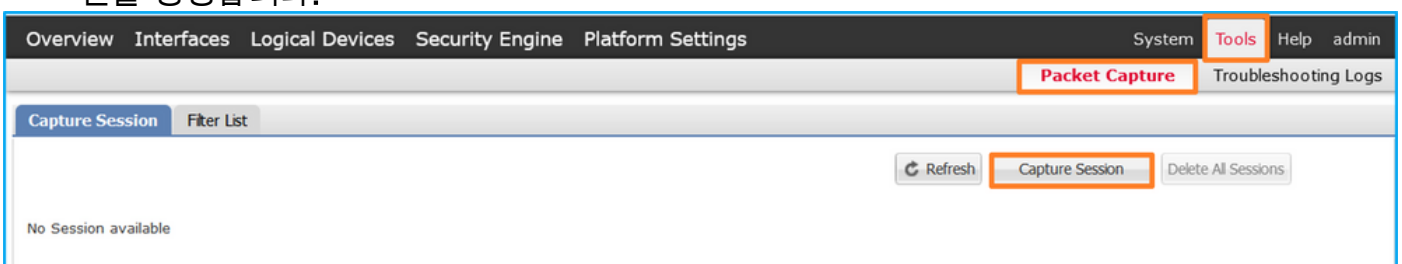


설정

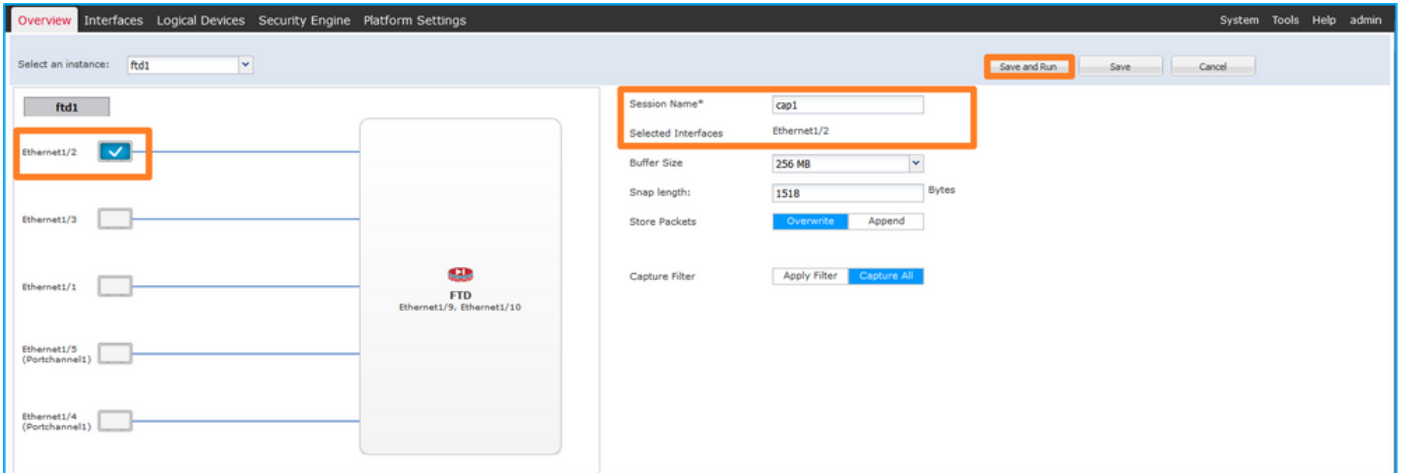
FCM

FCM에서 다음 단계를 수행하여 인터페이스 Ethernet1/2 또는 Portchannel1에서 패킷 캡처를 구성합니다.

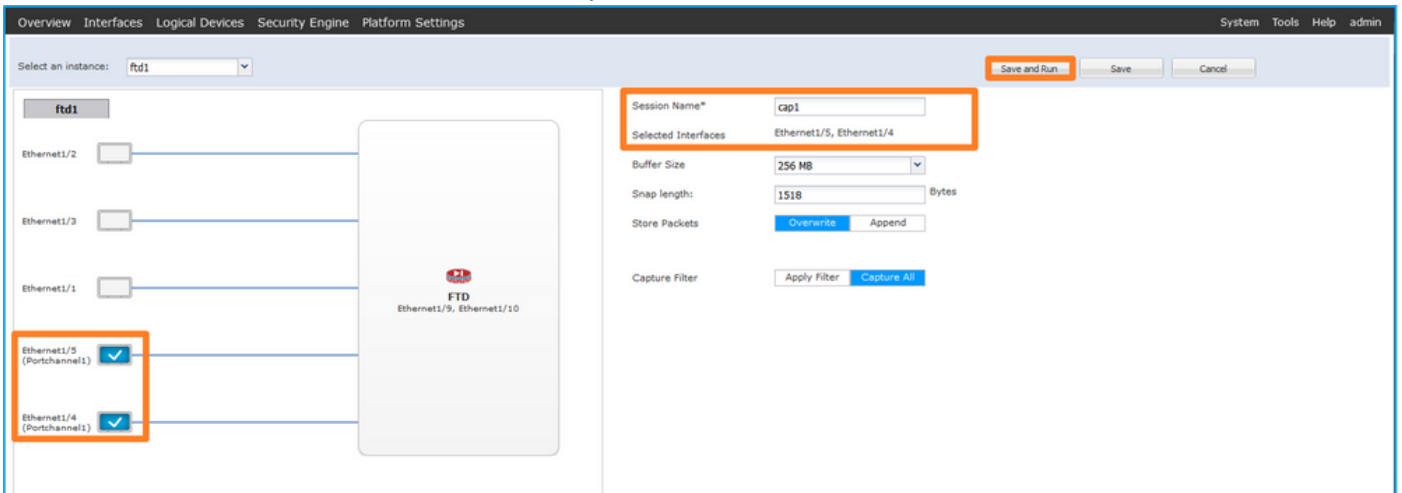
1. Tools(도구) > Packet Capture(패킷 캡처) > Capture Session(캡처 세션)을 사용하여 새 캡처 세션을 생성합니다.



2. 인터페이스 Ethernet1/2를 선택하고 세션 이름을 제공한 다음 Save and Run(저장 및 실행)을 클릭하여 캡처를 활성화합니다.



3. 포트 채널 인터페이스의 경우 모든 물리적 멤버 인터페이스를 선택하고 세션 이름을 제공한 다음 Save and Run을 클릭하여 캡처를 활성화합니다.



FXOS CLI

FXOS CLI에서 다음 단계에 따라 인터페이스 Ethernet1/2 또는 Portchannel1에서 패킷 캡처를 구성합니다.

1. 애플리케이션 유형 및 식별자를 식별합니다.

```
firepower# scope ssa
firepower /ssa # show app-instance
App Name Identifier Slot ID Admin State Oper State Running Version Startup Version
Deploy Type Turbo Mode Profile Name Cluster State Cluster Role
-----
ftd ftd1 1 Enabled Online 7.2.0.82 7.2.0.82
Native No Not Applicable None
```

2. 포트 채널 인터페이스의 경우 멤버 인터페이스를 식별합니다.

```
firepower# connect fxos
<output skipped>
firepower(fxos)# show port-channel summary
Flags: D - Down P - Up in port-channel (members)
I - Individual H - Hot-standby (LACP only)
```

```

s - Suspended    r - Module-removed
S - Switched    R - Routed
U - Up (port-channel)
M - Not in use. Min-links not met

```

```

-----
Group Port-      Type      Protocol  Member Ports
Channel
-----
1    Po1(SU)      Eth       LACP      Eth1/4(P)  Eth1/5(P)

```

3. 캡처 세션을 생성합니다.

```

firepower# scope packet-capture
firepower /packet-capture # create session cap1
firepower /packet-capture/session* # create phy-port Eth1/2
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # set app-identifier ftd1
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # enable
firepower /packet-capture/session* # commit
firepower /packet-capture/session #

```

포트 채널 인터페이스의 경우 각 멤버 인터페이스에 대해 별도의 캡처가 구성됩니다.

```

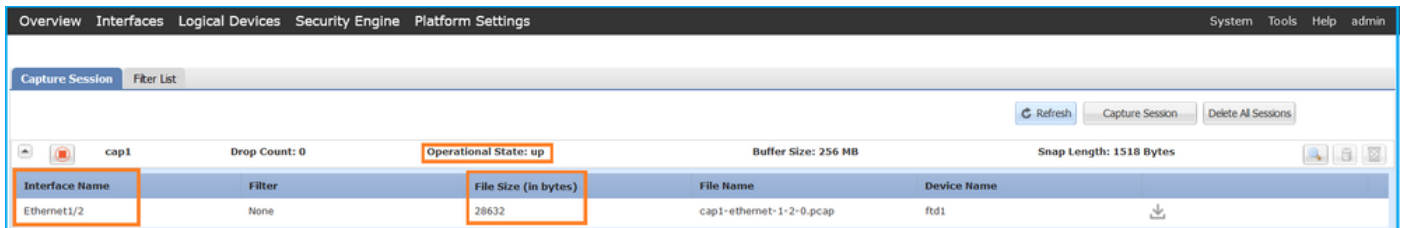
firepower# scope packet-capture
firepower /packet-capture # create session cap1
firepower /packet-capture/session* # create phy-port Eth1/4
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # set app-identifier ftd1
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # create phy-port Eth1/5
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # set app-identifier ftd1
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # enable
firepower /packet-capture/session* # commit
firepower /packet-capture/session #

```

확인

FCM

인터페이스 이름을 확인하고 작동 상태가 작동 중인지, 파일 크기(바이트)가 증가하는지 확인합니다.



멤버 인터페이스가 Ethernet1/4 및 Ethernet1/5인 Portchannel1:

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/5	None	160	cap1-ethernet-1-5-0.pcap	fd1
Ethernet1/4	None	85000	cap1-ethernet-1-4-0.pcap	fd1

FXOS CLI

scope packet-capture에서 캡처 세부 정보를 확인합니다.

```
firepower# scope packet-capture
firepower /packet-capture # show session cap1
```

Traffic Monitoring Session:

```
Packet Capture Session Name: cap1
Session: 1
Admin State: Enabled
Oper State: Up
Oper State Reason: Active
Config Success: Yes
Config Fail Reason:
Append Flag: Overwrite
Session Mem Usage: 256 MB
Session Pcap Snap Len: 1518 Bytes
Error Code: 0
Drop Count: 0
```

Physical ports involved in Packet Capture:

```
Slot Id: 1
Port Id: 2
Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap
Pcapsize: 75136 bytes
Filter:
Sub Interface: 0
Application Instance Identifier: ftd1
Application Name: ftd
```

멤버 인터페이스가 Ethernet1/4 및 Ethernet1/5인 포트 채널 1:

```
firepower# scope packet-capture
firepower /packet-capture # show session cap1
```

Traffic Monitoring Session:

```
Packet Capture Session Name: cap1
Session: 1
Admin State: Enabled
Oper State: Up
Oper State Reason: Active
Config Success: Yes
Config Fail Reason:
Append Flag: Overwrite
Session Mem Usage: 256 MB
Session Pcap Snap Len: 1518 Bytes
Error Code: 0
Drop Count: 0
```

Physical ports involved in Packet Capture:

```
Slot Id: 1
Port Id: 4
```

Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-4-0.pcap

Pcapsize: 310276 bytes

Filter:

Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

Slot Id: 1

Port Id: 5

Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-5-0.pcap

Pcapsize: 160 bytes

Filter:

Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

캡처 파일 수집

Firepower 4100/9300 내부 스위치 캡처 파일 수집 섹션의 단계를 수행합니다.

캡처 파일 분석

패킷 캡처 파일 판독기 응용 프로그램을 사용하여 Ethernet1/2용 캡처 파일을 엽니다. 첫 번째 패킷을 선택하고 핵심 사항을 확인합니다.

1. ICMP 에코 요청 패킷만 캡처됩니다. 각 패킷은 캡처되어 2번 표시됩니다.
2. 원래 패킷 헤더에 VLAN 태그가 없습니다.
3. 내부 스위치는 인그레스 인터페이스 Ethernet1/2를 식별하는 추가 포트 VLAN 태그(102)를 삽입합니다.
4. 내부 스위치는 추가 VN 태그를 삽입합니다.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-07-13 06:23:58.285080930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found!)
2	2022-07-13 06:23:58.285082858	192.0.2.100	198.51.100.100	ICMP	102	0x9dec (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found!)
3	2022-07-13 06:23:59.309048886	192.0.2.100	198.51.100.100	ICMP	108	0x9ed0 (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found!)
4	2022-07-13 06:23:59.309193731	192.0.2.100	198.51.100.100	ICMP	102	0x9ed0 (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found!)
5	2022-07-13 06:24:00.333054190	192.0.2.100	198.51.100.100	ICMP	108	0x9f20 (40736)	64	Echo (ping) request id=0x001a, seq=9/2304, ttl=64 (no response found!)
6	2022-07-13 06:24:00.333056014	192.0.2.100	198.51.100.100	ICMP	102	0x9f20 (40736)	64	Echo (ping) request id=0x001a, seq=9/2304, ttl=64 (no response found!)
7	2022-07-13 06:24:01.357173530	192.0.2.100	198.51.100.100	ICMP	108	0xf02d (40749)	64	Echo (ping) request id=0x001a, seq=10/2560, ttl=64 (no response found!)
8	2022-07-13 06:24:01.357174708	192.0.2.100	198.51.100.100	ICMP	102	0xf02d (40749)	64	Echo (ping) request id=0x001a, seq=10/2560, ttl=64 (no response found!)
9	2022-07-13 06:24:02.381073741	192.0.2.100	198.51.100.100	ICMP	108	0xf088 (40840)	64	Echo (ping) request id=0x001a, seq=11/2816, ttl=64 (no response found!)
10	2022-07-13 06:24:02.381074999	192.0.2.100	198.51.100.100	ICMP	102	0xf088 (40840)	64	Echo (ping) request id=0x001a, seq=11/2816, ttl=64 (no response found!)
11	2022-07-13 06:24:03.405199041	192.0.2.100	198.51.100.100	ICMP	108	0xa077 (41079)	64	Echo (ping) request id=0x001a, seq=12/3072, ttl=64 (no response found!)
12	2022-07-13 06:24:03.405200261	192.0.2.100	198.51.100.100	ICMP	102	0xa077 (41079)	64	Echo (ping) request id=0x001a, seq=12/3072, ttl=64 (no response found!)
13	2022-07-13 06:24:04.429155683	192.0.2.100	198.51.100.100	ICMP	108	0xa10f (41231)	64	Echo (ping) request id=0x001a, seq=13/3328, ttl=64 (no response found!)
14	2022-07-13 06:24:04.429156831	192.0.2.100	198.51.100.100	ICMP	102	0xa10f (41231)	64	Echo (ping) request id=0x001a, seq=13/3328, ttl=64 (no response found!)
15	2022-07-13 06:24:05.453156612	192.0.2.100	198.51.100.100	ICMP	108	0xa16a (41322)	64	Echo (ping) request id=0x001a, seq=14/3584, ttl=64 (no response found!)
16	2022-07-13 06:24:05.453158052	192.0.2.100	198.51.100.100	ICMP	102	0xa16a (41322)	64	Echo (ping) request id=0x001a, seq=14/3584, ttl=64 (no response found!)
17	2022-07-13 06:24:06.477127687	192.0.2.100	198.51.100.100	ICMP	108	0xa1e9 (41449)	64	Echo (ping) request id=0x001a, seq=15/3840, ttl=64 (no response found!)
18	2022-07-13 06:24:06.477129899	192.0.2.100	198.51.100.100	ICMP	102	0xa1e9 (41449)	64	Echo (ping) request id=0x001a, seq=15/3840, ttl=64 (no response found!)
19	2022-07-13 06:24:07.501291314	192.0.2.100	198.51.100.100	ICMP	108	0xa1f6 (41462)	64	Echo (ping) request id=0x001a, seq=16/4096, ttl=64 (no response found!)
20	2022-07-13 06:24:07.501293041	192.0.2.100	198.51.100.100	ICMP	102	0xa1f6 (41462)	64	Echo (ping) request id=0x001a, seq=16/4096, ttl=64 (no response found!)
21	2022-07-13 06:24:08.525098956	192.0.2.100	198.51.100.100	ICMP	108	0xa257 (41559)	64	Echo (ping) request id=0x001a, seq=17/4352, ttl=64 (no response found!)
22	2022-07-13 06:24:08.525092088	192.0.2.100	198.51.100.100	ICMP	102	0xa257 (41559)	64	Echo (ping) request id=0x001a, seq=17/4352, ttl=64 (no response found!)
23	2022-07-13 06:24:09.549236500	192.0.2.100	198.51.100.100	ICMP	108	0xa2a9 (41641)	64	Echo (ping) request id=0x001a, seq=18/4608, ttl=64 (no response found!)
24	2022-07-13 06:24:09.549238564	192.0.2.100	198.51.100.100	ICMP	102	0xa2a9 (41641)	64	Echo (ping) request id=0x001a, seq=18/4608, ttl=64 (no response found!)
25	2022-07-13 06:24:10.573110146	192.0.2.100	198.51.100.100	ICMP	108	0xa345 (41797)	64	Echo (ping) request id=0x001a, seq=19/4864, ttl=64 (no response found!)
26	2022-07-13 06:24:10.573112504	192.0.2.100	198.51.100.100	ICMP	102	0xa345 (41797)	64	Echo (ping) request id=0x001a, seq=19/4864, ttl=64 (no response found!)
27	2022-07-13 06:24:11.597086027	192.0.2.100	198.51.100.100	ICMP	108	0xa349 (41801)	64	Echo (ping) request id=0x001a, seq=20/5120, ttl=64 (no response found!)
28	2022-07-13 06:24:11.597088170	192.0.2.100	198.51.100.100	ICMP	102	0xa349 (41801)	64	Echo (ping) request id=0x001a, seq=20/5120, ttl=64 (no response found!)
29	2022-07-13 06:24:12.621061022	192.0.2.100	198.51.100.100	ICMP	108	0xa3dc (41948)	64	Echo (ping) request id=0x001a, seq=21/5376, ttl=64 (no response found!)


```

> Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_1, id 0
  Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)
  VN-Tag
  1... .. = Direction: From Bridge
  .0... .. = Pointer: vif_id
  ..00 0000 0000 1010 .. = Destination: 10
  .. .. = Looped: No
  .. .. = Reserved: 0
  .. .. = Version: 0
  .. .. 0000 0000 0000 = Source: 0
  Type: 802.1Q Virtual LAN (0x8100)
  802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
  000... .. = Priority: Best Effort (default) (0)
  ..0... .. = DEI: Ineligible
  ... 0000 0110 0110 = ID: 102
  Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
  Internet Control Message Protocol
  
```

두 번째 패킷을 선택하고 핵심 사항을 확인합니다.

1. ICMP 에코 요청 패킷만 캡처됩니다. 각 패킷은 캡처되어 2번 표시됩니다.
2. 원래 패킷 헤더에 VLAN 태그가 없습니다.

3. 내부 스위치는 인그레스 인터페이스 Ethernet1/2를 식별하는 추가 포트 VLAN 태그(102)를 삽입합니다.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-07-13 06:23:58.285080930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found)
2	2022-07-13 06:23:58.285082858	192.0.2.100	198.51.100.100	ICMP	102	0x9dec (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found)
3	2022-07-13 06:23:59.309048886	192.0.2.100	198.51.100.100	ICMP	108	0x9e0d (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found)
4	2022-07-13 06:23:59.309193731	192.0.2.100	198.51.100.100	ICMP	102	0x9e0d (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found)
5	2022-07-13 06:24:00.333054190	192.0.2.100	198.51.100.100	ICMP	108	0x9f20 (40736)	64	Echo (ping) request id=0x001a, seq=9/2304, ttl=64 (no response found)
6	2022-07-13 06:24:00.333056014	192.0.2.100	198.51.100.100	ICMP	102	0x9f20 (40736)	64	Echo (ping) request id=0x001a, seq=9/2304, ttl=64 (no response found)
7	2022-07-13 06:24:01.357173530	192.0.2.100	198.51.100.100	ICMP	108	0x9f2d (40749)	64	Echo (ping) request id=0x001a, seq=10/2560, ttl=64 (no response found)
8	2022-07-13 06:24:01.357174708	192.0.2.100	198.51.100.100	ICMP	102	0x9f2d (40749)	64	Echo (ping) request id=0x001a, seq=10/2560, ttl=64 (no response found)
9	2022-07-13 06:24:02.381073741	192.0.2.100	198.51.100.100	ICMP	108	0x9f88 (40840)	64	Echo (ping) request id=0x001a, seq=11/2816, ttl=64 (no response found)
10	2022-07-13 06:24:02.381074999	192.0.2.100	198.51.100.100	ICMP	102	0x9f88 (40840)	64	Echo (ping) request id=0x001a, seq=11/2816, ttl=64 (no response found)
11	2022-07-13 06:24:03.405199041	192.0.2.100	198.51.100.100	ICMP	108	0xa077 (41079)	64	Echo (ping) request id=0x001a, seq=12/3072, ttl=64 (no response found)
12	2022-07-13 06:24:03.405200261	192.0.2.100	198.51.100.100	ICMP	102	0xa077 (41079)	64	Echo (ping) request id=0x001a, seq=12/3072, ttl=64 (no response found)
13	2022-07-13 06:24:04.429155683	192.0.2.100	198.51.100.100	ICMP	108	0xa10f (41231)	64	Echo (ping) request id=0x001a, seq=13/3328, ttl=64 (no response found)
14	2022-07-13 06:24:04.429156831	192.0.2.100	198.51.100.100	ICMP	102	0xa10f (41231)	64	Echo (ping) request id=0x001a, seq=13/3328, ttl=64 (no response found)
15	2022-07-13 06:24:05.453156612	192.0.2.100	198.51.100.100	ICMP	108	0xa16a (41322)	64	Echo (ping) request id=0x001a, seq=14/3584, ttl=64 (no response found)
16	2022-07-13 06:24:05.453158052	192.0.2.100	198.51.100.100	ICMP	102	0xa16a (41322)	64	Echo (ping) request id=0x001a, seq=14/3584, ttl=64 (no response found)
17	2022-07-13 06:24:06.477127687	192.0.2.100	198.51.100.100	ICMP	108	0xa1e9 (41449)	64	Echo (ping) request id=0x001a, seq=15/3840, ttl=64 (no response found)
18	2022-07-13 06:24:06.477129899	192.0.2.100	198.51.100.100	ICMP	102	0xa1e9 (41449)	64	Echo (ping) request id=0x001a, seq=15/3840, ttl=64 (no response found)
19	2022-07-13 06:24:07.501291314	192.0.2.100	198.51.100.100	ICMP	108	0xa1f6 (41462)	64	Echo (ping) request id=0x001a, seq=16/4096, ttl=64 (no response found)
20	2022-07-13 06:24:07.501293041	192.0.2.100	198.51.100.100	ICMP	102	0xa1f6 (41462)	64	Echo (ping) request id=0x001a, seq=16/4096, ttl=64 (no response found)
21	2022-07-13 06:24:08.525089956	192.0.2.100	198.51.100.100	ICMP	108	0xa257 (41559)	64	Echo (ping) request id=0x001a, seq=17/4352, ttl=64 (no response found)
22	2022-07-13 06:24:08.525092888	192.0.2.100	198.51.100.100	ICMP	102	0xa257 (41559)	64	Echo (ping) request id=0x001a, seq=17/4352, ttl=64 (no response found)
23	2022-07-13 06:24:09.549236500	192.0.2.100	198.51.100.100	ICMP	108	0xa2a9 (41641)	64	Echo (ping) request id=0x001a, seq=18/4608, ttl=64 (no response found)
24	2022-07-13 06:24:09.549238564	192.0.2.100	198.51.100.100	ICMP	102	0xa2a9 (41641)	64	Echo (ping) request id=0x001a, seq=18/4608, ttl=64 (no response found)
25	2022-07-13 06:24:10.573110146	192.0.2.100	198.51.100.100	ICMP	108	0xa345 (41797)	64	Echo (ping) request id=0x001a, seq=19/4864, ttl=64 (no response found)
26	2022-07-13 06:24:10.573112504	192.0.2.100	198.51.100.100	ICMP	102	0xa345 (41797)	64	Echo (ping) request id=0x001a, seq=19/4864, ttl=64 (no response found)
27	2022-07-13 06:24:11.597886277	192.0.2.100	198.51.100.100	ICMP	108	0xa349 (41801)	64	Echo (ping) request id=0x001a, seq=20/5120, ttl=64 (no response found)
28	2022-07-13 06:24:11.597888170	192.0.2.100	198.51.100.100	ICMP	102	0xa349 (41801)	64	Echo (ping) request id=0x001a, seq=20/5120, ttl=64 (no response found)
29	2022-07-13 06:24:12.621061022	192.0.2.100	198.51.100.100	ICMP	108	0xa3dc (41948)	64	Echo (ping) request id=0x001a, seq=21/5376, ttl=64 (no response found)

```

> Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture_u0_1, id 0
  > Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)
  > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
    000. .... = Priority: Best Effort (default) (0)
    ...0 .... = DEI: Ineligible
    ... 0000 0101 0100 = ID: 102
    Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
  > Internet Control Message Protocol
  
```

Portchannel1 멤버 인터페이스에 대한 캡처 파일을 엽니다. 첫 번째 패킷을 선택하고 핵심 사항을 확인합니다.

1. ICMP 에코 요청 패킷만 캡처됩니다. 각 패킷은 캡처되어 2번 표시됩니다.
2. 원래 패킷 헤더에 VLAN 태그가 없습니다.
3. 내부 스위치는 인그레스 인터페이스 Portchannel1을 식별하는 추가 포트 VLAN 태그 1001을 삽입합니다.
4. 내부 스위치는 추가 VN 태그를 삽입합니다.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-05 23:07:31.865872877	192.0.2.100	198.51.100.100	ICMP	108	0x322e (12846)	64	Echo (ping) request id=0x002d, seq=245/62720, ttl=64 (no response found)
2	2022-08-05 23:07:31.865875131	192.0.2.100	198.51.100.100	ICMP	102	0x322e (12846)	64	Echo (ping) request id=0x002d, seq=245/62720, ttl=64 (no response found)
3	2022-08-05 23:07:32.867144598	192.0.2.100	198.51.100.100	ICMP	108	0x32b9 (12985)	64	Echo (ping) request id=0x002d, seq=246/62976, ttl=64 (no response found)
4	2022-08-05 23:07:32.867145852	192.0.2.100	198.51.100.100	ICMP	102	0x32b9 (12985)	64	Echo (ping) request id=0x002d, seq=246/62976, ttl=64 (no response found)
5	2022-08-05 23:07:33.881904285	192.0.2.100	198.51.100.100	ICMP	108	0x32d8 (13016)	64	Echo (ping) request id=0x002d, seq=247/63232, ttl=64 (no response found)
6	2022-08-05 23:07:33.881904191	192.0.2.100	198.51.100.100	ICMP	102	0x32d8 (13016)	64	Echo (ping) request id=0x002d, seq=247/63232, ttl=64 (no response found)
7	2022-08-05 23:07:34.883049425	192.0.2.100	198.51.100.100	ICMP	108	0x3373 (13171)	64	Echo (ping) request id=0x002d, seq=248/63488, ttl=64 (no response found)
8	2022-08-05 23:07:34.883051649	192.0.2.100	198.51.100.100	ICMP	102	0x3373 (13171)	64	Echo (ping) request id=0x002d, seq=248/63488, ttl=64 (no response found)
9	2022-08-05 23:07:35.883478016	192.0.2.100	198.51.100.100	ICMP	108	0x3427 (13351)	64	Echo (ping) request id=0x002d, seq=249/63744, ttl=64 (no response found)
10	2022-08-05 23:07:35.883479190	192.0.2.100	198.51.100.100	ICMP	102	0x3427 (13351)	64	Echo (ping) request id=0x002d, seq=249/63744, ttl=64 (no response found)
11	2022-08-05 23:07:36.889741625	192.0.2.100	198.51.100.100	ICMP	108	0x34de (13534)	64	Echo (ping) request id=0x002d, seq=250/64000, ttl=64 (no response found)
12	2022-08-05 23:07:36.889742853	192.0.2.100	198.51.100.100	ICMP	102	0x34de (13534)	64	Echo (ping) request id=0x002d, seq=250/64000, ttl=64 (no response found)
13	2022-08-05 23:07:37.913770117	192.0.2.100	198.51.100.100	ICMP	108	0x354c (13644)	64	Echo (ping) request id=0x002d, seq=251/64256, ttl=64 (no response found)
14	2022-08-05 23:07:37.913772219	192.0.2.100	198.51.100.100	ICMP	102	0x354c (13644)	64	Echo (ping) request id=0x002d, seq=251/64256, ttl=64 (no response found)
15	2022-08-05 23:07:38.937829879	192.0.2.100	198.51.100.100	ICMP	108	0x3602 (13826)	64	Echo (ping) request id=0x002d, seq=252/64512, ttl=64 (no response found)
16	2022-08-05 23:07:38.937831215	192.0.2.100	198.51.100.100	ICMP	102	0x3602 (13826)	64	Echo (ping) request id=0x002d, seq=252/64512, ttl=64 (no response found)
17	2022-08-05 23:07:39.961786128	192.0.2.100	198.51.100.100	ICMP	108	0x36ed (14061)	64	Echo (ping) request id=0x002d, seq=253/64768, ttl=64 (no response found)
18	2022-08-05 23:07:39.961787284	192.0.2.100	198.51.100.100	ICMP	102	0x36ed (14061)	64	Echo (ping) request id=0x002d, seq=253/64768, ttl=64 (no response found)
19	2022-08-05 23:07:40.985773090	192.0.2.100	198.51.100.100	ICMP	108	0x37d5 (14293)	64	Echo (ping) request id=0x002d, seq=254/65024, ttl=64 (no response found)

```

> Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_3, id 0
  > Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: a2:76:f2:00:00:25 (a2:76:f2:00:00:25)
  > VN-Tag
    1. .... = Direction: From Bridge
    .0. .... = Pointer: vif_id
    ..00 0000 0101 0100 = Destination: 84
    ... .. = Looped: No
    ... .. = Reserved: 0
    ... .. = Version: 0
    ... 0000 0000 0000 = Source: 0
    Type: 802.1Q Virtual LAN (0x8100)
  > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1001
    000. .... = Priority: Best Effort (default) (0)
    ...0 .... = DEI: Ineligible
    ... 0011 1110 1001 = ID: 1001
    Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
  > Internet Control Message Protocol
  
```

두 번째 패킷을 선택하고 핵심 사항을 확인합니다.

1. ICMP 에코 요청 패킷만 캡처됩니다. 각 패킷은 캡처되어 2번 표시됩니다.
2. 원래 패킷 헤더에 VLAN 태그가 없습니다.

3. 내부 스위치는 인그레스 인터페이스 Portchannel1을 식별하는 추가 포트 VLAN 태그 1001을 삽입합니다.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-05 23:07:31.865872877	192.0.2.100	198.51.100.100	ICMP	108	0x322e (12846)	64	Echo (ping) request id=0x002d, seq=245/62720, ttl=64 (nc
2	2022-08-05 23:07:31.865875131	192.0.2.100	198.51.100.100	ICMP	102	0x322e (12846)	64	Echo (ping) request id=0x002d, seq=245/62720, ttl=64 (nc
3	2022-08-05 23:07:32.867144598	192.0.2.100	198.51.100.100	ICMP	108	0x32b9 (12985)	64	Echo (ping) request id=0x002d, seq=246/62976, ttl=64 (nc
4	2022-08-05 23:07:32.867145852	192.0.2.100	198.51.100.100	ICMP	102	0x32b9 (12985)	64	Echo (ping) request id=0x002d, seq=246/62976, ttl=64 (nc
5	2022-08-05 23:07:33.881902485	192.0.2.100	198.51.100.100	ICMP	108	0x32d8 (13016)	64	Echo (ping) request id=0x002d, seq=247/63232, ttl=64 (nc
6	2022-08-05 23:07:33.881904191	192.0.2.100	198.51.100.100	ICMP	102	0x32d8 (13016)	64	Echo (ping) request id=0x002d, seq=247/63232, ttl=64 (nc
7	2022-08-05 23:07:34.883049425	192.0.2.100	198.51.100.100	ICMP	108	0x3373 (13171)	64	Echo (ping) request id=0x002d, seq=248/63488, ttl=64 (nc
8	2022-08-05 23:07:34.883051649	192.0.2.100	198.51.100.100	ICMP	102	0x3373 (13171)	64	Echo (ping) request id=0x002d, seq=248/63488, ttl=64 (nc
9	2022-08-05 23:07:35.883478016	192.0.2.100	198.51.100.100	ICMP	108	0x3427 (13351)	64	Echo (ping) request id=0x002d, seq=249/63744, ttl=64 (nc
10	2022-08-05 23:07:35.883479190	192.0.2.100	198.51.100.100	ICMP	102	0x3427 (13351)	64	Echo (ping) request id=0x002d, seq=249/63744, ttl=64 (nc
11	2022-08-05 23:07:36.889741625	192.0.2.100	198.51.100.100	ICMP	108	0x34de (13534)	64	Echo (ping) request id=0x002d, seq=250/64000, ttl=64 (nc
12	2022-08-05 23:07:36.889742853	192.0.2.100	198.51.100.100	ICMP	102	0x34de (13534)	64	Echo (ping) request id=0x002d, seq=250/64000, ttl=64 (nc
13	2022-08-05 23:07:37.913770117	192.0.2.100	198.51.100.100	ICMP	108	0x354c (13644)	64	Echo (ping) request id=0x002d, seq=251/64256, ttl=64 (nc
14	2022-08-05 23:07:37.913772219	192.0.2.100	198.51.100.100	ICMP	102	0x354c (13644)	64	Echo (ping) request id=0x002d, seq=251/64256, ttl=64 (nc
15	2022-08-05 23:07:38.937829879	192.0.2.100	198.51.100.100	ICMP	108	0x3602 (13826)	64	Echo (ping) request id=0x002d, seq=252/64512, ttl=64 (nc
16	2022-08-05 23:07:38.937831215	192.0.2.100	198.51.100.100	ICMP	102	0x3602 (13826)	64	Echo (ping) request id=0x002d, seq=252/64512, ttl=64 (nc
17	2022-08-05 23:07:39.961786128	192.0.2.100	198.51.100.100	ICMP	108	0x36ed (14061)	64	Echo (ping) request id=0x002d, seq=253/64768, ttl=64 (nc
18	2022-08-05 23:07:39.961787284	192.0.2.100	198.51.100.100	ICMP	102	0x36ed (14061)	64	Echo (ping) request id=0x002d, seq=253/64768, ttl=64 (nc
19	2022-08-05 23:07:40.985773090	192.0.2.100	198.51.100.100	ICMP	108	0x37d5 (14293)	64	Echo (ping) request id=0x002d, seq=254/65024, ttl=64 (nc

> Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: a2:76:f2:00:00:25 (a2:76:f2:00:00:25)		0000 a2 76 f2 00 00 25 00 50 56 9d e8 be 81 00 03 e9
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1001		0010 08 00 45 00 00 54 32 2e 40 00 40 01 1b 7f c0 00
000. = Priority: Best Effort (default) (0)		0020 02 64 c6 33 64 64 08 00 1e d6 00 2d 00 f5 a6 a2
...0 = DEI: Ineligible		0030 ed 62 00 00 00 00 7a 2f 0b 00 00 00 00 10 11
.... 0011 1110 1001 = ID: 1001		0040 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21
Type: IPv4 (0x0800)		0050 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31
Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100		0060 32 33 34 35 36 37
Internet Control Message Protocol		

설명

전면 인터페이스에서 패킷 캡처가 구성된 경우, 스위치는 각 패킷을 동시에 두 번 캡처합니다.

- 포트 VLAN 태그를 삽입한 후
- VN 태그를 삽입한 후

연산 순서에 따라 VN 태그는 포트 VLAN 태그 삽입보다 후반에 삽입됩니다. 그러나 캡처 파일에서 VN 태그가 있는 패킷은 포트 VLAN 태그가 있는 패킷보다 먼저 표시됩니다.

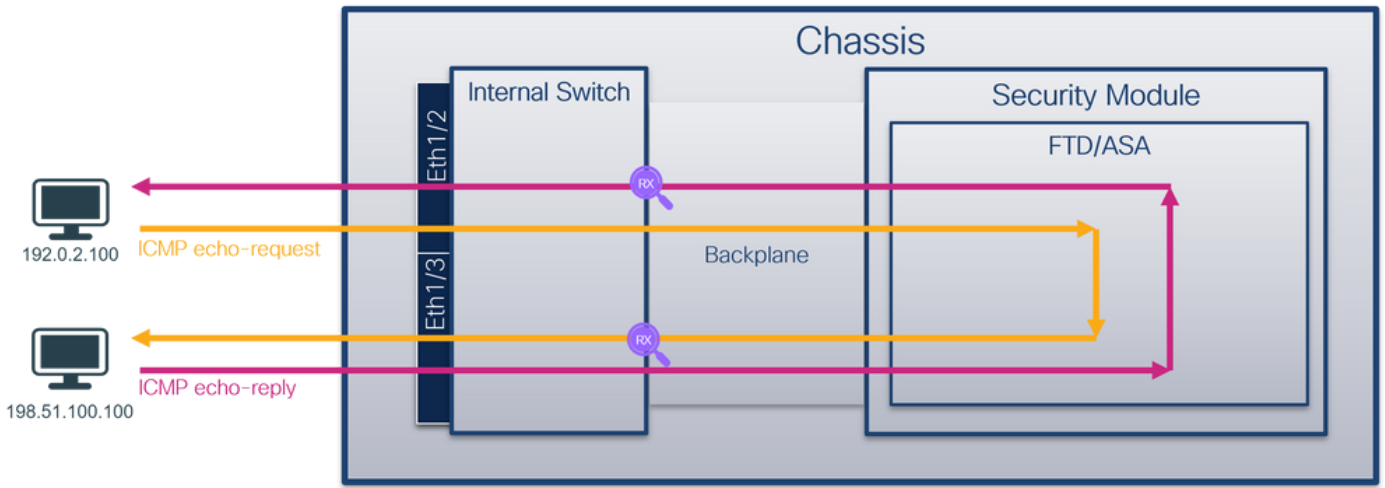
이 표에서는 작업을 요약합니다.

작업	캡처 지점	캡처된 패킷의 내부 포트 VLAN	방향	캡처된 트래픽
인터페이스 Ethernet1/2에서 패킷 캡처 구성 및 확인	이더넷1/2	102	인그레스 전용	호스트 192.0.2.100에서 호스트 198.51.100.100으로의 ICMP 에코
멤버 인터페이스 Ethernet1/4 및 Ethernet1/5를 사용하여 인터페이스 Portchannel1에서 패킷 캡처 구성 및 확인	이더넷1/4 이더넷1/5	1001	인그레스 전용	호스트 192.0.2.100에서 호스트 198.51.100.100으로의 ICMP 에코

백플레인 인터페이스의 패킷 캡처

FCM 및 CLI를 사용하여 백플레인 인터페이스에서 패킷 캡처를 구성하고 확인합니다.

토폴로지, 패킷 흐름 및 캡처 포인트

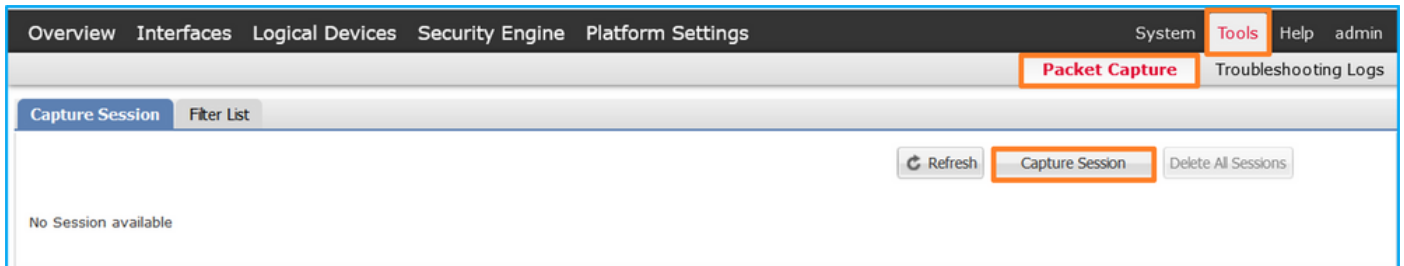


설정

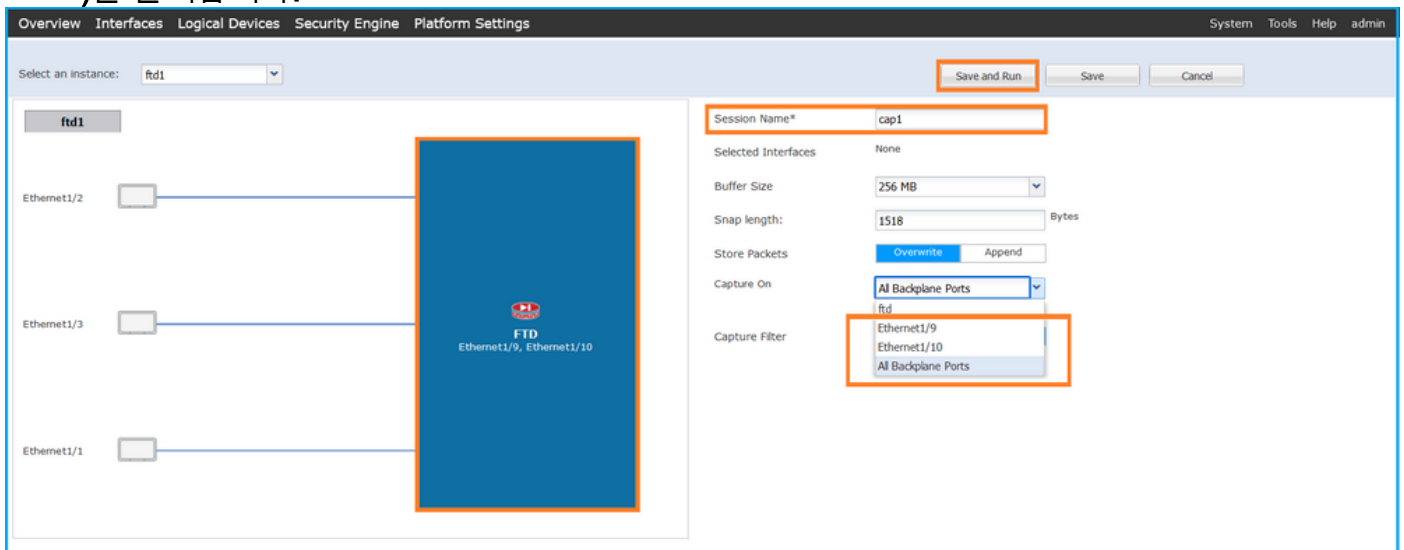
FCM

FCM에서 다음 단계를 수행하여 백플레인 인터페이스의 패킷 캡처를 구성합니다.

1. Tools(도구) > Packet Capture(패킷 캡처) > Capture Session(캡처 세션)을 사용하여 새 캡처 세션을 생성합니다.



2. 모든 백플레인 인터페이스의 패킷을 캡처하려면 드롭다운 목록에서 애플리케이션을 선택한 다음 All Backplane Ports(모든 백플레인 포트)를 선택합니다. 또는 특정 백플레인 인터페이스를 선택합니다. 이 경우 백플레인 인터페이스 Ethernet1/9 및 Ethernet1/10을 사용할 수 있습니다. 캡처를 활성화하려면 Session Name(세션 이름)을 입력하고 Save and Run(저장 및 실행)을 클릭합니다.



FXOS CLI

백플레인 인터페이스에서 패킷 캡처를 구성하려면 FXOS CLI에서 다음 단계를 수행합니다.

1. 애플리케이션 유형 및 식별자를 식별합니다.

```
firepower# scope ssa
firepower /ssa# show app-instance
App Name      Identifier Slot ID   Admin State Oper State      Running Version Startup Version
Deploy Type  Turbo Mode Profile Name Cluster State  Cluster Role
-----
ftd          ftd1         1           Enabled   Online         7.2.0.82      7.2.0.82
Native      No           Not Applicable None
```

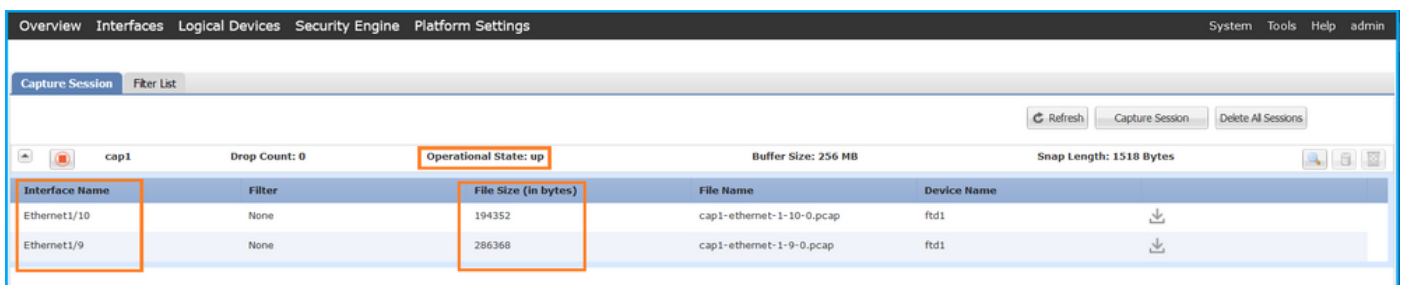
2. 캡처 세션을 생성합니다.

```
firepower# scope packet-capture
firepower /packet-capture # create session cap1
firepower /packet-capture/session* # create phy-port Eth1/9
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # set app-identifier ftd1
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # create phy-port Eth1/10
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # set app-identifier ftd1
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # enable
firepower /packet-capture/session* # commit
firepower /packet-capture/session #
```

확인

FCM

인터페이스 이름을 확인하고 작동 상태가 작동 중인지, 파일 크기(바이트)가 증가하는지 확인합니다.



FXOS CLI

scope packet-capture에서 캡처 세부 정보를 확인합니다.

```
firepower# scope packet-capture
firepower /packet-capture # show session cap1
```

```
Traffic Monitoring Session:
  Packet Capture Session Name: cap1
  Session: 1
  Admin State: Enabled
  Oper State: Up
  Oper State Reason: Active
```

Config Success: Yes
Config Fail Reason:
Append Flag: Overwrite
Session Mem Usage: 256 MB
Session Pcap Snap Len: 1518 Bytes
Error Code: 0
Drop Count: 0

Physical ports involved in Packet Capture:

Slot Id: 1
Port Id: 10
Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-10-0.pcap
Pcapsize: 1017424 bytes

Filter:

Sub Interface: 0
Application Instance Identifier: ftd1
Application Name: ftd

Slot Id: 1
Port Id: 9
Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-9-0.pcap
Pcapsize: 1557432 bytes

Filter:

Sub Interface: 0
Application Instance Identifier: ftd1
Application Name: ftd

캡처 파일 수집

Firepower 4100/9300 내부 스위치 캡처 파일 수집 섹션의 단계를 수행합니다.

캡처 파일 분석

패킷 캡처 파일 리더 애플리케이션을 사용하여 캡처 파일을 엽니다. 백플레인 인터페이스가 여러 개인 경우 각 백플레인 인터페이스의 모든 캡처 파일을 열어야 합니다. 이 경우 패킷은 백플레인 인터페이스 Ethernet1/9에서 캡처됩니다.

첫 번째 및 두 번째 패킷을 선택하고 핵심 사항을 확인합니다.

1. 각 ICMP 에코 요청 패킷이 캡처되어 2번 표시됩니다.
2. 원래 패킷 헤더에 VLAN 태그가 없습니다.
3. 내부 스위치는 이그레스 인터페이스 Ethernet1/3을 식별하는 추가 포트 VLAN 태그(103)를 삽입합니다.
4. 내부 스위치는 추가 VN 태그를 삽입합니다.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-07-14 20:20:36.513854256	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (no response found!)
2	2022-07-14 20:20:36.513857289	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (reply in 3)
3	2022-07-14 20:20:36.514117394	198.51.100.100	192.0.2.100	ICMP	108	0xc2c2 (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 2)
4	2022-07-14 20:20:36.514119312	198.51.100.100	192.0.2.100	ICMP	108	0xc2c2 (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64
5	2022-07-14 20:20:37.537723822	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040)	64	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (no response found!)
6	2022-07-14 20:20:37.537726588	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040)	64	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (reply in 7)
7	2022-07-14 20:20:37.588046165	198.51.100.100	192.0.2.100	ICMP	108	0xc9b9 (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 6)
8	2022-07-14 20:20:37.538048311	198.51.100.100	192.0.2.100	ICMP	108	0xc9b9 (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64
9	2022-07-14 20:20:38.561776064	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (no response found!)
10	2022-07-14 20:20:38.561778310	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (reply in 11)
11	2022-07-14 20:20:38.562048288	198.51.100.100	192.0.2.100	ICMP	108	0xc4c4 (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 10)
12	2022-07-14 20:20:38.562050333	198.51.100.100	192.0.2.100	ICMP	108	0xc4c4 (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64
13	2022-07-14 20:20:39.5850677043	192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366)	64	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (no response found!)
14	2022-07-14 20:20:39.585678455	192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366)	64	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (reply in 15)
15	2022-07-14 20:20:39.585936554	198.51.100.100	192.0.2.100	ICMP	108	0xcdbd (52621)	64	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64 (request in 14)
16	2022-07-14 20:20:39.585937900	198.51.100.100	192.0.2.100	ICMP	108	0xcdbd (52621)	64	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64
17	2022-07-14 20:20:40.609804804	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (23419)	64	Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (no response found!)
18	2022-07-14 20:20:40.609807618	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (23419)	64	Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (reply in 19)
19	2022-07-14 20:20:40.610179685	198.51.100.100	192.0.2.100	ICMP	108	0xcdf8 (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64 (request in 18)
20	2022-07-14 20:20:40.610181944	198.51.100.100	192.0.2.100	ICMP	108	0xcdf8 (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64
21	2022-07-14 20:20:41.633805153	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (no response found!)
22	2022-07-14 20:20:41.633806997	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (reply in 23)
23	2022-07-14 20:20:41.634084102	198.51.100.100	192.0.2.100	ICMP	108	0xc3e6 (52790)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64 (request in 22)
24	2022-07-14 20:20:41.634085368	198.51.100.100	192.0.2.100	ICMP	108	0xc3e6 (52790)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64
25	2022-07-14 20:20:42.657709988	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (no response found!)
26	2022-07-14 20:20:42.657711660	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (reply in 27)
27	2022-07-14 20:20:42.657980675	198.51.100.100	192.0.2.100	ICMP	108	0xc649 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64 (request in 26)
28	2022-07-14 20:20:42.657981971	198.51.100.100	192.0.2.100	ICMP	108	0xc649 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64
29	2022-07-14 20:20:43.681736697	192.0.2.100	198.51.100.100	ICMP	108	0x5c52 (23634)	64	Echo (ping) request id=0x0001, seq=22/5632, ttl=64 (no response found!)

> Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
> Ethernet II, Src: Cisco b9:77:2d (58:97:bd:b9:77:2d), Dst: VMware 9d:e7:50 (00:50:56:9d:e7:50)

```

> VH-Tag
0. .... = Direction: To Bridge
0. .... = Pointer: vif_id
..00 0000 0000 0000 .. = Destination: 0
..... 0. .... = Looped: No
..... 0. .... = Reserved: 0
..... 0. .... = Version: 0
..... 0000 0000 1010 = Source: 10
Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 103
000. .... = Priority: Best Effort (default) (0)
...0 ..... = DEI: Ineligible
... 0000 0110 0111 = ID: 103
Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
> Internet Control Message Protocol
  
```

0000 00 50 56 9d e7 50 58 97 bd b9 77 2d 89 26 00 00 -PV-PX-..w-&-
0010 00 0a 81 00 00 67 08 00 45 00 00 54 59 90 40 00g-E-TY@
0020 40 01 f4 1c 00 02 64 c6 33 64 64 08 00 22 68 @-----d 3dd-~h
0030 00 01 00 0f 89 7a d0 62 00 00 00 00 b3 d7 09 00z-b.....
0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b
0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b!# \$%&'()*+
0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,.../0123 4567

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-07-14 20:20:36.513854256	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (no response found!)
2	2022-07-14 20:20:36.513857289	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (reply in 3)
3	2022-07-14 20:20:36.514117394	198.51.100.100	192.0.2.100	ICMP	108	0xc2c2 (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 2)
4	2022-07-14 20:20:36.514119312	198.51.100.100	192.0.2.100	ICMP	108	0xc2c2 (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64
5	2022-07-14 20:20:37.537723822	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040)	64	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (no response found!)
6	2022-07-14 20:20:37.537726588	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040)	64	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (reply in 7)
7	2022-07-14 20:20:37.588046165	198.51.100.100	192.0.2.100	ICMP	108	0xc9b9 (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 6)
8	2022-07-14 20:20:37.538048311	198.51.100.100	192.0.2.100	ICMP	108	0xc9b9 (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64
9	2022-07-14 20:20:38.561776064	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (no response found!)
10	2022-07-14 20:20:38.561778310	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (reply in 11)
11	2022-07-14 20:20:38.562048288	198.51.100.100	192.0.2.100	ICMP	108	0xc4c4 (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 10)
12	2022-07-14 20:20:38.562050333	198.51.100.100	192.0.2.100	ICMP	108	0xc4c4 (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64
13	2022-07-14 20:20:39.5850677043	192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366)	64	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (no response found!)
14	2022-07-14 20:20:39.585678455	192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366)	64	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (reply in 15)
15	2022-07-14 20:20:39.585936554	198.51.100.100	192.0.2.100	ICMP	108	0xcdbd (52621)	64	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64 (request in 14)
16	2022-07-14 20:20:39.585937900	198.51.100.100	192.0.2.100	ICMP	108	0xcdbd (52621)	64	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64
17	2022-07-14 20:20:40.609804804	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (23419)	64	Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (no response found!)
18	2022-07-14 20:20:40.609807618	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (23419)	64	Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (reply in 19)
19	2022-07-14 20:20:40.610179685	198.51.100.100	192.0.2.100	ICMP	108	0xcdf8 (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64 (request in 18)
20	2022-07-14 20:20:40.610181944	198.51.100.100	192.0.2.100	ICMP	108	0xcdf8 (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64
21	2022-07-14 20:20:41.633805153	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (no response found!)
22	2022-07-14 20:20:41.633806997	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (reply in 23)
23	2022-07-14 20:20:41.634084102	198.51.100.100	192.0.2.100	ICMP	108	0xc3e6 (52790)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64 (request in 22)
24	2022-07-14 20:20:41.634085368	198.51.100.100	192.0.2.100	ICMP	108	0xc3e6 (52790)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64
25	2022-07-14 20:20:42.657709988	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (no response found!)
26	2022-07-14 20:20:42.657711660	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (reply in 27)
27	2022-07-14 20:20:42.657980675	198.51.100.100	192.0.2.100	ICMP	108	0xc649 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64 (request in 26)
28	2022-07-14 20:20:42.657981971	198.51.100.100	192.0.2.100	ICMP	108	0xc649 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64
29	2022-07-14 20:20:43.681736697	192.0.2.100	198.51.100.100	ICMP	108	0x5c52 (23634)	64	Echo (ping) request id=0x0001, seq=22/5632, ttl=64 (no response found!)

> Frame 2: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
> Ethernet II, Src: Cisco b9:77:2d (58:97:bd:b9:77:2d), Dst: VMware 9d:e7:50 (00:50:56:9d:e7:50)

```

> VH-Tag
0. .... = Direction: To Bridge
0. .... = Pointer: vif_id
..00 0000 0000 0000 .. = Destination: 0
..... 0. .... = Looped: No
..... 0. .... = Reserved: 0
..... 0. .... = Version: 0
..... 0000 0000 1010 = Source: 10
Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 103
000. .... = Priority: Best Effort (default) (0)
...0 ..... = DEI: Ineligible
... 0000 0110 0111 = ID: 103
Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
> Internet Control Message Protocol
  
```

0000 00 50 56 9d e7 50 58 97 bd b9 77 2d 89 26 00 00 -PV-PX-..w-&-
0010 00 0a 81 00 00 67 08 00 45 00 00 54 59 90 40 00g-E-TY@
0020 40 01 f4 1c 00 02 64 c6 33 64 64 08 00 22 68 @-----d 3dd-~h
0030 00 01 00 0f 89 7a d0 62 00 00 00 00 b3 d7 09 00z-b.....
0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b
0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b!# \$%&'()*+
0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,.../0123 4567

세 번째 및 네 번째 패킷을 선택하고 핵심 사항을 확인합니다.

1. 각 ICMP 에코 응답이 캡처되어 2번 표시됩니다.
2. 원래 패킷 헤더에 VLAN 태그가 없습니다.
3. 내부 스위치는 이그레스 인터페이스 Ethernet1/2를 식별하는 추가 포트 VLAN 태그(102)를 삽입합니다.
4. 내부 스위치는 추가 VN 태그를 삽입합니다.

Frame 3: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
 Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VMware 9d:e8:be (00:50:56:9d:e8:be)

4 VN-Tag
 3 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
 2 Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100
 Internet Control Message Protocol

설명

백플레인 인터페이스에서 패킷 캡처가 구성된 경우 스위치는 각 패킷을 동시에 두 번 캡처합니다. 이 경우, 내부 스위치는 보안 모듈의 애플리케이션이 포트 VLAN 태그 및 VN 태그와 함께 이미 태그된 패킷을 수신합니다. VLAN 태그는 내부 새시에서 네트워크로 패킷을 전달하는 데 사용하는 이그레스 인터페이스를 식별합니다. ICMP 에코 요청 패킷의 VLAN 태그 103은 이그레스 인터페이스로 Ethernet1/3을 식별하고, ICMP 에코 응답 패킷의 VLAN 태그 102는 이그레스 인터페이스로 Ethernet1/2를 식별합니다. 내부 스위치는 패킷이 네트워크로 전달되기 전에 VN 태그 및 내부 인터페이스 VLAN 태그를 제거합니다.

이 표에서는 작업을 요약합니다.

작업	캡처 지점	캡처된 패킷의 내부 포트 VLAN	방향	캡처된 트래픽
백플레인 인터페이스에서 패킷 캡처 구성 및 확인	백플레인 인터페이스	102 103	인그레스 전용	호스트 192.0.2.100에서 호스트 198.51.100.100으로의 ICMP 에코 요청 호스트 198.51.100.100에서 호스트 192.0.2.100으로 ICMP 에코 응답

애플리케이션 및 애플리케이션 포트의 패킷 캡처

사용자가 애플리케이션 캡처 방향을 지정하는 경우 애플리케이션 또는 애플리케이션 포트 패킷 캡처는 항상 백플레인 인터페이스에서, 또한 전면 인터페이스에서 구성됩니다.

주로 두 가지 활용 사례가 있습니다.

- 특정 전면 인터페이스를 떠나는 패킷에 대해 백플레인 인터페이스의 패킷 캡처를 구성합니다. 예를 들어, Ethernet1/2 인터페이스를 떠나는 패킷에 대해 백플레인 인터페이스 Ethernet1/9에

서 패킷 캡처를 구성합니다.

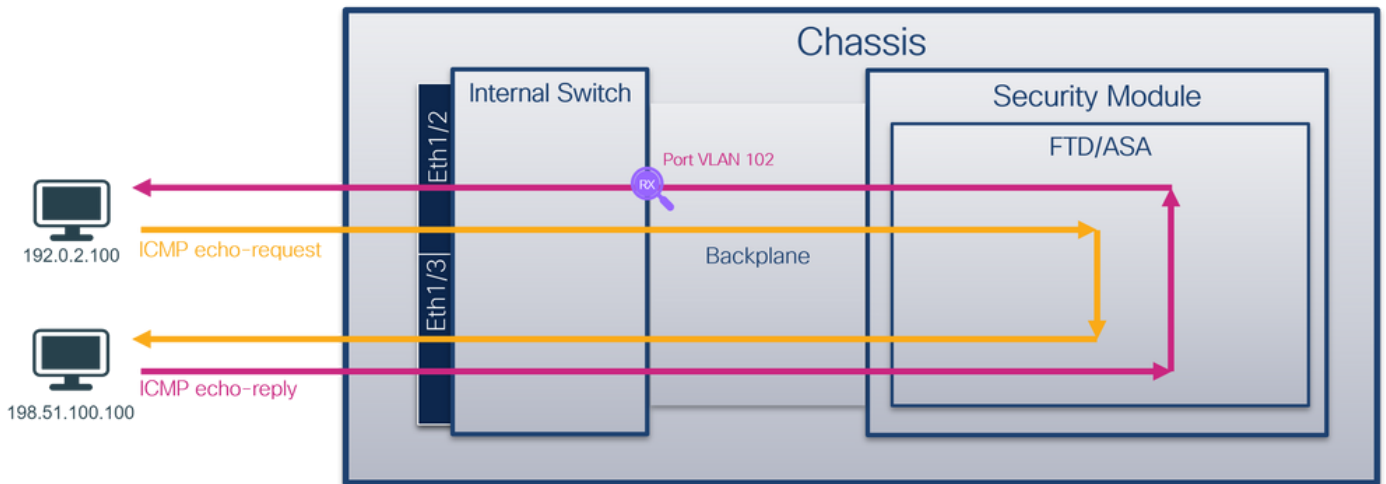
- 특정 전면 인터페이스 및 백플레인 인터페이스에서 동시 패킷 캡처를 구성합니다. 예를 들어, 인터페이스 Ethernet1/2를 떠나는 패킷에 대해 인터페이스 Ethernet1/2 및 백플레인 인터페이스 Ethernet1/9에서 동시 패킷 캡처를 구성합니다.

이 섹션에서는 두 가지 사용 사례를 다룹니다.

작업 1

FCM 및 CLI를 사용하여 백플레인 인터페이스에서 패킷 캡처를 구성하고 확인합니다. 애플리케이션 포트 Ethernet1/2가 이그레스 인터페이스로 식별되는 패킷이 캡처됩니다. 이 경우 ICMP 응답이 캡처됩니다.

토폴로지, 패킷 흐름 및 캡처 포인트

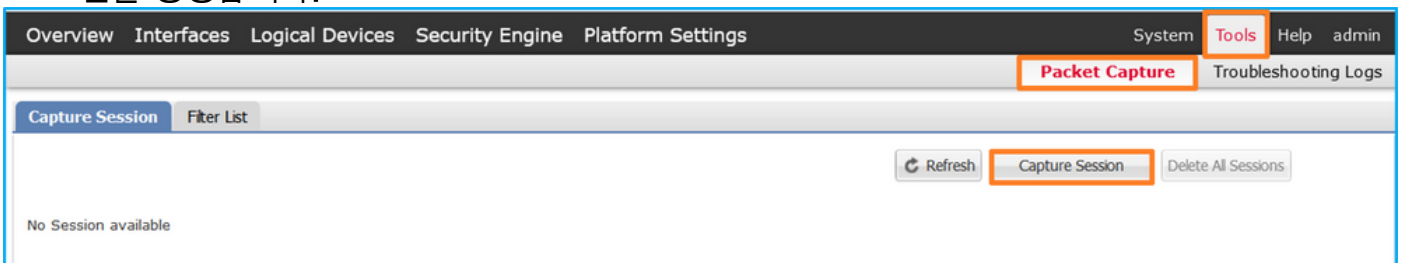


설정

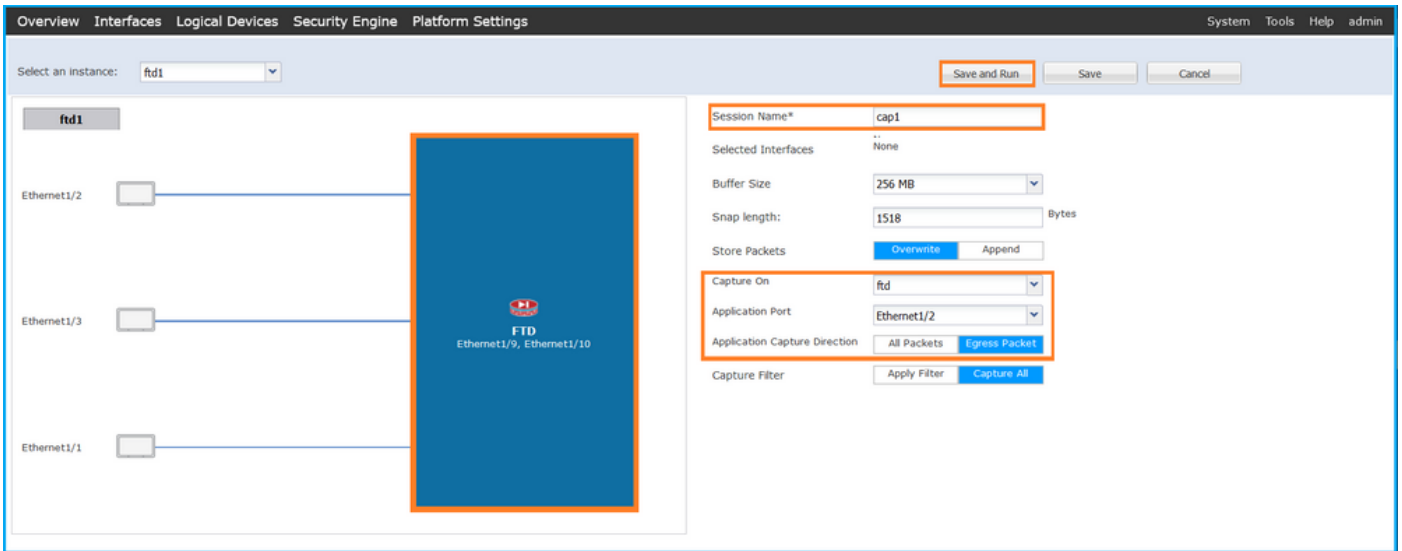
FCM

FCM에서 다음 단계를 수행하여 FTD 애플리케이션 및 애플리케이션 포트 Ethernet1/2에서 패킷 캡처를 구성합니다.

1. Tools(도구) > Packet Capture(패킷 캡처) > Capture Session(캡처 세션)을 사용하여 새 캡처 세션을 생성합니다.



2. Application Port(애플리케이션 포트) 드롭다운 목록에서 애플리케이션 Ethernet1/2를 선택하고 Application Capture Direction(애플리케이션 캡처 방향)에서 Egress Packet(이그레스 패킷)을 선택합니다. 캡처를 활성화하려면 Session Name(세션 이름)을 입력하고 Save and Run(저장 및 실행)을 클릭합니다.



FXOS CLI

백플레인 인터페이스에서 패킷 캡처를 구성하려면 FXOS CLI에서 다음 단계를 수행합니다.

1. 애플리케이션 유형 및 식별자를 식별합니다.

```
firepower# scope ssa
firepower /ssa# show app-instance
App Name Identifier Slot ID Admin State Oper State Running Version Startup Version
Deploy Type Turbo Mode Profile Name Cluster State Cluster Role
-----
ftd ftd1 1 Enabled Online 7.2.0.82 7.2.0.82
Native No Not Applicable None
```

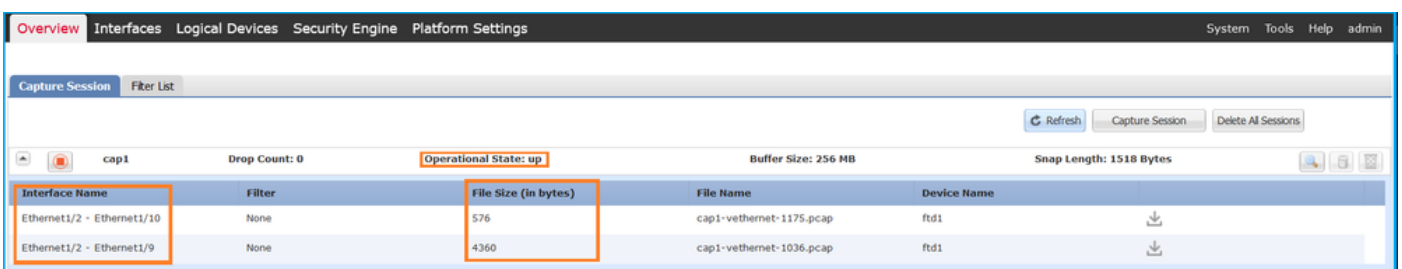
2. 캡처 세션을 생성합니다.

```
firepower# scope packet-capture
firepower /packet-capture # create session cap1
firepower /packet-capture/session* # create app-port 1 112 Ethernet1/2 ftd
firepower /packet-capture/session/app-port* # set app-identifier ftd1
firepower /packet-capture/session/app-port* # set filter ""
firepower /packet-capture/session/app-port* # set subinterface 0
firepower /packet-capture/session/app-port* # up
firepower /packet-capture/session* # commit
firepower /packet-capture/session #
```

확인

FCM

인터페이스 이름을 확인하고 작동 상태가 작동 중인지, 파일 크기(바이트)가 증가하는지 확인합니다.



FXOS CLI

scope packet-capture에서 캡처 세부 정보를 확인합니다.

```
firepower# scope packet-capture
firepower /packet-capture # show session cap1
```

Traffic Monitoring Session:

```
Packet Capture Session Name: cap1
Session: 1
Admin State: Enabled
Oper State: Up
Oper State Reason: Active
Config Success: Yes
Config Fail Reason:
Append Flag: Overwrite
Session Mem Usage: 256 MB
Session Pcap Snap Len: 1518 Bytes
Error Code: 0
Drop Count: 0
```

Application ports involved in Packet Capture:

```
Slot Id: 1
Link Name: 112
Port Name: Ethernet1/2
App Name: ftd
Sub Interface: 0
Application Instance Identifier: ftd1
```

Application ports resolved to:

```
Name: vnic1
Eq Slot Id: 1
Eq Port Id: 9
Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1036.pcap
Pcapsize: 53640 bytes
Vlan: 102
Filter:

Name: vnic2
Eq Slot Id: 1
Eq Port Id: 10
Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1175.pcap
Pcapsize: 1824 bytes
Vlan: 102
Filter:
```

캡처 파일 수집

Firepower 4100/9300 내부 스위치 캡처 파일 수집 섹션의 단계를 수행합니다.

캡처 파일 분석

패킷 캡처 파일 리더 애플리케이션을 사용하여 캡처 파일을 엽니다. 여러 백플레인 인터페이스의 경우 각 백플레인 인터페이스의 모든 캡처 파일을 열어야 합니다. 이 경우 패킷은 백플레인 인터페이스 Ethernet1/9에서 캡처됩니다.

첫 번째 및 두 번째 패킷을 선택하고 핵심 사항을 확인합니다.

1. 각 ICMP 에코 응답이 캡처되어 2번 표시됩니다.

2. 원래 패킷 헤더에 VLAN 태그가 없습니다.

3. 내부 스위치는 이그레스 인터페이스 Ethernet1/2를 식별하는 추가 포트 VLAN 태그(102)를 삽입합니다.

4. 내부 스위치는 추가 VN 태그를 삽입합니다.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 10:03:22.231237959	198.51.100.100	192.0.2.100	ICMP	108	0x42f8 (17144)	64	Echo (ping) reply
2	2022-08-01 10:03:22.231239747	198.51.100.100	192.0.2.100	ICMP	108	0x42f8 (17144)	64	Echo (ping) reply
3	2022-08-01 10:03:23.232244769	198.51.100.100	192.0.2.100	ICMP	108	0x4303 (17331)	64	Echo (ping) reply
4	2022-08-01 10:03:23.232247753	198.51.100.100	192.0.2.100	ICMP	108	0x43b3 (17331)	64	Echo (ping) reply
5	2022-08-01 10:03:24.234703981	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64	Echo (ping) reply
6	2022-08-01 10:03:24.234706751	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64	Echo (ping) reply
7	2022-08-01 10:03:25.258672449	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64	Echo (ping) reply
8	2022-08-01 10:03:25.258674861	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64	Echo (ping) reply
9	2022-08-01 10:03:26.282663169	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64	Echo (ping) reply
10	2022-08-01 10:03:26.282666183	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64	Echo (ping) reply
11	2022-08-01 10:03:27.306671694	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64	Echo (ping) reply
12	2022-08-01 10:03:27.306674378	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64	Echo (ping) reply
13	2022-08-01 10:03:28.330664677	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64	Echo (ping) reply
14	2022-08-01 10:03:28.330667153	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64	Echo (ping) reply
15	2022-08-01 10:03:29.35493931	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply
16	2022-08-01 10:03:29.354936706	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply
17	2022-08-01 10:03:30.378795204	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64	Echo (ping) reply
18	2022-08-01 10:03:30.378798172	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64	Echo (ping) reply
19	2022-08-01 10:03:31.402772217	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64	Echo (ping) reply
20	2022-08-01 10:03:31.402774775	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64	Echo (ping) reply
21	2022-08-01 10:03:32.426693254	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64	Echo (ping) reply
22	2022-08-01 10:03:32.426695691	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64	Echo (ping) reply

```
> Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
  Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VwWare 9d:e8:be (00:50:56:9d:e8:be)
```

```

VN-Tag
0... .. = Direction: To Bridge
0... .. = Pointer: vif_id
..00 0000 0000 0000 .. = Destination: 0
... .. = Looped: No
... .. = Reserved: 0
... .. = Version: 0
... .. 0000 0000 1010 = Source: 10
Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
000... .. = Priority: Best Effort (default) (0)
...0 .. = DEI: Ineligible
... 0000 0110 0110 = ID: 102
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100
Internet Control Message Protocol
```

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 10:03:22.231237959	198.51.100.100	192.0.2.100	ICMP	108	0x42f8 (17144)	64	Echo (ping) reply
2	2022-08-01 10:03:22.231239747	198.51.100.100	192.0.2.100	ICMP	108	0x42f8 (17144)	64	Echo (ping) reply
3	2022-08-01 10:03:23.232244769	198.51.100.100	192.0.2.100	ICMP	108	0x4303 (17331)	64	Echo (ping) reply
4	2022-08-01 10:03:23.232247753	198.51.100.100	192.0.2.100	ICMP	108	0x43b3 (17331)	64	Echo (ping) reply
5	2022-08-01 10:03:24.234703981	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64	Echo (ping) reply
6	2022-08-01 10:03:24.234706751	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64	Echo (ping) reply
7	2022-08-01 10:03:25.258672449	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64	Echo (ping) reply
8	2022-08-01 10:03:25.258674861	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64	Echo (ping) reply
9	2022-08-01 10:03:26.282663169	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64	Echo (ping) reply
10	2022-08-01 10:03:26.282666183	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64	Echo (ping) reply
11	2022-08-01 10:03:27.306671694	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64	Echo (ping) reply
12	2022-08-01 10:03:27.306674378	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64	Echo (ping) reply
13	2022-08-01 10:03:28.330664677	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64	Echo (ping) reply
14	2022-08-01 10:03:28.330667153	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64	Echo (ping) reply
15	2022-08-01 10:03:29.35493931	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply
16	2022-08-01 10:03:29.354936706	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply
17	2022-08-01 10:03:30.378795204	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64	Echo (ping) reply
18	2022-08-01 10:03:30.378798172	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64	Echo (ping) reply
19	2022-08-01 10:03:31.402772217	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64	Echo (ping) reply
20	2022-08-01 10:03:31.402774775	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64	Echo (ping) reply
21	2022-08-01 10:03:32.426693254	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64	Echo (ping) reply
22	2022-08-01 10:03:32.426695691	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64	Echo (ping) reply

```
> Frame 2: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
  Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VwWare 9d:e8:be (00:50:56:9d:e8:be)
```

```

VN-Tag
0... .. = Direction: To Bridge
0... .. = Pointer: vif_id
..00 0000 0000 0000 .. = Destination: 0
... .. = Looped: No
... .. = Reserved: 0
... .. = Version: 0
... .. 0000 0000 1010 = Source: 10
Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
000... .. = Priority: Best Effort (default) (0)
...0 .. = DEI: Ineligible
... 0000 0110 0110 = ID: 102
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100
Internet Control Message Protocol
```

설명

이 경우 포트 VLAN 태그가 102인 Ethernet1/2는 ICMP 에코 응답 패킷의 이그레스 인터페이스입니다.

애플리케이션 캡처 방향이 캡처 옵션에서 이그레스로 설정된 경우 이더넷 헤더에 포트 VLAN 태그

102가 있는 패킷은 인그레스 방향의 백플레인 인터페이스에서 캡처됩니다.

이 표에서는 작업을 요약합니다.

작업	캡처 지점	캡처된 패킷의 내부 포트 VLAN	방향	캡처된 트래픽
애플리케이션 및 애플리케이션 포트 Ethernet1/2에서 캡처 구성 및 확인	백플레인 인터페이스	102	인그레스 전용	호스트 198.51.100.100에서 호스트 192.0.2.100으로 ICMP 에코 등

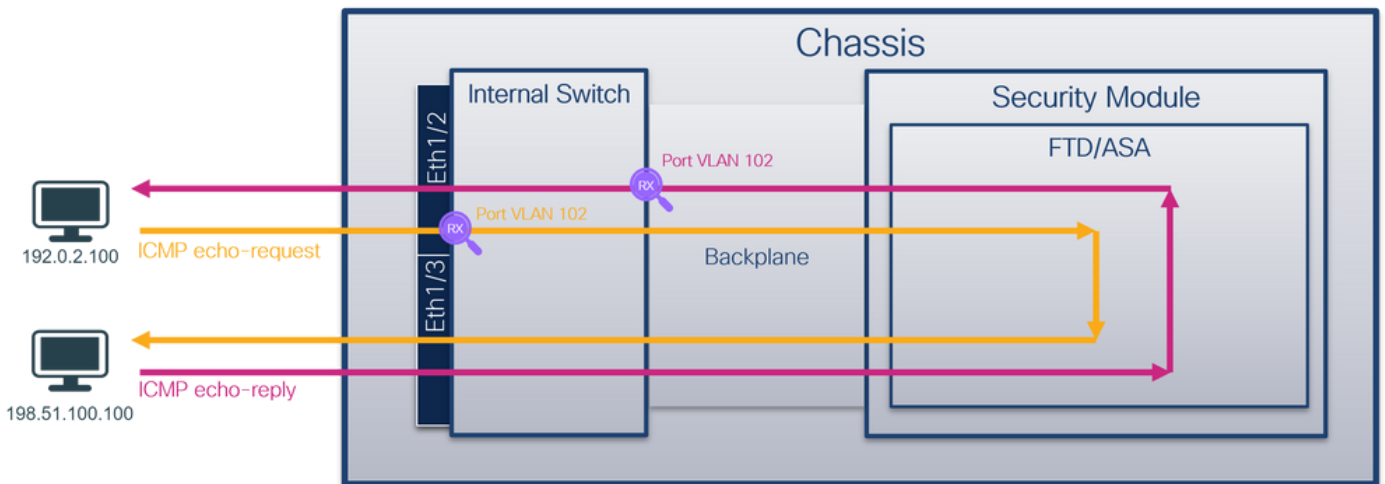
작업 2

FCM 및 CLI를 사용하여 백플레인 인터페이스 및 전면 인터페이스 Ethernet1/2에서 패킷 캡처를 구성하고 확인합니다.

동시 패킷 캡처가 다음 위치에 구성됩니다.

- 전면 인터페이스 - 인터페이스 Ethernet1/2에 포트 VLAN 102가 있는 패킷이 캡처됩니다. 캡처된 패킷은 ICMP 에코 요청입니다.
- 백플레인 인터페이스 - Ethernet1/2가 이그레스 인터페이스로 식별되는 패킷 또는 포트 VLAN 102의 패킷이 캡처됩니다. 캡처된 패킷은 ICMP 에코 응답입니다.

토폴로지, 패킷 흐름 및 캡처 포인트

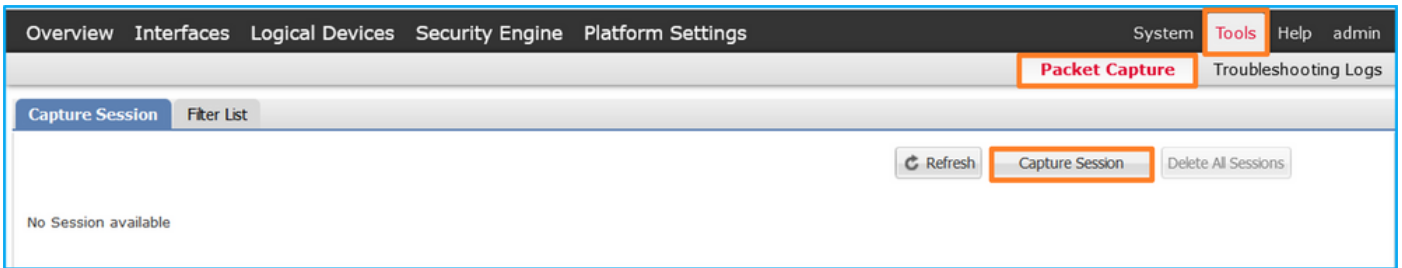


설정

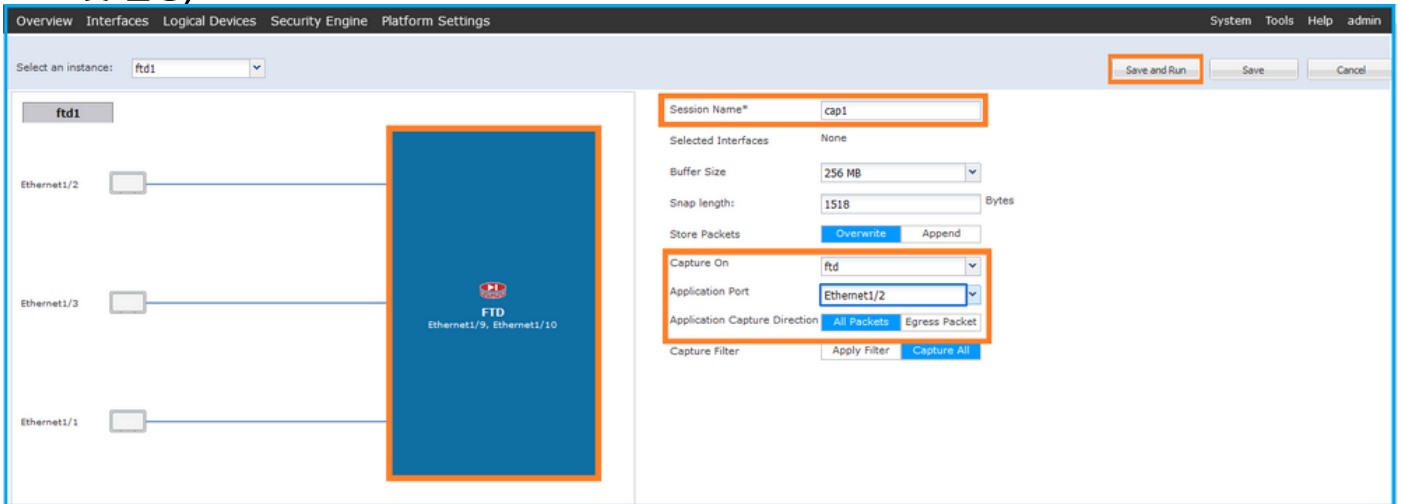
FCM

FCM에서 다음 단계를 수행하여 FTD 애플리케이션 및 애플리케이션 포트 Ethernet1/2에서 패킷 캡처를 구성합니다.

1. Tools(도구) > Packet Capture(패킷 캡처) > Capture Session(캡처 세션)을 사용하여 새 캡처 세션을 생성합니다.



2. Application Port(애플리케이션 포트) 드롭다운 목록에서 FTD 애플리케이션 Ethernet1/2를 선택하고 Application Capture Direction(애플리케이션 캡처 방향)에서 All Packets(모든 패킷)를 선택합니다. 캡처를 활성화하려면 Session Name(세션 이름)을 입력하고 Save and Run(저장 및 실행)을 클릭합니다.



FXOS CLI

백플레인 인터페이스에서 패킷 캡처를 구성하려면 FXOS CLI에서 다음 단계를 수행합니다.

1. 애플리케이션 유형 및 식별자를 식별합니다.

```
firepower# scope ssa
firepower /ssa# show app-instance
App Name  Identifier Slot ID  Admin State Oper State  Running Version Startup Version
Deploy Type Turbo Mode Profile Name Cluster State  Cluster Role
-----
ftd      ftd1      1          Enabled   Online   7.2.0.82   7.2.0.82
Native   No        Not Applicable  None
```

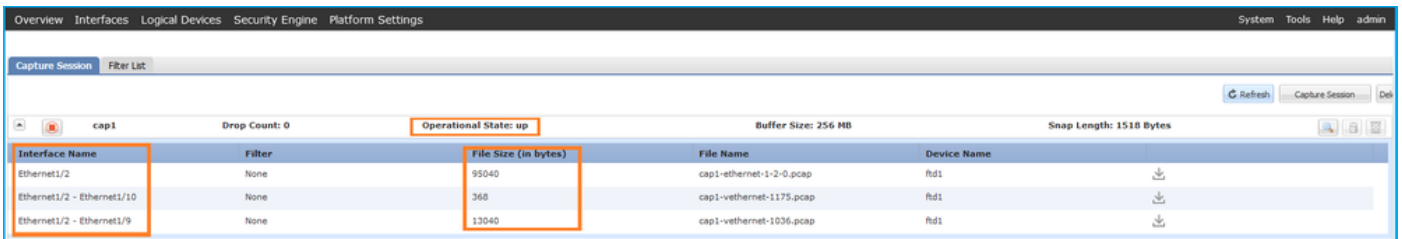
2. 캡처 세션을 생성합니다.

```
firepower# scope packet-capture
firepower /packet-capture # create session cap1
firepower /packet-capture/session* # create phy-port eth1/2
firepower /packet-capture/session/phy-port* # set app-identifier ftd1
firepower /packet-capture/session/phy-port* # exit
firepower /packet-capture/session* # create app-port 1 link12 Ethernet1/2 ftd
firepower /packet-capture/session/app-port* # set app-identifier ftd1
firepower /packet-capture/session* # enable
firepower /packet-capture/session* # commit
firepower /packet-capture/session # commit
```

확인

FCM

인터페이스 이름을 확인하고 작동 상태가 작동 중인지, 파일 크기(바이트)가 증가하는지 확인합니다.



Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/2	None	95040	cap1-ethernet-1-2-0.pcap	ftd1
Ethernet1/2 - Ethernet1/10	None	368	cap1-vethernet-1175.pcap	ftd1
Ethernet1/2 - Ethernet1/9	None	13040	cap1-vethernet-1036.pcap	ftd1

FXOS CLI

scope packet-capture에서 캡처 세부 정보를 확인합니다.

```
firepower# scope packet-capture
firepower /packet-capture # show session cap1
```

Traffic Monitoring Session:

```
Packet Capture Session Name: cap1
Session: 1
Admin State: Enabled
Oper State: Up
Oper State Reason: Active
Config Success: Yes
Config Fail Reason:
Append Flag: Overwrite
Session Mem Usage: 256 MB
Session Pcap Snap Len: 1518 Bytes
Error Code: 0
Drop Count: 0
```

Physical ports involved in Packet Capture:

```
Slot Id: 1
Port Id: 2
Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap
Pcapsize: 410444 bytes
Filter:
Sub Interface: 0
Application Instance Identifier: ftd1
Application Name: ftd
```

Application ports involved in Packet Capture:

```
Slot Id: 1
Link Name: link12
Port Name: Ethernet1/2
App Name: ftd
Sub Interface: 0
Application Instance Identifier: ftd1
```

Application ports resolved to:

```
Name: vnic1
Eq Slot Id: 1
Eq Port Id: 9
Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1036.pcap
Pcapsize: 128400 bytes
Vlan: 102
Filter:
```



```
Name: vnic2
Eq Slot Id: 1
Eq Port Id: 10
Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1175.pcap
Pcapsize: 2656 bytes
Vlan: 102
Filter:
```

캡처 파일 수집

Firepower 4100/9300 내부 스위치 캡처 파일 수집 섹션의 단계를 수행합니다.

캡처 파일 분석

패킷 캡처 파일 리더 애플리케이션을 사용하여 캡처 파일을 엽니다. 여러 백플레인 인터페이스의 경우 각 백플레인 인터페이스의 모든 캡처 파일을 열어야 합니다. 이 경우 패킷은 백플레인 인터페이스 Ethernet1/9에서 캡처됩니다.

인터페이스 Ethernet1/2에 대한 캡처 파일을 열고 첫 번째 패킷을 선택한 다음 핵심 사항을 확인합니다.

1. ICMP 에코 요청 패킷만 캡처됩니다. 각 패킷은 캡처되어 2번 표시됩니다.
2. 원래 패킷 헤더에 VLAN 태그가 없습니다.
3. 내부 스위치는 인그레스 인터페이스 Ethernet1/2를 식별하는 추가 포트 VLAN 태그(102)를 삽입합니다.
4. 내부 스위치는 추가 VN 태그를 삽입합니다.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 11:33:19.070693081	192.0.2.100	198.51.100.100	ICMP	108	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found!)
2	2022-08-01 11:33:19.070695347	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found!)
3	2022-08-01 11:33:19.071217121	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found!)
4	2022-08-01 11:33:19.071218458	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found!)
5	2022-08-01 11:33:20.072036625	192.0.2.100	198.51.100.100	ICMP	108	0xc0ae (49326)	64	Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found!)
6	2022-08-01 11:33:20.072038399	192.0.2.100	198.51.100.100	ICMP	102	0xc0ae (49326)	64	Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found!)
7	2022-08-01 11:33:21.073266030	192.0.2.100	198.51.100.100	ICMP	108	0xc167 (49511)	64	Echo (ping) request id=0x0013, seq=3/768, ttl=64 (no response found!)
8	2022-08-01 11:33:21.073268327	192.0.2.100	198.51.100.100	ICMP	102	0xc167 (49511)	64	Echo (ping) request id=0x0013, seq=3/768, ttl=64 (no response found!)
9	2022-08-01 11:33:22.074576640	192.0.2.100	198.51.100.100	ICMP	108	0xc175 (49525)	64	Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found!)
10	2022-08-01 11:33:22.074578010	192.0.2.100	198.51.100.100	ICMP	102	0xc175 (49525)	64	Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found!)
11	2022-08-01 11:33:23.075779089	192.0.2.100	198.51.100.100	ICMP	108	0xc208 (49672)	64	Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found!)
12	2022-08-01 11:33:23.075781513	192.0.2.100	198.51.100.100	ICMP	102	0xc208 (49672)	64	Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found!)
13	2022-08-01 11:33:24.081839490	192.0.2.100	198.51.100.100	ICMP	108	0xc211 (49681)	64	Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found!)
14	2022-08-01 11:33:24.081841386	192.0.2.100	198.51.100.100	ICMP	102	0xc211 (49681)	64	Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found!)
15	2022-08-01 11:33:25.105806249	192.0.2.100	198.51.100.100	ICMP	108	0xc2e2 (49890)	64	Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found!)
16	2022-08-01 11:33:25.105807895	192.0.2.100	198.51.100.100	ICMP	102	0xc2e2 (49890)	64	Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found!)
17	2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	ICMP	108	0xc3b4 (50100)	64	Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found!)
18	2022-08-01 11:33:26.129838114	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100)	64	Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found!)
19	2022-08-01 11:33:27.153828653	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found!)
20	2022-08-01 11:33:27.153830291	192.0.2.100	198.51.100.100	ICMP	102	0xc476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found!)
21	2022-08-01 11:33:28.177847175	192.0.2.100	198.51.100.100	ICMP	108	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found!)
22	2022-08-01 11:33:28.177849075	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found!)
23	2022-08-01 11:33:29.201804760	192.0.2.100	198.51.100.100	ICMP	108	0xc578 (50552)	64	Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found!)
24	2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	102	0xc578 (50552)	64	Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found!)
25	2022-08-01 11:33:30.225834765	192.0.2.100	198.51.100.100	ICMP	108	0xc585 (50565)	64	Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found!)
26	2022-08-01 11:33:30.225836385	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (50565)	64	Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found!)
27	2022-08-01 11:33:31.249828955	192.0.2.100	198.51.100.100	ICMP	108	0xc618 (50712)	64	Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found!)
28	2022-08-01 11:33:31.249831121	192.0.2.100	198.51.100.100	ICMP	102	0xc618 (50712)	64	Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found!)
29	2022-08-01 11:33:32.273867960	192.0.2.100	198.51.100.100	ICMP	108	0xc64f (50767)	64	Echo (ping) request id=0x0013, seq=14/3584, ttl=64 (no response found!)


```
> Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_1, id 0
> Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)
  VN-Tag
  1. .... = Direction: From Bridge
  .0. .... = Pointer: vif_id
  ..00 0000 0000 1010 .... = Destination: 10
  .... = Looped: No
  .... = Reserved: 0
  .... = Version: 0
  .... 0000 0000 0000 = Source: 0
  Type: 802.1Q Virtual LAN (0x8100)
  802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
  000. .... = Priority: Best Effort (default) (0)
  ...0 .... = DEI: Ineligible
  .... 0000 0110 0110 = ID: 102
  Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
  Internet Control Message Protocol
```

두 번째 패킷을 선택하고 핵심 사항을 확인합니다.

1. ICMP 에코 요청 패킷만 캡처됩니다. 각 패킷은 캡처되어 2번 표시됩니다.
2. 원래 패킷 헤더에 VLAN 태그가 없습니다.
3. 내부 스위치는 인그레스 인터페이스 Ethernet1/2를 식별하는 추가 포트 VLAN 태그(102)를 삽입합니다.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 11:33:19.071512698	198.51.100.100	192.0.2.100	ICMP	108	0x4f27 (20263)	64	Echo (ping) reply id=0x0013, seq=1/256, ttl=64
2	2022-08-01 11:33:19.071514882	198.51.100.100	192.0.2.100	ICMP	108	0x4f27 (20263)	64	Echo (ping) reply id=0x0013, seq=1/256, ttl=64
3	2022-08-01 11:33:20.072677302	198.51.100.100	192.0.2.100	ICMP	108	0x4770 (20475)	64	Echo (ping) reply id=0x0013, seq=2/512, ttl=64
4	2022-08-01 11:33:20.072679384	198.51.100.100	192.0.2.100	ICMP	108	0x4ffb (20475)	64	Echo (ping) reply id=0x0013, seq=2/512, ttl=64
5	2022-08-01 11:33:21.073913640	198.51.100.100	192.0.2.100	ICMP	108	0x50ac (20652)	64	Echo (ping) reply id=0x0013, seq=3/768, ttl=64
6	2022-08-01 11:33:21.073915690	198.51.100.100	192.0.2.100	ICMP	108	0x50ac (20652)	64	Echo (ping) reply id=0x0013, seq=3/768, ttl=64
7	2022-08-01 11:33:22.075239381	198.51.100.100	192.0.2.100	ICMP	108	0x513e (20798)	64	Echo (ping) reply id=0x0013, seq=4/1024, ttl=64
8	2022-08-01 11:33:22.075241491	198.51.100.100	192.0.2.100	ICMP	108	0x513e (20798)	64	Echo (ping) reply id=0x0013, seq=4/1024, ttl=64
9	2022-08-01 11:33:23.076447152	198.51.100.100	192.0.2.100	ICMP	108	0x51c9 (20937)	64	Echo (ping) reply id=0x0013, seq=5/1280, ttl=64
10	2022-08-01 11:33:23.076449303	198.51.100.100	192.0.2.100	ICMP	108	0x51c9 (20937)	64	Echo (ping) reply id=0x0013, seq=5/1280, ttl=64
11	2022-08-01 11:33:24.082407896	198.51.100.100	192.0.2.100	ICMP	108	0x528e (21134)	64	Echo (ping) reply id=0x0013, seq=6/1536, ttl=64
12	2022-08-01 11:33:24.082410099	198.51.100.100	192.0.2.100	ICMP	108	0x528e (21134)	64	Echo (ping) reply id=0x0013, seq=6/1536, ttl=64
13	2022-08-01 11:33:25.106382424	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64	Echo (ping) reply id=0x0013, seq=7/1792, ttl=64
14	2022-08-01 11:33:25.106384549	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64	Echo (ping) reply id=0x0013, seq=7/1792, ttl=64
15	2022-08-01 11:33:26.130437851	198.51.100.100	192.0.2.100	ICMP	108	0x53a6 (21414)	64	Echo (ping) reply id=0x0013, seq=8/2048, ttl=64
16	2022-08-01 11:33:26.130440320	198.51.100.100	192.0.2.100	ICMP	108	0x53a6 (21414)	64	Echo (ping) reply id=0x0013, seq=8/2048, ttl=64
17	2022-08-01 11:33:27.154398212	198.51.100.100	192.0.2.100	ICMP	108	0x5446 (21574)	64	Echo (ping) reply id=0x0013, seq=9/2304, ttl=64
18	2022-08-01 11:33:27.154400198	198.51.100.100	192.0.2.100	ICMP	108	0x5446 (21574)	64	Echo (ping) reply id=0x0013, seq=9/2304, ttl=64
19	2022-08-01 11:33:28.178469866	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64	Echo (ping) reply id=0x0013, seq=10/2560, ttl=64
20	2022-08-01 11:33:28.178471810	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64	Echo (ping) reply id=0x0013, seq=10/2560, ttl=64
21	2022-08-01 11:33:29.202395869	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21740)	64	Echo (ping) reply id=0x0013, seq=11/2816, ttl=64
22	2022-08-01 11:33:29.202398067	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21740)	64	Echo (ping) reply id=0x0013, seq=11/2816, ttl=64
23	2022-08-01 11:33:30.226398735	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64	Echo (ping) reply id=0x0013, seq=12/3072, ttl=64
24	2022-08-01 11:33:30.226401817	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64	Echo (ping) reply id=0x0013, seq=12/3072, ttl=64
25	2022-08-01 11:33:31.250387808	198.51.100.100	192.0.2.100	ICMP	108	0x55f2 (22002)	64	Echo (ping) reply id=0x0013, seq=13/3328, ttl=64
26	2022-08-01 11:33:31.250389971	198.51.100.100	192.0.2.100	ICMP	108	0x55f2 (22002)	64	Echo (ping) reply id=0x0013, seq=13/3328, ttl=64
27	2022-08-01 11:33:32.274416011	198.51.100.100	192.0.2.100	ICMP	108	0x5660 (22112)	64	Echo (ping) reply id=0x0013, seq=14/3584, ttl=64
28	2022-08-01 11:33:32.274418229	198.51.100.100	192.0.2.100	ICMP	108	0x5660 (22112)	64	Echo (ping) reply id=0x0013, seq=14/3584, ttl=64
29	2022-08-01 11:33:33.298397657	198.51.100.100	192.0.2.100	ICMP	108	0x56e7 (22247)	64	Echo (ping) reply id=0x0013, seq=15/3840, ttl=64


```

> Frame 2: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
> Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VMware 9d:e8:be (00:50:56:9d:e8:be)
  0000  00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00  -PV...X...M...&...
  0010  00 0a 81 00 00 66 08 00 45 00 00 54 4f 27 00 00  -.....F...E...TO...
  0020  40 01 3e 86 c6 33 64 64 c0 00 02 64 00 00 95 7c  -@>...3dd...d...|
  0030  00 13 00 01 f2 b9 e7 62 00 00 00 00 cb 7f 06 00  -.....b.....
  0040  00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b  -.....
  0050  1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b  -.....l"*$%&'()*+
  0060  2c 2d 2e 2f 30 31 32 33 34 35 36 37             -./:0123 4567
  
```



```

VN-Tag
0..... = Direction: To Bridge
.0..... = Pointer: vif_id
..00 0000 0000 0000 .. = Destination: 0
.....0..... = Looped: No
.....0..... = Reserved: 0
.....00..... = Version: 0
..... 0000 0000 1010 = Source: 10
Type: 802.1Q Virtual LAN (0x8100)

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
000..... = Priority: Best Effort (default) (0)
..0..... = DEI: Ineligible
....0000 0110 0110 = ID: 102
Type: IPv4 (0x0000)

Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100
Internet Control Message Protocol
  
```

설명

Application Capture Direction의 All Packets 옵션을 선택한 경우 선택한 애플리케이션 포트 Ethernet1/2와 관련된 2개의 동시 패킷 캡처가 구성됩니다. 전면 인터페이스 Ethernet1/2의 캡처 및 선택한 백플레인 인터페이스의 캡처

전면 인터페이스에서 패킷 캡처가 구성된 경우, 스위치는 각 패킷을 동시에 두 번 캡처합니다.

- 포트 VLAN 태그를 삽입한 후
- VN 태그를 삽입한 후

연산 순서에 따라 VN 태그는 포트 VLAN 태그 삽입보다 후반에 삽입됩니다. 그러나 캡처 파일에서 VN 태그가 있는 패킷은 포트 VLAN 태그가 있는 패킷보다 먼저 표시됩니다. 이 예에서 ICMP 에코 요청 패킷의 VLAN 태그(102)는 Ethernet1/2를 인그레스 인터페이스로 식별합니다.

백플레인 인터페이스에서 패킷 캡처가 구성된 경우 스위치는 각 패킷을 동시에 두 번 캡처합니다. 내부 스위치는 보안 모듈의 애플리케이션이 포트 VLAN 태그 및 VN 태그와 함께 이미 태깅한 패킷을 수신합니다. 포트 VLAN 태그는 내부 새시에서 네트워크로 패킷을 전달하는 데 사용하는 이그레스 인터페이스를 식별합니다. 이 예에서 ICMP 에코 응답 패킷의 VLAN 태그 102는 이그레스 인터페이스로 Ethernet1/2를 식별합니다.

내부 스위치는 패킷이 네트워크로 전달되기 전에 VN 태그 및 내부 인터페이스 VLAN 태그를 제거합니다.

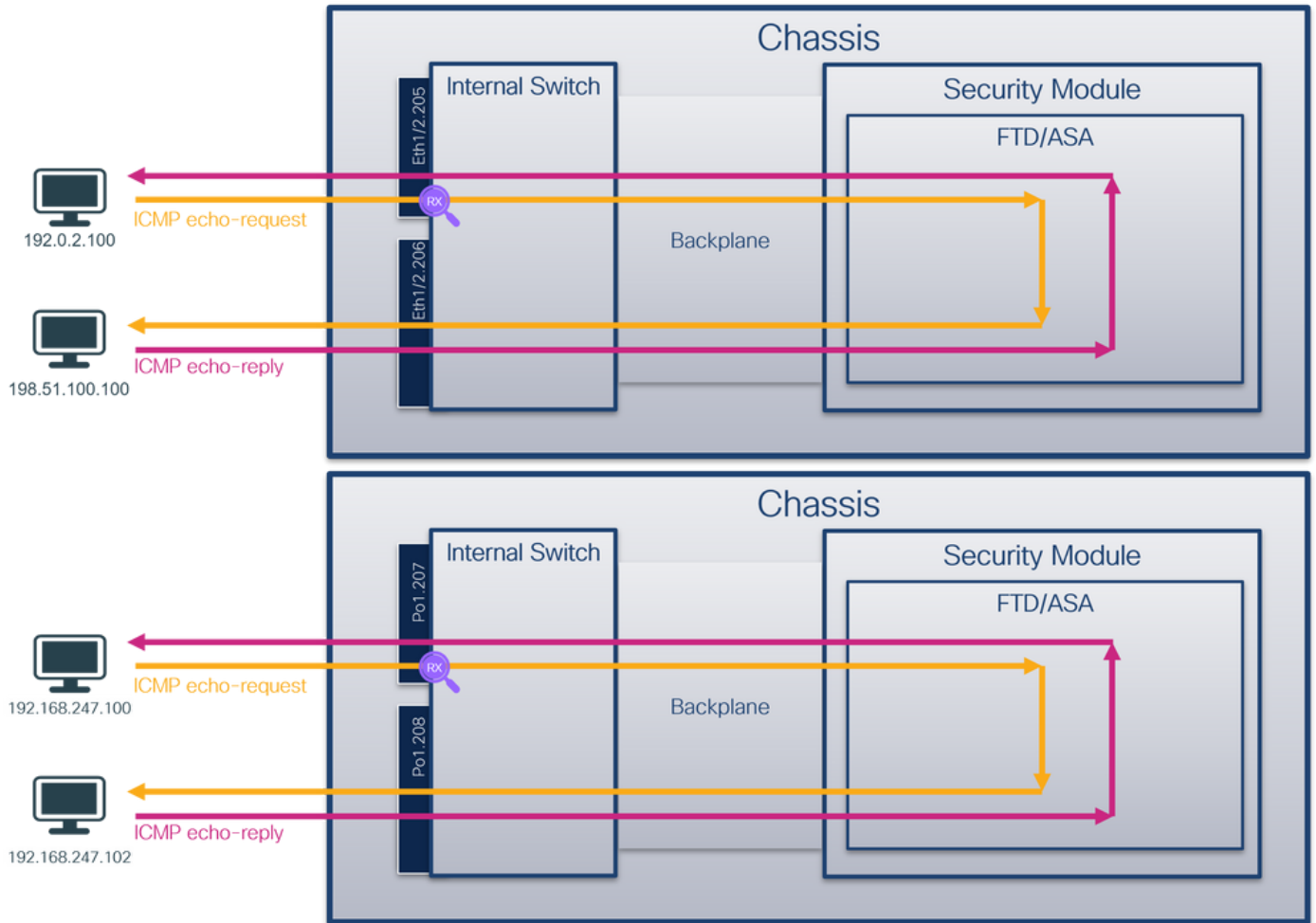
이 표에서는 작업을 요약합니다.

작업	캡처 지점	캡처된 패킷의 내부 포트 VLAN	방향	캡처된 트래픽
애플리케이션 및 애플리케이션 포트 Ethernet1/2에서 캡처 구성 및 확인	백플레인 인터페이스	102	인그레스 전용	호스트 198.51.100.100에서 호스트 192.0.2.100으로 ICMP 에코 요청
	인터페이스 Ethernet1/2	102	인그레스 전용	호스트 192.0.2.100에서 호스트 198.51.100.100으로의 ICMP 에코 응답

물리적 또는 포트 채널 인터페이스의 하위 인터페이스에서 패킷 캡처

FCM 및 CLI를 사용하여 하위 인터페이스 Ethernet1/2.205 또는 포트 채널 하위 인터페이스 Portchannel1.207에서 패킷 캡처를 구성하고 확인합니다. 하위 인터페이스의 하위 인터페이스 및 캡처는 컨테이너 모드의 FTD 애플리케이션에 대해서만 지원됩니다. 이 경우 Ethernet1/2.205 및 Portchannel1.207에서 패킷 캡처가 구성됩니다.

토폴로지, 패킷 흐름 및 캡처 포인트

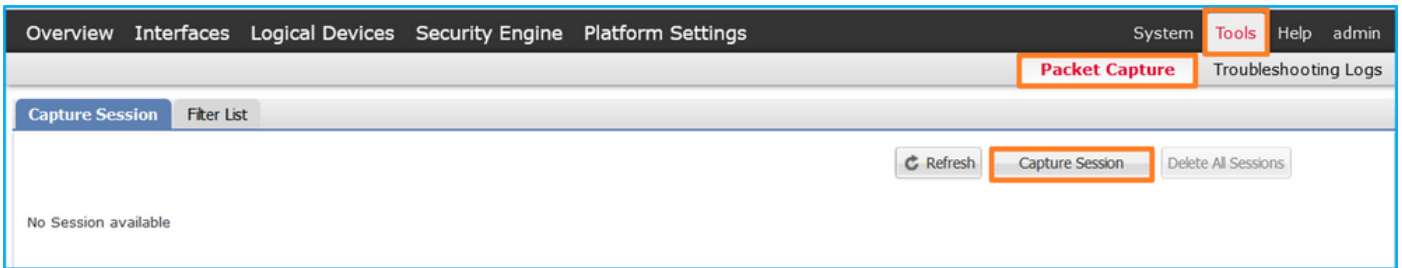


설정

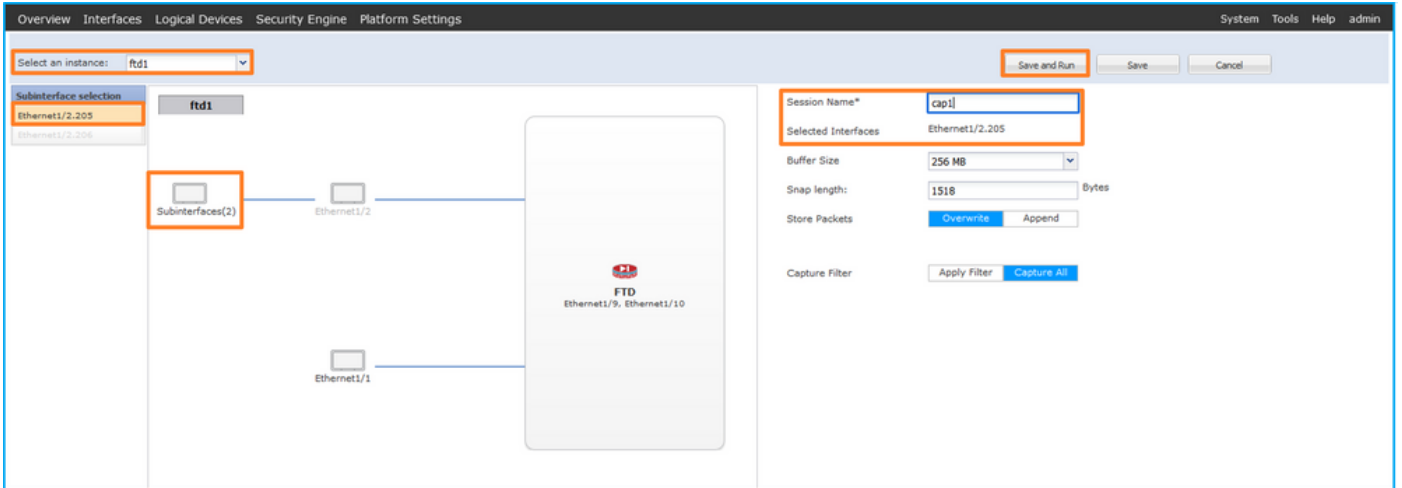
FCM

FCM에서 다음 단계를 수행하여 FTD 애플리케이션 및 애플리케이션 포트 Ethernet1/2에서 패킷 캡처를 구성합니다.

1. Tools(도구) > Packet Capture(패킷 캡처) > Capture Session(캡처 세션)을 사용하여 새 캡처 세션을 생성합니다.



2. 특정 애플리케이션 인스턴스 ftd1, 하위 인터페이스 Ethernet1/2.205를 선택하고 세션 이름을 제공한 다음 **Save and Run**을 클릭하여 캡처를 활성화합니다.



3. 포트 채널 하위 인터페이스의 경우 Cisco 버그 ID 때문에 CSCvq33119 하위 [인터페이스](#)가 FCM에 표시되지 않습니다. FXOS CLI를 사용하여 포트 채널 하위 인터페이스에서 캡처를 구성합니다.

FXOS CLI

하위 인터페이스 Ethernet1/2.205 및 Portchannel1.207에서 패킷 캡처를 구성하려면 FXOS CLI에서 다음 단계를 수행합니다.

1. 애플리케이션 유형 및 식별자를 식별합니다.

```
firepower# scope ssa
firepower /ssa # show app-instance
App Name  Identifier Slot ID   Admin State Oper State      Running Version Startup Version
Deploy Type Turbo Mode Profile Name Cluster State  Cluster Role
-----
ftd       ftd1       1           Enabled   Online         7.2.0.82      7.2.0.82
Container No          RP20        Not Applicable None
ftd       ftd2       1           Enabled   Online         7.2.0.82      7.2.0.82
Container No          RP20        Not Applicable None
```

2. 포트 채널 인터페이스의 경우 멤버 인터페이스를 식별합니다.

```
firepower# connect fxos
<output skipped>
firepower (fxos) # show port-channel summary
Flags: D - Down          P - Up in port-channel (members)
       I - Individual    H - Hot-standby (LACP only)
       s - Suspended     r - Module-removed
       S - Switched      R - Routed
```

U - Up (port-channel)
M - Not in use. Min-links not met

Group	Port-Channel	Type	Protocol	Member	Ports
1	Po1(SU)	Eth	LACP	Eth1/3(P)	Eth1/3(P)

3. 캡처 세션을 생성합니다.

```
firepower# scope packet-capture
firepower /packet-capture # create session cap1
firepower /packet-capture/session* # create phy-port Eth1/2
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # set app-identifier ftd1
firepower /packet-capture/session/phy-port* # set subinterface 205
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # enable
firepower /packet-capture/session* # commit
firepower /packet-capture/session #
```

포트 채널 하위 인터페이스의 경우 각 포트 채널 멤버 인터페이스에 대한 패킷 캡처를 생성합니다.

```
firepower# scope packet-capture
firepower /packet-capture # create filter vlan207
firepower /packet-capture/filter* # set ovlan 207
firepower /packet-capture/filter* # up
firepower /packet-capture* # create session cap1
firepower /packet-capture/session* create phy-port Eth1/3
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # set app-identifier ftd1
firepower /packet-capture/session/phy-port* # set subinterface 207
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # create phy-port Eth1/4
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # set app-identifier ftd1
firepower /packet-capture/session/phy-port* # set subinterface 207
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # enable
firepower /packet-capture/session* # commit
firepower /packet-capture/session #
```

확인

FCM

인터페이스 이름을 확인하고 작동 상태가 작동 중인지, 파일 크기(바이트)가 증가하는지 확인합니다.



FXOS CLI에 구성된 포트 채널 하위 인터페이스 캡처도 FCM에서 볼 수 있습니다. 그러나 다음과 같이 편집할 수는 없습니다.

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/4-207	None	624160	cap1-ethernet-1-4-0.pcap	Not available
Ethernet1/3-207	None	160	cap1-ethernet-1-3-0.pcap	Not available

FXOS CLI

scope packet-capture에서 캡처 세부 정보를 확인합니다.

```
firepower# scope packet-capture
firepower /packet-capture # show session cap1
```

Traffic Monitoring Session:

```
Packet Capture Session Name: cap1
Session: 1
Admin State: Enabled
Oper State: Up
Oper State Reason: Active
Config Success: Yes
Config Fail Reason:
Append Flag: Overwrite
Session Mem Usage: 256 MB
Session Pcap Snap Len: 1518 Bytes
Error Code: 0
Drop Count: 0
```

Physical ports involved in Packet Capture:

```
Slot Id: 1
Port Id: 2
Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap
Pcapsize: 9324 bytes
Filter:
Sub Interface: 205
Application Instance Identifier: ftd1
Application Name: ftd
```

멤버 인터페이스가 Ethernet1/3 및 Ethernet1/4인 포트 채널 1:

```
firepower# scope packet-capture
firepower /packet-capture # show session cap1
```

Traffic Monitoring Session:

```
Packet Capture Session Name: cap1
Session: 1
Admin State: Enabled
Oper State: Up
Oper State Reason: Active
Config Success: Yes
Config Fail Reason:
Append Flag: Overwrite
Session Mem Usage: 256 MB
Session Pcap Snap Len: 1518 Bytes
Error Code: 0
Drop Count: 0
```

Physical ports involved in Packet Capture:

```
Slot Id: 1
```

```

Port Id: 3
Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-3-0.pcap
Pcapsize: 160 bytes
Filter:
Sub Interface: 207
Application Instance Identifier: ftd1
Application Name: ftd
Slot Id: 1
Port Id: 4
Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-4-0.pcap
Pcapsize: 624160 bytes
Filter:
Sub Interface: 207
Application Instance Identifier: ftd1
Application Name: ftd

```

캡처 파일 수집

Firepower 4100/9300 내부 스위치 캡처 파일 수집 섹션의 단계를 수행합니다.

캡처 파일 분석

패킷 캡처 파일 리더 애플리케이션을 사용하여 캡처 파일을 엽니다. 첫 번째 패킷을 선택하고 핵심 사항을 확인합니다.

1. ICMP 에코 요청 패킷만 캡처됩니다. 각 패킷은 캡처되어 2번 표시됩니다.
2. 원래 패킷 헤더에는 VLAN 태그 205가 있습니다.
3. 내부 스위치는 인그레스 인터페이스 Ethernet1/2를 식별하는 추가 포트 VLAN 태그(102)를 삽입합니다.
4. 내부 스위치는 추가 VN 태그를 삽입합니다.

The screenshot displays a network packet capture analysis tool. The top section shows a list of 27 packets, all ICMP Echo requests. The first packet is highlighted, and its details are shown in the bottom section. The details include a VN-Tag with three sub-interfaces (802.1Q Virtual LAN) and an Internet Protocol Version 4 header. The sub-interfaces are labeled with IDs 102, 205, and 205. The IP header shows the source IP as 192.0.2.100 and the destination IP as 198.51.100.10.

두 번째 패킷을 선택하고 핵심 사항을 확인합니다.

1. ICMP 에코 요청 패킷만 캡처됩니다. 각 패킷은 캡처되어 2번 표시됩니다.
2. 원래 패킷 헤더에는 VLAN 태그 205가 있습니다.

Wireshark packet capture showing ICMP Echo requests. The packet list pane highlights the first packet (ID 1) and the packet details pane shows the protocol structure. The packet bytes pane displays the raw data.

이제 Portchannel1.207에 대한 캡처 파일을 엽니다. 첫 번째 패킷을 선택하고 핵심 사항을 확인합니다

1. ICMP 에코 요청 패킷만 캡처됩니다. 각 패킷은 캡처되어 2번 표시됩니다.
2. 원래 패킷 헤더에는 VLAN 태그 207이 있습니다.
3. 내부 스위치는 인그레스 인터페이스 Portchannel1을 식별하는 추가 포트 VLAN 태그 1001을 삽입합니다.
4. 내부 스위치는 추가 VN 태그를 삽입합니다.

Wireshark packet capture showing ICMP Echo requests. The packet list pane highlights the first packet (ID 1) and the packet details pane shows the protocol structure. The packet bytes pane displays the raw data.

두 번째 패킷을 선택하고 핵심 사항을 확인합니다.

1. ICMP 에코 요청 패킷만 캡처됩니다. 각 패킷은 캡처되어 2번 표시됩니다.
2. 원래 패킷 헤더에는 VLAN 태그 207이 있습니다.

설명

전면 인터페이스에서 패킷 캡처가 구성된 경우, 스위치는 각 패킷을 동시에 두 번 캡처합니다.

- 포트 VLAN 태그를 삽입한 후
- VN 태그를 삽입한 후

연산 순서에 따라 VN 태그는 포트 VLAN 태그 삽입보다 후반에 삽입됩니다. 그러나 캡처 파일에서 VN 태그가 있는 패킷은 포트 VLAN 태그가 있는 패킷보다 먼저 표시됩니다. 또한 하위 인터페이스의 경우 캡처 파일에서 모든 초 패킷은 포트 VLAN 태그를 포함하지 않습니다.

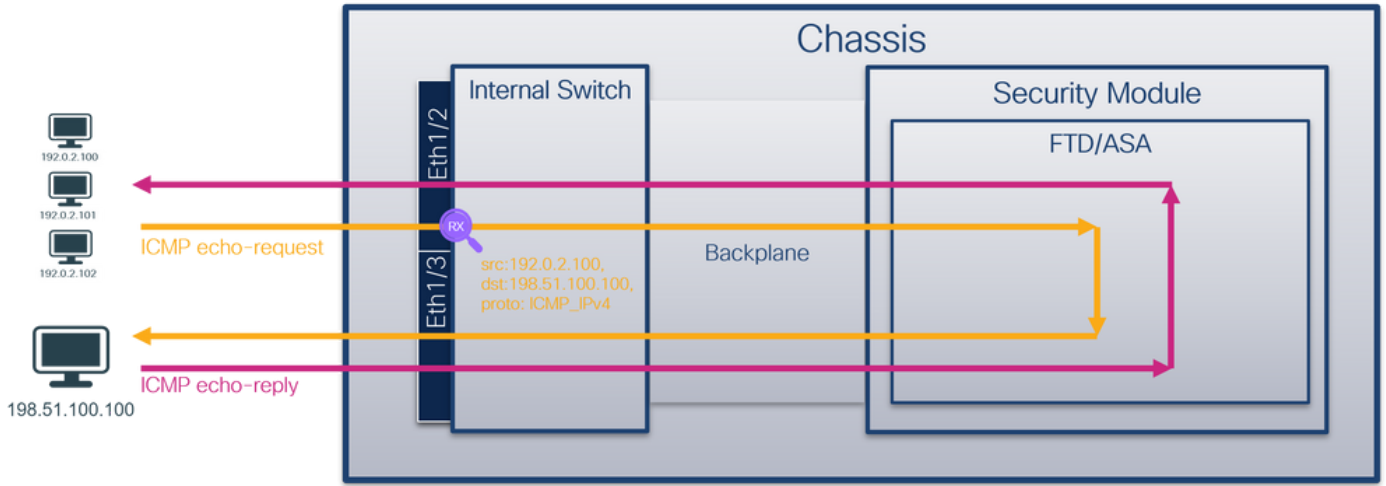
이 표에서는 작업을 요약합니다.

작업	캡처 지점	캡처된 패킷의 내부 포트 VLAN	방향	캡처된 트래픽
하위 인터페이스 Ethernet1/2.205에서 패킷 캡처 구성 및 확인	이더넷 1/2.205	102	인그레스 전용	호스트 192.0.2.100에서 호스트 198.51.100.100으로의 ICMP 에코 요청
멤버 인터페이스 Ethernet1/3 및 Ethernet1/4를 사용하여 Portchannel1 하위 인터페이스에서 패킷 캡처 구성 및 확인	이더넷1/3 이더넷1/4	1001	인그레스 전용	192.168.207.100에서 호스트 192.168.207.102로의 ICMP 에코 요청

패킷 캡처 필터

FCM 및 CLI를 사용하여 Ethernet1/2 인터페이스에서 필터를 사용하여 패킷 캡처를 구성하고 확인합니다.

토폴로지, 패킷 흐름 및 캡처 포인트

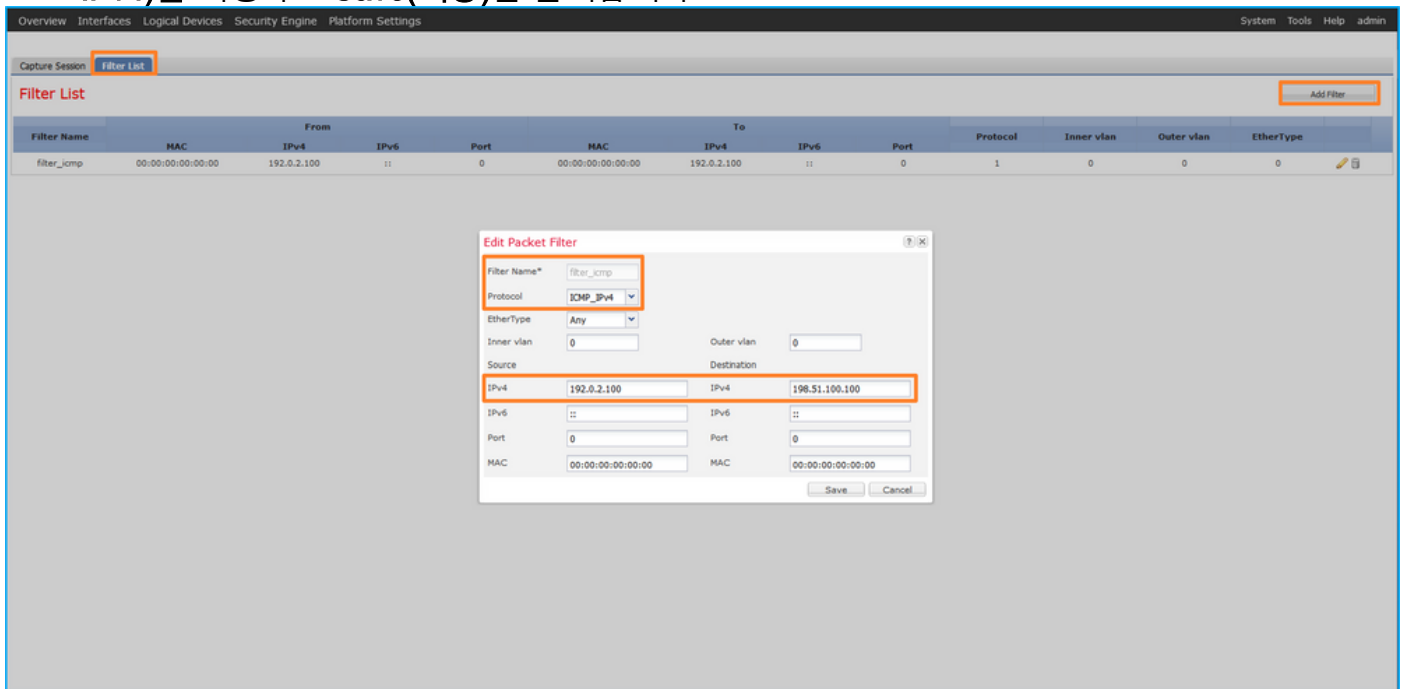


설정

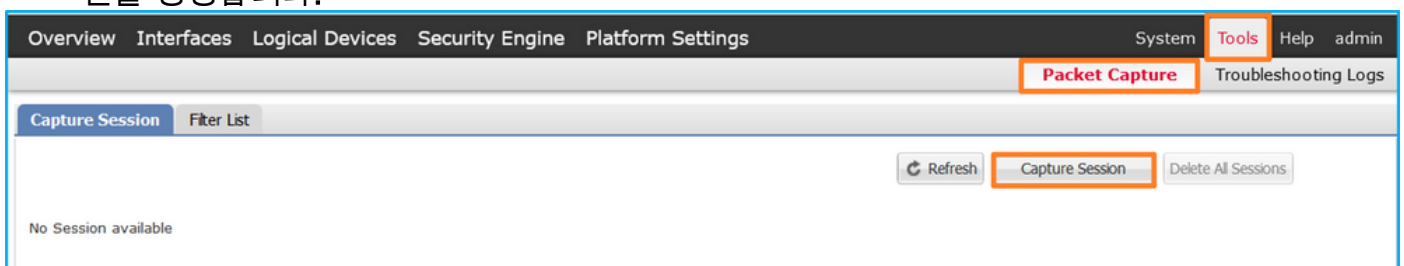
FCM

FCM에서 다음 단계를 수행하여 호스트 192.0.2.100에서 호스트 198.51.100.100으로의 ICMP 에코 요청 패킷에 대한 캡처 필터를 구성하고 이를 인터페이스 Ethernet1/2의 패킷 캡처에 적용합니다.

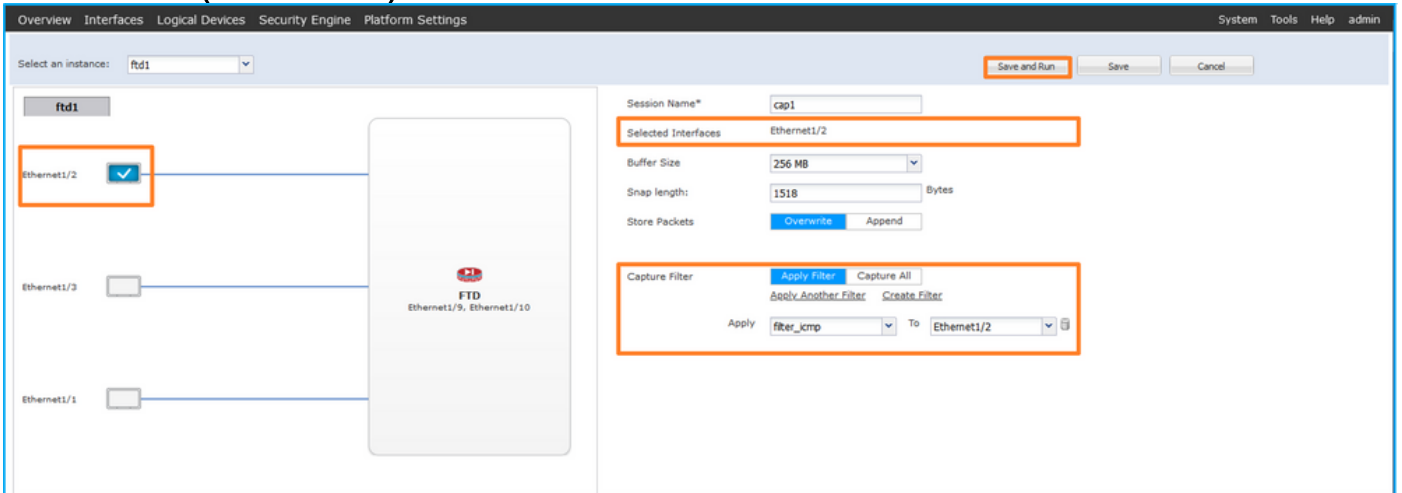
1. Tools > Packet Capture > Filter List > Add Filter를 사용하여 캡처 필터를 생성합니다.
2. Filter Name(필터 이름), Protocol(프로토콜), Source IPv4(소스 IPv4), Destination IPv4(대상 IPv4)를 지정하고 Save(저장)를 클릭합니다.



3. Tools(도구) > Packet Capture(패킷 캡처) > Capture Session(캡처 세션)을 사용하여 새 캡처 세션을 생성합니다.



4. Ethernet1/2를 선택하고 **Session Name(세션 이름)**을 입력한 다음 캡처 필터를 적용하고 **Save and Run(저장 및 실행)**을 클릭하여 캡처를 활성화합니다.



FXOS CLI

백플레인 인터페이스에서 패킷 캡처를 구성하려면 FXOS CLI에서 다음 단계를 수행합니다.

1. 애플리케이션 유형 및 식별자를 식별합니다.

```
firepower# scope ssa
firepower /ssa# show app-instance
```

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version
ftd	ftd1	1	Enabled	Online	7.2.0.82	7.2.0.82

2. <https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>에서 IP 프로토콜 번호를 **확인**합니다. 이 경우 ICMP 프로토콜 번호는 1입니다.

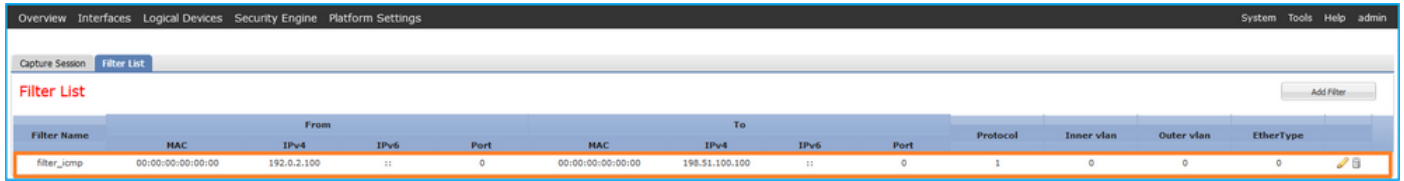
3. 캡처 세션을 생성합니다.

```
2.
firepower# scope packet-capture
firepower /packet-capture # create filter filter_icmp
firepower /packet-capture/filter* # set destip 198.51.100.100
firepower /packet-capture/filter* # set protocol 1
firepower /packet-capture/filter* # set srcip 192.0.2.100
firepower /packet-capture/filter* # exit
firepower /packet-capture* # create session cap1
firepower /packet-capture/session* # create phy-port Ethernet1/2
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # set app-identifier ftd1
firepower /packet-capture/session/phy-port* # set filter filter_icmp
firepower /packet-capture/session/phy-port* # exit
firepower /packet-capture/session* # enable
firepower /packet-capture/session* # commit
firepower /packet-capture/session #
```

확인

FCM

인터페이스 이름을 확인하고 작동 상태가 작동 중인지, 파일 크기(바이트)가 증가하는지 확인합니다.



인터페이스 이름, 필터, 작동 상태를 확인하고 파일 크기(바이트)가 증가하는지 확인합니다. Tools(툴) > Packet Capture(패킷 캡처) > Capture Session(캡처 세션)에서 확인할 수 있습니다.



FXOS CLI

scope packet-capture에서 캡처 세부 정보를 확인합니다.

```
firepower# scope packet-capture
firepower /packet-capture # show filter detail
```

Configure a filter for packet capture:

```
Name: filter_icmp
Protocol: 1
Ivlan: 0
Ovlan: 0
Src Ip: 192.0.2.100
Dest Ip: 198.51.100.100
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0
Src Ipv6: ::
Dest Ipv6: ::
```

```
firepower /packet-capture # show session cap1
```

Traffic Monitoring Session:

```
Packet Capture Session Name: cap1
Session: 1
Admin State: Enabled
Oper State: Up
Oper State Reason: Active
Config Success: Yes
Config Fail Reason:
Append Flag: Overwrite
Session Mem Usage: 256 MB
Session Pcap Snap Len: 1518 Bytes
Error Code: 0
Drop Count: 0
```

Physical ports involved in Packet Capture:

```
Slot Id: 1
Port Id: 2
Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap
```

Pcapsize: 213784 bytes
 Filter: filter_icmp
 Sub Interface: 0
 Application Instance Identifier: ftd1
 Application Name: ftd

캡처 파일 수집

Firepower 4100/9300 내부 스위치 캡처 파일 수집 섹션의 단계를 수행합니다.

캡처 파일 분석

패킷 캡처 파일 리더 애플리케이션을 사용하여 캡처 파일을 엽니다. 첫 번째 패킷을 선택하고 핵심 사항을 확인합니다.

1. ICMP 에코 요청 패킷만 캡처됩니다. 각 패킷은 캡처되어 2번 표시됩니다.
2. 원래 패킷 헤더에 VLAN 태그가 없습니다.
3. 내부 스위치는 인그레스 인터페이스 Ethernet1/2를 식별하는 추가 포트 VLAN 태그(102)를 삽입합니다.
4. 내부 스위치는 추가 VN 태그를 삽입합니다.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-02 15:46:55.603277760	192.0.2.100	198.51.100.100	ICMP	108	0x0012 (18)	64	Echo (ping) request id=0x0018, seq=349/23809, ttl=64 (no r
2	2022-08-02 15:46:55.603279688	192.0.2.100	198.51.100.100	ICMP	102	0x0012 (18)	64	Echo (ping) request id=0x0018, seq=349/23809, ttl=64 (no r
3	2022-08-02 15:46:56.627139252	192.0.2.100	198.51.100.100	ICMP	108	0x00db (219)	64	Echo (ping) request id=0x0018, seq=350/24065, ttl=64 (no r
4	2022-08-02 15:46:56.627140919	192.0.2.100	198.51.100.100	ICMP	102	0x00db (219)	64	Echo (ping) request id=0x0018, seq=350/24065, ttl=64 (no r
5	2022-08-02 15:46:57.651185193	192.0.2.100	198.51.100.100	ICMP	108	0x01cb (459)	64	Echo (ping) request id=0x0018, seq=351/24321, ttl=64 (no r
6	2022-08-02 15:46:57.651186787	192.0.2.100	198.51.100.100	ICMP	102	0x01cb (459)	64	Echo (ping) request id=0x0018, seq=351/24321, ttl=64 (no r
7	2022-08-02 15:46:58.675153317	192.0.2.100	198.51.100.100	ICMP	108	0x01d6 (470)	64	Echo (ping) request id=0x0018, seq=352/24577, ttl=64 (no r
8	2022-08-02 15:46:58.675154503	192.0.2.100	198.51.100.100	ICMP	102	0x01d6 (470)	64	Echo (ping) request id=0x0018, seq=352/24577, ttl=64 (no r
9	2022-08-02 15:46:59.699152639	192.0.2.100	198.51.100.100	ICMP	108	0x01f4 (500)	64	Echo (ping) request id=0x0018, seq=353/24833, ttl=64 (no r
10	2022-08-02 15:46:59.699153835	192.0.2.100	198.51.100.100	ICMP	102	0x01f4 (500)	64	Echo (ping) request id=0x0018, seq=353/24833, ttl=64 (no r
11	2022-08-02 15:47:00.723142641	192.0.2.100	198.51.100.100	ICMP	108	0x01f9 (505)	64	Echo (ping) request id=0x0018, seq=354/25089, ttl=64 (no r
12	2022-08-02 15:47:00.723144643	192.0.2.100	198.51.100.100	ICMP	102	0x01f9 (505)	64	Echo (ping) request id=0x0018, seq=354/25089, ttl=64 (no r
13	2022-08-02 15:47:01.747162204	192.0.2.100	198.51.100.100	ICMP	108	0x026e (622)	64	Echo (ping) request id=0x0018, seq=355/25345, ttl=64 (no r
14	2022-08-02 15:47:01.747163783	192.0.2.100	198.51.100.100	ICMP	102	0x026e (622)	64	Echo (ping) request id=0x0018, seq=355/25345, ttl=64 (no r
15	2022-08-02 15:47:02.771209952	192.0.2.100	198.51.100.100	ICMP	108	0x02bc (700)	64	Echo (ping) request id=0x0018, seq=356/25601, ttl=64 (no r
16	2022-08-02 15:47:02.771211062	192.0.2.100	198.51.100.100	ICMP	102	0x02bc (700)	64	Echo (ping) request id=0x0018, seq=356/25601, ttl=64 (no r
17	2022-08-02 15:47:03.772258550	192.0.2.100	198.51.100.100	ICMP	108	0x032f (815)	64	Echo (ping) request id=0x0018, seq=357/25857, ttl=64 (no r
18	2022-08-02 15:47:03.772259724	192.0.2.100	198.51.100.100	ICMP	102	0x032f (815)	64	Echo (ping) request id=0x0018, seq=357/25857, ttl=64 (no r
19	2022-08-02 15:47:04.791118519	192.0.2.100	198.51.100.100	ICMP	108	0x040f (1039)	64	Echo (ping) request id=0x0018, seq=358/26113, ttl=64 (no r
20	2022-08-02 15:47:04.791119721	192.0.2.100	198.51.100.100	ICMP	102	0x040f (1039)	64	Echo (ping) request id=0x0018, seq=358/26113, ttl=64 (no r


```

> Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_1, i
> Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)
  VN-Tag
  1... .. = Direction: From Bridge
  .0. .... = Pointer: vif_id
  ..00 0000 0000 1010 .. = Destination: 10
  .... .. = Looped: No
  .... .. = Reserved: 0
  .... .. = Version: 0
  .... .. = Source: 0
  Type: 802.1Q Virtual LAN (0x8100)
  802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
  000. .... = Priority: Best Effort (default) (0)
  ...0 .... = DEI: Ineligible
  ... 0000 0110 0110 = ID: 102
  Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
  Internet Control Message Protocol
  
```

두 번째 패킷을 선택하고 핵심 사항을 확인합니다.

1. ICMP 에코 요청 패킷만 캡처됩니다. 각 패킷은 캡처되어 2번 표시됩니다.
2. 원래 패킷 헤더에 VLAN 태그가 없습니다.
3. 내부 스위치는 인그레스 인터페이스 Ethernet1/2를 식별하는 추가 포트 VLAN 태그(102)를 삽입합니다.

No.	Time	Source	Destination	Protocol	Length	IP ID	TTL	Info
1	2022-08-02 15:46:55.60327760	192.0.2.100	198.51.100.100	ICMP	108	0x0012 (18)	64	Echo (ping) request id=0x0018, seq=349/23809, ttl=64 (no r
2	2022-08-02 15:46:55.603279688	192.0.2.100	198.51.100.100	ICMP	102	0x0012 (18)	64	Echo (ping) request id=0x0018, seq=349/23809, ttl=64 (no r
3	2022-08-02 15:46:56.627139252	192.0.2.100	198.51.100.100	ICMP	108	0x00db (219)	64	Echo (ping) request id=0x0018, seq=350/24065, ttl=64 (no r
4	2022-08-02 15:46:56.627140919	192.0.2.100	198.51.100.100	ICMP	102	0x00db (219)	64	Echo (ping) request id=0x0018, seq=350/24065, ttl=64 (no r
5	2022-08-02 15:46:57.651185193	192.0.2.100	198.51.100.100	ICMP	108	0x01cb (459)	64	Echo (ping) request id=0x0018, seq=351/24321, ttl=64 (no r
6	2022-08-02 15:46:57.651186787	192.0.2.100	198.51.100.100	ICMP	102	0x01cb (459)	64	Echo (ping) request id=0x0018, seq=351/24321, ttl=64 (no r
7	2022-08-02 15:46:58.675153317	192.0.2.100	198.51.100.100	ICMP	108	0x01d6 (470)	64	Echo (ping) request id=0x0018, seq=352/24577, ttl=64 (no r
8	2022-08-02 15:46:58.675154503	192.0.2.100	198.51.100.100	ICMP	102	0x01d6 (470)	64	Echo (ping) request id=0x0018, seq=352/24577, ttl=64 (no r
9	2022-08-02 15:46:59.699152639	192.0.2.100	198.51.100.100	ICMP	108	0x01f4 (500)	64	Echo (ping) request id=0x0018, seq=353/24833, ttl=64 (no r
10	2022-08-02 15:46:59.699153835	192.0.2.100	198.51.100.100	ICMP	102	0x01f4 (500)	64	Echo (ping) request id=0x0018, seq=353/24833, ttl=64 (no r
11	2022-08-02 15:47:00.723142641	192.0.2.100	198.51.100.100	ICMP	108	0x01f9 (505)	64	Echo (ping) request id=0x0018, seq=354/25089, ttl=64 (no r
12	2022-08-02 15:47:00.723144643	192.0.2.100	198.51.100.100	ICMP	102	0x01f9 (505)	64	Echo (ping) request id=0x0018, seq=354/25089, ttl=64 (no r
13	2022-08-02 15:47:01.747162204	192.0.2.100	198.51.100.100	ICMP	108	0x026e (622)	64	Echo (ping) request id=0x0018, seq=355/25345, ttl=64 (no r
14	2022-08-02 15:47:01.747163783	192.0.2.100	198.51.100.100	ICMP	102	0x026e (622)	64	Echo (ping) request id=0x0018, seq=355/25345, ttl=64 (no r
15	2022-08-02 15:47:02.771209952	192.0.2.100	198.51.100.100	ICMP	108	0x02bc (700)	64	Echo (ping) request id=0x0018, seq=356/25601, ttl=64 (no r
16	2022-08-02 15:47:02.771211062	192.0.2.100	198.51.100.100	ICMP	102	0x02bc (700)	64	Echo (ping) request id=0x0018, seq=356/25601, ttl=64 (no r
17	2022-08-02 15:47:03.772258550	192.0.2.100	198.51.100.100	ICMP	108	0x032f (815)	64	Echo (ping) request id=0x0018, seq=357/25857, ttl=64 (no r
18	2022-08-02 15:47:03.772259724	192.0.2.100	198.51.100.100	ICMP	102	0x032f (815)	64	Echo (ping) request id=0x0018, seq=357/25857, ttl=64 (no r
19	2022-08-02 15:47:04.791118519	192.0.2.100	198.51.100.100	ICMP	108	0x040f (1039)	64	Echo (ping) request id=0x0018, seq=358/26113, ttl=64 (no r
20	2022-08-02 15:47:04.791119721	192.0.2.100	198.51.100.100	ICMP	102	0x040f (1039)	64	Echo (ping) request id=0x0018, seq=358/26113, ttl=64 (no r

> Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture_u0_1, i		0000 58 97 bd b9 77 0e 00 50 56 9d e8 be 81 00 00 66 X...w..P.V.....f
> Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)		0010 08 00 45 00 00 54 00 12 40 00 40 01 4d 9b c0 00 ..E..T...@.M...
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102		0020 02 64 c6 33 64 64 08 00 9e 67 00 18 01 5d e2 46 .d.3dd...g...J.F
> 000. = Priority: Best Effort (default) (0)		0030 e9 62 00 00 00 c1 a6 0c 00 00 00 00 10 11 b:.....
> ...0 = DEI: Ineligible		0040 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 !
> 0000 0110 0110 = ID: 102		0050 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 *%\$%&'()*+,-./01
> Type: IPv4 (0x0800)		0060 32 33 34 35 36 37 234567
> Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100		
> Internet Control Message Protocol		

설명

전면 인터페이스에서 패킷 캡처가 구성된 경우, 스위치는 각 패킷을 동시에 두 번 캡처합니다.

- 포트 VLAN 태그를 삽입한 후
- VN 태그를 삽입한 후

연산 순서에 따라 VN 태그는 포트 VLAN 태그 삽입보다 후반에 삽입됩니다. 그러나 캡처 파일에서 VN 태그가 있는 패킷은 포트 VLAN 태그가 있는 패킷보다 먼저 표시됩니다.

캡처 필터를 적용하면 인그레스 방향의 필터와 일치하는 패킷만 캡처됩니다.

이 표에서는 작업을 요약합니다.

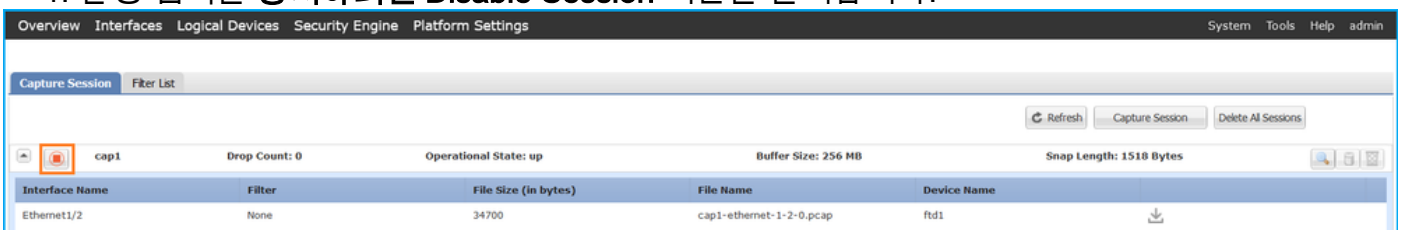
작업	캡처 지점	캡처된 패킷의 내부 포트 VLAN	방향	사용자 필터	캡처된 트래픽
전면 인터페이스 Ethernet1/2에서 필터를 사용하여 패킷 캡처 구성 및 확인	이더넷 1/2	102	인그레스 전용	프로토콜: ICMP 출처: 192.0.2.100 대상: 198.51.100.100	호스트 192.0.2.100에서 호스트 198.51.100.100으로의 ICMP 코 요청

Firepower 4100/9300 내부 스위치 캡처 파일 수집

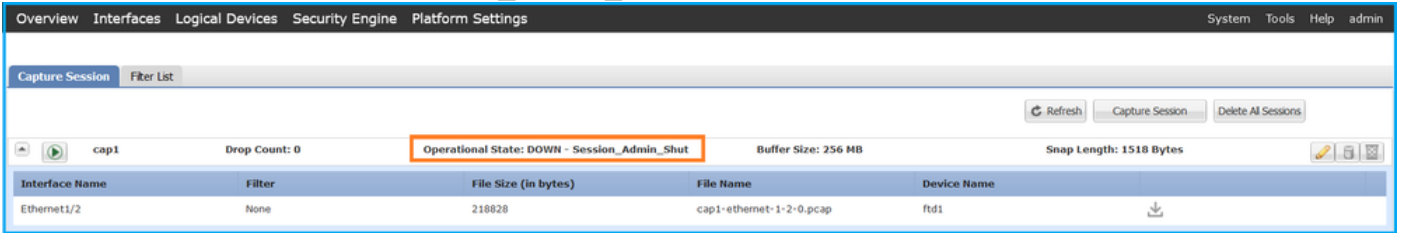
FCM

FCM에서 다음 단계를 수행하여 내부 스위치 캡처 파일을 수집합니다.

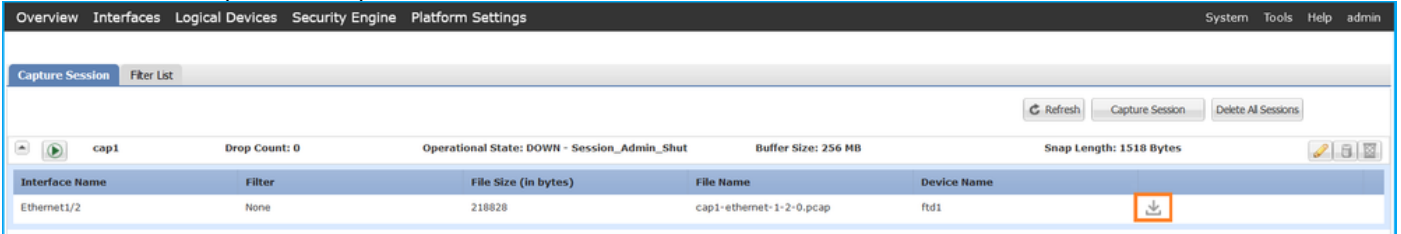
1. 활성 캡처를 중지하려면 **Disable Session** 버튼을 클릭합니다.



2. 작동 상태가 DOWN - Session_Admin_Shut:



3. Download(다운로드)를 클릭하여 캡처 파일을 다운로드합니다.



포트 채널 인터페이스의 경우 각 멤버 인터페이스에 대해 이 단계를 반복합니다.

FXOS CLI

캡처 파일을 수집하려면 FXOS CLI에서 다음 단계를 수행합니다.

1. 활성 캡처를 중지합니다.

```
firepower# scope packet-capture
firepower /packet-capture # scope session cap1
firepower /packet-capture/session # disable
firepower /packet-capture/session* # commit
firepower /packet-capture/session # up
firepower /packet-capture # show session cap1 detail
```

Traffic Monitoring Session:

```
Packet Capture Session Name: cap1
Session: 1
  Admin State: Disabled
  Oper State: Down
  Oper State Reason: Admin Disable
Config Success: Yes
Config Fail Reason:
Append Flag: Overwrite
Session Mem Usage: 256 MB
Session Pcap Snap Len: 1518 Bytes
Error Code: 0
Drop Count: 0
```

Physical ports involved in Packet Capture:

```
Slot Id: 1
Port Id: 2
Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap
Pcapsize: 115744 bytes
Filter:
Sub Interface: 0
Application Instance Identifier: ftd1
Application Name: ftd
```

2. local-mgmt 명령 범위에서 캡처 파일을 업로드합니다.


```
firepower# connect local-mgmt
firepower(local-mgmt)# copy /packet-capture/session-1/cap1-ethernet-1-2-0.pcap ?
ftp:          Dest File URI
http:         Dest File URI
https:        Dest File URI
scp:          Dest File URI
sftp:         Dest File URI
tftp:         Dest File URI
usbdrive:     Dest File URI
volatile:     Dest File URI
workspace:    Dest File URI
```

```
firepower(local-mgmt)# copy /packet-capture/session-1/cap1-ethernet-1-2-0.pcap
ftp://ftpuser@10.10.10.1/cap1-ethernet-1-2-0.pcap
```

Password:

포트 채널 인터페이스의 경우 각 멤버 인터페이스의 캡처 파일을 복사합니다.

지침, 제한 및 모범 사례 내부 스위치 패킷 캡처

Firepower 4100/9300 내부 스위치 캡처와 관련된 지침 및 제한 사항에 대해서는 *Cisco Firepower 4100/9300 FXOS Chassis Manager 컨피그레이션 가이드* 또는 *Cisco Firepower 4100/9300 FXOS CLI 컨피그레이션 가이드*, [문제 해결 장](#), [패킷 캡처 섹션](#)을 참조하십시오.

다음은 TAC 사례에서 패킷 캡처 사용을 기반으로 한 모범 사례 목록입니다.

- 지침 및 제한 사항에 유의하십시오.
- 모든 포트 채널 멤버 인터페이스에서 패킷을 캡처하고 모든 캡처 파일을 분석합니다.
- 캡처 필터를 사용합니다.
- 캡처 필터가 구성된 경우 NAT가 패킷 IP 주소에 미치는 영향을 고려하십시오.
- 기본값인 1518바이트와 다를 경우 프레임 크기를 지정하는 스냅 길이를 늘리거나 줄입니다. 크기가 작으면 캡처된 패킷의 수가 증가하고, 그 반대의 경우도 마찬가지입니다.
- 필요에 따라 버퍼 크기를 조정합니다.
- FCM 또는 FXOS CLI의 삭제 수를 확인합니다. 버퍼 크기 제한에 도달하면 드롭 카운트 카운터가 증가합니다.
- Wireshark의 !vntag 필터를 사용하여 VN-tag 없이 패킷만 표시합니다. 이는 전면 인터페이스 패킷 캡처 파일에서 VN 태그가 지정된 패킷을 숨기는 데 유용합니다.
- Wireshark에서 frame.number&1 필터를 사용하여 홀수 프레임만 표시합니다. 이는 백플레인 인터페이스 패킷 캡처 파일에서 중복 패킷을 숨기는 데 유용합니다.
- TCP와 같은 프로토콜의 경우 Wireshark는 기본적으로 특정 조건의 패킷을 다른 색으로 표시하는 색상화 규칙을 적용합니다. 캡처 파일의 중복 패킷으로 인해 내부 스위치 캡처가 발생하는 경우 패킷이 오탐으로 채색되고 표시될 수 있습니다. 패킷 캡처 파일을 분석하고 필터를 적용하는 경우 표시된 패킷을 새 파일로 내보내고 대신 새 파일을 엽니다.

구성 및 확인 보안 방화벽 3100

Firepower 4100/9300과 달리 Secure Firewall 3100의 내부 스위치는 `capture <name> switch` 명령을 통해 애플리케이션 명령줄 인터페이스에 구성되며, 여기서 `switch` 옵션은 캡처가 내부 스위치에 구성되도록 지정합니다.

다음은 `switch` 옵션을 사용하는 `capture` 명령입니다.

> **capture cap_sw switch ?**

```
buffer          Configure size of capture buffer, default is 256MB
ethernet-type   Capture Ethernet packets of a particular type, default is IP
interface       Capture packets on a specific interface
ivlan           Inner Vlan
match           Capture packets based on match criteria
ovlan           Outer Vlan
packet-length   Configure maximum length to save from each packet, default is
64 bytes
real-time       Display captured packets in real-time. Warning: using this
option with a slow console connection may result in an
excessive amount of non-displayed packets due to performance
limitations.
stop            Stop packet capture
trace           Trace the captured packets
type            Capture packets based on a particular type
<cr>
```

패킷 캡처 컨피그레이션의 일반적인 단계는 다음과 같습니다.

1. 인그레스 인터페이스를 지정합니다.

스위치 캡처 컨피그레이션은 인그레스 인터페이스 nameif를 수락합니다. 사용자는 데이터 인터페이스 이름, 내부 업링크 또는 관리 인터페이스를 지정할 수 있습니다.

> **capture capsw switch interface ?**

Available interfaces to listen:

```
in_data_uplink1  Capture packets on internal data uplink1 interface
in_mgmt_uplink1  Capture packets on internal mgmt uplink1 interface
inside           Name of interface Ethernet1/1.205

management       Name of interface Management1/1
```

2. 이더넷 프레임 EtherType을 지정합니다. 기본 이더 유형은 IP입니다. ethernet-type 옵션 값은 EtherType을 지정합니다.

> **capture capsw switch interface inside ethernet-type ?**

```
802.1Q
<0-65535>  Ethernet type
arp
ip
ip6
pppoed
pppoes
rarp
sgt
vlan
```

3. 일치 조건을 지정합니다. capture match 옵션은 일치 기준을 지정합니다.

> **capture capsw switch interface inside match ?**

```
<0-255>  Enter protocol number (0 - 255)
ah
eigrp
esp
gre
icmp
icmp6
igmp
igrp
ip
```

```
ipinip
ipsec
mac      Mac-address filter
nos
ospf
pcp
pim
pptp
sctp
snp
spi      SPI value
tcp
udp
<cr>
```

4. 버퍼 크기, 패킷 길이 등과 같은 기타 선택적 매개변수를 지정합니다.
5. 캡처를 활성화합니다. `no capture <name> switch stop` 명령은 캡처를 활성화합니다.

```
> capture capsw switch interface inside match ip
>no capture capsw switch stop
```

6. 캡처 세부사항을 확인합니다.

- 관리 상태가 **활성화**되었고, 작동 상태는 **작동** 및 **활성**입니다.
- 패킷 캡처 파일 크기 Pcapsize가 증가합니다.
- `show capture <cap_name>` 출력의 캡처된 패킷 수는 0이 아닙니다.
- 캡처 경로 **Pcapfile**. 캡처된 패킷은 자동으로 `/mnt/disk0/packet-capture/` 폴더에 저장됩니다.
- 조건을 캡처합니다. 소프트웨어는 캡처 조건에 따라 캡처 필터를 자동으로 생성합니다.

```
> show capture capsw
27 packet captured on disk using switch capture
Reading of capture file from disk is not supported
```

```
>show capture capsw detail
```

Packet Capture info

```
  Name:          capsw
Session:         1
  Admin State:   enabled
  Oper State:    up
Oper State Reason: Active
Config Success:  yes
Config Fail Reason:
Append Flag:     overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code:      0
Drop Count:      0
```

Total Physical ports involved in Packet Capture: 1

Physical port:

```
Slot Id:        1
Port Id:        1
Pcapfile:       /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize:       18838
Filter:         capsw-1-1
```

Packet Capture Filter Info

```
  Name:          capsw-1-1
Protocol:       0
Ivlan:         0
```

Ovlan: 205
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0
0 packet captured on disk using switch capture
Reading of capture file from disk is not supported

7. 필요한 경우 캡처를 중지합니다.

```
> capture capsw switch stop
```

```
>show capture capsw detail
```

Packet Capture info

Name: capsw
Session: 1
Admin State: disabled
Oper State: down
Oper State Reason: Session_Admin_Shut
Config Success: yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1
Port Id: 1
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize: 24
Filter: capsw-1-1

Packet Capture Filter Info

Name: capsw-1-1
Protocol: 0
Ivlan: 0
Ovlan: 205
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0
0 packet captured on disk using switch capture
Reading of capture file from disk is not supported

8. 캡처 파일을 수집합니다. **Collect Secure Firewall 3100 Internal Switch Capture Files** 섹션의 단계를 수행합니다.

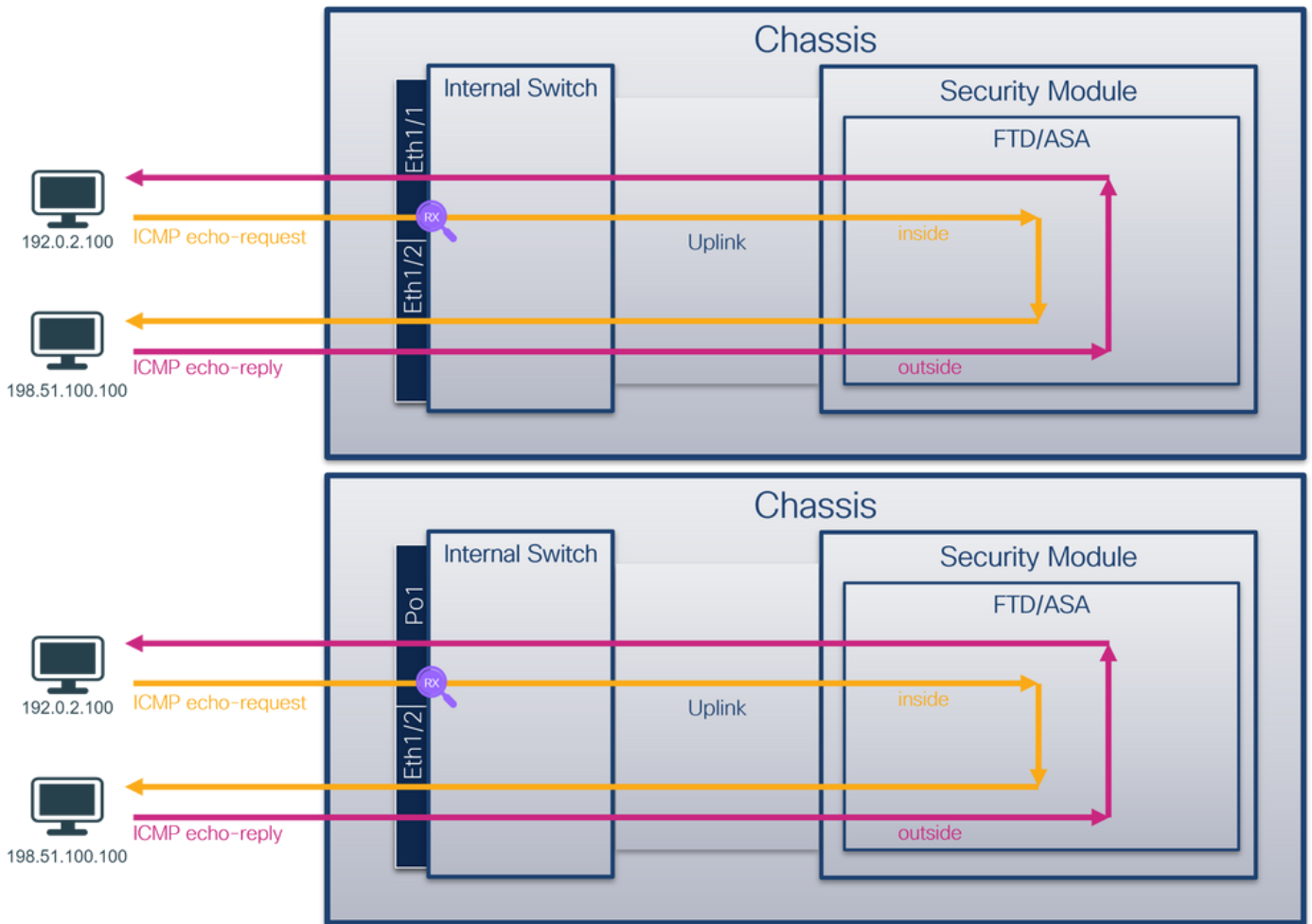
버전 7.2에서는 내부 스위치 캡처 컨피그레이션이 FMC 또는 FDM에서 지원되지 않습니다. ASA 소프트웨어 버전 9.18(1) 이상의 경우 ASDM 버전 7.18.1.x 이상에서 내부 스위치 캡처를 구성할 수 있습니다.

이러한 시나리오에서는 Secure Firewall 3100 내부 스위치 캡처의 일반적인 활용 사례를 다룹니다.

물리적 또는 포트 채널 인터페이스의 패킷 캡처

FTD 또는 ASA CLI를 사용하여 인터페이스 Ethernet1/1 또는 Portchannel1 인터페이스에서 패킷 캡처를 구성하고 확인합니다. 두 인터페이스 모두 nameif 내부에 있습니다.

토폴로지, 패킷 흐름 및 캡처 포인트



설정

ASA 또는 FTD CLI에서 다음 단계를 수행하여 인터페이스 Ethernet1/1 또는 Port-channel1에서 패킷 캡처를 구성합니다.

1. nameif 확인:

```
> show nameif
Interface          Name          Security
Ethernet1/1       inside       0
Ethernet1/2       outside      0
Management1/1    diagnostic  0
```

> **show nameif**

Interface	Name	Security
Port-channel1	inside	0
Ethernet1/2	outside	0
Management1/1	diagnostic	0

2. 캡처 세션을 생성합니다.

> **capture capsw switch interface inside**

3. 캡처 세션을 활성화합니다.

> **no capture capsw switch stop**

확인

캡처 세션 이름, 관리 및 운영 상태, 인터페이스 슬롯 및 식별자를 확인합니다. Pcapsize 값(바이트)이 증가하고 캡처된 패킷 수가 0이 아닌지 확인합니다.

> **show capture capsw detail**

Packet Capture info

Name: capsw
Session: 1
Admin State: enabled
Oper State: up
Oper State Reason: Active
Config Success: yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1
Port Id: 1
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize: 12653
Filter: capsw-1-1

Packet Capture Filter Info

Name: capsw-1-1
Protocol: 0
Ivlan: 0
Ovlan: 0
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

79 packets captured on disk using switch capture

Reading of capture file from disk is not supported

Port-channel1의 경우 모든 멤버 인터페이스에 캡처가 구성됩니다.

> **show capture capsw detail**

Packet Capture info

Name: capsw
Session: 1
Admin State: enabled
Oper State: up
Oper State Reason: Active
Config Success: yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0

Total Physical ports involved in Packet Capture: 2

Physical port:

Slot Id: 1
Port Id: 4
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-4-0.pcap
Pcapsize: 28824
Filter: capsw-1-4

Packet Capture Filter Info

Name: capsw-1-4
Protocol: 0
Ivlan: 0
Ovlan: 0
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Physical port:

Slot Id: 1
Port Id: 3
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-3-0.pcap
Pcapsize: 18399
Filter: capsw-1-3

Packet Capture Filter Info

Name: capsw-1-3
Protocol: 0
Ivlan: 0
Ovlan: 0
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0

Dest Port: 0
Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

56 packet captured on disk using switch capture

Reading of capture file from disk is not supported

포트 채널 멤버 인터페이스는 FXOS local-mgmt 명령 셸에서 **show portchannel summary** 명령을 통해 확인할 수 있습니다.

> **connect fxos**

...

KSEC-FPR3100-1 **connect local-mgmt**

KSEC-FPR3100-1(local-mgmt) **show portchannel summary**

Flags: D - Down P - Up in port-channel (members)

I - Individual H - Hot-standby (LACP only)

s - Suspended r - Module-removed

S - Switched R - Routed

U - Up (port-channel)

M - Not in use. Min-links not met

```
-----  
Group Port-      Type      Protocol  Member Ports  
Channel  
-----  
1      Po1(U)      Eth       LACP      Eth1/3(P)  Eth1/4(P)
```

LACP KeepAlive Timer:

```
-----  
Channel  PeerKeepAliveTimerFast  
-----
```

```
1      Po1(U)      False
```

Cluster LACP Status:

```
-----  
Channel  ClusterSpanned  ClusterDetach  ClusterUnitID  ClusterSysID  
-----
```

```
1      Po1(U)      False          False          0              clust
```

ASA에서 FXOS에 액세스하려면 **connect fxos admin** 명령을 실행합니다. 다중 컨텍스트의 경우 관리 컨텍스트에서 명령을 실행합니다.

캡처 파일 수집

Collect Secure Firewall 3100 Internal Switch Capture Files 섹션의 단계를 수행합니다.

캡처 파일 분석

패킷 캡처 파일 판독기 응용 프로그램을 사용하여 Ethernet1/1에 대한 캡처 파일을 엽니다. 첫 번째 패킷을 선택하고 핵심 사항을 확인합니다.

1. ICMP 에코 요청 패킷만 캡처됩니다.
2. 원래 패킷 헤더에 VLAN 태그가 없습니다.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-07 19:50:06.925768	192.0.2.100	198.51.100.100	ICMP	102	0x9a10 (39440)	64	Echo (ping) request id=0x0034, seq=1/256, ttl=64 (no res
2	2022-08-07 19:50:07.921684	192.0.2.100	198.51.100.100	ICMP	102	0x9a3a (39482)	64	Echo (ping) request id=0x0034, seq=2/512, ttl=64 (no res
3	2022-08-07 19:50:08.924468	192.0.2.100	198.51.100.100	ICMP	102	0x9aa6 (39590)	64	Echo (ping) request id=0x0034, seq=3/768, ttl=64 (no res
4	2022-08-07 19:50:09.928484	192.0.2.100	198.51.100.100	ICMP	102	0x9afe (39678)	64	Echo (ping) request id=0x0034, seq=4/1024, ttl=64 (no res
5	2022-08-07 19:50:10.928245	192.0.2.100	198.51.100.100	ICMP	102	0x9b10 (39696)	64	Echo (ping) request id=0x0034, seq=5/1280, ttl=64 (no res
6	2022-08-07 19:50:11.9329144	192.0.2.100	198.51.100.100	ICMP	102	0x9b34 (39732)	64	Echo (ping) request id=0x0034, seq=6/1536, ttl=64 (no res
7	2022-08-07 19:50:12.934153	192.0.2.100	198.51.100.100	ICMP	102	0x9b83 (39811)	64	Echo (ping) request id=0x0034, seq=7/1792, ttl=64 (no res
8	2022-08-07 19:50:13.934155	192.0.2.100	198.51.100.100	ICMP	102	0x9b8b (39819)	64	Echo (ping) request id=0x0034, seq=8/2048, ttl=64 (no res
9	2022-08-07 19:50:14.932804	192.0.2.100	198.51.100.100	ICMP	102	0x9c07 (39943)	64	Echo (ping) request id=0x0034, seq=9/2304, ttl=64 (no res
10	2022-08-07 19:50:15.937143	192.0.2.100	198.51.100.100	ICMP	102	0x9cc6 (40134)	64	Echo (ping) request id=0x0034, seq=10/2560, ttl=64 (no res
11	2022-08-07 19:50:16.934848	192.0.2.100	198.51.100.100	ICMP	102	0x9d68 (40296)	64	Echo (ping) request id=0x0034, seq=11/2816, ttl=64 (no res
12	2022-08-07 19:50:17.936908	192.0.2.100	198.51.100.100	ICMP	102	0x9ded (40429)	64	Echo (ping) request id=0x0034, seq=12/3072, ttl=64 (no res
13	2022-08-07 19:50:18.939584	192.0.2.100	198.51.100.100	ICMP	102	0x9e5a (40538)	64	Echo (ping) request id=0x0034, seq=13/3328, ttl=64 (no res
14	2022-08-07 19:50:19.941262	192.0.2.100	198.51.100.100	ICMP	102	0x9efb (40699)	64	Echo (ping) request id=0x0034, seq=14/3584, ttl=64 (no res
15	2022-08-07 19:50:20.940716	192.0.2.100	198.51.100.100	ICMP	102	0x9f50 (40784)	64	Echo (ping) request id=0x0034, seq=15/3840, ttl=64 (no res
16	2022-08-07 19:50:21.940288	192.0.2.100	198.51.100.100	ICMP	102	0x9fe4 (40923)	64	Echo (ping) request id=0x0034, seq=16/4096, ttl=64 (no res
17	2022-08-07 19:50:22.943302	192.0.2.100	198.51.100.100	ICMP	102	0xa031 (41009)	64	Echo (ping) request id=0x0034, seq=17/4352, ttl=64 (no res
18	2022-08-07 19:50:23.944679	192.0.2.100	198.51.100.100	ICMP	102	0xa067 (41063)	64	Echo (ping) request id=0x0034, seq=18/4608, ttl=64 (no res

Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)		0000	bc e7 12 34 9a 14 00 50 56 9d e8 be 08 00 45 00	...	4...P V...E
Ethernet II, Src: VMware_9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco_34:9a:14 (bc:e7:12:34:9a:14)		0010	00 54 9a 10 40 00 40 01 b3 9c c0 00 64 c6 33	..T..@..d-3	
Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100		0020	64 64 08 00 c6 91 00 34 00 01 61 17 f0 62 00 00	dd...4...a-b-	
Internet Control Message Protocol		0030	00 00 18 ec 08 00 00 00 00 00 10 11 12 13 14 15	
		0040	16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25!	%\$
		0050	26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35	&'()*+,-./012345	
		0060	36 37 55 55 55 55	67UUUU	

Portchannel1 멤버 인터페이스에 대한 캡처 파일을 엽니다. 첫 번째 패킷을 선택하고 핵심 사항을 확인합니다.

1. ICMP 에코 요청 패킷만 캡처됩니다.
2. 원래 패킷 헤더에 VLAN 태그가 없습니다.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-07 20:40:58.657533	192.0.2.100	198.51.100.100	ICMP	102	0x9296 (37526)	64	Echo (ping) request id=0x0035, seq=1/256, ttl=64 (no res
2	2022-08-07 20:40:59.658611	192.0.2.100	198.51.100.100	ICMP	102	0x9370 (37744)	64	Echo (ping) request id=0x0035, seq=2/512, ttl=64 (no res
3	2022-08-07 20:41:00.655662	192.0.2.100	198.51.100.100	ICMP	102	0x93f0 (37872)	64	Echo (ping) request id=0x0035, seq=3/768, ttl=64 (no res
4	2022-08-07 20:41:01.659749	192.0.2.100	198.51.100.100	ICMP	102	0x946f (37999)	64	Echo (ping) request id=0x0035, seq=4/1024, ttl=64 (no res
5	2022-08-07 20:41:02.660624	192.0.2.100	198.51.100.100	ICMP	102	0x94a4 (38052)	64	Echo (ping) request id=0x0035, seq=5/1280, ttl=64 (no res
6	2022-08-07 20:41:03.663226	192.0.2.100	198.51.100.100	ICMP	102	0x952d (38189)	64	Echo (ping) request id=0x0035, seq=6/1536, ttl=64 (no res
7	2022-08-07 20:41:04.661262	192.0.2.100	198.51.100.100	ICMP	102	0x958d (38285)	64	Echo (ping) request id=0x0035, seq=7/1792, ttl=64 (no res
8	2022-08-07 20:41:05.665955	192.0.2.100	198.51.100.100	ICMP	102	0x95d8 (38360)	64	Echo (ping) request id=0x0035, seq=8/2048, ttl=64 (no res
9	2022-08-07 20:41:06.666538	192.0.2.100	198.51.100.100	ICMP	102	0x964b (38475)	64	Echo (ping) request id=0x0035, seq=9/2304, ttl=64 (no res
10	2022-08-07 20:41:07.667298	192.0.2.100	198.51.100.100	ICMP	102	0x972b (38699)	64	Echo (ping) request id=0x0035, seq=10/2560, ttl=64 (no res
11	2022-08-07 20:41:08.670540	192.0.2.100	198.51.100.100	ICMP	102	0x980a (38922)	64	Echo (ping) request id=0x0035, seq=11/2816, ttl=64 (no res
12	2022-08-07 20:41:09.668278	192.0.2.100	198.51.100.100	ICMP	102	0x9831 (38961)	64	Echo (ping) request id=0x0035, seq=12/3072, ttl=64 (no res
13	2022-08-07 20:41:10.672417	192.0.2.100	198.51.100.100	ICMP	102	0x98a2 (39074)	64	Echo (ping) request id=0x0035, seq=13/3328, ttl=64 (no res
14	2022-08-07 20:41:11.671369	192.0.2.100	198.51.100.100	ICMP	102	0x98f7 (39159)	64	Echo (ping) request id=0x0035, seq=14/3584, ttl=64 (no res
15	2022-08-07 20:41:12.675462	192.0.2.100	198.51.100.100	ICMP	102	0x99e4 (39396)	64	Echo (ping) request id=0x0035, seq=15/3840, ttl=64 (no res
16	2022-08-07 20:41:13.674993	192.0.2.100	198.51.100.100	ICMP	102	0x9a84 (39556)	64	Echo (ping) request id=0x0035, seq=16/4096, ttl=64 (no res
17	2022-08-07 20:41:14.674093	192.0.2.100	198.51.100.100	ICMP	102	0x9af3 (39667)	64	Echo (ping) request id=0x0035, seq=17/4352, ttl=64 (no res
18	2022-08-07 20:41:15.676904	192.0.2.100	198.51.100.100	ICMP	102	0x9b8e (39822)	64	Echo (ping) request id=0x0035, seq=18/4608, ttl=64 (no res

Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)		0000	bc e7 12 34 9a 2c 00 50 56 9d e8 be 08 00 45 00	...	4...P V...E
Ethernet II, Src: VMware_9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco_34:9a:2c (bc:e7:12:34:9a:2c)		0010	00 54 92 96 40 00 40 01 bb 16 c0 00 64 c6 33	..T..@..d-3	
Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100		0020	64 64 08 00 58 a8 00 35 00 01 4d 23 f0 62 00 00	dd...X...5...MH b-	
Internet Control Message Protocol		0030	00 00 0e c8 04 00 00 00 00 00 10 11 12 13 14 15	
		0040	16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25!	%\$
		0050	26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35	&'()*+,-./012345	
		0060	36 37 55 55 55 55	67UUUU	

설명

스위치 캡처는 Ethernet1/1 또는 Portchannel1 인터페이스에 구성됩니다.

이 표에서는 작업을 요약합니다.

작업

인터페이스 Ethernet1/1에서 패킷 캡처 구성 및 확인
 멤버 인터페이스 Ethernet1/3 및 Ethernet1/4를 사용하여 인터페이스 Portchannel1에서 패킷 캡처 구성 및 확인

캡처 지점
 이더넷1/1
 이더넷1/3
 이더넷1/4

내부 필터
 없음
 없음

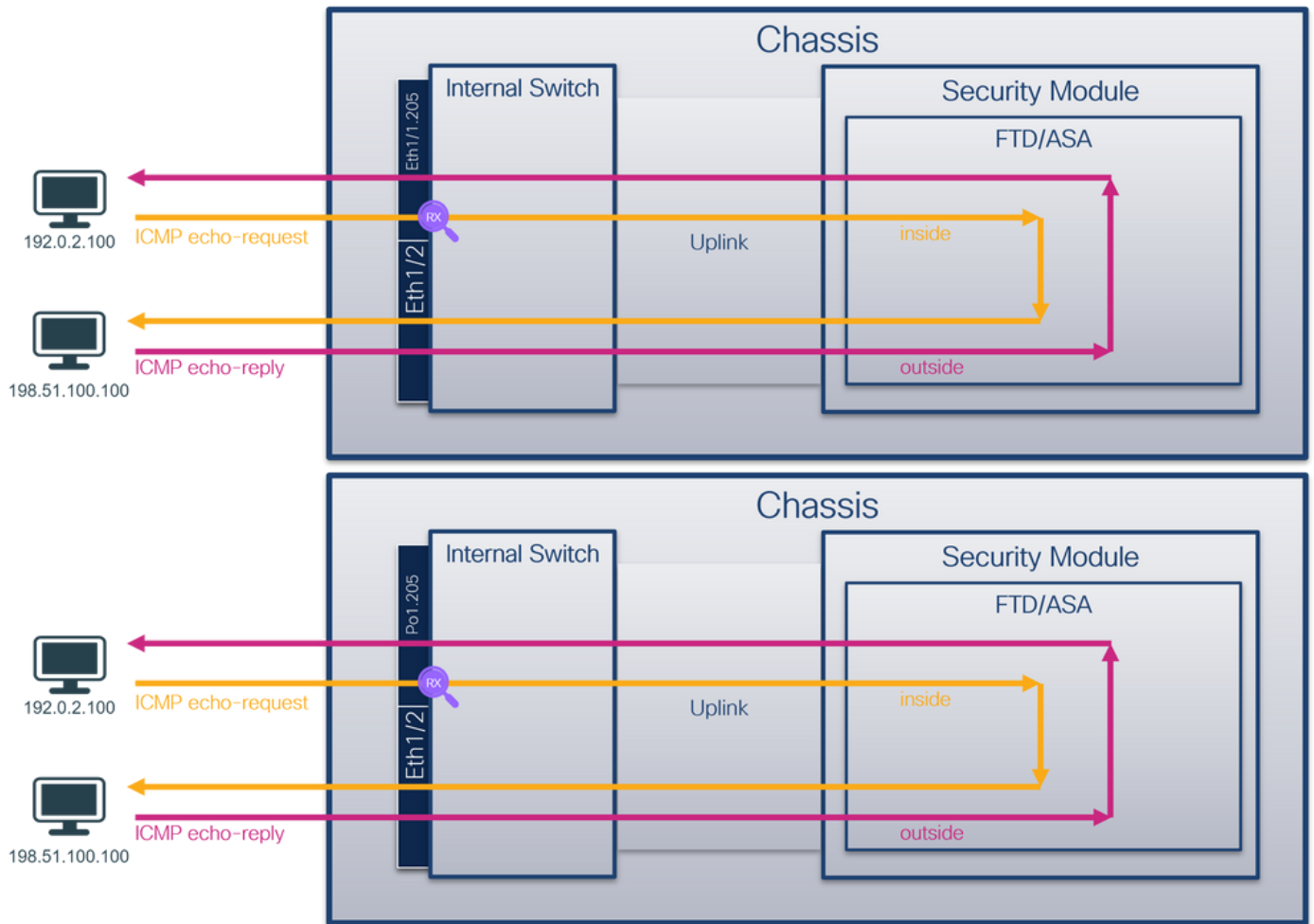
방향
 인그레스 전용
 인그레스 전용

캡처된 트래픽
 호스트 192.0.2.100에서 호스트 198.51.100.100으로의 ICMP 에코 요청
 호스트 192.0.2.100에서 호스트 198.51.100.100으로의 ICMP 에코 요청

물리적 또는 포트 채널 인터페이스의 하위 인터페이스에서 패킷 캡처

FTD 또는 ASA CLI를 사용하여 하위 인터페이스 Ethernet1/1.205 또는 Portchannel1.205에서 패킷 캡처를 구성하고 확인합니다. 두 하위 인터페이스 모두 nameif 내부에 있습니다.

토폴로지, 패킷 흐름 및 캡처 포인트



설정

ASA 또는 FTD CLI에서 다음 단계를 수행하여 인터페이스 Ethernet1/1 또는 Port-channel1에서 패킷 캡처를 구성합니다.

1. nameif 확인:

```
> show nameif
Interface      Name      Security
Ethernet1/1.205  inside    0
Ethernet1/2    outside    0
Management1/1  diagnostic 0
```

```
> show nameif
Interface      Name      Security
Port-channel1.205  inside    0
Ethernet1/2    outside    0
Management1/1  diagnostic 0
```

2. 캡처 세션을 생성합니다.

```
> capture capsw switch interface inside
```

3. 캡처 세션을 활성화합니다.

```
> no capture capsw switch stop
```

확인

캡처 세션 이름, 관리 및 운영 상태, 인터페이스 슬롯 및 식별자를 확인합니다. Pcapsize 값(바이트)이 증가하고 캡처된 패킷 수가 0이 아닌지 확인합니다.

```
> show capture capsw detail
```

```
Packet Capture info
```

```
Name: capsw
Session: 1
Admin State: enabled
Oper State: up
Oper State Reason: Active
Config Success: yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0
```

```
Total Physical ports involved in Packet Capture: 1
```

```
Physical port:
```

```
Slot Id: 1
Port Id: 1
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize: 6360
Filter: capsw-1-1
```

```
Packet Capture Filter Info
```

```
Name: capsw-1-1
Protocol: 0
Ivlan: 0
Ovlan: 205
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0
```

```
Total Physical breakout ports involved in Packet Capture: 0
```

```
46 packets captured on disk using switch capture
```

```
Reading of capture file from disk is not supported
```

이 경우 외부 VLAN Ovlan=205의 필터가 생성되어 인터페이스에 적용됩니다.

Port-channel1의 경우 Ovlan=205 필터를 사용하는 캡처가 모든 멤버 인터페이스에 구성됩니다.

```
> show capture capsw detail
```

```
Packet Capture info
```

```
Name: capsw
Session: 1
Admin State: enabled
Oper State: up
```

Oper State Reason: Active

Config Success: yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0

Total Physical ports involved in Packet Capture: 2

Physical port:

Slot Id: 1
Port Id: 4
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-4-0.pcap
Pcapsize: 23442
Filter: capsw-1-4

Packet Capture Filter Info

Name: capsw-1-4
Protocol: 0
Ivlan: 0
Ovlan: 205
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Physical port:

Slot Id: 1
Port Id: 3
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-3-0.pcap
Pcapsize: 5600
Filter: capsw-1-3

Packet Capture Filter Info

Name: capsw-1-3
Protocol: 0
Ivlan: 0
Ovlan: 205
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

49 packet captured on disk using switch capture

Reading of capture file from disk is not supported

포트 채널 멤버 인터페이스는 FXOS local-mgmt 명령 셸에서 **show portchannel summary** 명령을 통해 확인할 수 있습니다.

```
> connect fxos
...
KSEC-FPR3100-1 connect local-mgmt
KSEC-FPR3100-1(local-mgmt) show portchannel summary
Flags: D - Down P - Up in port-channel (members)
I - Individual H - Hot-standby (LACP only)
s - Suspended r - Module-removed
S - Switched R - Routed
U - Up (port-channel)
M - Not in use. Min-links not met
```

```
-----
Group Port-      Type      Protocol  Member Ports
Channel
-----
1      Po1(U)    Eth      LACP      Eth1/3(P)  Eth1/4(P)
```

LACP KeepAlive Timer:

```
-----
Channel PeerKeepAliveTimerFast
-----
1      Po1(U)    False
```

Cluster LACP Status:

```
-----
Channel ClusterSpanned ClusterDetach ClusterUnitID ClusterSysID
-----
1      Po1(U)    False      False      0          clust
```

ASA에서 FXOS에 액세스하려면 **connect fxos admin** 명령을 실행합니다. 다중 컨텍스트의 경우 관리 컨텍스트에서 이 명령을 실행합니다.

캡처 파일 수집

Collect Secure Firewall 3100 Internal Switch Capture Files 섹션의 단계를 수행합니다.

캡처 파일 분석

패킷 캡처 파일 판독기 응용 프로그램을 사용하여 Ethernet1/1.205에 대한 캡처 파일을 엽니다. 첫 번째 패킷을 선택하고 핵심 사항을 확인합니다.

1. ICMP 에코 요청 패킷만 캡처됩니다.
2. 원래 패킷 헤더에 VLAN 태그 205가 있습니다.

The screenshot shows a network traffic capture analysis tool. The top part displays a list of captured packets, all of which are ICMP Echo (ping) requests. The first packet is highlighted with a red box, showing its IP ID as 0x411f (16671) and TTL as 64. Below this, a detailed view of the first packet's header is shown, with a red box highlighting the Ethernet II header. The Ethernet II header shows the source MAC address as VMware_9d:e8:be (00:50:56:9d:e8:be) and the destination MAC address as Cisco_34:9a:14 (bc:e7:12:34:9a:14). The header also shows the priority as Best Effort (default) (0) and the type as IPv4 (0x0800). The trailer is 55555555. The bottom part of the screenshot shows the Internet Protocol Version 4 header, which is highlighted in yellow, and the Internet Control Message Protocol header, which is highlighted in green.

Portchannel1 멤버 인터페이스에 대한 캡처 파일을 엽니다. 첫 번째 패킷을 선택하고 핵심 사항을 확인합니다.

1. ICMP 에코 요청 패킷만 캡처됩니다.
2. 원래 패킷 헤더에 VLAN 태그 205가 있습니다.

The image shows a packet capture analysis. The top table lists 18 ICMP Echo (ping) requests from source 192.0.2.100 to destination 198.51.100.100. The first packet is highlighted with a red box and labeled '1'. Below the table, the details for the first packet are shown. A red box highlights the Ethernet II header, specifically the 'Virtual LAN, PRI: 0, DEI: 0, ID: 205' field, which is labeled '2'. The Internet Protocol Version 4 and Internet Control Message Protocol headers are also visible.

설명

스위치 캡처는 하위 인터페이스 Ethernet1/1.205 또는 Portchannel1.205에서 구성되며 외부 VLAN 205와 일치하는 필터가 있습니다.

이 표에서는 작업을 요약합니다.

작업	캡처 지점	내부 필터	방향	캡처된 트래픽
하위 인터페이스 Ethernet1/1.205에서 패킷 캡처 구성 및 확인	이더넷 1/1	외부 VLAN 205	인그레스 전용	호스트 192.0.2.100에서 호스트 198.51.100.100으로의 ICMP 에코
멤버 인터페이스 Ethernet1/3 및 Ethernet1/4를 사용하여 하위 인터페이스 Portchannel1.205에서 패킷 캡처를 구성하고 확인합니다.	이더넷 1/4	외부 VLAN 205	인그레스 전용	호스트 192.0.2.100에서 호스트 198.51.100.100으로의 ICMP 에코

내부 인터페이스의 패킷 캡처

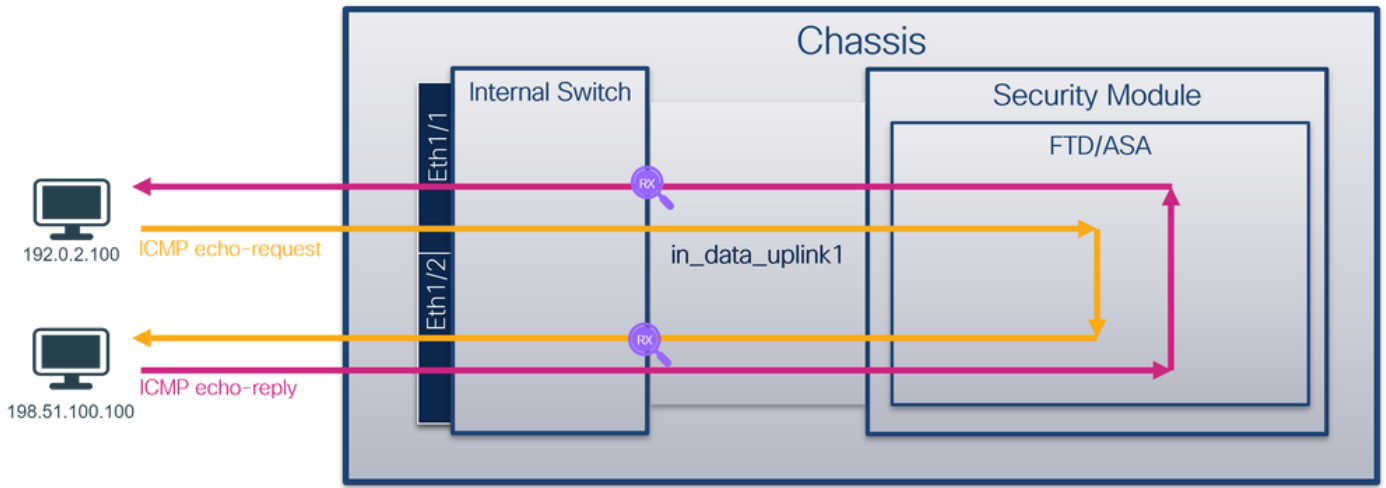
보안 방화벽에는 2개의 내부 인터페이스가 있습니다.

- in_data_uplink1 - 애플리케이션을 내부 스위치에 연결합니다.
- in_mgmt_uplink1 - 관리 인터페이스에 대한 SSH 또는 sftunnel이라고도 하는 FMC와 FTD 간의 관리 연결과 같은 관리 연결을 위한 전용 패킷 경로를 제공합니다.

작업 1

FTD 또는 ASA CLI를 사용하여 업링크 인터페이스 in_data_uplink1에서 패킷 캡처를 구성하고 확인합니다.

토폴로지, 패킷 흐름 및 캡처 포인트



설정

ASA 또는 FTD CLI에서 다음 단계를 수행하여 인터페이스 `in_data_uplink1`의 패킷 캡처를 구성합니다.

1. 캡처 세션을 생성합니다.

```
> capture capsw switch interface in_data_uplink1
```

2. 캡처 세션을 활성화합니다.

```
> no capture capsw switch stop
```

확인

캡처 세션 이름, 관리 및 운영 상태, 인터페이스 슬롯 및 식별자를 확인합니다. Pcapsize 값(바이트)이 증가하고 캡처된 패킷 수가 0이 아닌지 확인합니다.

```
> show capture capsw detail
```

Packet Capture info

```

Name:          capsw
Session:       1
Admin State:   enabled
Oper State:    up
Oper State Reason: Active
Config Success: yes
Config Fail Reason:
Append Flag:   overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code:    0
Drop Count:    0

```

Total Physical ports involved in Packet Capture: 1

Physical port:

```

Slot Id:      1
Port Id:      18
Pcapfile:     /mnt/disk0/packet-capture/sess-1-capsw-data-uplink1.pcap
Pcapsize:     7704
Filter:       capsw-1-18

```

Packet Capture Filter Info

```
Name:          capsw-1-18
Protocol:      0
Ivlan:        0
Ovlan:        0
Src Ip:        0.0.0.0
Dest Ip:       0.0.0.0
Src Ipv6:      ::
Dest Ipv6:     ::
Src MAC:       00:00:00:00:00:00
Dest MAC:      00:00:00:00:00:00
Src Port:      0
Dest Port:     0
Ethertype:    0
```

Total Physical breakout ports involved in Packet Capture: 0

66 packets captured on disk using switch capture

Reading of capture file from disk is not supported

이 경우, 보안 방화벽(3130)의 in_data_uplink1 인터페이스인 내부 ID 18로 인터페이스에 캡처가 생성됩니다. FXOS local-mgmt 명령 셸의 show portmanager switch status 명령은 인터페이스 ID를 표시합니다.

> connect fxos

...

KSEC-FPR3100-1 connect local-mgmt

KSEC-FPR3100-1(local-mgmt) show portmanager switch status

Dev/Port	Mode	Link	Speed	Duplex	Loopback Mode	Port Manager
0/1	SGMII	Up	1G	Full	None	Link-Up
0/2	SGMII	Up	1G	Full	None	Link-Up
0/3	SGMII	Up	1G	Full	None	Link-Up
0/4	SGMII	Up	1G	Full	None	Link-Up
0/5	SGMII	Down	1G	Half	None	Mac-Link-Down
0/6	SGMII	Down	1G	Half	None	Mac-Link-Down
0/7	SGMII	Down	1G	Half	None	Mac-Link-Down
0/8	SGMII	Down	1G	Half	None	Mac-Link-Down
0/9	1000_BaseX	Down	1G	Full	None	Link-Down
0/10	1000_BaseX	Down	1G	Full	None	Link-Down
0/11	1000_BaseX	Down	1G	Full	None	Link-Down
0/12	1000_BaseX	Down	1G	Full	None	Link-Down
0/13	1000_BaseX	Down	1G	Full	None	Link-Down
0/14	1000_BaseX	Down	1G	Full	None	Link-Down
0/15	1000_BaseX	Down	1G	Full	None	Link-Down
0/16	1000_BaseX	Down	1G	Full	None	Link-Down
0/17	1000_BaseX	Up	1G	Full	None	Link-Up
0/18	KR2	Up	50G	Full	None	Link-Up
0/19	KR	Up	25G	Full	None	Link-Up
0/20	KR	Up	25G	Full	None	Link-Up
0/21	KR4	Down	40G	Full	None	Link-Down
0/22	n/a	Down	n/a	Full	N/A	Reset
0/23	n/a	Down	n/a	Full	N/A	Reset
0/24	n/a	Down	n/a	Full	N/A	Reset
0/25	1000_BaseX	Down	1G	Full	None	Link-Down
0/26	n/a	Down	n/a	Full	N/A	Reset
0/27	n/a	Down	n/a	Full	N/A	Reset
0/28	n/a	Down	n/a	Full	N/A	Reset
0/29	1000_BaseX	Down	1G	Full	None	Link-Down
0/30	n/a	Down	n/a	Full	N/A	Reset
0/31	n/a	Down	n/a	Full	N/A	Reset
0/32	n/a	Down	n/a	Full	N/A	Reset
0/33	1000_BaseX	Down	1G	Full	None	Link-Down

0/34	n/a	Down	n/a	Full	N/A	Reset
0/35	n/a	Down	n/a	Full	N/A	Reset
0/36	n/a	Down	n/a	Full	N/A	Reset

ASA에서 FXOS에 액세스하려면 **connect fxos admin** 명령을 실행합니다. 다중 컨텍스트의 경우 관리 컨텍스트에서 이 명령을 실행합니다.

캡처 파일 수집

Collect Secure Firewall 3100 Internal Switch Capture Files 섹션의 단계를 수행합니다.

캡처 파일 분석

패킷 캡처 파일 판독기 응용 프로그램을 사용하여 인터페이스 in_data_uplink1의 캡처 파일을 엽니다. 키 포인트를 확인합니다. 이 경우 ICMP 에코 요청 및 에코 응답 패킷이 캡처됩니다. 애플리케이션에서 내부 스위치로 전송된 패킷입니다.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-07 22:40:06.685606	192.0.2.100	198.51.100.100	ICMP	102	0x4d93 (19859)	64	Echo (ping) request id=0x003a, seq=33/8448, ttl=64 (repl
2	2022-08-07 22:40:06.685615	198.51.100.100	192.0.2.100	ICMP	102	0x6cdc (27868)	64	Echo (ping) reply id=0x003a, seq=33/8448, ttl=64 (requ
3	2022-08-07 22:40:07.684219	192.0.2.100	198.51.100.100	ICMP	102	0x40e8 (19944)	64	Echo (ping) request id=0x003a, seq=34/8704, ttl=64 (repl
4	2022-08-07 22:40:07.689300	198.51.100.100	192.0.2.100	ICMP	102	0x6db2 (28082)	64	Echo (ping) reply id=0x003a, seq=34/8704, ttl=64 (requ
5	2022-08-07 22:40:08.685736	192.0.2.100	198.51.100.100	ICMP	102	0x4edc (20188)	64	Echo (ping) request id=0x003a, seq=35/8960, ttl=64 (repl
6	2022-08-07 22:40:08.690806	198.51.100.100	192.0.2.100	ICMP	102	0x6dbf (28095)	64	Echo (ping) reply id=0x003a, seq=35/8960, ttl=64 (requ
7	2022-08-07 22:40:09.690737	192.0.2.100	198.51.100.100	ICMP	102	0x4f2d (20269)	64	Echo (ping) request id=0x003a, seq=36/9216, ttl=64 (repl
8	2022-08-07 22:40:09.690744	198.51.100.100	192.0.2.100	ICMP	102	0x6e80 (28288)	64	Echo (ping) reply id=0x003a, seq=36/9216, ttl=64 (requ
9	2022-08-07 22:40:10.692266	192.0.2.100	198.51.100.100	ICMP	102	0x4fb1 (20401)	64	Echo (ping) request id=0x003a, seq=37/9472, ttl=64 (repl
10	2022-08-07 22:40:10.692272	198.51.100.100	192.0.2.100	ICMP	102	0x6ed5 (28373)	64	Echo (ping) reply id=0x003a, seq=37/9472, ttl=64 (requ
11	2022-08-07 22:40:11.691159	192.0.2.100	198.51.100.100	ICMP	102	0x5008 (20488)	64	Echo (ping) request id=0x003a, seq=38/9728, ttl=64 (repl
12	2022-08-07 22:40:11.691166	198.51.100.100	192.0.2.100	ICMP	102	0x6f3b (28475)	64	Echo (ping) reply id=0x003a, seq=38/9728, ttl=64 (requ
13	2022-08-07 22:40:12.692135	192.0.2.100	198.51.100.100	ICMP	102	0x50b8 (20664)	64	Echo (ping) request id=0x003a, seq=39/9984, ttl=64 (repl
14	2022-08-07 22:40:12.692709	198.51.100.100	192.0.2.100	ICMP	102	0x6fd7 (28631)	64	Echo (ping) reply id=0x003a, seq=39/9984, ttl=64 (requ
15	2022-08-07 22:40:13.697320	192.0.2.100	198.51.100.100	ICMP	102	0x5184 (20868)	64	Echo (ping) request id=0x003a, seq=40/10240, ttl=64 (req
16	2022-08-07 22:40:13.697327	198.51.100.100	192.0.2.100	ICMP	102	0x703e (28734)	64	Echo (ping) reply id=0x003a, seq=40/10240, ttl=64 (rec
17	2022-08-07 22:40:14.698512	192.0.2.100	198.51.100.100	ICMP	102	0x51d8 (20952)	64	Echo (ping) request id=0x003a, seq=41/10496, ttl=64 (rec
18	2022-08-07 22:40:14.698518	198.51.100.100	192.0.2.100	ICMP	102	0x70dd (28893)	64	Echo (ping) reply id=0x003a, seq=41/10496, ttl=64 (rec

설명

업링크 인터페이스에서 스위치 캡처가 구성된 경우 애플리케이션에서 내부 스위치로 전송된 패킷만 캡처됩니다. 애플리케이션으로 전송된 패킷은 캡처되지 않습니다.

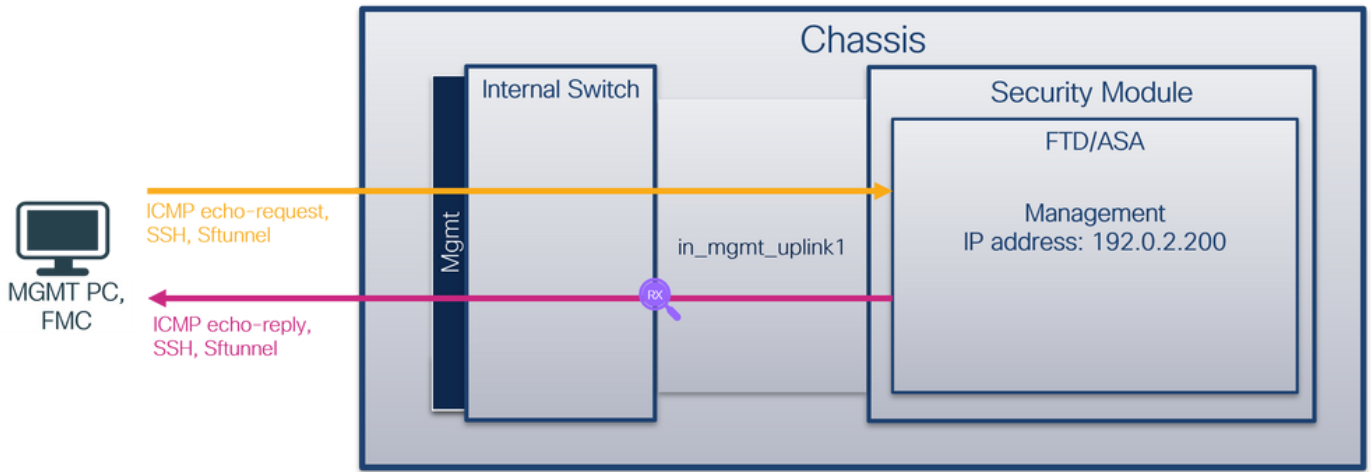
이 표에서는 작업을 요약합니다.

작업	캡처 지점	내부 필터	방향	캡처된 트래픽
업링크 인터페이스에서 패킷 캡처를 구성하고 확인합니다. in_data_uplink1	in_data_uplink1	없음	인그레스 전용	호스트 192.0.2.100에서 호스트 198.51.100.100으로의 ICMP 에코 요청 및 호스트 198.51.100.100에서 호스트 192.0.2.100으로 ICMP 에코 응답

작업 2

FTD 또는 ASA CLI를 사용하여 업링크 인터페이스 in_mgmt_uplink1에서 패킷 캡처를 구성하고 확인합니다. 관리 플레인 연결의 패킷만 캡처됩니다.

토폴로지, 패킷 흐름 및 캡처 포인트



설정

ASA 또는 FTD CLI에서 다음 단계를 수행하여 인터페이스 `in_mgmt_uplink1`에 패킷 캡처를 구성합니다.

1. 캡처 세션을 생성합니다.

```
> capture capsw switch interface in_mgmt_uplink1
```

2. 캡처 세션을 활성화합니다.

```
> no capture capsw switch stop
```

확인

캡처 세션 이름, 관리 및 운영 상태, 인터페이스 슬롯 및 식별자를 확인합니다. `Pcapsize` 값(바이트)이 증가하고 캡처된 패킷 수가 0이 아닌지 확인합니다.

```
> show capture capsw detail
```

Packet Capture info

```
Name:          capsw
Session:       1
Admin State:   enabled
Oper State:    up
Oper State Reason: Active
Config Success: yes
Config Fail Reason:
Append Flag:   overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code:    0
Drop Count:    0
```

Total Physical ports involved in Packet Capture: 1

Physical port:

```
Slot Id:       1
Port Id:       19
Pcapfile:      /mnt/disk0/packet-capture/sess-1-capsw-mgmt-uplink1.pcap
Pcapsize:     137248
Filter:        capsw-1-19
```

Packet Capture Filter Info

```
Name:          capsw-1-19
Protocol:     0
Ivlan:       0
Ovlan:       0
Src Ip:      0.0.0.0
Dest Ip:     0.0.0.0
Src Ipv6:    ::
Dest Ipv6:   ::
Src MAC:     00:00:00:00:00:00
Dest MAC:    00:00:00:00:00:00
Src Port:    0
Dest Port:   0
Ethertype:   0
```

Total Physical breakout ports involved in Packet Capture: 0

281 packets captured on disk using switch capture

Reading of capture file from disk is not supported

이 경우 Secure Firewall 3130의 in_mgmt_uplink1 인터페이스인 내부 ID 19로 인터페이스에 캡처가 생성됩니다. FXOS local-mgmt 명령 셸의 show portmanager switch status 명령은 인터페이스 ID를 표시합니다.

> connect fxos

...

KSEC-FPR3100-1 connect local-mgmt

KSEC-FPR3100-1(local-mgmt) show portmanager switch status

Dev/Port	Mode	Link	Speed	Duplex	Loopback Mode	Port Manager
0/1	SGMII	Up	1G	Full	None	Link-Up
0/2	SGMII	Up	1G	Full	None	Link-Up
0/3	SGMII	Up	1G	Full	None	Link-Up
0/4	SGMII	Up	1G	Full	None	Link-Up
0/5	SGMII	Down	1G	Half	None	Mac-Link-Down
0/6	SGMII	Down	1G	Half	None	Mac-Link-Down
0/7	SGMII	Down	1G	Half	None	Mac-Link-Down
0/8	SGMII	Down	1G	Half	None	Mac-Link-Down
0/9	1000_BaseX	Down	1G	Full	None	Link-Down
0/10	1000_BaseX	Down	1G	Full	None	Link-Down
0/11	1000_BaseX	Down	1G	Full	None	Link-Down
0/12	1000_BaseX	Down	1G	Full	None	Link-Down
0/13	1000_BaseX	Down	1G	Full	None	Link-Down
0/14	1000_BaseX	Down	1G	Full	None	Link-Down
0/15	1000_BaseX	Down	1G	Full	None	Link-Down
0/16	1000_BaseX	Down	1G	Full	None	Link-Down
0/17	1000_BaseX	Up	1G	Full	None	Link-Up
0/18	KR2	Up	50G	Full	None	Link-Up
0/19	KR	Up	25G	Full	None	Link-Up
0/20	KR	Up	25G	Full	None	Link-Up
0/21	KR4	Down	40G	Full	None	Link-Down
0/22	n/a	Down	n/a	Full	N/A	Reset
0/23	n/a	Down	n/a	Full	N/A	Reset
0/24	n/a	Down	n/a	Full	N/A	Reset
0/25	1000_BaseX	Down	1G	Full	None	Link-Down
0/26	n/a	Down	n/a	Full	N/A	Reset
0/27	n/a	Down	n/a	Full	N/A	Reset
0/28	n/a	Down	n/a	Full	N/A	Reset
0/29	1000_BaseX	Down	1G	Full	None	Link-Down
0/30	n/a	Down	n/a	Full	N/A	Reset
0/31	n/a	Down	n/a	Full	N/A	Reset
0/32	n/a	Down	n/a	Full	N/A	Reset
0/33	1000_BaseX	Down	1G	Full	None	Link-Down

0/34	n/a	Down	n/a	Full	N/A	Reset
0/35	n/a	Down	n/a	Full	N/A	Reset
0/36	n/a	Down	n/a	Full	N/A	Reset

ASA에서 FXOS에 액세스하려면 **connect fxos admin** 명령을 실행합니다. 다중 컨텍스트의 경우 관리 컨텍스트에서 이 명령을 실행합니다.

캡처 파일 수집

Collect Secure Firewall 3100 Internal Switch Capture Files 섹션의 단계를 수행합니다.

캡처 파일 분석

패킷 캡처 파일 판독기 응용 프로그램을 사용하여 인터페이스 **in_mgmt_uplink1**에 대한 캡처 파일을 엽니다. 핵심 사항을 확인합니다. 이 경우 관리 IP 주소 192.0.2.200의 패킷만 표시됩니다. 예를 들어 SSH, Sftunnel 또는 ICMP 에코 응답 패킷이 있습니다. 내부 스위치를 통해 애플리케이션 관리 인터페이스에서 네트워크로 전송된 패킷입니다.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
196	2022-08-07 23:21:45.133362	192.0.2.200	192.0.2.101	TCP	1518	0xb7d0 (47056)	64	39181 → 8305 [ACK] Seq=61372 Ack=875 Win=1384 Len=1448 TS...
197	2022-08-07 23:21:45.133385	192.0.2.200	192.0.2.101	TCP	1518	0xb7d1 (47057)	64	39181 → 8305 [ACK] Seq=62820 Ack=875 Win=1384 Len=1448 TS...
198	2022-08-07 23:21:45.133388	192.0.2.200	192.0.2.101	TLSv1.2	990	0xb7d2 (47058)	64	Application Data
199	2022-08-07 23:21:45.928772	192.0.2.200	192.0.2.100	ICMP	78	0xbd48 (48456)	64	Echo (ping) reply id=0x0001, seq=4539/47889, ttl=64
200	2022-08-07 23:21:45.949024	192.0.2.200	192.0.2.101	TLSv1.2	128	0x4a97 (19095)	64	Application Data
201	2022-08-07 23:21:45.949027	192.0.2.200	192.0.2.101	TCP	70	0x4a98 (19096)	64	8305 → 58885 [ACK] Seq=21997 Ack=26244 Win=4116 Len=0 TSv...
202	2022-08-07 23:21:46.019895	192.0.2.200	192.0.2.101	TLSv1.2	100	0x4a99 (19097)	64	Application Data
203	2022-08-07 23:21:46.019899	192.0.2.200	192.0.2.101	TLSv1.2	96	0x4a9a (19098)	64	Application Data
204	2022-08-07 23:21:46.019903	192.0.2.200	192.0.2.101	TCP	70	0x4a9b (19099)	64	8305 → 58885 [ACK] Seq=22053 Ack=26274 Win=4116 Len=0 TSv...
205	2022-08-07 23:21:46.019906	192.0.2.200	192.0.2.101	TCP	70	0x4a9c (19100)	64	8305 → 58885 [ACK] Seq=22053 Ack=26300 Win=4116 Len=0 TSv...
206	2022-08-07 23:21:46.136415	192.0.2.200	192.0.2.101	TCP	70	0xb7d3 (47059)	64	39181 → 8305 [ACK] Seq=65188 Ack=921 Win=1384 Len=0 TSval...
207	2022-08-07 23:21:46.958148	192.0.2.200	192.0.2.100	ICMP	78	0xbd9e (48542)	64	Echo (ping) reply id=0x0001, seq=4540/48145, ttl=64
208	2022-08-07 23:21:47.980409	192.0.2.200	192.0.2.100	ICMP	78	0xbd9f (48543)	64	Echo (ping) reply id=0x0001, seq=4541/48146, ttl=64
209	2022-08-07 23:21:48.406312	192.0.2.200	192.0.2.101	TCP	70	0x4a9d (19101)	64	8305 → 58885 [ACK] Seq=22053 Ack=26366 Win=4116 Len=0 TSv...
210	2022-08-07 23:21:48.903236	192.0.2.200	192.0.2.101	TLSv1.2	747	0x4a9e (19102)	64	Application Data
211	2022-08-07 23:21:48.994386	192.0.2.200	192.0.2.100	ICMP	78	0xbe48 (48712)	64	Echo (ping) reply id=0x0001, seq=4542/48657, ttl=64
212	2022-08-07 23:21:50.008576	192.0.2.200	192.0.2.100	ICMP	78	0xbe49 (48713)	64	Echo (ping) reply id=0x0001, seq=4543/48658, ttl=64
213	2022-08-07 23:21:50.140167	192.0.2.200	192.0.2.101	TCP	1518	0xb7d4 (47060)	64	39181 → 8305 [ACK] Seq=65188 Ack=921 Win=1384 Len=1448 TS...
214	2022-08-07 23:21:50.140171	192.0.2.200	192.0.2.101	TCP	1518	0xb7d5 (47061)	64	39181 → 8305 [ACK] Seq=66636 Ack=921 Win=1384 Len=1448 TS...
215	2022-08-07 23:21:50.140175	192.0.2.200	192.0.2.101	TLSv1.2	990	0xb7d6 (47062)	64	Application Data
216	2022-08-07 23:21:51.015884	192.0.2.200	192.0.2.100	ICMP	78	0xbec1 (48833)	64	Echo (ping) reply id=0x0001, seq=4544/49169, ttl=64
217	2022-08-07 23:21:51.142842	192.0.2.200	192.0.2.101	TCP	70	0xb7d7 (47063)	64	39181 → 8305 [ACK] Seq=69004 Ack=967 Win=1384 Len=0 TSval...
218	2022-08-07 23:21:52.030118	192.0.2.200	192.0.2.100	ICMP	78	0xbf02 (48898)	64	Echo (ping) reply id=0x0001, seq=4545/49425, ttl=64
219	2022-08-07 23:21:53.042744	192.0.2.200	192.0.2.100	ICMP	78	0xbf59 (48985)	64	Echo (ping) reply id=0x0001, seq=4546/49681, ttl=64
220	2022-08-07 23:21:53.073144	192.0.2.200	192.0.2.100	SSH	170	0xad34 (44340)	64	Server: Encrypted packet (len=112)
221	2022-08-07 23:21:53.194906	192.0.2.200	192.0.2.100	TCP	64	0xad35 (44341)	64	22 → 53249 [ACK] Seq=1025 Ack=881 Win=946 Len=0
222	2022-08-07 23:21:53.905480	192.0.2.200	192.0.2.101	TLSv1.2	747	0x4a9f (19103)	64	Application Data
223	2022-08-07 23:21:54.102899	192.0.2.200	192.0.2.100	ICMP	78	0xbf63 (48995)	64	Echo (ping) reply id=0x0001, seq=4547/49937, ttl=64
224	2022-08-07 23:21:54.903675	192.0.2.200	192.0.2.101	TCP	70	0x4aa0 (19104)	64	8305 → 58885 [ACK] Seq=23407 Ack=26424 Win=4116 Len=0 TSv...
225	2022-08-07 23:21:55.136700	192.0.2.200	192.0.2.100	TCP	70	0xbf64 (48996)	64	Echo (ping) reply id=0x0001, seq=4548/50103, ttl=64

설명

관리 업링크 인터페이스에서 스위치 캡처가 구성된 경우 애플리케이션 관리 인터페이스에서 전송된 인그레스 패킷만 캡처됩니다. 애플리케이션 관리 인터페이스로 향하는 패킷은 캡처되지 않습니다.

이 표에서는 작업을 요약합니다.

작업	캡처 지점	내부 필터	방향	캡처된 트래픽
관리 업링크 인터페이스에서 패킷 캡처 구성 및 확인	in_mgmt_uplink1	없음	인그레스 전용 (내부 스위치를 통해 관리 인터페이스에서 네트워크로)	FTD 관리 IP 주소 192.0.2.200에서 호스트 192.0.2.100으로 ICMP 에코 응답 FTD 관리 IP 주소 192.0.2.200에서 FMC IP 주소 192.0.2.101로 Sftunnel FTD 관리 IP 주소 192.0.2.200에서 호스트

패킷 캡처 필터

내부 스위치 패킷 캡처 필터는 데이터 프레임 캡처와 동일한 방식으로 구성됩니다. 필터를 구성하려면 **ethernet-type** 및 **match** 옵션을 사용합니다.

설정

ASA 또는 FTD CLI에서 다음 단계를 수행하여 Ethernet1/1 인터페이스에서 호스트 198.51.100.100의 ARP 프레임 또는 ICMP 패킷과 일치하는 필터를 사용하여 패킷 캡처를 구성합니다.

1. nameif 확인:

```
> show nameif
Interface           Name           Security
Ethernet1/1        inside         0
Ethernet1/2        outside        0
Management1/1     diagnostic     0
```

2. ARP 또는 ICMP에 대한 캡처 세션을 생성합니다.

```
> capture capsw switch interface inside ethernet-type arp

> capture capsw switch interface inside match icmp 198.51.100.100
```

확인

캡처 세션 이름 및 필터를 확인합니다. Ethertype 값은 10진수로 2054, 16진수로 0x0806입니다.

```
> show capture capsw detail
Packet Capture info
Name:          capsw
Session:       1
Admin State:   disabled
Oper State:    down
Oper State Reason: Session_Admin_Shut
Config Success: yes
Config Fail Reason:
Append Flag:   overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code:    0
Drop Count:    0

Total Physical ports involved in Packet Capture: 1

Physical port:
Slot Id:       1
Port Id:       1
Pcapfile:      /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize:     0
Filter:        capsw-1-1
```

```
Packet Capture Filter Info
Name:          capsw-1-1
```

Protocol: 0
Ivlan: 0
Ovlan: 0
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 2054

Total Physical breakout ports involved in Packet Capture: 0

0 packet captured on disk using switch capture

Reading of capture file from disk is not supported

ICMP에 대한 필터 확인입니다. IP 프로토콜 1은 ICMP입니다.

> **show capture capsw detail**

Packet Capture info

Name: capsw
Session: 1
Admin State: disabled
Oper State: down
Oper State Reason: Session_Admin_Shut
Config Success: yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1
Port Id: 1
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize: 0
Filter: capsw-1-1

Packet Capture Filter Info

Name: capsw-1-1
Protocol: 1
Ivlan: 0
Ovlan: 0
Src Ip: 198.51.100.100
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

0 packets captured on disk using switch capture

Reading of capture file from disk is not supported

Secure Firewall 3100 내부 스위치 캡처 파일 수집

ASA 또는 FTD CLI를 사용하여 내부 스위치 캡처 파일을 수집합니다. FTD에서 캡처 파일은 CLI copy 명령을 통해 데이터 또는 진단 인터페이스를 통해 연결 가능한 대상으로 내보낼 수도 있습니다.

또는 파일을 전문가 모드에서 `/ngfw/var/common`에 복사하고 File Download 옵션을 통해 FMC에서 다운로드할 수 있습니다.

포트 채널 인터페이스의 경우 모든 멤버 인터페이스에서 패킷 캡처 파일을 수집해야 합니다.

ASA

ASA CLI에서 내부 스위치 캡처 파일을 수집하려면 의 다음 단계를 수행합니다.

1. 캡처를 중지합니다.

```
asa# capture capsw switch stop
```

2. 캡처 세션이 중지되었는지 확인하고 캡처 파일 이름을 확인합니다.

```
asa# show capture capsw detail
```

Packet Capture info

```
Name:                capsw
Session:             1
Admin State:        disabled
Oper State:         down
Oper State Reason:  Session_Admin_Shut
Config Success:     yes
Config Fail Reason:
Append Flag:        overwrite
Session Mem Usage:  256
Session Pcap Snap Len: 1518
Error Code:         0
Drop Count:         0
```

Total Physical ports involved in Packet Capture: 1

Physical port:

```
Slot Id:            1
Port Id:            1
Pcapfile:           /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize:           139826
Filter:             capsw-1-1
```

Packet Capture Filter Info

```
Name:               capsw-1-1
Protocol:           0
Ivlan:              0
Ovlan:              0
Src Ip:             0.0.0.0
Dest Ip:            0.0.0.0
Src Ipv6:           ::
Dest Ipv6:          ::
Src MAC:            00:00:00:00:00:00
Dest MAC:           00:00:00:00:00:00
```

```
Src Port:      0
Dest Port:    0
Ethertype:    0
```

Total Physical breakout ports involved in Packet Capture: 0

886 packets captured on disk using switch capture

Reading of capture file from disk is not supported

3. 원격 대상으로 파일을 내보내려면 CLI copy 명령을 사용합니다.

```
asa# copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap ?
cluster:      Copy to cluster: file system
disk0:        Copy to disk0: file system
disk1:        Copy to disk1: file system
flash:        Copy to flash: file system
ftp:          Copy to ftp: file system
running-config Update (merge with) current system configuration
scp:          Copy to scp: file system
smb:          Copy to smb: file system
startup-config Copy to startup configuration
system:       Copy to system: file system
tftp:         Copy to tftp: file system
```

```
asa# copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap tftp://198.51.100.10/
Source filename [/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap]?
Destination filename [sess-1-capsw-ethernet-1-1-0.pcap]?
Copy in progress...C
139826 bytes copied in 0.532 secs
```

FTD

FTD CLI에서 내부 스위치 캡처 파일을 수집하고 데이터 또는 진단 인터페이스를 통해 연결 가능한 서버에 복사하려면 다음 단계를 수행합니다.

1. 진단 CLI로 이동합니다.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Click 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
firepower> enable
Password: <-- Enter
firepower#
```

2. 캡처를 중지합니다.

```
firepower# capture capi switch stop
```

3. 캡처 세션이 중지되었는지 확인하고 캡처 파일 이름을 확인합니다.

```
firepower# show capture capsw detail
Packet Capture info
Name:          capsw
Session:       1
Admin State:   disabled
Oper State:    down
Oper State Reason: Session_Admin_Shut
Config Success: yes
```


Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1
Port Id: 1
Pcapfile: /mnt/disk0/packet-capture/**sess-1-capsw-ethernet-1-1-0.pcap**
Pcapsize: 139826
Filter: capsw-1-1

Packet Capture Filter Info

Name: capsw-1-1
Protocol: 0
Ivlan: 0
Ovlan: 0
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

886 packets captured on disk using switch capture

Reading of capture file from disk is not supported

4. 파일을 원격 대상으로 내보내려면 CLI copy 명령을 사용합니다.

```
firepower# copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap ?
cluster: Copy to cluster: file system
disk0: Copy to disk0: file system
disk1: Copy to disk1: file system
flash: Copy to flash: file system
ftp: Copy to ftp: file system
running-config Update (merge with) current system configuration
scp: Copy to scp: file system
smb: Copy to smb: file system
startup-config Copy to startup configuration
system: Copy to system: file system
tftp: Copy to tftp: file system
```

```
firepower# copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap tftp://198.51.100.10/
Source filename [/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap]?
Destination filename [sess-1-capsw-ethernet-1-1-0.pcap]?
Copy in progress...C
```

139826 bytes copied in 0.532 secs

파일 다운로드 옵션을 통해 FMC에서 캡처 파일을 수집하려면 다음 단계를 수행합니다.

1. 캡처를 중지합니다.

```
> capture capsw switch stop
```

2. 캡처 세션이 중지되었는지 확인하고 파일 이름과 전체 캡처 파일 경로를 확인합니다.

```
> show capture capsw detail
```

```
Packet Capture info
```

```
Name:                capsw
Session:              1
Admin State:         disabled
Oper State:          down
Oper State Reason:   Session_Admin_Shut
Config Success:      yes
Config Fail Reason:
Append Flag:         overwrite
Session Mem Usage:   256
Session Pcap Snap Len: 1518
Error Code:          0
Drop Count:          0
```

```
Total Physical ports involved in Packet Capture: 1
```

```
Physical port:
```

```
Slot Id:             1
Port Id:             1
Pcapfile:            /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize:            139826
Filter:              capsw-1-1
```

```
Packet Capture Filter Info
```

```
Name:                capsw-1-1
Protocol:             0
Ivlan:               0
Ovlan:               0
Src Ip:              0.0.0.0
Dest Ip:              0.0.0.0
Src Ipv6:            ::
Dest Ipv6:           ::
Src MAC:              00:00:00:00:00:00
Dest MAC:             00:00:00:00:00:00
Src Port:             0
Dest Port:            0
Ethertype:           0
```

```
Total Physical breakout ports involved in Packet Capture: 0
```

```
886 packets captured on disk using switch capture
```

```
Reading of capture file from disk is not supported
```

3. 전문가 모드로 전환하고 루트 모드로 전환합니다.

```
> expert
```

```
admin@firepower:~$ sudo su
```

```
root@firepower:/home/admin
```

4. 캡처 파일을 /ngfw/var/common/에 복사합니다.

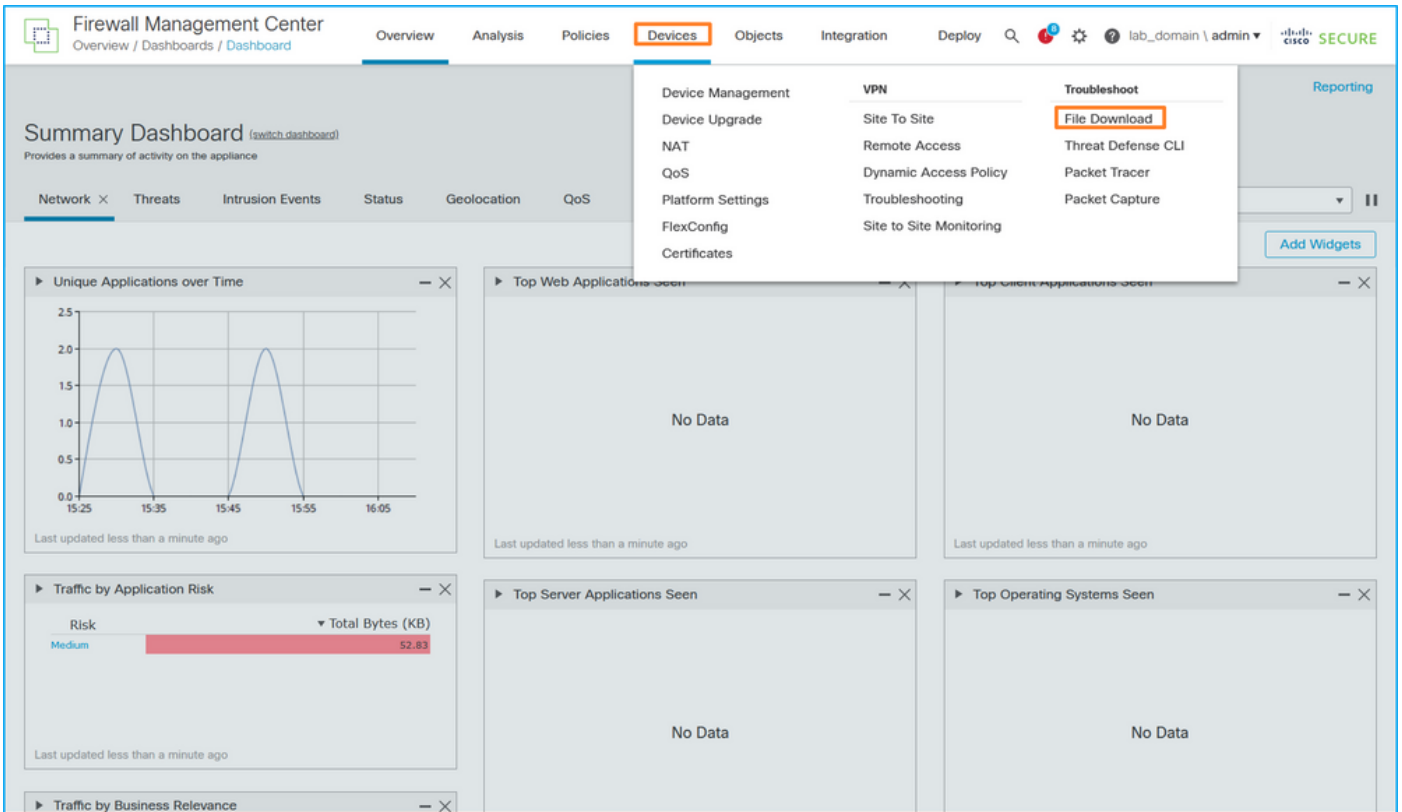
```
root@KSEC-FPR3100-1:/home/admin cp /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
/ngfw/var/common/
```

```
root@KSEC-FPR3100-1:/home/admin ls -l /ngfw/var/common/sess*
```

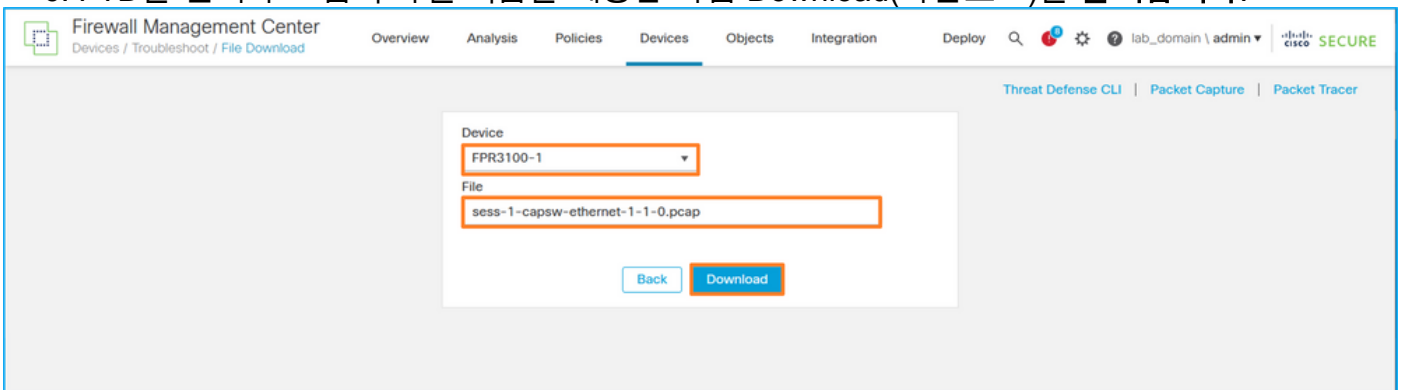
```
-rwxr-xr-x 1 root admin 139826 Aug  7 20:14 /ngfw/var/common/sess-1-capsw-ethernet-1-1-0.pcap
```

```
-rwxr-xr-x 1 root admin    24 Aug  6 21:58 /ngfw/var/common/sess-1-capsw-ethernet-1-3-0.pcap
```

5. FMC에서 Devices > File Download를 선택합니다.



6. FTD를 선택하고 캡처 파일 이름을 제공한 다음 Download(다운로드)를 클릭합니다.



내부 스위치 패킷 캡처에 대한 지침, 제한 및 모범 사례

지침 및 제한 사항:

- 여러 개의 스위치 캡처 컨피그레이션 세션이 지원되지만 한 번에 하나의 스위치 캡처 세션만 활성화할 수 있습니다. 2개 이상의 캡처 세션을 활성화하면 "ERROR: 최대 1개의 활성 패킷 캡처 세션 제한에 도달했으므로 세션을 활성화하지 못했습니다."
- 활성 스위치 캡처를 삭제할 수 없습니다.
- 애플리케이션에서 스위치 캡처를 읽을 수 없습니다. 사용자는 파일을 내보내야 합니다.
- 덤프, 디코드, 패킷 번호, 추적 등의 특정 데이터 플레인 캡처 옵션은 스위치 캡처에 대해 지원되지 않습니다.
- 다중 컨텍스트 ASA의 경우 데이터 인터페이스의 스위치 캡처가 사용자 컨텍스트에서 구성됩니다. 이 스위치는 인터페이스 in_data_uplink1 및 in_mgmt_uplink1에서 캡처하며 관리 컨텍스트에서만 지원됩니다.

다음은 TAC 사례에서 패킷 캡처 사용을 기반으로 한 모범 사례 목록입니다.

- 지침 및 제한 사항에 유의하십시오.
- 캡처 필터를 사용합니다.

- 캡처 필터가 구성된 경우 NAT가 패킷 IP 주소에 미치는 영향을 고려하십시오.
- 프레임 크기를 지정하는 패킷 길이를 늘리거나 줄입니다(기본값 1518바이트와 다를 경우). 크기가 작으면 캡처된 패킷의 수가 증가하고, 그 반대의 경우도 마찬가지입니다.
- 필요에 따라 버퍼 크기를 조정합니다.
- `show cap <cap_name> detail` 명령 출력의 Drop Count에 주의하십시오. 버퍼 크기 제한에 도달하면 드롭 카운트 카운터가 증가합니다.

관련 정보

- [Firepower 4100/9300 Chassis Manager 및 FXOS CLI 컨피그레이션 가이드](#)
- [Cisco Secure Firewall 3100 시작 가이드](#)
- [Cisco Firepower 4100/9300 FXOS 명령 참조](#)

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.