# **Configure and Verify Secure Firewall and Firepower Internal Switch Captures**

## Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
High-Level Overview of the System Architecture
High-Level Overview of the Internal Switch Operations
Packet Flow and Capture Points
Configuration and Verification on Firepower 4100/9300
Packet Capture on a Physical or Port-channel Interface
Packet Captures on Backplane Interfaces
Packet Captures on Application and Application Ports
Packet Capture on a Subinterface of a Physical or Port-channel Interface
Packet Capture Filters
Collect Firepower 4100/9300 Internal Switch Capture Files
Guidelines, Limitations, and Best Practices for Internal Switch Packet Capture
Configuration and Verification on Secure Firewall 3100/4200
Packet Capture on a Physical or Port-channel Interface
Packet Capture on a Subinterface of a Physical or Port-channel Interface
Packet Capture on Internal Interfaces
Packet Capture Filters
Collect Secure Firewall Internal Switch Capture Files
Guidelines, Limitations, and Best Practices for Internal Switch Packet Capture
Related Information

## Introduction

This document describes the configuration and verification of the Firepower, and the Secure Firewall internal switch captures.

## Prerequisites

## Requirements

Basic product knowledge, capture analysis.

## **Components Used**

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

The information in this document is based on these software and hardware versions:

- Secure Firewall 31xx, 42xx
- Firepower 41xx
- Firepower 93xx
- Cisco Secure eXtensible Operating System (FXOS) 2.12.0.x
- Cisco Secure Firewall Threat Defense (FTD) 7.2.0.x, 7.4.1-172
- Cisco Secure Firewall Management Center (FMC) 7.2.0.x, 7.4.1-172
- Adaptive Security Appliance (ASA) 9.18(1)x, 9.20(x)
- Wireshark 3.6.7 (https://www.wireshark.org/download.html)

## **Background Information**

## High-Level Overview of the System Architecture

From the packet flow perspective, the architecture of the Firepower 4100/9300 and Secure Firewall 3100/4200 can be visualized as shown in this figure:



The chassis includes these components:

- **Internal switch** forwards packet from the network to the application and vice versa. The internal switch is connected to the **front interfaces** that reside on the built-in interface module or external network modules and connect to external devices, for example, switches. Examples of front interfaces are Ethernet 1/1, Ethernet 2/4, and so on. The "front" is not a strong technical definition. In this document, it is used to distinguish interfaces connected to external devices from the backplane or uplink interfaces.
- **Backplane or uplink** an internal interface that connects the security module (SM) to the internal switch.
- **Management uplink** an internal interface exclusive to Secure Firewall 3100/4200 that provides management traffic path between the internal switch and the application.

This table shows backplane interfaces on Firepower 4100/9300 and uplink interfaces on Secure Firewall 3100/4200:

Platform	Number of supported security modules	Backplane/uplink interfaces	Management uplink interfaces	Mapped application interfaces
Firepower 4100 (except Firepower 4110/4112)	1	SM1: Ethernet1/9 Ethernet1/10	N/A	Internal-Data0/0 Internal-Data0/1
Firepower 4110/4112	1	Ethernet1/9	N/A	Internal-Data0/0 Internal-Data0/1
Firepower 9300	3	SM1: Ethernet1/9 Ethernet1/10 SM2: Ethernet1/11 Ethernet1/12 SM3: Ethernet1/13 Ethernet1/14	N/A	Internal-Data0/0 Internal-Data0/1 Internal-Data0/0 Internal-Data0/1 Internal-Data0/0 Internal-Data0/1
Secure Firewall 3100	1	SM1: in_data_uplink1	in_mgmt_uplink1	Internal-Data0/1 Management1/1
ecure Firewall 4200 1 SM1: in_dat		SM1: in_data_uplink1 SM1: in_data_uplink2 (only 4245)	in_mgmt_uplink1 in_mgmt_uplink2	Internal-Data0/1 Internal-Data0/2 (only 4245) Management1/1 Management1/2

In the case Firepower 4100/9300 with 2 backplane interfaces per module or Secure Firewall 4245 with 2 data uplink interfaces, the internal switch and the applications on the modules perform traffic load-balancing over the 2 interfaces.

- Security module, security engine, or blade the module where applications such as FTD or ASA are installed. Firepower 9300 supports up to 3 security modules.
- **Mapped application interface** the names of the backplane or uplink interfaces in applications, such as FTD or ASA.

Use the show interface detail command to verify internal interfaces:

```
<#root>
>
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
```

## **High-Level Overview of the Internal Switch Operations**

#### Firepower 4100/9300

To make a forwarding decision the internal switch uses an **interface VLAN tag**, or **port VLAN tag**, and a **virtual network tag** (**VN-tag**).

The port VLAN tag is used by the internal switch to identify an interface. The switch inserts the port VLAN tag into each ingress packet that came on front interfaces. The VLAN tag is automatically configured by the system and cannot be manually changed. The tag value can be checked in the **fxos** command shell:

<#root> 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

The VN-tag is also inserted by the internal switch and used to forward the packets to the application. It is automatically configured by the system and cannot be manually changed.

The port VLAN tag and the VN-tag are shared with the application. The application inserts the respective egress interface VLAN tags and the VN-tags into each packet. When a packet from the application is received by the internal switch on the backplane interfaces, the switch reads the egress interface VLAN tag and the VN-tag, identifies the application and the egress interface, strips the port VLAN tag and the VN-tag, and forwards the packet to the network.

#### Secure Firewall 3100/4200

Like in Firepower 4100/9300, the port VLAN tag is used by the internal switch to identify an interface.

The port VLAN tag is shared with the application. The application inserts the respective egress interface VLAN tags into each packet. When a packet from the application is received by the internal switch on the uplink interface, the switch reads the egress interface VLAN tag, identifies the egress interface, strips the port VLAN tag, and forwards the packet to the network.

## **Packet Flow and Capture Points**

### Firepower 4100/9300 and Secure Firewall 3100

The Firepower 4100/9300 and the Secure Firewall 3100 firewalls support packet captures on the interfaces of the internal switch.

This figure shows the packet capture points along the packet path within the chassis and the application:



The capture points are:

- 1. Internal switch front interface ingress capture point. A front interface is any interface connected to the peer devices such as switches.
- 2. Data plane interface ingress capture point
- 3. Snort capture point
- 4. Data plane interface egress capture point
- 5. Internal switch backplane or uplink ingress capture point. A backplane or uplink interface connects the internal switch to the application.

The internal switch supports only ingress interface captures. That is only the packets received from the network or from the ASA/FTD application can be captured. **Egress packet captures are not supported.** 

#### Secure Firewall 4200

The Secure Firewall 4200 firewalls support packet captures on the interfaces of the internal switch. This figure shows the packet capture points along the packet path within the chassis and the application:



The capture points are:

- 1. Internal switch front interface ingress capture point. A front interface is any interface connected to the peer devices such as switches.
- 2. Internal switch backplane interface egress capture point.
- 3. Data plane interface ingress capture point
- 4. Snort capture point
- 5. Data plane interface egress capture point
- 6. Internal switch backplane or uplink ingress capture point. A backplane or uplink interface connects the internal switch to the application.
- 7. Internal switch front interface egress capture point.

The internal switch optionally supports bidirectional - both ingress and egress - captures. By default, the internal switch captures packets in the ingress direction.

## **Configuration and Verification on Firepower 4100/9300**

The Firepower 4100/9300 internal switch captures can be configured in **Tools > Packet Capture** on FCM or in **scope packet-capture** in FXOS CLI. For the description of the packet capture options refer to the *Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide* or *Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide* or *Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide* or *Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide* or *Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide* or *Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide* or *Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide* or *Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide* or *Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide* or *Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide* or *Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide* or *Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide* or *Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide* or *Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide* or *Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*, chapter **Troubleshooting**, section **Packet Capture**.

These scenarios cover common use cases of Firepower 4100/9300 internal switch captures.

## Packet Capture on a Physical or Port-channel Interface

Use the FCM and CLI to configure and verify a packet capture on interface Ethernet1/2 or Portchannel1 interface. In the case of a port-channel interface, ensure to select all physical member interfaces.

#### Topology, packet flow, and the capture points

		Chassis								
		Internal Switch		Security Module						
		Eth1//		FTD/ASA						
192.0.2.100	ICMP echo-request	Eth 1/3	Backplane							
198.51.100.100	CMP echo-reply									

#### Configuration

#### FCM

Perform these steps on FCM to configure a packet capture on interfaces Ethernet1/2 or Portchannel1:

#### 1. Use **Tools > Packet Capture > Capture Session** to create a new capture session:

Overview Interfaces Logical Devices Security Engine Platform Settings	System	Tools Help admin
	Packet Capture	Troubleshooting Logs
Capture Session Fitter List		
C Refresh	Capture Session Delet	e All Sessions
No Session available		

2. Select the interface **Ethernet1/2**, provide the session name and click **Save and Run** to activate the capture:

Overview Interfaces Logical Devices Security Engine Platform Settings				Sys	tem Tools Help admin
Select an instance: ftd1 v			Save and Run	Save Cancel	
ftd1	Session Name* Selected Interfaces	Cap1 Ethernet1/2			
Ethernet1/2	Buffer Size Snap length:	256 MB 💌 1518 Bytes			
Ethernet1/3	Store Packets	Overwrite Append			
Ethernet1/1 Ethernet1/9, Ethernet1/10	Capture Filter	Apply Filter Capture All			
Ethernet1/5 (Portchannels)					
Ethernet1/4 (Portchannel3)					

3. In the case of a port-channel interface, select all physical member interfaces, provide the session name and click **Save and Run** to activate the capture:

Overview Interfaces Logical Devices Security Engine Platform Settings					System Tools Help admin
Select an instance: ftd1			Save and Run	Save	Cancel
ftd1	Session Name* Selected Interfaces	cap1 Ethernet1/5, Ethernet1/4			
Ethernet1/2	Buffer Size	256 MB			
Ethernet/3	Snap length: Store Packets	1518 bytes Overwrite Append			
Ethernet1/1 Ethernet1/0, Ethernet1/10	Capture Filter	Apply Filter Capture All			
Educati/S (PortSannel)					
Ethernet1/4 (Portchannel1)					

### **FXOS CLI**

Perform these steps on FXOS CLI to configure a packet capture on interfaces Ethernet1/2 or Portchannel1:

1. Identify the application type and identifier:

<#root>							
firepower#							
scope ssa							
firepower , show app-in	/ssa # nstance						
App Name	Identifier Slot ID	Admin State	Oper State	Running Version	Startup	Version	Deploy T
ftd	ftdl						
1	Enabled	Online	7.2.0.82	7.2.0.82	Native	No	

2. In the case of a port-channel interface, identify its member interfaces:

<#root>								
firepowe	er#							
connect fxos								
<output firepowe show por</output 	skipped> er(fxos)# ct-channel summar	ry						
Flags:	D - Down I - Individual s - Suspended	P - Up in port-channel (members) H - Hot-standby (LACP only) r - Module-removed						

	S - Switcl U - Up (po M - Not in	hed R ort-chann n use. Mi	- Routed el) n-links no	t met	
Group	Port- Channel	Туре	Protocol	Member Ports	
1	Pol(SU)	Eth	LACP	Eth1/4(P)	Eth1/5(P)
3.	Create a capt	ure session	n:		
<#roo	t>				
firepo	ower#				
scope	packet-captu	ure			
firepo	ower /packet	-capture	#		
create	e session cap	p1			
firepo	ower /packet	-capture/	session* #		
create	e phy-port E	th1/2			
firepo	ower /packet	-capture/	session/ph	y-port* #	
firepo	ower /packet	-capture/	session/ph	y-port* #	
set a <u>r</u>	pp-identifie	r ftd1			
firepo up	ower /packet	-capture/	session/ph	y-port* #	
firepo enable	ower /packet	-capture/	session* #		
firepo commit	ower /packet	-capture/	session* #		
firepo	ower /packet	-capture/	session #		

For port-channel interfaces, a separate capture for each member interface is configured:

<#root>

```
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 #

#### Verification

FCM

Verify the Interface Name, ensure that the Operational Status is up and that the File Size (in bytes) increases:

Overview	Interfaces	Logical Devices Securi	ity Engine Platfor	rm Settings				System	Tools	Help	admin
Capture Ses	sion Fiter Lis	t									
							C Refresh Capture	Session Delete Al	Sessions		
	cap1	Drop Count: 0	Opera	ational State: up	Buffer Size: 256 MB		Snap Length: 1518	Bytes	(	۹. ( ۵	1
Interface Na	ame	Filter		File Size (in bytes)	File Name	Device Name					
Ethernet1/2		None		28632	cap1-ethernet-1-2-0.pcap	ftd1		$\pm$			

Portchannel1 with member interfaces Ethernet1/4 and Ethernet1/5:

Overview Interfaces Lo	gical Devices Security Engine Platform	Settings				Sy	stem Tools Help admin
Capture Session Filter List							
						C Refresh Capture Session	Delete All Sessions
🔺 🔳 cap1	Drop Count: 0	Operatio	onal State: up	Buffer Size: 256 MB		Snap Length: 1518 Bytes	
Interface Name	Filter		File Size (in bytes)	File Name	Device Name		
Ethernet1/S	None		160	cap1-ethernet-1-5-0.pcap	ftd1	*	
Ethernet1/4	None	L	85000	cap1-ethernet-1-4-0.pcap	ftd1	*	

#### **FXOS CLI**

Verify the capture details in scope packet-capture:

<#root>

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: O
Drop Count: O
```

```
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
```

Port-channel 1 with member interfaces Ethernet1/4 and Ethernet1/5:

<#root>

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
```

#### **Collect capture files**

Perform the steps in the section Collect Firepower 4100/9300 Internal Switch Capture Files.

#### Capture file analysis

Use a packet capture file reader application to open the capture file for Ethernet1/2. Select the first packet

and check the key points:

- 1. Only ICMP echo-request packets are captured. Each packet is captured and shown 2 times.
- 2. The original packet header is without the VLAN tag.
- 3. The internal switch inserts additional port VLAN tag **102** that identifies the ingress interface Ethernet1/2.
- 4. The internal switch inserts an additional VN tag.

No. Time	Source	Destination	Protocol	Length	PD	JP 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) reques	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 (48428)	64 Echo (ping) reques	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) reques	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) reques	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) reques	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) reques	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) reques	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) reques	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) reques	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) reques	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) reques	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) reques	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) reques	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) reques	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) reques	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) reques	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) reques	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) reques	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) reques	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) reques	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) reques	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) reques	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) reques	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) reques	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) reques	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) reques	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) reques	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) reques	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) reques	id=0x001a, seq=21/5376, ttl=64 (no response found!)
ć							
> Frame 1: 108 bytes on wire (864 bits	s), 108 bytes	captured (864 bits)	on interf	ace capture u	0 1, id 0		0000 58 97 bd b9 77 0e 00 50 56 9d e8 be 89 26 80 0a X···w··P V····&··
> Ethernet II, Src: VMware 9d:e8:be (6	00:50:56:9d:e8	:be), Dst: Cisco b9	:77:0e (58	:97:bd:b9:77:	0e)		0010 00 00 81 00 00 66 08 00 45 00 00 54 9d ec 40 00 ·····f··E··T··@·
VN-Tag							0020 40 01 af c0 c0 00 02 64 c6 33 64 64 08 00 4e a2 @·····d ·3dd··N·
1	= Direc	tion: From Bridge					0030 00 1a 00 07 f4 64 ce 62 00 00 00 00 20 a2 07 00 ·····d·b ····
.0	= Point	ter: vif id					8840 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b
	= Desti	ination: 10					1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ····· !"# \$%&'()"+
···· ··· ··· ··· ··· 0 ····	= Loope	ed: No					2000 2C 2d 2e 2t 30 31 32 33 34 35 36 37 ,/0123 4567
0	= Reser	ved: 0	-				
	= Versi	ion: 0					
0000 000	00 0000 = Sourc	e: 0					
Type: 802.10 Virtual LAN (0x8100)	)						
802.10 Virtual LAN, PRI: 0, DEI: 0,	ID: 102						
000 Briority: B	Best Effort (de	fault) (0)	-				
0 = DEI: Inelig	gible		21				
0000 0110 0110 = ID: 102			~				
Type: IPv4 (0x0800)							
> Internet Protocol Version 4, Src: 19	92.0.2.100, Ds	t: 198.51.100.100					
> Internet Control Message Protocol			2				

Select the second packet and check the key points:

- 1. Only ICMP echo-request packets are captured. Each packet is captured and shown 2 times.
- 2. The original packet header is without the VLAN tag.
- 3. The internal switch inserts additional port VLAN tag **102** that identifies the ingress interface Ethernet1/2.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info	1
E.	1 2022-07-13 06:23:58.285080930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (48428)	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	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 06:24:08.525092088	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!)
<								
5.6	rame 2: 102 bytes on wire (816 bit	s) 102 bytes (	cantured (816 hits)	on interface	canture u	e 1. id e		0000 58 97 bd b9 77 0e 00 50 56 9d e8 be 81 00 00 66 Xw.P.Vf
11	thernet II. Src: Wheare Odie8the (	00:50:56:0d:08	the) Det: Cisco b9	77:00 (58:07	·bd:b0:77:	0_1, 10 0		0010 08 00 45 00 00 54 9d ec 40 00 40 01 af c0 c0 00
J.	RA2 10 Virtual LAN DRT: A DET: A	ID: 102	.uej, ust. cisco_us			ve)		0020 02 64 c6 33 64 64 08 00 4e a2 00 1a 00 07 f4 64 ·d·3dd·· N·····d
18	and - Dejority	Rost Effort (do	fault) (0)					0030 ce 62 00 00 00 00 20 a2 07 00 00 00 00 00 10 11 .b
	a - DET: Ingli	sible	aure) (0)	2				0040 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21
	0000 0110 0110 - TO: 102	gible		2				0050 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 "#\$%&"() *+,/01
	Type: TPut (0x0000)							0060 32 33 34 35 36 37 234567
L.h	Internet Protocol Version 4. Spc: 1	92.0.2.100 Ds	198.51.100.100	-				
	Internet Control Message Protocol			2				
Ľ	internet control nessage Protocol			-				

Open the capture files for Portchannel1 member interfaces. Select the first packet and check the key points:

- 1. Only ICMP echo-request packets are captured. Each packet is captured and shown 2 times.
- 2. The original packet header is without the VLAN tag.
- 3. The internal switch inserts an additional port VLAN tag **1001** that identifies the ingress interface Portchannel1.
- 4. The internal switch inserts an additional VN tag.

No	o. Time	Source	Destination	Protocol	Length	PD		IP TTL Info		1				T
	- 1 2022-08-05 23:07:31.865872877	192.0.2.100	198.51.100.100	ICMP	108	0x322e (	(12846)	64 Echo (pin	) request	id=0x002d,	seq=245/62720,	ttl=64	(nc	
П	2 2022-08-05 23:07:31.865875131	192.0.2.100	198.51.100.100	ICMP	102	0x322e (	(12846)	64 Echo (pin	) 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 (pin	) 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 (pin	) 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 (pin	) 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 (pin	) 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 (pin	) 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 (pin	) 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 (pin	) 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 (pin	) 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 (pin	) 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 (pin	) 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 (pin	) 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 (pin	) 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 (pin	) 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 (pin	) 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 (pin	) 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 (pin	) 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 (pin	) request	id=0x002d,	seq=254/65024,	ttl=64	(nc	ŀ
<													>	
>	Frame 1: 108 bytes on wire (864 bits)	), 108 bytes cap	tured (864 bits) on	interface	capture_u0_3,	i 0000	a2 76	f2 00 00 25 00 50	56 9d e8	be 89 26 80	54 · v · · · % · P	V · · · · & · T	r i	
>	Ethernet II, Src: VMware_9d:e8:be (00	0:50:56:9d:e8:be	), Dst: a2:76:f2:00	:00:25 (a2	:76:f2:00:00:25	) 0010	00 00	81 00 03 e9 08 00	45 00 00	54 32 2e 40	00	E T2.@.	•	
	VN-Tag					0020	40 01	1b 7f c0 00 02 64	C6 33 64	64 08 00 1e	d6 @·····d	· 3dd · · · ·		
ш	1	= Directio	on: From Bridge			0030	00 20	00 15 d0 d2 e0 02	14 15 16	17 19 10 10	16			
ш	.0	= Pointer:	vif_id			0040	1c 1d	10 1f 20 21 22 23	24 25 26	27 28 29 2a	2b ···· l"#	\$%8'()*4		
ш	00 0000 0101 0100	= Destinat	ion: 84			0060	2c 2d	2e 2f 30 31 32 33	34 35 36	37	/0123	4567		
ш	0	···· = Looped:	No 4								,			
ш		= Reserved	1: 0											
ш		= Version:	0											
ш	0000 0000	0000 = Source:	0											
н	Type: 802.10 Virtual LAN (0x8100)													
1	802.1Q Virtual LAN, PRI: 0, DEI: 0, 1	(D: 1001	A.A. 444											
ш	000 Be Priority: Be	st Effort (defau	ult) (0)											
ш	0 = DEI: Ineligi	ble	2											
ш	0011 1110 1001 = ID: 1001													
Ы	Type: IPV4 (0x0800)													
Н	Internet Protocol Version 4, Src: 193	2.0.2.100, Dst:	198.51.100.100 2											
П	Incernet control Message Protocol		-											

Select the second packet and check the key points:

- 1. Only ICMP echo-request packets are captured. Each packet is captured and shown 2 times.
- 2. The original packet header is without the VLAN tag.
- 3. The internal switch inserts an additional port VLAN tag **1001** that identifies the ingress interface Portchannel1.

No	D. Time	Source	Destination	Protocol	Length	IP ID		IP T	TL Info							^
r.	1 2022-08-05 23:07:31.865872877	192.0.2.100	198.51.100.100	ICMP	108	Øx322e	(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	Øx3373	(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	Øx3373	(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	~
<															>	
>	Frame 2: 102 bytes on wire (816 bits	), 102 bytes capt	ured (816 bits) on	interface ca	pture_u0_3,	i 0000	a2 76	f2 00	00 25 0	00 50	56 9d e8	be 81 00 03	e9 ·v··%·P	v		
>	Ethernet II, Src: VMware_9d:e8:be (0)	0:50:56:9d:e8:be)	, Dst: a2:76:f2:00	:00:25 (a2:76	:f2:00:00:2	25) 0010	08 00	45 00	00 54	32 2e	40 00 40	01 1b 7f c0	00 ··E··T2.	0.0		
	802.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 1001				0020	02 64	c6 33	64 64 (	98 00	1e d6 00	2d 00 f5 a6	a2 ·d·3dd··			
н	000 Be	st Effort (defau	lt) (0)			0030	ed 62	00 00	00 00	7a 2f	0b 00 00	00 00 00 10	11 ·b····z/		1	
н	0 = DEI: Ineligi	ble	3			0040	12 13	14 15	16 17	18 19	1a 1b 1c	1d 1e 1f 20	21		1	
ш	0011 1110 1001 = ID: 1001		-			0050	22 23	24 25	26 27 1	28 29	2a 20 2C	2d 2e 2f 30	31 "#\$%&"()	*+,/01	é.	
н	Type: IPv4 (0x0800)					0000	32 33	34 35	30 37				234567			
	Internet Protocol Version 4, Src: 19	2.0.2.100, Dst: 1	98.51.100.100													
	Internet Control Message Protocol		2													

### Explanation

When a packet capture on a front interface is configured, the switch simultaneously captures each packet twice:

- After the insertion of the port VLAN tag.
- After the insertion of the VN tag.

In the order of operations, the VN tag is inserted at a later stage than the port VLAN tag insertion. However, in the capture file, the packet with the VN tag is shown earlier than the packet with the port VLAN tag.

This table summarizes the task:

Task	Capture point	Internal port VLAN in captured packets	Direction	Captured traffic
Configure and verify a packet capture on interface Ethernet1/2	Ethernet1/2	102	Ingress only	ICMP echo requests from host 192.0.2.100 to host 198.51.100.100
Configure and verify a packet capture on interface Portchannel1 with member interfaces Ethernet1/4 and Ethernet1/5	Ethernet1/4 Ethernet1/5	1001	Ingress only	ICMP echo requests from host 192.0.2.100 to host 198.51.100.100

## **Packet Captures on Backplane Interfaces**

Use the FCM and CLI to configure and verify a packet capture on backplane interfaces.

#### Topology, packet flow, and the capture points



#### Configuration

#### FCM

Perform these steps on FCM to configure packet captures on backplane interfaces:

1. Use **Tools > Packet Capture > Capture Session** to create a new capture session:

Overview Interfaces Logical Devices Security Engine Platform Settings		Syster	Tools	Help	admin
		Packet Capture	Trouble	shootin	g Logs
Capture Session Fitter List					
C Refr	esh C	Capture Session De	ete All Sessio	ns	
No Session available					

2. To capture packets on all backplane interfaces, select the application, then **All Backplane Ports** from the **Capture On** the dropdown list. Alternatively, choose the specific backplane interface. In this case, backplane interfaces Ethernet1/9 and Ethernet1/10 are available. Provide the **Session Name** and click **Save and Run** to activate the capture:

Overview Interfaces Logical Devices Security Engine	Platform Settings		System Tools Help admi
Select an instance: ftd1 💌			Save and Run Save Cancel
ftd1		Session Name*	cap1
		Selected Interfaces	None
Ethernet1/2		Buffer Size	256 MB 💌
		Snap length:	1518 Bytes
		Store Packets	Overwrite Append
		Capture On	Al Backplane Ports
Ethernet1/3	FTD	Capture Filter	ftd Ethernet1/9
	Ethemet1/9, Ethemet1/10		Ethernet1/10 Al Backplane Ports
Ethernet1/1			

#### **FXOS CLI**

Perform these steps on FXOS CLI to configure packet captures on backplane interfaces:

1. Identify the application type and identifier:

```
<#root>
firepower#
scope ssa
firepower /ssa#
show app-instance
App Name Identifier Slot ID Admin State Oper State Running Version Startup Version Deploy Ty
    _____ _____
ftd
        ftd1
     1
        Enabled Online 7.2.0.82 7.2.0.82 Native
                                                                               No
  2. Create a capture session:
<#root>
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 #
```

#### Verification

#### FCM

Verify the **Interface Name**, ensure that the **Operational Status** is up and that the **File Size (in bytes)** increases:

Overview Interfa	ces Logical Devices Security Engine	Platform Settings				System Tools H	elp admin
Capture Session F	iter List						
					Capture Session	Delete All Sessions	
ap1	Drop Count: 0	Operational State: up	Buffer Size: 256 MB		Snap Length: 1518 Bytes	_	
Interface Name	Filter	File Size (in bytes)	File Name	Device Name			
Ethernet1/10	None	194352	cap1-ethernet-1-10-0.pcap	ftd1	子		
Ethernet1/9	None	286368	cap1-ethernet-1-9-0.pcap	ftd1	<u>+</u>		

#### **FXOS CLI**

Verify the capture details in scope packet-capture:

<#root>

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

#### **Collect capture files**

Perform the steps in the section Collect Firepower 4100/9300 Internal Switch Capture Files.

#### Capture file analysis

Use a packet capture file reader application to open the capture files. In the case of more than 1 backplane interface, ensure to open all capture files for each backplane interface. In this case, the packets are captured on the backplane interface Ethernet1/9.

Select the first and the second packets, and check the key points:

- 1. Each ICMP echo request packet is captured and shown 2 times.
- 2. The original packet header is without the VLAN tag.
- 3. The internal switch inserts additional port VLAN tag **103** that identifies the egress interface Ethernet1/3.
- 4. The internal switch inserts an additional VN tag.

Ma	Time	Source	Destination	Protocol	Length	19.10	IR TTI Info		
-	1 2022-07-14 20:20:36 513854256	192.0.2.100	198 51 100 100	TCMP	108	By5998 (22928)	64 Echo (ning) requi	ast in	1-8x8991, seg=15/3848, ttl=64 (no response foundl)
T	2 2022-07-14 20:20:30:513054250	192.0.2.100	198.51.100.100	TCMP	108	0x5990 (22928)	64 Echo (ping) requi	ost in	=8x8881, seg=15/3848, tt]=64 (renly in 3)
	3 2022-07-14 20:20:36 514117304	198 51 100 100	192 0 2 100	TCMP	108	BXCC2C (52268)	64 Echo (ping) reply	, i/	=0x0001 seq=15/3840 ttl=64 (request in 2)
	A 2022-07-14 20:20:30:514119312	198.51.100.100	192.0.2.100	ICMP	108	BXCC2C (52268)	64 Echo (ping) reply	i	=8x8881, seg=15/3848, tt]=64
	5 2022-07-14 20:20:37 537723922	192 0 2 100	108 51 100 100	TCMP	108	0x5200 (23040)	64 Echo (ping) requi	ast in	=0x0001 seg=16/4006 ttl=64 (no response foundl)
	6 2022-07-14 20:20:37.537726588	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040)	64 Echo (ping) requi	est in	=0x0001, seq=16/4006, tt]=64 (renly in 7)
	7 2022-07-14 20:20:37 538046165	108 51 100 100	192 0 2 100	TCMP	109	avccab (52370)	64 Echo (ping) reply	1 30	=0x0001 seq=16/4006 tt]=64 (request in 6)
	8 2022-07-14 20:20:37.538048311	198.51.100.100	192.0.2.100	TCMP	108	0xcc9b (52379)	64 Echo (ping) reply		1=0x0001, seq=16/4096, tt]=64
	9 2022-07-14 20:20:39 561776064	192.0.2.100	198.51.100.100	TCMP	108	0x5ab7 (23223)	64 Echo (ping) requi	net in	=0x0001, seq=17/4352, ttl=64 (no response foundl)
	10 2022-07-14 20-20-20 561770210	102 0 2 100	109 51 100 100	TCMP	100	0x5ab7 (23223)	64 Echo (ping) requi	act in	(-0x0001, seq=17/4352, tt]=64 (renly in 11)
	11 2022-07-14 20:20:30:501770310	198.51.100.100	192.0.2.100	TCMP	108	0x5607 (25225) 0xccc4 (52420)	64 Echo (ping) reply	/ 5/	1-0x0001, seq=17/4352, tt]=64 (request in 10)
	12 2022-07-14 20:20:38:302040200	100 51 100 100	102 0 2 100	TCMP	100	0xccc4 (52420)	64 Echo (ping) reply		(-0x0001, seq=17/4352, tt1=64 (request 10 10)
	12 2022-07-14 20:20:30:302030333	102 0 2 100	100 51 100 100	TCMP	100	0x5b46 (323266)	64 Echo (ping) repri	art in	(-0x0001, seq=10/4500, tt]=64 (no response found))
	14 2022-07-14 20:20:39:303077043	192.0.2.100	198.51.100.100	TCMP	100	0x5b46 (23366)	64 Echo (ping) reque	est in	1-0x0001, seq=10/4000, ttl=64 (no response roundr)
	15 2022-07-14 20:20:39:303070433	109 51 100 100	102 0 2 100	TCND	100	0x5040 (25500)	64 Echo (ping) requi	- ir	-0x0001, seq=10/4600, ttl=64 (request in 14)
	16 2022-07-14 20:20:39:303930334	100 51 100 100	102.0.2.100	TCND	100	0xcd0d (52021)	64 Echo (ping) reply	, 10	-0x0001, seq-10/4000, tt1-04 (request 11 14)
	10 2022-07-14 20:20:39.383937900	103 0 3 100	102 51 100 100	TCNP	100	0xcuau (52021)	64 Echo (ping) repi	y it	-0x0001, seq=10/4000, tt1=04
	19 2022-07-14 20:20:40.009804804	102.0.2.100	100 51 100 100	TCND	100	0x5070 (23419)	64 Echo (ping) requi	ort in	-0x0001, seg-19/4004, ttl=64 (norly in 10)
	10 2022-07-14 20:20:40.009807018	100 51 100 100	198.51.100.100	ICHP	100	0x5070 (23419)	64 Echo (ping) reque	est it	-0x0001, seq=19/4804, ttl=64 (reply in 19)
	19 2022-07-14 20.20.40.010179085	100 51 100 100	102.0.2.100	TCHP	100	0xcd8f (52023)	64 Echo (ping) reply		-0x0001, seg=19/4004, tt1=04 (request 10 10)
	20 2022-07-14 20:20:40:010181944	102 0 2 100	109 51 100 100	ICMP	100	0x5b7e (32023)	64 Echo (ping) repi	oct in	(-0x0001, seq=19/4004, ttl=04
	21 2022-07-14 20:20:41:033003133	102.0.2.100	100 51 100 100	TCMD	100	0x507e (23422)	64 Echo (ping) reque	est it	-0x0001, seq=20/5120, ttl=04 (no response round)
	22 2022-07-14 20.20.41.033800997	100 51 100 100	198.31.100.100	TCHP	100	0x307e (23422)	64 Echo (ping) reque	est It	-0x0001, seq=20/5120, ttl=04 (reply 11 25)
	23 2022-07-14 20:20:41.034084102	198.51.100.100	102.0.2.100	TCMP	108	0xce36 (52790)	64 Echo (ping) reply	, 10	(-0x0001, seq=20/5120, tt1=64 (request in 22)
	24 2022-07-14 20.20.41.034083308	103.0.3.100	100 51 100 100	TCHP	100	0xCES0 (32790)	64 Echo (ping) repry	ant in	-0x0001, seq-20/5120, ttl-64 (no perpense found))
	25 2022-07-14 20:20:42.057709898	192.0.2.100	198.51.100.100	TCMP	100	0x5010 (25536)	64 Echo (ping) reque	est it	(-0x0001, seq=21/5376, tt1=64 (no response round:)
	26 2022-07-14 20:20:42.657/11660	192.0.2.100	198.51.100.100	TCHP	108	0x5010 (23536)	64 Echo (ping) reque	est it	1-0x0001, seq=21/53/6, ttl=64 (repry 10 2/)
	27 2022-07-14 20:20:42.657980675	198.51.100.100	192.0.2.100	ICMP	108	0xce49 (52809)	64 Echo (ping) reply	/ 10	1=0x0001, seq=21/53/6, ttl=64 (request in 26)
	28 2022-07-14 20:20:42.65/9819/1	198.51.100.100	192.0.2.100	ICHP	108	0xce49 (52809)	64 Echo (ping) reply	/ 10	J=0x0001, Seq=21/5576, tt1=04
Ц.,	29 2022-07-14 20:20:43.081/3009/	192.0.2.100	198.51.100.100	ICMP	108	0X5C52 (23634)	64 Ecno (ping) reque	est 10	1=0x0001, seq=22/5632, tt1=64 (no response tound1)
<									
>	Frame 1: 108 bytes on wire (864 bit	ts), 108 bytes o	aptured (864 bits)	on interface	e capture_u	0_8, id 0		0000	00 50 56 9d e7 50 58 97 bd b9 77 2d 89 26 00 00 PV PX - w - & -
>	Ethernet II, Src: Cisco b9:77:2d (	58:97:bd:b9:77:2	d), Dst: VMware_9d	:e7:50 (00:50	9:56:9d:e7:	50)		0010	) 00 0a 81 00 00 67 08 00 45 00 00 54 59 90 40 00 ·····g··E··TY·@·
4	VN-Tag							0026	1 40 01 f4 1c c0 00 02 64 c6 33 64 64 08 00 22 68 @·····d ·3dd··"h
	0	= Direc	tion: To Bridge					0036	00 01 00 0f 89 7a d0 62 00 00 00 00 b3 d7 09 00z·b
	.0	= Point	er: vif_id					0040	00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b
		= Desti	nation: 0					0050	1 10 10 10 17 20 21 22 23 24 25 26 27 28 29 28 20 ···· 1"# \$78"()"+
	0 0	= Loope	d: No	A				0000	2C 20 2e 2t 30 31 32 33 34 35 36 37 ,/0123 4567
	0	= Reser	ved: 0	- I					
	60	= Versi	on: 0						
	0000 00	00 1010 = Sourc	e: 10						
	Type: 802.10 Virtual LAN (0x8100	)							
4	802.10 Virtual LAN, PRI: 0, DEI: 0	, ID: 103							
	000 = Priority:	Best Effort (de	fault) (0)	-					
	0 = DEI: Ineli	gible		2					
	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			2					
				-					

Select the third and the fourth packets, and check the key points:

- 1. Each ICMP echo reply is captured and shown 2 times.
- 2. The original packet header is without the VLAN tag.
- 3. The internal switch inserts additional port VLAN tag **102** that identifies the egress interface Ethernet1/2.

#### 4. The internal switch inserts an additional VN tag.

1 202-07-14 202:05.51185425       192.0.2.100       105.51.100.100       ICVP       108       0x5900 (2228)       64 fcho (ping) request       id=0x0001, seq=15/3840, ttl=64 (recpust n 2)         3 2022-07-14 202:05.511857269       192.0.2.100       108.51.100.100       102.0.2.100       ICVP       108       0x5200 (2288)       64 fcho (ping) request       id=0x0001, seq=15/3840, ttl=64 (recpust n 2)         4 2022-07-14 202:05.511871209       190.51.100.100       192.0.2.100       108.51.100.100       ICVP       108       0x5200 (2388)       64 fcho (ping) request       id=0x0001, seq=15/3840, ttl=64 (request n 2)         6 2022-07-14 202:07.53804151       192.0.2.100       108.51.100.100       ICVP       108       0x5300 (23840)       64 fcho (ping) request       id=0x0001, seq=16/4806, ttl=64 (request in 6)         7 2022-07-14 202:07.53804151       196.51.100.100       120.0.2.100       ICVP       108       0x5300 (23840)       64 fcho (ping) request       id=0x0001, seq=16/4806, ttl=64 (request in 6)         8 2022-07-14 202:07.53804151       196.51.100.100       ICVP       108       0x5200 (2233)       64 fcho (ping) request       id=0x0001, seq=17/4352, ttl=64 (request in 6)         10 2022-07-14 202:07.53804151       196.51.100.100       ICVP       108       0x5260 (2332)       64 fcho (ping) request       id=0x0001, seq=17/4352, ttl=64 (request in 6)         10
+ 2 2022-07-14 202:03.6 511857289 192.0.2.100 195.0.5.1000.100 1C/P 108 pt 0.6.2.100 1079 108 11 00.010 192.0.2.100 108 11 00.010 192.0.2.100 108 11 00.010 192.0.2.100 108 11 00.010 192.0.2.100 108 11 00.010 192.0.2.100 108 0x300 (23840) 64 Echo (ping) reply i id-0x001, seq=15/3840, ttl=64 (request in 2) id-0x001, seq=15/3840, ttl=64 (request in 6) id-0x001, seq=15/380, ttl=64 (request in 10) id-0x001, seq=15/380, ttl=64 (request in 10) id-0x001, seq=17/4352, ttl=64 (request in 14) id-0x001, seq=17/4352, ttl=64 (request in 14) id-0x001, seq=17/4352, ttl=64 (request in 14) id-0x001, seq=17/4352, ttl=64 (reqluest in 14) id-0x001, seq=13/4088, ttl=64 (reqluest in 14) id-0x001, seq=13/4088, ttl=64 (reqluest in 14) id-0x00
3         3         2022-07-14         2020-265.51411391         198.51.100.100         1029         108         0xcc2c         658         Ech (ping) reply id=xx0001, seq=15/3840, tl=64 (request in 2)           5         2022-07-14         202:07.53772558         192.0.2.100         198.51.100.100         1CP         108         0x5300         64 Echo (ping) reply id=x00001, seq=15/3840, tl=64 (request in 2)           7         2022-07-14         202:07.53772558         192.0.2.100         198.51.100.100         1CP         108         0x5300         63460         (ping) request         id=x00001, seq=16/4096, tl=64 (request in 6)           8         2022-07-14         202:07.538046151         198.51.100.100         1CP         108         0x5300         632400         64 Echo (ping) request         id=x00001, seq=16/4096, tl=64 (request in 6)           8         2022-07-14         202:07.538048311         198.51.100.100         1CP         108         0x5307         62232         64 Echo (ping) request         id=x00001, seq=17/4352, tl=64 (request in 2)           10         2022-07-14         202:07.538048311         198.51.100.100         102.02.100         1CP         108         0x5207         2223.02         64 Echo (ping) request         id=x00001, seq=17/4352, tl=64 (request in 2)           12         2022-07.14         202
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $
5 2022-07-14       20:20:37:53772382       192.0.2.100       198.51.100.100       ICMP       108       0x5a00       20:400       64 Echo (ping) request       id-ox0001, seq-16/4006, ttl-64 (no response found))         7 2022-07-14       20:20:37.538046315       198.51.100.100       192.0.2.100       ICMP       108       0x5a00       20:400       64 Echo (ping) reply       id-ox0001, seq-16/4006, ttl-64 (request in 6)         8 2022-07-14       20:20:37.538046311       192.0.2.100       192.0.2.100       ICMP       108       0xcc0b       (52379)       64 Echo (ping) request       id-ox0001, seq-16/4006, ttl-64 (request in 6)         9 2022-07-14       20:20:38.56177634       192.0.2.100       198.51.100.100       ICMP       108       0xcc0b       (52379)       64 Echo (ping) request       id-ox0001, seq-16/4006, ttl-64 (request in 0)         12 2022-07-14       20:20:38.561776341       192.0.2.100       ICMP       108       0xcccd       (52420)       64 Echo (ping) request       id-ox0001, seq-16/4006, ttl-64 (request in 10)         12 2022-07-14       20:20:38.56270833       192.0.2.100       ICMP       108       0xcccd       (52420)       64 Echo (ping) reqly       id-ox001, seq-16/4006, ttl-64 (request in 10)         12 2022-07-14       20:20:38.56270833       192.0.2.100       ICMP       108       0xcccds       (
6 2022-07-14       20:20:37:53726588       192.0.2.100       198.51.100.100       192.0.2.100       ICMP       108       0x5cb0       (23040)       64 Echo (ping) regust       id-0x0001, seq-16/4005, ttl-64 (requy in 7)         7 2022-07-14       20:20:37.538046155       198.51.100.100       192.0.2.100       ICMP       108       0xccb       (5237)       64 Echo (ping) reply       id-0x0001, seq-16/4005, ttl-64 (requy in 16)         9 2022-07-14       20:20:37.538046155       198.51.100.100       198.51.100.100       ICMP       108       0xccb       (5237)       64 Echo (ping) reply       id-0x0001, seq-16/4005, ttl-64 (reqly in 17)         10 2022-07-14       20:20:37.5370454       192.0.2.100       198.51.100.100       17.0P       108       0xccb       (522.40)       64 Echo (ping) reply       id-0x001, seq-17/4352, ttl-64       (reply in 11)         11 2022-07-14       20:20:37.56205033       198.51.100.100       17.0P       108       0xcccd       (524.40)       64 Echo (ping) reply       id-0x001, seq-17/4352, ttl-64       (reply in 13)         12 2022-07-14       20:20:37.556205033       198.51.100.100       17.0P       108       0xccd       (524.60)       64 Echo (ping) reply       id-0x001, seq-18/4068, ttl-64 (no response found])         14 2022-07-14       20:20:37.558597004       198.51.100.100       198.5
7 2022-07-14       20:20:27:538464515       198:51.100.100       109:92.0.2.100       ICMP       180       wcccbb (52379)       64 Echo (ping) reply       id-exo801, seq=16/4096, ttl-64         8 2022-07-14       20:20:37.538464511       195.6.1.100.100       ICMP       180       wcccbb (52379)       64 Echo (ping) request       id-exo801, seq=16/4096, ttl-64         9 2022-07-14       20:20:37.538464511       192.0.2.100       198.51.100.100       ICMP       180       wcccbb (52379)       64 Echo (ping) request       id-exo801, seq=17/4352, ttl-64 (no response found])         10 2022-07-14       20:20:37.538464511       192.0.2.100       198.51.100.100       ICMP       180       wccccd (52420)       64 Echo (ping) request       id-exo801, seq=17/4352, ttl-64 (no response found])         12 2022-07-14       20:20:35.5577043       198.51.100.100       ICMP       180       wccccd (52420)       64 Echo (ping) reply       id-exo801, seq=18/4668, ttl-64 (no response found])         14 2022-07-14       20:20:35.55577043       198.51.100.100       ICMP       180       wccded (52621)       64 Echo (ping) reply       id-exo801, seq=16/4068, ttl-64 (no response found])         14 2022-07-14       20:20:35.5557743       198.51.100.100       ICMP       180       wccded (52621)       64 Echo (ping) reply       id-exo801, seq=16/4068, ttl-64 (no response found])      <
8 2022-07-14 20:20:37.538048311       198.51.100.100       192.0.2.100       1CMP       108       0xccb (52379)       64 Echo (ping) regly       id=0x0001, seq=17/4352, ttl=64         9 2022-07-14 20:20:38.561776810       192.0.2.100       198.51.100.100       ICMP       108       0xcba7 (23223)       64 Echo (ping) reguest       id=0x0001, seq=17/4352, ttl=64 (regly in 11)         11 2022-07-14 20:20:38.561776810       192.0.2.100       198.51.100.100       ICMP       108       0xccc4 (52420)       64 Echo (ping) reguest       id=0x0001, seq=17/4352, ttl=64 (regly in 11)         12 2022-07-14 20:20:38.56240833       198.51.100.100       192.0.2.100       ICMP       108       0xccc4 (52420)       64 Echo (ping) regly       id=0x0001, seq=17/4352, ttl=64         13 2022-07-14 20:20:38.56240833       198.51.100.100       192.0.2.100       ICMP       108       0xccc4 (52420)       64 Echo (ping) regly       id=0x0001, seq=18/4068, ttl=64       (request in 10)         14 2022-07-14 20:20:39.5857043       192.0.2.100       IGMP       108       0xccds (2326)       64 Echo (ping) regly       id=0x0001, seq=18/4068, ttl=64       (request in 14)         16 2022-07-14 20:20:39.585970515       192.0.2.100       IGMP       108       0xccds (52621)       64 Echo (ping) regly       id=0x0001, seq=18/4068, ttl=64       (request in 14)         16 2022-07-14 20:20:40.600805484<
9 2022-07-14       20:20:33.561776064       192.0.2.100       196.51.100.100       1CVP       108       0x5h7 (23223)       64 Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (no response found])         10 2022-07-14       20:20:35.561778310       192.0.2.100       1CVP       108       0x5h7 (23223)       64 Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (request in 10)         12 2022-07-14       20:20:35.56270831       196.51.100.100       192.0.2.100       ICVP       108       0xccc4 (52420)       64 Echo (ping) reply       id=0x0001, seq=17/4352, ttl=64 (request in 10)         12 2022-07-14       20:20:35.56270831       196.51.100.100       192.0.2.100       ICVP       108       0xccc4 (52420)       64 Echo (ping) reply       id=0x0001, seq=17/4352, ttl=64 (request in 10)         14 2022-07-14       20:20:35.56570841       192.0.2.100       ICVP       108       0xccc4 (52420)       64 Echo (ping) request id=0x001, seq=17/4352, ttl=64 (request in 10)         14 2022-07-14       20:20:35.56570841       192.0.2.100       ICVP       108       0xccda (52621)       64 Echo (ping) request id=0x001, seq=17/4352, ttl=64 (request in 14)       10         16 2022-07-14       20:20:35.55570845       192.0.2.100       ICVP       108       0xcdad (52621)       64 Echo (ping) request id=0x001, seq=18/4068, ttl=64 (request in 14)       10       10       10       10
10       2022-07-14       20:20-714
11 2022-07-14 20:20:30.556205033       198.51.100.100 192.0.2.100       ICMP       108       0xcccd (5x420)       64 Echo (ping) reply       id-ox0001, seq=17/4352, ttl-64 (request in 10)         12 2022-07-14 20:20:30.556205033       198.51.100.100 192.0.2.100       ICMP       108       0xcccd (5x420)       64 Echo (ping) reply       id-ox0001, seq=17/4352, ttl-64 (no response found1)         14 2022-07-14 20:20:30.5567043       192.0.2.100       198.51.100.100       ICMP       108       0xcccd (5x420)       64 Echo (ping) request       id-ox0001, seq=17/4352, ttl-64 (no response found1)         14 2022-07-14 20:20:30.58567043       192.0.2.100       198.51.100.100       ICMP       108       0xcdsd (5261)       64 Echo (ping) request       id-ox0001, seq=18/4008, ttl-64 (no response found1)         16 2022-07-14 20:20:30.585930554       192.0.2.100       ICMP       108       0xcdsd (52621)       64 Echo (ping) request       id-ox0001, seq=18/4008, ttl-64 (request in 14)         16 2022-07-14 20:20:40.60930464       192.0.2.100       ISM.100.100       ICMP       108       0xcdsd (52623)       64 Echo (ping) request       id-ox001, seq=18/4008, ttl-64 (no response found1)         18 2022-07-14 20:20:40.609304561       192.0.2.100       ISM.100.100       ICMP       108       0xcdsd (52623)       64 Echo (ping) request       id-ox0001, seq=19/4864, ttl-64 (no response found1)         19 2022-07-14 2
12 2022-07-14 20:20:38.562650333       198.51.100.100       192.0.2.100       ICMP       108       0xcccd (5X20)       64 Echo (ping) reply       id-0x0001, seq=17/4352, ttl=64         13 2022-07-14 20:20:39.58567403       192.0.2.100       198.51.100.100       ICMP       108       0x5bd6 (23366)       64 Echo (ping) reply       id-0x0001, seq=17/4352, ttl=64         14 2022-07-14 20:20:39.58567403       192.0.2.100       198.51.100.100       ICMP       108       0x5bd6 (23366)       64 Echo (ping) reply       id-0x0001, seq=18/4068, ttl=64       (reply in 15)         15 2022-07-14 20:20:39.58593554       198.51.100.100       ICMP       108       0xcddd (52621)       64 Echo (ping) reply       id-0x0001, seq=18/4068, ttl=64       (reply in 15)         16 2022-07-14 20:20:40.609804804       192.0.2.100       ICMP       108       0xcddd (52621)       64 Echo (ping) reply       id-0x0001, seq=18/4068, ttl=64       (reply in 14)         18 202-07-14 20:20:40.609804804       192.0.2.100       198.51.100.100       ICMP       108       0xcdf (52623)       64 Echo (ping) reply       id-0x0001, seq=19/4864, ttl=64       (reply in 19)         19 2022-07-14 20:20:40.609804804       192.0.2.100       ICMP       108       0xcdf (52623)       64 Echo (ping) reply       id-0x0001, seq=19/4864, ttl=64       (reply in 19)         20 202-07-14 20:20:40.610180551
13 2022-07-14 20:20:30.585770431       192.0.2.100       198.51.100.100       ICMP       108       0x5bd6 (23366)       64 Echo (ping) request id-0x0001, seq=18/4608, ttl=44 (no response found!)         14 2022-07-14 20:20:30.5855770451       192.0.2.100       198.51.100.100       ICMP       108       0x5bd6 (23366)       64 Echo (ping) request id-0x0001, seq=18/4608, ttl=44 (no response found!)         15 2022-07-14 20:20:30.585930554       198.51.100.100       192.0.2.100       ICMP       108       0x5bd6 (23366)       64 Echo (ping) request id-0x0001, seq=18/4608, ttl=44 (request in 14)         16 2022-07-14 20:20:30.585930554       198.51.100.100       192.0.2.100       ICMP       108       0xcd8d (52621)       64 Echo (ping) reqly       id-0x0001, seq=18/4608, ttl=44 (request in 14)         17 2022-07-14 20:20:40.609984644       192.0.2.100       ICMP       108       0xc5b7 (23419)       64 Echo (ping) request id-0x0001, seq=18/4608, ttl=64 (no response found!)         18 2022-07-14 20:20:40.601079685       198.51.100.100       192.0.2.100       ICMP       108       0xc5b7 (2342)       64 Echo (ping) reqly       id-0x0001, seq=19/4864, ttl=64 (no response found!)         20 2022-07-14 20:20:40.6101818144       198.51.100.100       1CMP       108       0xc5b7 (2342)       64 Echo (ping) reqly       id-0x0001, seq=19/4864, ttl=64 (no response found!)         21 2022-07-14 20:20:41.633005971       192.0.2.100
14 2022-07-14 20:20:30.58578455       192.0.2.100       198.51.100.100       192.0.2.100       ICMP       108       0x5ds6 (23366)       64 Echo (ping) request       id-0x0001, seq-18/4608, ttl-64 (request in 14)         15 2022-07-14 20:20:30.585937506       198.51.100.100       192.0.2.100       ICMP       108       0xcdsd (52621)       64 Echo (ping) reply       id-0x0001, seq-18/4608, ttl-64 (request in 14)         16 2022-07-14 20:20:30.585937506       198.51.100.100       192.0.2.100       ICMP       108       0xcdsd (52621)       64 Echo (ping) reply       id-0x0001, seq-18/4608, ttl-64         17 2022-07-14 20:20:40.609807618       192.0.2.100       198.51.100.100       ICMP       108       0x5b7 (22419)       64 Echo (ping) reply       id-0x0001, seq-18/4608, ttl-64         18 2022-07-14 20:20:40.609807618       198.51.100.100       ICMP       108       0x5b7 (22419)       64 Echo (ping) reply       id-0x0001, seq-19/4664, ttl-64 (reply in 19)         19 2022-07-14 20:20:40.610181944       198.51.100.100       ICMP       108       0xcdsf (52623)       64 Echo (ping) reply       id-0x0001, seq-19/4664, ttl-64 (reply in 19)         20 202-07-14 20:20:40.610181944       198.51.100.100       ICMP       108       0xcdsf (52623)       64 Echo (ping) reply       id-0x001, seq-20/5120, ttl-64 (reply in 2)         21 2022-07-14 20:20:41.633080571       198.51.100.100
15 2022-07-14 20:20:39.585936554       198.51.100.100       192.0.2.100       ICMP       108       0xcd8d (52621)       64 Echo (ping) reply       id=0x0001, seq=18/4608, ttl=64 (request in 14)         16 2022-07-14 20:20:40.60980864       198.51.100.100       192.0.2.100       ICMP       108       0xcd8d (52621)       64 Echo (ping) reply       id=0x0001, seq=18/4608, ttl=64 (request in 14)         16 2022-07-14 20:20:40.60980864       192.0.2.100       ICMP       108       0xc3b7b (22419)       64 Echo (ping) reply       id=0x0001, seq=18/4608, ttl=64 (request in 14)         18 2022-07-14 20:20:40.60980864       192.0.2.100       198.51.100.100       ICMP       108       0xc3b7b (22419)       64 Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (request in 14)         19 2022-07-14 20:20:40.608087618       192.0.2.100       198.51.100.100       ICMP       108       0xc3b7b (22419)       64 Echo (ping) request id=0x001, seq=19/4864, ttl=64 (request in 18)         20 2022-07-14 20:20:40.610181944       198.51.100.100       120.2.100       ICMP       108       0xc3b7 (22422)       64 Echo (ping) reply       id=0x0001, seq=19/4864, ttl=64 (request in 18)         21 2022-07-14 20:20:41.63180513       192.0.2.100       198.51.100.100       ICMP       108       0xc3b7 (22422)       64 Echo (ping) request id=0x001, seq=20/5120, ttl=64 (request in 22)       22 2022-07-14 20:20:41.633806971       192.0.2.100
16 2022-07-14 20:20:30.589397900       198.51.100.100       192.0.2.100       1CVP       108       excdd (53521)       64 Echo (ping) reply       id-ex0001, seq-18/4608, ttl-64         17 2022-07-14 20:20:40.609804604       192.0.2.100       198.51.100.100       1CVP       108       exc5b7b (23419)       64 Echo (ping) reply       id-ex0001, seq-19/4864, ttl-64 (no response found)         18 2022-07-14 20:20:40.609807605       198.51.100.100       109.51.100.100       ICVP       108       exc5b7b (23419)       64 Echo (ping) request       id-ex0001, seq-19/4864, ttl-64 (reply in 19)         19 2022-07-14 20:20:40.609807605       198.51.100.100       102.92.100       ICVP       108       excdsf (52623)       64 Echo (ping) reply       id-ex0001, seq-19/4864, ttl-64 (reply in 19)         20 2022-07-14 20:20:40.60181944       198.51.100.100       12V.P       108       excdsf (52623)       64 Echo (ping) reply       id-ex0001, seq-19/4864, ttl-64       (reqly in 18)         21 2022-07-14 20:20:41.633806571       192.0.2.100       198.51.100.100       ICVP       108       excdsf (52623)       64 Echo (ping) reply       id-ex001, seq-20/5120, ttl-64 (reply in 23)         22 2022-07-14 20:20:41.633806571       192.0.2.100       198.51.100.100       ICVP       108       exc36 (52790)       64 Echo (ping) reply       id-ex001, seq-20/5120, ttl-64 (reply in 23)         24 2022-07
17 2022-07-14 20:20:40.609804804       192.0.2.100       198.51.100.100       ICMP       108       0x557b (22419)       64 Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (no response found!)         18 2022-07-14 20:20:40.609804804       192.0.2.100       198.51.100.100       ICMP       108       0x557b (22419)       64 Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (no response found!)         19 2022-07-14 20:20:40.609807618       192.0.2.100       199.51.100.100       ICMP       108       0x557b (22419)       64 Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (request in 18)         20 2022-07-14 20:20:40.610170651       192.0.2.100       192.0.2.100       ICMP       108       0xcdsf (52623)       64 Echo (ping) request id=0x001, seq=20/5120, ttl=64 (request in 18)         21 2022-07-14 20:20:41.633805151       192.0.2.100       198.51.100.100       ICMP       108       0xcdsf (52623)       64 Echo (ping) request id=0x001, seq=20/5120, ttl=64 (reqly in 23)         22 2022-07-14 20:20:41.633805151       192.0.2.100       198.51.100.100       ICMP       108       0xcdsf (52709)       64 Echo (ping) request id=0x001, seq=20/5120, ttl=64 (reqly in 23)         23 2022-07-14 20:20:41.633805157       192.0.2.100       198.51.100.100       ICMP       108       0xc356 (52790)       64 Echo (ping) request id=0x001, seq=20/5120, ttl=64 (reqly in 23)         24 2022-07-14 20:20:42.6577080588       198.51.100.100
18 2022-07-14 20:20:40.609807618       192.0.2.100       198.51.100.100       ICMP       108       0x557b (23419)       64 Echo (ping) request id-0x0001, seq-19/4864, ttl-64 (request in 19)         19 2022-07-14 20:20:40.601879865       198.51.100.100       192.0.2.100       ICMP       108       0x567b (23419)       64 Echo (ping) request id-0x0001, seq-19/4864, ttl-64 (request in 18)         20 2022-07-14 20:20:40.601879865       198.51.100.100       192.0.2.100       ICMP       108       0x567b (2342)       64 Echo (ping) request id-0x0001, seq-19/4864, ttl-64 (request in 18)         21 2022-07-14 20:20:41.633806571       192.0.2.100       198.51.100.100       ICMP       108       0x55b7 (23422)       64 Echo (ping) request id-0x0001, seq-20/5120, ttl-64 (reply in 23)         22 2022-07-14 20:20:41.633806571       192.0.2.100       198.51.100.100       ICMP       108       0x55b7 (23422)       64 Echo (ping) request id-0x001, seq-20/5120, ttl-64 (reply in 23)         23 2022-07-14 20:20:41.634884102       198.51.100.100       1CMP       108       0x55b7 (235270)       64 Echo (ping) request id-0x001, seq-20/5120, ttl-64 (reply in 23)         24 2022-07-14 20:20:42.657708058       198.51.100.100       ICMP       108       0x5cb7 (23570)       64 Echo (ping) request id-0x001, seq-20/5120, ttl-64       (request in 22)         25 2022-07-14 20:20:42.657708058       192.0.2.100       192.0.2.100       ICMP
10       Dirit of 14       20:20:07-14 <td< td=""></td<>
15 002:07-14 20:20:40.61081934       198.51.100.100 192.0.2.100       ICW       108       0xCd8f (5262)       64 Echo (ping) reply       1d=0x00001, seq=15/4000, (IC=0 (reples) in 10)         21 2022-07-14 20:20:40.61081944       198.51.100.100 192.0.2.100       ICW       108       0xCd8f (5262)       64 Echo (ping) reply       id=0x0001, seq=20/5120, tI1-64 (no response found)         22 2022-07-14 20:20:41.63300057       198.51.100.100 198.51.100.100       ICW       108       0xCd8f (5262)       64 Echo (ping) reply       id=0x0001, seq=20/5120, tI1-64 (reply in 23)         22 2022-07-14 20:20:41.63300057       198.51.100.100       ICW       108       0xCsbr (2342)       64 Echo (ping) reply       id=0x0001, seq=20/5120, tI1-64 (reply in 23)         23 2022-07-14 20:20:41.634084102       198.51.100.100       ICW       108       0xCsbr (2322)       64 Echo (ping) reply       id=0x0001, seq=20/5120, tI1-64 (reply in 23)         24 2022-07-14 20:20:42.657708988       198.51.100.100       ICW       108       0xCsbr (2353)       64 Echo (ping) reply       id=0x0001, seq=21/5370, tt1-64 (no response found])         25 2022-07-14 20:20:42.657708988       192.0.2.100       198.51.100.100       ICW       108       0x5bf0 (23536)       64 Echo (ping) request id=0x0001, seq=21/5376, tt1-64 (no response found])         26 2022-07-14 20:20:42.657708988       192.0.2.100       198.51.100.100       ICW
20 2022-07-14 20:20:41.63380533       1392.0.2.100       198.51.100.100       1CMP       108       0x55br (23422)       64 Etho (ping) request id-0x060; seq=20/5126; ttl-64 (no response found1)         22 2022-07-14 20:20:41.63380537       192.0.2.100       198.51.100.100       1CMP       108       0x55br (23422)       64 Etho (ping) request id-0x060; seq=20/5126; ttl-64 (no response found1)         22 2022-07-14 20:20:41.63380543       198.51.100.100       198.51.100.100       12CMP       108       0x55br (23422)       64 Etho (ping) request id-0x060; seq=20/5126; ttl-64 (nequest in 22)         24 2022-07-14 20:20:41.634805402       198.51.100.100       12CMP       108       0xcc36 (52790)       64 Etho (ping) request id-0x0601; seq=20/5126; ttl-64 (request in 22)         24 2022-07-14 20:20:42.657708088       192.0.2.100       108.51.100.100       1CMP       108       0xcc36 (52790)       64 Etho (ping) request id-0x0601; seq=20/5126; ttl-64       (ne response found1)         25 2022-07-14 20:20:42.657708088       192.0.2.100       198.51.100.100       ICMP       108       0x5bf0 (23536)       64 Etho (ping) request id-0x0601; seq=21/5376; ttl-64 (no response found1)         26 2022-07-14 20:20:42.657708088       192.0.2.100       198.51.100.100       ICMP       108       0x5bf0 (23536)       64 Etho (ping) request id-0x061; seq=21/5376; ttl-64 (no response found1)         27 2022-07-14 20:20:42.657708058       192.0.2.1
21 0022-07-14 20:20:41.63380697       192.0.2.100       198.51.100.100       ICMP       108       0x557e (2342)       64 Etho (ping) request       10-0x0801, seq-20/5120, t11-64 (reqly in 25)         22 0022-07-14 20:20:41.63380697       198.51.100.100       ICMP       108       0x557e (2342)       64 Etho (ping) request       10-0x0801, seq-20/5120, t11-64 (reqly in 25)         23 022-07-14 20:20:41.634805401       198.51.100.100       ICMP       108       0xc557e (2342)       64 Etho (ping) request       10-0x0801, seq-20/5120, t11-64 (request in 22)         24 0222-07-14 20:20:41.634805401       198.51.100.100       ICMP       108       0xc265 (52790)       64 Etho (ping) request       10-0x0801, seq-20/5120, t11-64       (request in 22)         24 0222-07-14 20:20:42.657709898       198.51.100.100       ICMP       108       0xc265 (52790)       64 Etho (ping) request       id-0x0801, seq-21/5376, tt1-64       (no response found1)         25 0222-07-14 20:20:42.657710898       192.0.2.100       198.51.100.100       ICMP       108       0x5676 (23536)       64 Etho (ping) request       id-0x0801, seq-21/5376, tt1-64 (no response found1)         26 022-07-14 20:20:42.65771466       192.0.2.100       198.51.100.100       ICMP       108       0x5676 (23586)       64 Etho (ping) request       id-0x0801, seq-21/5376, tt1-64 (no response found1)         27 0222-07-14 20:20:42.657780675
22 2022-07-14 2012:01:10:5300097       192:02:10:00       192:00:10:00       192:00:10:00       100*       192:00:10:00       192:00:10:00       100*       192:00:10:00       192:00:10:00       100*       00*       00*       00*       100*       100*       00*       00*       00*       10*       100*       00*       00*       00*       00*       00*       00*       10*       00*       00*       00*       00*       00*       10*
25 2022-07-14 20:20:41.63408356       198.51.100.100 192.6.7.100       ICMP       100       0 0 CCS5 (22/07)       0 4 Clin (ping) reply       100000001, seq=20/5120, CLI-00       (request in 22)         24 2022-07-14 20:20:41.63408356       198.51.100.100 192.6.7.100       ICMP       100       0 0 CCS5 (22/07)       64 Clin (ping) reply       i0000001, seq=20/5120, CLI-00       ICMP       100         25 2022-07-14 20:20:41.63408556       198.51.100.100       ICMP       100       0 0 CCS5 (22/07)       64 Clin (ping) reputst id-0x0001, seq=21/5376, ttl-64 (no response found)         26 2022-07-14 20:20:42.65770808       192.0.7.100       198.51.100.100       ICMP       100       0 0 CCS5 (22/07)       64 Clin (ping) request id-0x0001, seq=21/5376, ttl-64 (no response found)         26 2022-07-14 20:20:42.65770805       198.51.100.100       ICMP       100       0 0 CCS5 (23/536)       64 Echo (ping) request id-0x0001, seq=21/5376, ttl-64 (reply in 27)         27 2022-07-14 20:20:42.65770805       198.51.100.100       ICMP       100       0 0 CCS5 (23/536)       64 Echo (ping) reply       id-0x0001, seq=21/5376, ttl-64 (reply in 27)         27 2022-07-14 20:20:42.657980675       198.51.100.100       ICMP       100       0 0 CCS5 (23/536)       64 Echo (ping) reply       id-0x0001, seq=21/5376, ttl-64 (request in 26)
24 2022-07-14 20:20:42.657709806 192.0.2.100       196.31.100.100       192.0.2.100       ICMP       108       0xCe50 (22/90)       64 Echo (ping) reputy       1000X0001, 5eq=20/5120, tCl=64         25 2022-07-14 20:20:42.657709806 192.0.2.100       198.51.100.100       ICMP       108       0xS5f0 (23536)       64 Echo (ping) reputy       id=0x0001, seq=21/5376, ttl=64 (no response found!)         26 2022-07-14 20:20:42.657708067       198.51.100.100       ICMP       108       0xS5f0 (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       0xce49 (52809)       64 Echo (ping) reputy       id=0x0001, seq=21/5376, ttl=64 (request in 26)
25 2022-07-14     20:2
26 0222-07-14 20:2012.657308075 198.51.00-100 192.0.3.1.00-100 1CPP 108 055070 (25550) 64 ECho (ping) request i douxnoot, sequ21/53/6, ttl-46 (reply in 27) 27 2022-07-14 20:2012.657308075 198.51.00-100 192.0.3.1.00 1CPP 108 055509 (45 ECho (ping) request i douxnoot, sequ21/53/6, ttl-46 (request in 26)
27 2022-07-14 20:20:42.65/980675 198.51.100.100 192.0.2.100 ICMP 108 0xce49 (52809) 64 Echo (ping) reply 1d=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 0xce49 (52809) 64 Echo (ping) reply 10=0x0001, seq=21/5376, tt1=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 tound!)
< compared with the second s
> Frame 3: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture u0.8, id 0 0000 00 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00 PV ···X· ···W··&··
> Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: WWware 9d:e8:be (00:50:56:9d:e8:be) 0010 00 0a 81 00 00 66 08 00 45 00 00 54 cc 2c 00 00f. ET.,
VN-Tag
0 0000 00 01 00 0f 89 7a d0 62 00 00 00 03 d7 09 00z.b
.0
00 0000 0000 = Destination: 0
Type: 802.10 Victual IAN (0x8100)
802.10 Virtual LAM, PRT: A, DFT: A, TD: 102
and a priority Best Effort (default) (a)
Transa (174 (20000))
Internet Floreday Versaming and Floreday Version 1997 1971 1971 1971 1971 1971 1971 197

#### Explanation

When a packet capture on a backplane interface is configured, the switch simultaneously captures each packet twice. In this case, the internal switch receives packets that are already tagged by the application on the security module with the port VLAN tag and the VN tag. The VLAN tag identifies the egress interface that the internal chassis uses to forward the packets to the network. The VLAN tag 103 in ICMP echo request packets identifies Ethernet1/3 as the egress interface, while VLAN tag 102 in ICMP echo reply packets identifies Ethernet1/2 as the egress interface. The internal switch removes the VN tag and the internal interface VLAN tag before the packets are forwarded to the network.

This table summarizes the task:

Task	Capture point	Internal port VLAN in captured packets	Direction	Captured traffic
Configure and verify packet captures on backplane interfaces	Backplane interfaces	102 103	Ingress only	ICMP echo requests from host 192.0.2.100 to host 198.51.100.100 ICMP echo replies from host 198.51.100.100 to host 192.0.2.100

## **Packet Captures on Application and Application Ports**

Application or application port packet captures are always configured on backplane interfaces and additionally on the front interfaces if the user specifies the application capture direction.

There are mainly 2 use cases:

- Configure packet captures on backplane interfaces for packets that leave a specific front interface. For example, configure packet captures on the backplane interface Ethernet1/9 for packets that leave interface Ethernet1/2.
- Configure simultaneous packet captures on a specific front interface and the backplane interfaces. For example, configure simultaneous packet captures on interface Ethernet1/2 and on the backplane interface Ethernet1/9 for packets that leave interface Ethernet1/2.

This section covers both use cases.

#### Task 1

Use the FCM and CLI to configure and verify a packet capture on the backplane interface. Packets for which the application port Ethernet1/2 is identified as the egress interface are captured. In this case, ICMP replies are captured.



#### Topology, packet flow, and the capture points

#### Configuration

#### FCM

Perform these steps on FCM to configure a packet capture on the FTD application and the application port Ethernet1/2:

1. Use Tools > Packet Capture > Capture Session to create a new capture session:

Overview Interfaces Logical Devices Security Engine Platform Settings	System	Tools Help admin
	Packet Capture	Troubleshooting Logs
Capture Session Filter List		
C Refresh	Capture Session Delet	e All Sessions
No Session available		

2. Select the application, **Ethernet1/2** in the **Application Port** dropdown list and select **Egress Packet** in the **Application Capture Direction**. Provide the **Session Name** and click **Save and Run** to activate the capture:

Overview Interfaces Logical Devices Security Engine	Platform Settings		System Tools Help admin
Select an instance: ftd1			Save and Run Save Cancel
ftd1		Session Name*	cap1
		Selected Interfaces	None
Ethernet1/2		Buffer Size	256 MB
		Snap length:	1518 Bytes
		Store Packets	Overwrite Append
		Capture On	ftd
Ethernet1/3	<b>2</b>	Application Port	Ethernet1/2
	Ethernet1/9, Ethernet1/10	Application Capture Direction	All Packets Egress Packet
		Capture Filter	Apply Filter Capture All
Ethernet1/1			
L			

### FXOS CLI

Perform these steps on FXOS CLI to configure packet captures on backplane interfaces:

1. Identify the application type and identifier:

<#root>								
firepowe	er#							
scope sa	a							
firepowe show app	er /ssa# o-instance							
App Name	e Identi	fier Slot ID	Admin Sta	te Oper State 	Running Version	Startup	Version	Deploy Ty
ftd	ftd1							
1	L	Enabled	Online	7.2.0.82	7.2.0.82	Native	No	

2. Create a capture session:

```
<#root>
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 #
```

#### Verification

#### FCM

Verify the Interface Name, ensure that the Operational Status is up and that the File Size (in bytes) increases:

0	erview	Interfaces	Logical Devices	Security Engine	Platform	n Settings					System T	ools H	lp admin
Ca	pture Ses	ision Fiter Lis	t										
									C Refresh Capt	ure Session	Delete Al Se	essions	
۲		cap1	Drop Cour	it: 0	Operati	onal State: up	Buffer Size: 256 MI	В	Snap Length: 1518	Bytes			
In	terface Na	ame	Filter			File Size (in bytes)	File Name	Device Name					
Et	hernet1/2	- Ethernet1/10	None			576	cap1-vethernet-1175.pcap	ftd1		$\pm$			
Et	hernet1/2	- Ethernet1/9	None			4360	cap1-vethemet-1036.pcap	ftd1		$\pm$			

## FXOS CLI

Verify the capture details in scope packet-capture:

<#root>

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: O Drop Count: O

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:
```

#### **Collect capture files**

Perform the steps in the section Collect Firepower 4100/9300 Internal Switch Capture Files.

#### Capture file analysis

Use a packet capture file reader application to open the capture files. In the case of multiple backplane interfaces, ensure to open all capture files for each backplane interface. In this case, the packets are captured on the backplane interface Ethernet1/9.

Select the first and the second packets, and check the key points:

- 1. Each ICMP echo reply is captured and shown 2 times.
- 2. The original packet header is without the VLAN tag.
- 3. The internal switch inserts additional port VLAN tag **102** that identifies the egress interface Ethernet1/2.
- 4. The internal switch inserts an additional VN tag.

No. Time	Source	Destination	Protocol	Length	PD	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	id=0x	0012, seq=1/256, ttl=64	1	
2 2022-08-01 10:03:22.231239747	198.51.100.100	192.0.2.100	ICMP	108	0x42f8 (17144)	64 Echo (ping) reply	id=0x	0012, seq=1/256, ttl=64	1	
3 2022-08-01 10:03:23.232244769	198.51.100.100	192.0.2.100	ICMP	108	0X43U3 (17331)	ee scuo (bruß) Lebrà	id=0x	0012, seq=2/512, ttl=64	1	
4 2022-08-01 10:03:23.232247753	198.51.100.100	192.0.2.100	ICMP	108	0x43b3 (17331)	64 Echo (ping) reply	id=0x	0012, seq=2/512, ttl=64	1	
5 2022-08-01 10:03:24.234703981	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64 Echo (ping) reply	id=0x	0012, seq=3/768, ttl=64	1	
6 2022-08-01 10:03:24.234706751	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64 Echo (ping) reply	id=0x	0012, seq=3/768, ttl=64	1	
7 2022-08-01 10:03:25.258672449	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64 Echo (ping) reply	id=0x	0012, seq=4/1024, ttl=6	54	
8 2022-08-01 10:03:25.258674861	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64 Echo (ping) reply	id=0x	0012, seq=4/1024, ttl=6	54	
9 2022-08-01 10:03:26.282663169	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64 Echo (ping) reply	id=0x	0012, seq=5/1280, ttl=6	54	
10 2022-08-01 10:03:26.282666183	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64 Echo (ping) reply	id=0x	0012, seq=5/1280, ttl=6	54	
11 2022-08-01 10:03:27.306671694	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64 Echo (ping) reply	id=0x	0012, seq=6/1536, ttl=6	54	
12 2022-08-01 10:03:27.306674378	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64 Echo (ping) reply	id=0x	0012, seq=6/1536, ttl=6	54	
13 2022-08-01 10:03:28.330664677	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64 Echo (ping) reply	id=0x	0012, seq=7/1792, ttl=6	54	
14 2022-08-01 10:03:28.330667153	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64 Echo (ping) reply	id=0x	0012, seq=7/1792, ttl=6	54	
15 2022-08-01 10:03:29.354795931	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64 Echo (ping) reply	id=0x	0012, seq=8/2048, ttl=6	54	
16 2022-08-01 10:03:29.354936706	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64 Echo (ping) reply	id=0x	0012, seq=8/2048, ttl=6	54	
17 2022-08-01 10:03:30.378795204	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64 Echo (ping) reply	id=0x	0012, seq=9/2304, ttl=6	54	
18 2022-08-01 10:03:30.378798172	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64 Echo (ping) reply	id=0x	0012, seq=9/2304, ttl=6	54	
19 2022-08-01 10:03:31.402772217	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18842)	64 Echo (ping) reply	id=0x	0012, seq=10/2560, ttl=	-64	
20 2022-08-01 10:03:31.402774775	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64 Echo (ping) reply	id=0x	0012, seq=10/2560, ttl=	64	
21 2022-08-01 10:03:32.426693254	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64 Echo (ping) reply	1d=0x	0012, seq=11/2816, ttl=	-64	
e										
<u>x</u>										
> Frame 1: 108 bytes on wire (864 bit	s), 108 bytes ca	ptured (864 bits) o	n interface ca	apture_u0_	8, 1d 0		0000 000	50 56 9d e8 be 58 97	bd b9 77 0e 89 26 00 00	·PV···X· ··w··&··
> Ethernet II, Src: Cisco_b9:77:0e (5)	8:97:bd:b9:77:0e	), Dst: VMware_9d:e	8:be (00:50:56	5:9d:e8:be	)		0010 00	03 81 00 00 66 08 00	45 00 00 54 42 18 00 00	A D add add
VN-Tag							0020 40	12 00 01 dd ad o7 62	00 00 02 04 00 00 90 04	6.2200 0
0	= Directi	on: To Bridge					0040 00	00 00 00 10 11 12 13	14 15 16 17 18 19 1a 1b	
.0	= Pointer	tives 0					0050 1c	1d 1e 1f 20 21 22 23	24 25 26 27 28 29 2a 2b	···· !"# \$%&'()*+
	Destina	ition: 0					0060 2c	2d 2e 2f 30 31 32 33	34 35 36 37	,/0123 4567
		NO 4								
	- ····· = Neserve									
0000 00	00 1010 = Sources	10								
Type: 802.10 Victual LAN (0v8100)	)	10								
882.10 Virtual LAN, PRI: 0, DEI: 0.	ID: 102		_							
080 = Priority:	Rest Effort (defa	ult) (0)								
	rible	2								
0000 0110 0110 = ID: 102		-	· ·							
Type: IPv4 (0x0800)										
Internet Protocol Version 4, Src: 1	98.51.100.100, D	st: 192.0.2.100								
Internet Control Message Protocol		2								

### Explanation

In this case, Ethernet1/2 with port VLAN tag 102 is the egress interface for the ICMP echo reply packets.

When the application capture direction is set to **Egress** in the capture options, packets with the port VLAN tag 102 in the Ethernet header are captured on the backplane interfaces in the ingress direction.

This table summarizes the task:

Task	Capture point	Internal port VLAN in captured packets	Direction	Captured traffic
Configure and verify captures on application and application port Ethernet1/2	Backplane interfaces	102	Ingress only	ICMP echo replies from host 198.51.100.100 to host 192.0.2.100

#### Task 2

Use the FCM and CLI to configure and verify a packet capture on the backplane interface and the front interface Ethernet1/2.

Simultaneous packet captures are configured on:

- Front interface the packets with the port VLAN 102 on the interface Ethernet1/2 are captured. Captured packets are ICMP echo requests.
- Backplane interfaces packets for which Ethernet1/2 is identified as the egress interface, or the packets with the port VLAN 102, are captured. Captured packets are ICMP echo replies.

#### Topology, packet flow, and the capture points



#### Configuration

#### FCM

Perform these steps on FCM to configure a packet capture on the FTD application and the application port Ethernet1/2:

1. Use **Tools > Packet Capture > Capture Session** to create a new capture session:

Overview Interfaces Logica	l Devices Security Engine	Platform Settings	System	Tools Help admin
			Packet Capture	Troubleshooting Logs
Capture Session Filter List				
		C Refresh	Capture Session Dele	te All Sessions
No Session available				

2. Select the FTD application, **Ethernet1/2** in the **Application Port** dropdown list and select **All Packets** in the **Application Capture Direction**. Provide the **Session Name** and click **Save and Run** to activate the capture:

Overview Interfaces Logical Devices Security Engine	Platform Settings				System Tools Help admin
Select an instance: ftd1 v	indom ordinge				Save and Run Save Cancel
ftd1		Session Name*	cap1		
		Selected Interfaces	None		
Ethamat1/2		Buffer Size	256 MB 💙		
		Snap length:	1518	Bytes	
		Store Packets	Overwrite Append		
		Capture On	ftd 👻	1	
Ethernet1/3		Application Port	Ethernet1/2		
Tanana T	FTD Ethernet1/9, Ethernet1/10	Application Capture Directi	All Packets Egress Packet		
		Capture Filter	Apply Filter Capture All		
Ethernet1/1					

#### **FXOS CLI**

Perform these steps on FXOS CLI to configure packet captures on backplane interfaces:

1. Identify the application type and identifier:

```
<#root>
firepower#
scope ssa
firepower /ssa#
show app-instance
App Name Identifier Slot ID Admin State Oper State Running Version Startup Version Deploy Ty
    _____ _____
ftd
        ftd1
     1
        Enabled Online 7.2.0.82 7.2.0.82 Native
                                                                               No
  2. Create a capture session:
<#root>
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
```

#### Verification

#### FCM

Verify the **Interface Name**, ensure that the **Operational Status** is up and that the **File Size (in bytes)** increases:

Overview Interfaces	Overview Interfaces Logical Devices Security Engine Platform Settings System Tools Help admin										
Capture Session Filter L	ist.										
						G Refresh Capture Session Del					
a ap1	Drop Count: 0	Operational State: up	Buffer Size: 256 MB		Snap Length: 1518 Bytes						
Interface Name	Filter	File Size (in bytes)	File Name	Device Name							
Ethernet1/2	None	95040	cap1-ethernet-1-2-0.pcap	ftd1	2						
Ethernet1/2 - Ethernet1/10	None	368	cap1-vethernet-1175.pcap	ftd1	<u>*</u>						
Ethernet1/2 - Ethernet1/9	None	13040	cap1-vethernet-1036.pcap	ftd1	2						

#### **FXOS CLI**

Verify the capture details in scope packet-capture:

<#root>

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/capl-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/capl-vethernet-1175.pcap

Pcapsize: 2656 bytes

Vlan: 102

Filter:
```

#### **Collect capture files**

Perform the steps in the section Collect Firepower 4100/9300 Internal Switch Capture Files.

#### **Capture file analysis**

Use a packet capture file reader application to open the capture files. In the case of multiple backplane interfaces, ensure to open all capture files for each backplane interface. In this case, the packets are captured on the backplane interface Ethernet1/9.

Open the capture file for the interface Ethernet1/2, select the first packet, and check the key points:

- 1. Only ICMP echo request packets are captured. Each packet is captured and shown 2 times.
- 2. The original packet header is without the VLAN tag.
- 3. The internal switch inserts additional port VLAN tag **102** that identifies the ingress interface Ethernet1/2.
- 4. The internal switch inserts an additional VN tag.

No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info		
-	1 2022-08-01 11:33:19.070693081	192.0.2.100	198.51.100.100	ICMP	108 1	0xc009 (49161)	64 Echo (ping) re	equest	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) re	equest	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 ECRO (ping) r	equest	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) re	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) re	equest	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) re	equest	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) r	equest	id=0x0013, seg=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) r	equest	id=0x0013, seg=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	Øxc175 (49525)	64 Echo (ping) r	equest	id=0x0013, seg=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	Øxc175 (49525)	64 Echo (ping) r	equest	id=0x0013, seg=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) r	equest	id=0x0013, seg=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	8xc288 (49672)	64 Echo (ping) r	equest	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	Øxc211 (49681)	64 Echo (ping) p	equest	id=0x0013, seq=6/1536, ttl=64 (no response foundl)
	14 2022-08-01 11:33:24.081841386	192.0.2.100	198,51,100,100	TCMP	102	Øxc211 (49681)	64 Echo (ping) p	equest	id=0x0013, seq=6/1536, ttl=64 (no response foundl)
	15 2022-08-01 11:33:25 105806249	192.0.2.100	198.51.100.100	TCMP	108	0xc2e2 (49890)	64 Echo (ping) r	equest	id=0x0013, seq=7/1792, tt]=64 (no response found1)
	16 2022-08-01 11:33:25.105807895	192.0.2.100	198,51,100,100	ICMP	102	0xc2e2 (49890)	64 Echo (ping) r	equest	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	TCMP	102	0xc2b2 (49090)	64 Echo (ping) r	equest	id=0x0013, seq=8/2048, ttl=64 (no response found1)
	19 2022-08-01 11:33:26 120939114	192.0.2.100	199,51,100,100	TCMP	102	avc3h4 (50100)	64 Echo (ping) r	equest	(d=0x0013, seq=0/2040, ttl=64 (no response found1)
	10 2022-00-01 11-33-27 153030653	192 0 2 100	109 51 100 100	TCMP	100	0xc476 (50204)	64 Echo (ping) n	equest	(d-0x0013, seq=0/2304, ttl=64 (no response found1)
	20 2022-00-01 11-33-27 153020033	192.0.2.100	100 51 100 100	TCMD	100	0xc476 (50294)	64 Echo (ping) n	equest	id=0x0013, seq=0/2304, ttl=64 (no response found1)
	20 2022-00-01 11-33-20 177047175	192.0.2.100	198.51.100.100	TCMP	102	0xc470 (50254)	64 Echo (ping) r	equest	id=0x0013, seq=10/3560, ttl=64 (no response found!)
	22 2022-00-01 11-33-20 177040075	192.0.2.100	100 51 100 100	TCMD	100	0xc516 (50454)	64 Echo (ping) n	equest	id-avaala seg-10/2560, ttl-64 (no response foundl)
	22 2022-00-01 11:33:20.177049075	192.0.2.100	100 51 100 100	TCMD	102	0xc510 (50454)	64 Echo (ping) n	equest	id=0x0013, seq=10/2000, tt1=04 (no response found1)
	23 2022-00-01 11:33:29.201004/00	192.0.2.100	198.51.100.100	TCMD	100	0xc578 (50552)	64 Echo (ping) n	equest	id-0x0013, seq=11/2010, tt1=04 (no response found1)
	24 2022-08-01 11:55:29.201800488	192.0.2.100	198.51.100.100	TCHP	102	0x(578 (50552)	64 Echo (ping) 14	equest	id-outpoint, seq=11/2010, (t1=64 (no response found))
	25 2022-08-01 11:33:30.225834/65	192.0.2.100	198.51.100.100	TCHP	108	0xc585 (50505)	64 Echo (ping) P	equest	id-oxool3, seq=12/3072, tt1=64 (no response found1)
	26 2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (50565)	64 Echo (ping) P	equest	1d=0x0013, seq=12/30/2, tt1=64 (no response found)
	27 2022-08-01 11:33:31.249828955	192.0.2.100	198.51.100.100	ICMP	108	0xc618 (50/12)	64 Echo (ping) P	equest	1d=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 (50/12)	64 Echo (ping) r	equest	1d=0x0013, seq=13/3328, tt1=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) r	equest	1d=0x0013, seq=14/3584, ttl=64 (no response found!)
5									
>	Frame 1: 108 bytes on wire (864 bi	ts), 108 bytes ca	ptured (864 bits) o	n interface ca	pture_u0_	1, id 0		000	0 58 97 bd b9 77 0e 00 50 56 9d e8 be 89 26 80 0a X ··· W · P V ··· & ··
>	Ethernet II, Src: VMware 9d:e8:be	(00:50:56:9d:e8:b	e), Dst: Cisco b9:7	7:0e (58:97:bd	:b9:77:0e	2)		001	0 00 00 81 00 00 66 08 00 45 00 00 54 c0 09 40 00 ·····f·· E··T··@·
4	vN-Tag							002	8 48 81 80 83 60 80 82 64 66 33 64 64 88 88 80 7C g d .300
	1	= Directi	ion: From Bridge					003	0 00 13 00 01 T2 09 07 62 00 00 00 00 00 7T 06 00
	.0	··· ··· = Pointer	<pre>r: vif_id</pre>					004	
	00 0000 0000 1010	= Destina	ation: 10						a 2c 2d 2e 2f 30 31 32 33 34 35 36 37
	···· ··· ··· ··· ··· ··· ··· ··· ··· ·	= Looped:	NO 🧹	11					, ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
		= Reserve	hd: 0	· I					
	00	= Version	n: 0						
	0000 00	00 0000 = Source:	0						
L	Type: 802.10 Virtual LAN (0x810)	))							
4	802.1Q Virtual LAN, PRI: 0, DEI: 0	, ID: 102							
	000 = Priority:	Best Effort (defa	ault) (0)						
11	0 = DEI: Inel:	gible		3 1					
11	0000 0110 0110 = ID: 102								
L	Type: IPv4 (0x0800)								
>	Internet Protocol Version 4, Src:	192.0.2.100, Dst:	198.51.100.100						
>	Internet Control Message Protocol			2					

Select the second packet and check the key points:

- 1. Only ICMP echo request packets are captured. Each packet is captured and shown 2 times.
- 2. The original packet header is without the VLAN tag.
- 3. The internal switch inserts additional port VLAN tag **102** that identifies the ingress interface Ethernet1/2.

N	o. 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 1	0xc009 (49161	) 64 Echo (pi	ing) 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 (pi	ing) 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 (pi	ing) 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 (pi	ing) 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 (pi	ing) 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	Øxc0ae (49326	) 64 Echo (pi	ing) 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 (pi	ing) 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	Øxc167 (49511	) 64 Echo (pi	ing) 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	Øxc175 (49525	) 64 Echo (pi	ing) 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	Øxc175 (49525	) 64 Echo (pi	ing) 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 (pi	ing) 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 (pi	ing) 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	Øxc211 (49681	) 64 Echo (pi	ing) 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	Øxc211 (49681	) 64 Echo (pi	ing) 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 (pi	ing) 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 (pi	ing) 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 (pi	ing) 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 (pi	ing) 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 (pi	ing) request	id=0x0013, seq=9/2304, ttl=64 (no response found!)
	20 2022-08-01 11:33:27.153830201	192.0.2.100	198.51.100.100	ICMP	102	0xc476 (50294	) 64 Echo (pi	ing) 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 (pi	ing) 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 (pi	ing) 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 (pi	ing) 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 (pi	ing) 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 (pi	ing) request	id=0x0013, seq=12/3072, ttl=64 (no response found!)
	26 2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (50565	) 64 Echo (pi	ing) 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 (pi	ing) 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 (pi	ing) 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 (pi	ing) request	id=0x0013, seq=14/3584, ttl=64 (no response found!)
<									
	Frame 2: 102 bytes on wire (816 bi	ts), 102 bytes ca	ptured (816 bits) c	n interface ca	opture_u0	1, id 0		00	00 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:t	e), Dst: Cisco b9:7	7:0e (58:97:be	1:69:77:00	•)		00	10 08 00 45 00 00 54 c0 09 40 00 40 01 8d a3 c0 00 ··E··T··@·@····
	802.1Q Virtual LAN, PRI: 0, DEI: 0	, ID: 102						00	20 02 64 c6 33 64 64 08 00 8d 7c 00 13 00 01 f2 b9 ·d·3dd···
н	000 = Priority:	Best Effort (def	ault) (0)						30 e7 62 00 00 00 00 cb 7f 06 00 00 00 00 00 10 11 ·b·····
н	0 = DEI: Inel:	igible		3 1					40 12 13 14 15 16 17 18 19 1a 15 1c 1d 1e 1f 20 21
Е	0000 0110 0110 = ID: 102								20 22 23 24 23 20 27 28 29 28 20 20 20 20 20 21 30 31 #3+8 () *+,-,/01 60 32 33 34 35 36 37 234567
н	Type: IPv4 (0x0800)								52 55 54 55 50 57 Z34307
3	Internet Protocol Version 4, Src:	192.0.2.100, Dst:	198.51.100.100						
3	Internet Control Message Protocol			2					
н									

Open the capture file for the interface Ethernet1/9, select the first and the second packets, and check the key points:

- 1. Each ICMP echo reply is captured and shown 2 times.
- 2. The original packet header is without the VLAN tag.
- 3. The internal switch inserts additional port VLAN tag **102** that identifies the egress interface

#### Ethernet1/2.

4. The internal switch inserts an additional VN tag.

						10 Miles 1. 4		
No. Time Si	Source	Destination	Protocol	Length	PD	PTTL Pro		a anna
1 2022-08-01 11:33:19.0/1512098 1	198.51.100.100	192.0.2.100	TCMP	108	0x4127 (20203)	64 Echo (ping) reply	10=	0x0013, Seq=1/250, tt1=04
2 2022-08-01 11:33:19.0/1514882 1	198.51.100.100	192.0.2.100	ICMP	108	0x4f27 (20263)	64 Echo (ping) reply	10=	0x0013, seq=1/250, tt1=64
3 2022-08-01 11:33:20.072677302 1	198.51.100.100	192.0.2.100	ICMP	108	0X4110 (20475)	64 ECHO (ping) repi	10=	0x0013, seq=2/512, tt1=64
4 2022-08-01 11:33:20.072679384 1	198.51.100.100	192.0.2.100	ICMP	108	0x4ffb (20475)	64 Echo (ping) reply	1d=	0x0013, seq=2/512, ttl=64
5 2022-08-01 11:33:21.073913640 1	198.51.100.100	192.0.2.100	ICMP	108	0x50ac (20652)	64 Echo (ping) reply	1d=	0x0013, seq=3/768, tt1=64
6 2022-08-01 11:33:21.073915690 1	198.51.100.100	192.0.2.100	ICMP	108	0x50ac (20652)	64 Echo (ping) reply	1d=	0x0013, seq=3/768, tt1=64
7 2022-08-01 11:33:22.075239381 1	198.51.100.100	192.0.2.100	ICMP	108	0x513e (20798)	64 Echo (ping) reply	1d=	0x0013, seq=4/1024, tt1=64
8 2022-08-01 11:33:22.075241491 1	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 1	198.51.100.100	192.0.2.100	ICMP	108	0x51c9 (20937)	64 Echo (ping) reply	1d=	0x0013, seq=5/1280, tt1=64
10 2022-08-01 11:33:23.076449303 1	198.51.100.100	192.0.2.100	ICMP	108	0x51c9 (20937)	64 Echo (ping) reply	id=	0x0013, seq=5/1280, tt1=64
11 2022-08-01 11:33:24.082407896 1	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 1	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 1	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 1	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 1	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 1	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 1	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 1	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 1	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 1	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 1	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21748)	64 Echo (ping) reply	id=	0x0013, seq=11/2816, ttl=64
22 2022-08-01 11:33:29.202398067 1	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21748)	64 Echo (ping) reply	id=	0x0013, seq=11/2816, ttl=64
23 2022-08-01 11:33:30.226398735 1	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 11:33:30.226401017 1	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 1	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 1	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 1	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 1	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 1	198.51.100.100	192.0.2.100	ICMP	108	0x56e7 (22247)	64 Echo (ping) reply	id=	0x0013, seq=15/3840, ttl=64
<								
> Frame 1: 108 bytes on wire (864 bits)	), 108 bytes ca	ptured (864 bits) o	n interface ca	opture u0	8, id 0		0000 4	80 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00 ··PV···X· ··w··&··
> Ethernet II, Src: Cisco b9:77:0e (58:	:97:bd:b9:77:0e	), Dst: VMware 9d:e	8:be (00:50:50	:9d:e8:be	)		0010	00 0a 81 00 00 66 08 00 45 00 00 54 4f 27 00 00f. E. TO'
VN-Tag					·		0020	40 01 3e 86 c6 33 64 64 c0 00 02 64 00 00 95 7c @·>··3dd ···d···
0	= Directi	on: To Bridge					0030	30 13 00 01 f2 b9 e7 62 00 00 00 eb 7f 06 00bb
.0	= Pointer	: vif id					0040	að dð dð dð 10 11 12 13 14 15 16 17 18 19 1a 1b
00 0000 0000 0000	= Destina	tion: 0					0050	ic 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ···· !"# \$%&"()*+
	= Looped:	No					0060	2c 2d 2e 2t 30 31 32 33 34 35 36 37 ,=./0123 4567
	= Reserve	d: 0	• •					
	= Version	: 0						
	1010 = Source:	10						
Type: 802.10 Virtual LAN (0x8100)		**						
802.10 Virtual LAN, PRI: 0, DFI: 0. T	ID: 102							
000 = Priority: Res	st Effort (defa	ult) (0)						
	ble		2					
0000 0110 0110 = ID: 102			<b>7</b>					
Type: IPv4 (0x0800)								
Internet Protocol Version A. Src: 108	8 51 100 100 D	st: 192 8 2 188						
Internet Control Message Protocol								
and her control nessage protocol								

#### Explanation

If the option **All Packets** in the **Application Capture Direction** is selected, 2 simultaneous packet captures related to the selected application port Ethernet1/2 are configured: a capture on the front interface Ethernet1/2 and a capture on selected backplane interfaces.

When a packet capture on a front interface is configured, the switch simultaneously captures each packet twice:

- After the insertion of the port VLAN tag.
- After the insertion of the VN tag.

In the order of operations, the VN tag is inserted at a later stage than the port VLAN tag insertion. But in the capture file, the packet with the VN tag is shown earlier than the packet with the port VLAN tag. In this example, the VLAN tag 102 in ICMP echo request packets identifies Ethernet1/2 as the ingress interface.

When a packet capture on a backplane interface is configured, the switch simultaneously captures each packet twice. The internal switch receives packets that are already tagged by the application on the security module with the port VLAN tag and the VN tag. The port VLAN tag identifies the egress interface that the internal chassis uses to forward the packets to the network. In this example, the VLAN tag 102 in ICMP echo reply packets identifies Ethernet1/2 as the egress interface.

The internal switch removes the VN tag and the internal interface VLAN tag before the packets are forwarded to the network.

This table summarizes the task:

Task Capture poin	t Internal port	Direction	Captured traffic	
-------------------	-----------------	-----------	------------------	
		VLAN in captured packets		
--	--------------------------	-----------------------------	--------------	---
Configure and verify captures on application and application port Ethernet1/2	Backplane interfaces	102	Ingress only	ICMP echo replies from host 198.51.100.100 to host 192.0.2.100
	Interface Ethernet1/2	102	Ingress only	ICMP echo requests from host 192.0.2.100 to host 198.51.100.100

# Packet Capture on a Subinterface of a Physical or Port-channel Interface

Use the FCM and CLI to configure and verify a packet capture on subinterface Ethernet1/2.205 or portchannel subinterface Portchannel1.207. Subinterfaces and captures on subinterfaces are supported only for the FTD application in container mode. In this case, a packet capture on Ethernet1/2.205 and Portchannel1.207 are configured.

## Topology, packet flow, and the capture points



## Configuration

## FCM

Perform these steps on FCM to configure a packet capture on the FTD application and the application port Ethernet1/2:

1. Use **Tools > Packet Capture > Capture Session** to create a new capture session:

Overview	Interfaces	Logical Devices	Security Engine	Platform Settings		System	Tools Help admin
						Packet Capture	Troubleshooting Logs
Capture Ses	sion Filter Lis	t					
					C Refresh	Capture Session Dek	te All Sessions
No Session av	vailable						

2. Select the specific application instance ftd1, the subinterface Ethernet1/2.205, provide the session name, and click **Save and Run** to activate the capture:

Overview Interfaces Logical Devices Security Engine Platform Settings			System Tools Help admin
Select an instance: ftd1 v			Save and Run Save Cancel
Subinterface selection ftd1 Ethernet1/2.205 Ethernet1/2.206		Session Name* Selected Interfaces	Cap1
Subjeterfaces(2) Phoreal1/2		Buffer Size Snap length:	256 M8 Y 1518 Bytes
		Store Packets Capture Filter	Overwrite Append Apply Filter Capture AB
	FTD Ethernet1/9, Ethernet1/10		
Ethernet1/1			

3. In the case of a port-channel subinterface, due to the Cisco bug ID <u>CSCvq33119</u> subinterfaces are not visible in the FCM. Use the FXOS CLI to configure captures on port-channel subinterfaces.

#### **FXOS CLI**

Perform these steps on FXOS CLI to configure a packet capture on subinterfaces Ethernet1/2.205 and Portchannel1.207:

1. Identify the application type and identifier:

<#root>								
firepower#								
scope ssa								
firepower /	/ssa #							
show app-in	nstance							
App Name	Identif	ier Slot ID 	Admin Stat	e Oper State 	Running Version	Startup Vers	ion 	Deploy Ty
ftd	ftdl							
1 ftd	ftd2	Enabled 1	Online Enabled	7.2.0.82 Online	7.2.0.82 7.2.0.82	Container 7.2.0.82	No	R Container

2. In the case of a port-channel interface, identify its member interfaces:

<#root>

firepower#

connect fxos

<output skipped>
firepower(fxos)#

#### show port-channel summary

P - Up in port-channel (members) Flags: D - Down 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 \_\_\_\_\_ Туре Group Port-Protocol Member Ports Channel \_\_\_\_\_ Pol(SU) Eth LACP Eth1/3(P) Eth1/3(P) 1

3. Create a capture session:

#### <#root>

#### 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\* #

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

For port-channel subinterfaces, create a packet capture for each port-channel member interface:

```
<#root>
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* #
```

```
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 #

## Verification

set app ftd

#### FCM

Verify the Interface Name, ensure that the Operational Status is up and that the File Size (in bytes) increases:

Overview Interfaces Logical Devices Security Engine Platform Settings				System Tool	s Help admin
Capture Session Fiter List					
				G Refresh Capture Session Delete Al Sessio	05
a caoi Dros-Count: 0	Operational State: up	Buffer Size: 256 MB	Snap Length	1518 Bytes	
					0.0100
Interface Name Filter	File Size (in bytes)	File Name	Device Name		
Ethernet1/2.205 None	233992	cap1-ethemet-1-2-0.pcap	ftd1	¥]	

Port-channel subinterface captures configured on FXOS CLI are also visible on FCM; however, they cannot be edited:

Overview Interfaces Logical Dev	ices Security Engine Platform Settings					System Tools I	Help admin
Capture Session Filter List							
					Capture Session	Delete Al Sessions	
a esp1	Drop Count: 0	Operational State: up	Buffer Size: 256 MB		Snap Length: 1518 Bytes		4.8.0
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**

Verify the capture details in scope packet-capture:

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: O Drop Count: O

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

Port-channel 1 with member interfaces Ethernet1/3 and Ethernet1/4:

<#root> 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

```
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
```

#### **Collect capture files**

Perform the steps in the section Collect Firepower 4100/9300 Internal Switch Capture Files.

#### Capture file analysis

Use a packet capture file reader application to open the capture file. Select the first packet and check the key points:

- 1. Only ICMP echo request packets are captured. Each packet is captured and shown 2 times.
- 2. The original packet header has the VLAN tag 205.
- 3. The internal switch inserts additional port VLAN tag **102** that identifies the ingress interface Ethernet1/2.
- 4. The internal switch inserts an additional VN tag.

No. Time Source	Destination	Protocol Le	nath	P 10	PTTL Ma	_	
1 2022-08-04 07:21:56.993302102 192.0.2.100	198.51.100.100	TCMP 11	12	8x9574 (38268)	64 Echo (ping) requi	est in	d=0x0022, seq=1/256, ttl=64 (no response found!)
2 2822-88-84 87:21:56.993383597 192.8.2.186	198, 51, 100, 100	TCMP 10	32	8x9574 (38268)	64 Echo (ping) requi	est in	d=0x0022, seq=1/256, ttl=64 (no response foundl)
3 2022-08-04 07:22:06.214264777 192.0.2.100	198,51,100,100	ICMP 11	12	0x9a81 (39553)	64 Echo (ping) requ	est ic	d=0x0022, seg=10/2560, ttl=64 (no response foundl)
4 2022-08-04 07:22:06.214267373 192.0.2.100	198.51.100.100	TCMP 10	32	0x9a81 (39553)	64 Echo (ping) requi	est in	d=0x0022, seq=10/2560, ttl=64 (no response foundl)
5 2022-08-04 07:22:07.215113393 192.0.2.100	198,51,100,100	ICMP 11	12	0x9ac3 (39619)	64 Echo (ping) requ	est ic	d=0x0022, seg=11/2816, ttl=64 (no response found1)
6 2022-08-04 07:22:07.215115445 192.0.2.100	198,51,100,100	TCMP 10	32	0x9ac3 (39619)	64 Echo (ping) requi	est in	d=0x0022, seg=11/2816, tt]=64 (no response found])
7 2022-08-04 07:22:08 220038577 102.0.2.100	198.51.100.100	TCMP 11	12	avah33 (30731)	64 Echo (ping) requi	est in	d=0x0022, seq=12/3072, tt]=64 (no response found1)
8 2022-08-04 07:22:08 220040820 102 0 2 100	108 51 100 100	TCMP 10	32	avab33 (30731)	64 Echo (ping) requ	ast in	d=0x0022 sen=12/3072 tt]=64 (no response found1)
9 2822-08-04 07:22:09.253944681 192.0.2.100	198.51.100.100	ICMP 11	12	0x9c8e (39958)	64 Echo (ping) requ	est in	d=8x0022, seg=13/3328, ttl=64 (no response foundl)
10 2022-08-04 07:22:00 253046800 102 0.2 100	198, 51, 100, 100	TCMP 10	32	avacae (30050)	64 Echo (ping) requ	ast in	d-avaazz, sen=13/3328, tt]=64 (no response found1)
11 2022-08-04 07:22:10 277053070 102 0 2 100	109 51 100 100	TCMP 11	12	avacch (40130)	64 Echo (ping) requ	ast in	d=0x0022, seq=14/3594 ttl=64 (no response found1)
12 2022-08-04 07:22:10 277054736 102.0.2.100	198,51,100,100	TCMP 10	32	avacch (40139)	64 Echo (ping) requi	est in	d=0x0022, seq=14/3584, tt]=64 (no response found1)
13 2022-09-04 07:22:11 201031202 102 0 2 100	109 51 100 100	TCMP 11	12	avades (40233)	64 Echo (ping) requ	ast in	4-0x0022, seq=15/3040, tt]=64 (no response found1)
14 2022-08-04 07:22:11 201032600 102 0 2 100	100 51 100 100	TCMP 10	32	0x0d84 (40324)	64 Echo (ping) requ	ast in	4-0x0022, seq=15/3040, ttl=64 (no response found1)
15 2022-08-04 07:22:11.301933000 192.0.2.100	198.51.100.100	ICMP 11	12	0x9da2 (40354)	64 Echo (ping) requ	est in	d=0x0022, seq=15/3046, ttl=64 (no response found1)
16 2022-09-04 07:22:12 225027905 102 0 2 100	100 51 100 100	TCMP 10	32	0x0da2 (40354)	64 Echo (ping) requ	ast in	d-avaara saa-16/4006 ttl=64 (no response foundl)
17 2022-08-04 07:22:12.32595/055 152.012110	198.51.100.100	ICMP 11	12	0x9002 (40354)	64 Echo (ping) requ	est in	d=0x0022, seq=17/4352, ttl=64 (no response foundl)
19 2022-00-04 07:22:13:320980040 192:0.2:100	198.51.100.100	ICMP 10	32	0x9e07 (40455)	64 Echo (ping) requi	est in	d=0x0022, seq=17/4352, ttl=64 (no response found1)
10 2022-00-04 07:22:15:520990250 192:0.2:100	198.51.100.100	ICMP 10	12	0x9607 (40455)	64 Echo (ping) requi	est it	d=0x0022, seq=17/4552, cc1=04 (no response found1)
20 2022-00-04 07:22:14:341944775 192:0:2:10	100 51 100 100	TCMD 10	32	0x0063 (40554)	64 Echo (ping) requ	ost in	d-avaaraa saa-10/4600 ttl-64 (no response foundl)
20 2022-08-04 07:22:14.341940249 192.0.2.100	198.51.100.100	ICMP 10	12	0x9e0a (40554)	64 Echo (ping) requi	est it	d=0x0022, seq=10/4060, ttl=64 (no response found1)
21 2022-00-04 07:22:15.303941300 192.0.2.100	198.51.100.100	ICMP 1	12	0x9erb (40099)	64 Echo (ping) requi	est it	d=0x0022, seq=19/4004, ttl=64 (no response found1)
22 2022-00-04 07:22:15:303942300 192:0.2:100	100 51 100 100	TCMD 11	12	0x9610 (40099)	64 Echo (ping) requi	est it	d-ox0022, seq-19/4004, ttl-64 (no response found))
25 2022-08-04 07:22:10.589975045 192.0.2.100	198.51.100.100	ICMP 1	12	0x91e8 (40936)	64 Echo (ping) requi	est it	d=0x0022, seq=20/5120, ttl=64 (no response found1)
24 2022-08-04 07:22:10.369975129 192.0.2.100	198.51.100.100	ICMP 10	12	0x9108 (40950)	64 Echo (ping) requi	est it	d=0x0022, seq=20/5120, ttl=64 (no response foundl)
25 2022-00-04 07:22:17.413930452 192.0.2.100	198.51.100.100	TCMD 10	12	0x2079 (41001)	64 Echo (ping) requi	est it	d=0x0022, seq=21/5576, tt1=64 (no response found1)
20 2022-00-04 07:22:17.413930090 192.0.2.100	198.51.100.100	TCHP IN	12	0xa0/9 (41081)	64 Echo (ping) requi	est it	d=0x0022, seq=21/5376, (t1=64 (no response found1)
2/ 2022-08-04 0/:22:18.43/954335 192.0.2.100	198.51.100.100	ICHP I.	12	6xalle (41246)	er scup (brug) redu	est It	unoxoozz, seq=zz/sosz, ((1=64 (no response round))
<							
> Frame 1: 112 bytes on wire (896 bits), 112 byte	s captured (896 bits)	on interface capt	ure_u0_	1, id 0		0000	a2 76 f2 00 00 1b 00 50 56 9d e8 be 89 26 80 54 ···································
> Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:	e8:be), Dst: a2:76:f2:	00:00:1b (a2:76:f	2:00:00	:1b)		0010	00 00 81 00 00 66 81 00 00 cd 08 00 45 00 00 54fET
✓ VN-Tag						0020	95 74 40 00 40 01 b8 38 c0 00 02 64 c6 33 64 64 ·t@·@··8 ···d·3dd
1 Di	rection: From Bridge					0030	08 00 eb 95 00 22 00 01 88 73 eb 62 00 00 00 00 ····· <sup>-</sup> ···s·b····
.0	inter: vif_id					0040	d9 9d 00 00 00 00 00 00 10 11 12 13 14 15 16 17
00 0000 0101 0100 = De	stination: 84					0050	10 19 10 10 10 10 10 11 20 21 22 25 24 25 20 27 11 1 #\$400
e e	oped: No	4 1					20 29 20 20 20 20 20 20 20 20 20 31 52 55 54 55 50 57 () +,-1, 01254507
0 = Re	served: 0	· I					
00 = Ve	rsion: 0						
0000 0000 0000 = So	urce: 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		31					
0000 0110 0110 = ID: 102		-					
Type: 802.1Q Virtual LAN (0x8100)							
✓ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 205							
000 = Priority: Best Effort	(default) (0)						
0 = DEI: Ineligible							
0000 1100 1101 = ID: 205		2					
Type: IPv4 (0x0800)		<b>4</b>					
> Internet Protocol Version 4, Src: 192.0.2.100,	Dst: 198.51.100.100						
> Internet Control Message Protocol							

Select the second packet and check the key points:

- 1. Only ICMP echo request packets are captured. Each packet is captured and shown 2 times.
- 2. The original packet header has the VLAN tag 205.

N	o. Time	Source	Destination	rotocol	Length	PD	IP TTL Info		
	1 2022-08-04 07:21:56.993302102	192.0.2.100	198.51.100.100	CMP	112	0x9574 (38260)	64 Echo (ping) requ	est i	d=0x0022, seq=1/256, ttl=64 (no response found!)
	2 2022-08-04 07:21:56.993303597	192.0.2.100	198.51.100.100	CMP	102	0x9574 (38260)	64 Echo (ping) requ	est i	d=0x0022, seq=1/256, ttl=64 (no response found!)
	3 2022-08-04 07:22:06.214264777	192.0.2.100	198.51.100.100	CMP	112	0x9a81 (39553)	64 Echo (ping) requ	est i	d=0x0022, seq=10/2560, ttl=64 (no response found!)
	4 2022-08-04 07:22:06.214267373	192.0.2.100	198.51.100.100	CMP	102	0x9a81 (39553)	64 Echo (ping) requ	est i	d=0x0022, seq=10/2560, ttl=64 (no response found!)
	5 2022-08-04 07:22:07.215113393	192.0.2.100	198.51.100.100	CMP	112	0x9ac3 (39619)	64 Echo (ping) requ	est i	d=0x0022, seq=11/2816, ttl=64 (no response found!)
	6 2022-08-04 07:22:07.215115445	192.0.2.100	198.51.100.100 1	CMP	102	0x9ac3 (39619)	64 Echo (ping) requ	est i	d=0x0022, seq=11/2816, ttl=64 (no response found!)
	7 2022-08-04 07:22:08.229938577	192.0.2.100	198.51.100.100	CMP	112	0x9b33 (39731)	64 Echo (ping) requ	est i	d=0x0022, seq=12/3072, ttl=64 (no response found!)
	8 2022-08-04 07:22:08.229940829	192.0.2.100	198.51.100.100	CMP	102	0x9b33 (39731)	64 Echo (ping) requ	est in	d=0x0022, seq=12/3072, ttl=64 (no response found!)
	9 2022-08-04 07:22:09.253944601	192.0.2.100	198.51.100.100	CMP	112	0x9c0e (39950)	64 Echo (ping) requ	est i	d=0x0022, seg=13/3328, ttl=64 (no response found!)
	10 2022-08-04 07:22:09.253946899	192.0.2.100	198.51.100.100	CMP	102	0x9c0e (39950)	64 Echo (ping) requ	est i	d=0x0022, seq=13/3328, ttl=64 (no response found!)
	11 2022-08-04 07:22:10.277953070	192.0.2.100	198.51.100.100 1	CMP	112	0x9ccb (40139)	64 Echo (ping) requ	est i	d=0x0022, seq=14/3584, ttl=64 (no response found!)
	12 2022-08-04 07:22:10.277954736	192.0.2.100	198.51.100.100	CMP	102	0x9ccb (40139)	64 Echo (ping) requ	est i	d=0x0022, seg=14/3584, ttl=64 (no response found!)
	13 2022-08-04 07:22:11.301931282	192.0.2.100	198.51.100.100	CMP	112	0x9d84 (40324)	64 Echo (ping) requ	est i	d=0x0022, seg=15/3840, ttl=64 (no response found!)
	14 2022-08-04 07:22:11.301933600	192.0.2.100	198.51.100.100	CMP	102	0x9d84 (40324)	64 Echo (ping) requ	est i	d=0x0022, seg=15/3840, ttl=64 (no response found!)
	15 2022-08-04 07:22:12.325936521	192.0.2.100	198.51.100.100	CMP	112	0x9da2 (40354)	64 Echo (ping) requ	est i	d=0x0022, seq=16/4096, ttl=64 (no response found!)
	16 2022-08-04 07:22:12.325937895	192.0.2.100	198.51.100.100	CMP	102	0x9da2 (40354)	64 Echo (ping) requ	est in	d=0x0022, seg=16/4096, ttl=64 (no response found!)
	17 2022-08-04 07:22:13.326988040	192.0.2.100	198.51.100.100	CMP	112	0x9e07 (40455)	64 Echo (ping) requ	est in	d=0x0022, seg=17/4352, ttl=64 (no response found!)
	18 2022-08-04 07:22:13.326990258	192.0.2.100	198.51.100.100	CMP	102	0x9e07 (40455)	64 Echo (ping) requ	est i	d=0x0022, seq=17/4352, ttl=64 (no response found!)
	19 2022-08-04 07:22:14.341944773	192.0.2.100	198.51.100.100	CMP	112	0x9e6a (40554)	64 Echo (ping) requ	est in	d=0x0022, seq=18/4608, ttl=64 (no response found!)
	20 2022-08-04 07:22:14.341946249	192.0.2.100	198.51.100.100	CMP	102	0x9e6a (40554)	64 Echo (ping) requ	est i	d=0x0022, seg=18/4608, ttl=64 (no response found!)
	21 2022-08-04 07:22:15.365941588	192.0.2.100	198.51.100.100	CMP	112	0x9efb (40699)	64 Echo (ping) requ	est i	d=0x0022, seq=19/4864, ttl=64 (no response found!)
	22 2022-08-04 07:22:15.365942566	192.0.2.100	198.51.100.100	CMP	102	0x9efb (40699)	64 Echo (ping) requ	est in	d=0x0022, seq=19/4864, ttl=64 (no response found!)
	23 2022-08-04 07:22:16.389973843	192.0.2.100	198.51.100.100	CMP	112	0x9fe8 (40936)	64 Echo (ping) requ	est i	d=0x0022, seg=20/5120, ttl=64 (no response found!)
	24 2022-08-04 07:22:16.389975129	192.0.2.100	198.51.100.100	CMP	102	0x9fe8 (40936)	64 Echo (ping) requ	est i	d=0x0022, seq=20/5120, ttl=64 (no response found!)
	25 2022-08-04 07:22:17.413936452	192.0.2.100	198.51.100.100	CMP	112	0xa079 (41081)	64 Echo (ping) requ	est i	d=0x0022, seq=21/5376, ttl=64 (no response found!)
	26 2022-08-04 07:22:17.413938090	192.0.2.100	198.51.100.100	CMP	102	0xa079 (41081)	64 Echo (ping) requ	est i	d=0x0022, seq=21/5376, ttl=64 (no response found!)
	27 2022-08-04 07:22:18.437954335	192.0.2.100	198.51.100.100	CMP	112	0xa11e (41246)	64 Echo (ping) requ	est i	d=0x0022, seg=22/5632, ttl=64 (no response found!)
						: :			
E	France 2: 102 butes on wine (016 bit	<ol> <li>103 but oc. co</li> </ol>	ntuned (016 bits) on	intenface c		1. 14.0		0000	22 76 f2 00 00 th 00 50 56 od 08 ha 81 00 00 cd
	Frame 2: 102 bytes on wire (816 bit	(s), 102 Dytes ca	iptured (816 Dits) on	interface ca	ipture_ue	1, 10 0		0000	a2 76 72 00 00 10 00 50 50 90 68 06 81 00 00 cu ······························
	Ethernet II, SFC: Whare Solesibe (	00:50:56:90:68:0	e), DSt: az:/6:T2:00:	00:10 (az:/0	5:12:00:00	9:10)		0020	02 64 c6 33 64 64 08 00 eb 95 00 22 00 01 88 73 d-3dd
Г	802.10 VIFtual LAN, PRI: 0, DEI: 0,	IU: 205 Post Effort (dof)	sult) (0)					0030	eb 62 00 00 00 00 d9 9d 00 00 00 00 00 10 11
н	obo Priority:	sible	aurc) (0)					0040	12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21
Т		RIDIG	_					0050	22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 "#\$%&'() *+,/01
Т	0000 1100 1101 = 10: 205		2					0060	32 33 34 35 36 37 234567
T.	Tatemat Destacel Mension 4 Sec. 4	03 0 3 100 0-+-	100 51 100 100	-					
	Internet Protocol Version 4, Src: 1	92.0.2.100, DST:	198.51.100.100						
Ľ	internet control Message Protocol								

Now open the capture files for Portchannel1.207. Select the first packet and check the key points

- 1. Only ICMP echo request packets are captured. Each packet is captured and shown 2 times.
- 2. The original packet header has the VLAN tag **207**.
- 3. The internal switch inserts an additional port VLAN tag **1001** that identifies the ingress interface Portchannel1.
- 4. The internal switch inserts an additional VN tag.

No. Time	Source	Destination	Protocol	Length	1910	IP TTI Info	_	
1 2022 00 04 00-10-24 572540050	103 160 347 100	103 160 347 103	TCMD	100	0+(00+ (34734)	DEE Eshe (pipe) per	most id	-0x007h see-0/0 ttl-3FE (no personal found))
1 2022-08-04 08:18:24.572548809	192.108.247.100	192.100.247.102	TCHP	120	0,0099 (24754)	255 Echo (pring) req	uest 10	-oxoorb, seq=oro, cc1=255 (no response round))
2 2022-08-04 08:18:24.572550075	192.108.247.100	192.168.247.102	TCHP	118	0x0090 (24734)	255 Echo (ping) red	uest 10	=0x007b, seq=070, tt1=255 (no response round:)
3 2022-08-04 08:18:24.573286630	192.168.247.100	192.168.247.102	ICMP	128	0x609f (24735)	255 Echo (ping) red	uest 1d	=0x007b, seq=1/256, tt1=255 (no response round!)
4 2022-08-04 08:18:24.573287640	192.168.247.100	192.168.247.102	ICMP	118	0x609f (24735)	255 Echo (ping) red	uest 1d	=0x007b, seq=1/256, tt1=255 (no response found!)
5 2022-08-04 08:18:24.573794751	192.168.247.100	192.168.247.102	ICMP	128	0x60a0 (24736)	255 Echo (ping) req	uest 1d	=0x007b, seq=2/512, ttl=255 (no response found!)
6 2022-08-04 08:18:24.573795748	192.168.247.100	192.168.247.102	ICMP	118	0x60a0 (24736)	255 Echo (ping) req	uest id	=0x007b, seq=2/512, ttl=255 (no response found!)
7 2022-08-04 08:18:24.574368638	192.168.247.100	192.168.247.102	ICMP	128	0x60a1 (24737)	255 Echo (ping) req	uest id	=0x007b, seq=3/768, ttl=255 (no response found!)
8 2022-08-04 08:18:24.574369574	192.168.247.100	192.168.247.102	ICMP	118	0x60a1 (24737)	255 Echo (ping) req	uest id	=0x007b, seq=3/768, ttl=255 (no response found!)
9 2022-08-04 08:18:24.574914512	192.168.247.100	192.168.247.102	ICMP	128	0x60a2 (24738)	255 Echo (ping) req	uest id	=0x007b, seq=4/1024, ttl=255 (no response found!)
10 2022-08-04 08:18:24.574915415	192.168.247.100	192.168.247.102	ICMP	118	0x60a2 (24738)	255 Echo (ping) req	uest id	=0x007b, seq=4/1024, ttl=255 (no response found!)
11 2022-08-04 08:18:24.575442569	192.168.247.100	192.168.247.102	ICMP	128	0x60a3 (24739)	255 Echo (ping) req	uest id	=0x007b, seq=5/1280, ttl=255 (no response found!)
12 2022-08-04 08:18:24.575443601	192.168.247.100	192.168.247.102	ICMP	118	0x60a3 (24739)	255 Echo (ping) req	uest id	=0x007b, seq=5/1280, ttl=255 (no response found!)
13 2022-08-04 08:18:24.575918119	192.168.247.100	192.168.247.102	ICMP	128	0x60a4 (24740)	255 Echo (ping) red	uest id	=0x007b, seq=6/1536, ttl=255 (no response found!)
14 2022-08-04 08:18:24.575919057	192.168.247.100	192.168.247.102	ICMP	118	0x60a4 (24740)	255 Echo (ping) red	uest id	=0x007b, seg=6/1536, ttl=255 (no response found!)
15 2022-08-04 08:18:24.576407671	192.168.247.100	192.168.247.102	ICMP	128	0x60a5 (24741)	255 Echo (ping) red	uest id	=0x007b, seg=7/1792, ttl=255 (no response found!)
16 2022-08-04 08:18:24.576408585	192.168.247.100	192.168.247.102	ICMP	118	0x60a5 (24741)	255 Echo (ping) red	uest id	=0x007b, seg=7/1792, ttl=255 (no response found!)
17 2022-08-04 08:18:24.576885643	192,168,247,100	192.168.247.102	TCMP	128	8x68a6 (24742)	255 Echo (ping) red	uest id	=0x007b, seg=8/2048, ttl=255 (no response found!)
18 2022-08-04 08:18:24.576886561	192,168,247,100	192, 168, 247, 102	TCMP	118	8x68a6 (24742)	255 Echo (ping) rec	uest id	=0x007b, seg=8/2048, ttl=255 (no response found!)
10 2022-00-04 00-10-24 577304330	102 169 247 100	102 169 247 102	TCMD	129	0x60a7 (24742)	255 Echo (ping) rec	mast id	=0x007b, seq=0/2000, ttl=255 (no response foundl)
20 2022-00-04 00-10-24 577305234	102 160 247 100	102 169 247 102	TCMD	110	0x60a7 (24743)	255 Echo (ping) rec	most id	=0x007b, seq=0/2304, ttl=255 (no response found1)
20 2022-00-04 00:10:24:577097633	103 160 347 100	102.108.247.102	TCMD	120	0x60a9 (24743)	255 Echo (ping) rec	west id	-0x007b, seq=5/2504, cc1=255 (no response found)
21 2022-08-04 08:10:24.577987052	192.100.247.100	192.100.247.102	TCHP	120	0x0000 (24744)	255 Echo (ping) req	uest id	-0x007b, seq=10/2500, cc1=255 (no response found!)
22 2022-08-04 08:18:24.57/989290	192.168.247.100	192.168.247.102	TCMP	118	0x60a8 (24744)	255 Echo (ping) red	uest 1d	=0x007b, seq=10/2560, ttl=255 (no response foundi)
23 2022-08-04 08:18:24.5/8448/81	192.168.247.100	192.168.247.102	TCMP	128	0x60a9 (24745)	255 Echo (ping) red	uest 1d	=0x007b, seq=11/2816, tt1=255 (no response found!)
24 2022-08-04 08:18:24.578449909	192.168.247.100	192.168.247.102	ICMP	118	0x60a9 (24745)	255 Echo (ping) red	uest 1d	=0x007b, seq=11/2816, ttl=255 (no response found!)
25 2022-08-04 08:18:24.578900043	192.168.247.100	192.168.247.102	ICMP	128	0x60aa (24746)	255 Echo (ping) req	uest id	=0x007b, seq=12/3072, tt1=255 (no response found!)
26 2022-08-04 08:18:24.578900897	192.168.247.100	192.168.247.102	ICMP	118	0x60aa (24746)	255 Echo (ping) req	uest id	=0x007b, seq=12/3072, ttl=255 (no response found!)
27 2022-08-04 08:18:24.579426962	192.168.247.100	192.168.247.102	ICMP	128	0x60ab (24747)	255 Echo (ping) req	uest id	=0x007b, seq=13/3328, ttl=255 (no response found!)
ć								
> Forme 1: 130 butes on wine (1034 bits	1 130 button car	uned (1034 bits) o	o intenfaco	conturo un	3 14 0		0000 03	75 f2 00 00 1c 00 17 df d6 oc 00 90 36 90 3d
Ethernet II Src: Cisco desc:00 (00)	17.4f.46.00.00)	Det: 32:76:62:00:0	0.1c (22.76)	·f2.00.00.1/	-)		0010 00	3 60 81 60 63 e9 81 60 60 cf 68 60 45 60 60 64
V Ethernet II, Sith Cisco dolecido (dol	17.01.00.00.00);	DSC: 02:70:12:00:0	0.10 (32.70	.12.00.00.10	-/		0020 66	9 9e 00 00 ff 01 ea dd c0 a8 f7 64 c0 a8 f7 66 'df
vivi-tag	- Direction	. Foom Doidgo					0030 08	8 00 e5 c8 00 7b 00 00 00 00 00 02 4d 8c 4a 78 ·····{···M·Jx
	- Deleter	i From Brituge					0040 at	o cd ab cd
.0	= Pointer:	V11_10					0050 at	b cd ab cd
	= Descinati	on: 61	A				0060 ab	b cd ab cd
0	= Looped: N	0	* 1				0070 ab	b cd ab cd
	= Reserved:	0						
	= Version:	9						
0000 0000	0000 = Source: 0							
Type: 802.1Q Virtual LAN (0x8100)								
✓ 802.1Q Virtual LAN, PRI: 0, DEI: 0, 1	D: 1001							
000 Be	st Effort (defaul	t) (0)	2					
0 = DEI: Ineligi	ble		31					
0011 1110 1001 = ID: 1001			-					
Type: 802.1Q Virtual LAN (0x8100)								
802.1Q Virtual LAN, PRI: 0, DEI: 0, 1	(D: 207							
000 Be	st Effort (defaul	t) (0)						
0 = DEI: Ineligi	ble							
0000 1100 1111 = ID: 207			2					
Type: IPv4 (0x0800)			4					
> Internet Protocol Version 4, Src: 192	2.168.247.100. Ds	: 192,168,247,102						
> Internet Control Message Protocol	,							
and the second sec								

Select the second packet and check the key points:

- 1. Only ICMP echo request packets are captured. Each packet is captured and shown 2 times.
- 2. The original packet header has the VLAN tag 207.

No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info	
-	1 2022-08-04 08:18:24.572548869	192.168.247.100	192.168.247.102	ICMP	128	0x609e (24734)	255 Echo (ping) request	id=0x007b, seq=0/0, ttl=255 (no response found!)
	2 2022-08-04 08:18:24.572550073	192.168.247.100	192.168.247.102	ICMP	118	0x609e (24734)	255 Echo (ping) request	id=0x007b, seq=0/0, ttl=255 (no response found!)
	3 2022-08-04 08:18:24.573286630	192.168.247.100	192.168.247.102	ICMP	128	0x609f (24735)	255 Echo (ping) request	id=0x007b, seq=1/256, ttl=255 (no response found!)
	4 2022-08-04 08:18:24.573287640	192.168.247.100	192.168.247.102	ICMP	118	0x609f (24735)	255 Echo (ping) request	id=0x007b, seg=1/256, ttl=255 (no response found!)
	5 2022-08-04 08:18:24.573794751	192.168.247.100	192.168.247.102	ICMP	128	0x60a0 (24736)	255 Echo (ping) request	id=0x007b, seq=2/512, ttl=255 (no response found!)
	6 2022-08-04 08:18:24.573795748	192.168.247.100	192.168.247.102	ICMP	118	0x60a0 (24736)	255 Echo (ping) request	id=0x007b, seq=2/512, ttl=255 (no response found!)
	7 2022-08-04 08:18:24.574368638	192.168.247.100	192.168.247.102	ICMP	128	0x60a1 (24737)	255 Echo (ping) request	id=0x007b, seq=3/768, ttl=255 (no response found!)
	8 2022-08-04 08:18:24.574369574	192.168.247.100	192.168.247.102	ICMP	118	0x60a1 (24737)	255 Echo (ping) request	id=0x007b, seg=3/768, ttl=255 (no response found!)
	9 2022-08-04 08:18:24.574914512	192.168.247.100	192.168.247.102	ICMP	128	0x60a2 (24738)	255 Echo (ping) request	id=0x007b, seg=4/1024, ttl=255 (no response found!)
	10 2022-08-04 08:18:24.574915415	192.168.247.100	192.168.247.102	ICMP	118	0x60a2 (24738)	255 Echo (ping) request	id=0x007b, seg=4/1024, ttl=255 (no response found!)
	11 2022-08-04 08:18:24.575442569	192.168.247.100	192.168.247.102	ICMP	128	0x60a3 (24739)	255 Echo (ping) request	id=0x007b, seq=5/1280, ttl=255 (no response found!)
	12 2022-08-04 08:18:24.575443601	192.168.247.100	192.168.247.102	ICMP	118	0x60a3 (24739)	255 Echo (ping) request	id=0x007b, seq=5/1280, ttl=255 (no response found!)
	13 2022-08-04 08:18:24.575918119	192.168.247.100	192.168.247.102	ICMP	128	0x60a4 (24740)	255 Echo (ping) request	id=0x007b, seq=6/1536, ttl=255 (no response found!)
	14 2022-08-04 08:18:24.575919057	192.168.247.100	192.168.247.102	ICMP	118	0x60a4 (24740)	255 Echo (ping) request	id=0x007b, seg=6/1536, ttl=255 (no response found!)
	15 2022-08-04 08:18:24.576407671	192.168.247.100	192.168.247.102	ICMP	128	0x60a5 (24741)	255 Echo (ping) request	id=0x007b, seq=7/1792, ttl=255 (no response found!)
	16 2022-08-04 08:18:24.576408585	192.168.247.100	192.168.247.102	ICMP	118	0x60a5 (24741)	255 Echo (ping) request	id=0x007b, seq=7/1792, ttl=255 (no response found!)
	17 2022-08-04 08:18:24.576885643	192.168.247.100	192.168.247.102	ICMP	128	0x60a6 (24742)	255 Echo (ping) request	id=0x007b, seq=8/2048, ttl=255 (no response found!)
	18 2022-08-04 08:18:24.576886561	192.168.247.100	192.168.247.102	ICMP	118	0x60a6 (24742)	255 Echo (ping) request	id=0x007b, seq=8/2048, ttl=255 (no response found!)
	19 2022-08-04 08:18:24.577394328	192.168.247.100	192.168.247.102	ICMP	128	0x60a7 (24743)	255 Echo (ping) request	id=0x007b, seq=9/2304, ttl=255 (no response found!)
	20 2022-08-04 08:18:24.577395234	192.168.247.100	192.168.247.102	ICMP	118	0x60a7 (24743)	255 Echo (ping) request	id=0x007b, seq=9/2304, ttl=255 (no response found!)
	21 2022-08-04 08:18:24.577987632	192.168.247.100	192.168.247.102	ICMP	128	0x60a8 (24744)	255 Echo (ping) request	id=0x007b, seq=10/2560, ttl=255 (no response found!)
	22 2022-08-04 08:18:24.577989290	192.168.247.100	192.168.247.102	ICMP	118	0x60a8 (24744)	255 Echo (ping) request	id=0x007b, seq=10/2560, ttl=255 (no response found!)
	23 2022-08-04 08:18:24.578448781	192.168.247.100	192.168.247.102	ICMP	128	0x60a9 (24745)	255 Echo (ping) request	id=0x007b, seq=11/2816, ttl=255 (no response found!)
	24 2022-08-04 08:18:24.578449909	192.168.247.100	192.168.247.102	ICMP	118	0x60a9 (24745)	255 Echo (ping) request	id=0x007b, seq=11/2816, ttl=255 (no response found!)
	25 2022-08-04 08:18:24.578900043	192.168.247.100	192.168.247.102	ICMP	128	0x60aa (24746)	255 Echo (ping) request	id=0x007b, seq=12/3072, ttl=255 (no response found!)
	26 2022-08-04 08:18:24.578900897	192.168.247.100	192.168.247.102	ICMP	118	0x60aa (24746)	255 Echo (ping) request	id=0x007b, seq=12/3072, ttl=255 (no response found!)
	27 2022-08-04 08:18:24.579426962	192.168.247.100	192.168.247.102	ICMP	128	0x60ab (24747)	255 Echo (ping) request	id=0x007b, seq=13/3328, ttl=255 (no response found!)
< C								
E.	Ename 3: 110 butes on wine (044 bits)	110 butor cont	unad (044 hits) on	ntonfaco ca	sture up 2	ida		a2 76 f2 00 00 1c 00 17 df d6 oc 00 01 00 00 cf
1	Frame 2: 118 bytes on wire (944 bits)	, 118 bytes capto	ned (944 bits) on .	Interface ca	pture_u0_3,	, 10 0	0000	a2 76 12 00 00 10 00 17 01 06 00 00 81 00 00 01
ú	Page to Vietual LAN DRI & DET O T	17:01:00:ec:00),	USL: 02:70:T2:00:0	2:1C (az:/o:	2:00:00:10	.)	0020	f7 64 c8 a8 f7 66 88 88 e5 c8 88 7b 88 88 89 a d f.
ľ	and a second the second	u: 207	+) (0)				0030	00 02 4d 8c 4a 78 ab cd ab cd ab cd ab cd ab cd ab cdM. 3x
	ooo Priority: Be	SC ETTOPC (Geraul	() (0)				0040	ab cd
	0000 1100 1111 - TD: 207	bie		2			0050	ab cd
н	Tupol Thut (0x0000)			21			0060	ab cd
	Internet Protocol Version 4 Sec: 103	169 347 100 Det	. 103 169 347 103	_			0070	ab cd ab cd ab cd
11	Internet Control Message Protocol	.100.247.100, 05	. 192.106.247.102					
11	internet control nessage Protocol							
1								

#### Explanation

When a packet capture on a front interface is configured, the switch simultaneously captures each packet twice:

- After the insertion of the port VLAN tag.
- After the insertion of the VN tag.

In the order of operations, the VN tag is inserted at a later stage than the port VLAN tag insertion. But in the capture file, the packet with the VN tag is shown earlier than the packet with the port VLAN tag. Additionally, in the case of subinterfaces, in the capture files, every second packet does not contain the port VLAN tag.

This table summarizes the task:

Task	Capture point	Internal port VLAN in captured packets	Direction	Captured traffic
Configure and verify a packet capture on subinterface Ethernet1/2.205	Ethernet1/2.205	102	Ingress only	ICMP echo requests from host 192.0.2.100 to host 198.51.100.100
Configure and verify a packet capture on Portchannel1 subinterface with member interfaces Ethernet1/3 and Ethernet1/4	Ethernet1/3 Ethernet1/4	1001	Ingress only	ICMP echo requests from 192.168.207.100 to host 192.168.207.102

# **Packet Capture Filters**

Use the FCM and CLI to configure and verify a packet capture on interface Ethernet1/2 with a filter.

## Topology, packet flow, and the capture points



## Configuration

## FCM

Perform these steps on FCM to configure a capture filter for ICMP echo request packets from host 192.0.2.100 to host 198.51.100.100 and apply it to packet capture on interface Ethernet1/2:

- 1. Use **Tools > Packet Capture > Filter List > Add Filter** to create a capture filter.
- 2. Specify the Filter Name, Protocol, Source IPv4, Destination IPv4 and click Save:

Overview Inter	faces Logical Devices Si	ecurity Engine Plat	form Settings									System Tools	Help admin
Capture Session	Filter List												
Filter List												A	id Filter
	_	From		_	_	То			_			_	_
Filter Name	MAC	IPv4	IPv6	Port	MAC	IPv4	IPv6	Port	Protocol	Inner vlan	Outer vlan	EtherType	
filter_icmp	00:00:00:00:00:00	192.0.2.100	п	0	00:00:00:00:00:00	192.0.2.100	П	0	1	0	0	0	/ 8
				Edit Packe	t Filter			(? X					
				Filter Name*	filter_icmp								
				Protocol	ICMP IPv4 ¥								
				EtherType	Any 👻								
				Inner vlan	0	Outer vlan	0						
				Source		Destination							
				IPv4	192.0.2.100	IPv4	198.51.100.100						
				IPv6		IPv6	:						
				Port	0	Port	0						
				MAC	00:00:00:00:00:00	MAC	00:00:00:00:00:00	0					
							Save	Cancel					
								_					

3. Use **Tools > Packet Capture > Capture Session** to create a new capture session:

Overview Interfaces Logical Devices Security Engine Platform Settings	System	Tools Help admin
	Packet Capture	Troubleshooting Logs
Capture Session Fiter List		
C Refresh	Capture Session Delet	e All Sessions
No Session available		

4. Select Ethernet1/2, provide the **Session Name**, apply the capture filter and click **Save and Run** to activate the capture:

Overview Interfaces Logical Devices Security Engine Platform Settings	System Tools Help admin
Select an instance: Rtd1 V	Save and Run Save Cancel
ftd1	Session Name* cap1 Selected Interfaces Ethernet1/2
Ethernet1/2	Buffer Size 256 MB Y Snap length: 1518 Bytes Store Packets Overwrite Append
Ethernet1/3 FTD FTD Ethernet1/9, Ethernet1/10	Capture Filter Capture Filter Capture All Apply Filter Create Filter Apply Filter_icmp To Ethemet1/2
EthernetI/1	

#### **FXOS CLI**

Perform these steps on FXOS CLI to configure packet captures on backplane interfaces:

1. Identify the application type and identifier:

<#root>								
firepower#								
scope ssa								
firepower , show app-in	/ssa# nstance							
App Name	Identifier Slot ID	Admin State	Oper State	Running Version	Startup	Version	Deploy T	Г <b>у</b>
ftd	ftdl							
1	Enabled	Online	7.2.0.82	7.2.0.82	Native	No		

2. Identify the IP protocol number in <u>https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml</u>. In this case, the ICMP protocol number is 1.

3. Create a capture session:

```
<#root>
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 filter filter_icmp
firepower /packet-capture/session/phy-port* #
exit
firepower /packet-capture/session* #
enable
firepower /packet-capture/session* #
commit
firepower /packet-capture/session #
```

## Verification

## FCM

Verify the Interface Name, ensure that the Operational Status is up and that the File Size (in bytes) increases:

Overview Interf	faces Logical Devices Se	ecurity Engine Plat	form Settings									System Tools	Help admin
Chabura Carring	Share Link												
Filter List	nter List												ód Filter
		From				То							
Filter Name	мас	IPv4	IPv6	Port	мас	IPv4	IPv6	Port	Protocol	Inner vlan	Outer vlan	EtherType	
filter_icmp	00:00:00:00:00:00	192.0.2.100		0	00:00:00:00:00:00	198.51.100.100		0	1	0	0	0	/8

Verify the Interface Name, the Filter, ensure the Operational Status is up, and the File Size (in bytes) increases in Tools > Packet Capture > Capture Session:

Overview Int	erfaces L	ogical Devices	Security Engine	Platform Settings					System Tools H	lelp admin
Capture Session	Filter List									
								C Refresh Capture Session	Delete All Sessions	
•	cap1		Prop Count: 0		Operational State: up		Buffer Size: 256 MB	Snap Length: 1518 Bytes		
Interface Nam	е	Filter		File Size (in bytes)	File Name	Device Name				
Ethernet1/2		filter_icmp		84340	cap1-ethernet-1-2-0.pcap	ftd1	*			

### **FXOS CLI**

Verify the capture details in scope packet-capture:

<#root>

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
```

#### **Collect capture files**

Perform the steps in the section Collect Firepower 4100/9300 Internal Switch Capture Files.

#### **Capture file analysis**

Use a packet capture file reader application to open the capture file. Select the first packet and check the key points

- 1. Only ICMP echo request packets are captured. Each packet is captured and shown 2 times.
- 2. The original packet header is without the VLAN tag.
- 3. The internal switch inserts additional port VLAN tag **102** that identifies the ingress interface Ethernet1/2.
- 4. The internal switch inserts an additional VN tag.

No. Time	Source	Destination	Protocol	Length	PD	IP TTL Info						^
1 2022-08-02 15:46:55.603277760	192.0.2.100	198.51.100.100	ICMP	108 -	0x0012 (1	8) 64 Ech	o (ping) ı	request id=	0x0018, s	seq=349/23809,	ttl=64 (r	io r
2 2022-08-02 15:46:55.603279688	192.0.2.100	198.51.100.100	ICMP	102	0x0012 (1	<li>8) 64 Ech</li>	o (ping) n	request id=	0x0018, s	seq=349/23809,	ttl=64 (r	or
3 2022-08-02 15:46:56.627139252	192.0.2.100	198.51.100.100	ICMP	108	0x00db (2	(19) 64 Ech	o (ping) ı	request id=	0x0018, s	seq=350/24065,	ttl=64 (r	or
4 2022-08-02 15:46:56.627140919	192.0.2.100	198.51.100.100	ICMP	102	0x00db (2	(19) 64 Ech	o (ping) n	request id=	0x0018, s	seq=350/24065,	ttl=64 (r	or
5 2022-08-02 15:46:57.651185193	192.0.2.100	198.51.100.100	ICMP	108	0x01cb (4	59) 64 Ech	o (ping) ı	request id=	0x0018, s	seq=351/24321,	ttl=64 (r	or
6 2022-08-02 15:46:57.651186787	192.0.2.100	198.51.100.100	ICMP	102	0x01cb (4	59) 64 Ech	o (ping) ı	request id=	0x0018, s	seq=351/24321,	ttl=64 (r	or
7 2022-08-02 15:46:58.675153317	192.0.2.100	198.51.100.100	ICMP	108	0x01d6 (4	(70) 64 Ech	o (ping) ı	request id=	0x0018, s	seq=352/24577,	ttl=64 (r	or
8 2022-08-02 15:46:58.675154503	192.0.2.100	198.51.100.100	ICMP	102	0x01d6 (4	(70) 64 Ech	o (ping) ı	request id=	0x0018, s	seq=352/24577,	ttl=64 (r	or
9 2022-08-02 15:46:59.699152639	192.0.2.100	198.51.100.100	ICMP	108	0x01f4 (5	00) 64 Ech	o (ping) ı	request id=	0x0018, s	seq=353/24833,	ttl=64 (r	or
10 2022-08-02 15:46:59.699153835	192.0.2.100	198.51.100.100	ICMP	102	0x01f4 (5	64 Ech	o (ping) ı	request id=	0x0018, s	seq=353/24833,	ttl=64 (r	or
11 2022-08-02 15:47:00.723142641	192.0.2.100	198.51.100.100	ICMP	108	0x01f9 (5	05) 64 Ech	o (ping) ı	request id=	0x0018, s	seq=354/25089,	ttl=64 (r	or
12 2022-08-02 15:47:00.723144643	192.0.2.100	198.51.100.100	ICMP	102	0x01f9 (5	64 Ech	o (ping) ı	request id=	0x0018, s	seq=354/25089,	ttl=64 (r	or
13 2022-08-02 15:47:01.747162204	192.0.2.100	198.51.100.100	ICMP	108	0x026e (6	22) 64 Ech	o (ping) ı	request id=	0x0018, s	seq=355/25345,	ttl=64 (r	or
14 2022-08-02 15:47:01.747163783	192.0.2.100	198.51.100.100	ICMP	102	0x026e (6	22) 64 Ech	o (ping) ı	request id=	0x0018, s	seq=355/25345,	ttl=64 (r	or
15 2022-08-02 15:47:02.771209952	192.0.2.100	198.51.100.100	ICMP	108	0x02bc (7	'00) 64 Ech	o (ping) ı	request id=	0x0018, s	seq=356/25601,	ttl=64 (r	or
16 2022-08-02 15:47:02.771211062	192.0.2.100	198.51.100.100	ICMP	102	0x02bc (7	'00) 64 Ech	o (ping) n	request id=	0x0018, s	seq=356/25601,	ttl=64 (r	or
17 2022-08-02 15:47:03.772258550	192.0.2.100	198.51.100.100	ICMP	108	0x032f (8	(15) 64 Ech	o (ping) ı	request id=	0x0018, s	seq=357/25857,	ttl=64 (r	or
18 2022-08-02 15:47:03.772259724	192.0.2.100	198.51.100.100	ICMP	102	0x032f (8	15) 64 Ech	o (ping) ı	request id=	0x0018, s	seq=357/25857,	ttl=64 (r	or
19 2022-08-02 15:47:04.791118519	192.0.2.100	198.51.100.100	ICMP	108	0x040f (1	(039) 64 Ech	o (ping) ı	request id=	0x0018, s	seq=358/26113,	ttl=64 (r	or
20 2022-08-02 15:47:04.791119721	192.0.2.100	198.51.100.100	ICMP	102	0x040f (1	.039) 64 Ech	o (ping) ı	request id=	0x0018, s	seq=358/26113,	ttl=64 (r	or v
<												>
> Frame 1: 108 bytes on wire (864 bit	ts), 108 bytes ca	ptured (864 bits) o	n interface c	apture_u0_	1, i 0000	58 97 bd b9 77	0e 00 50	56 9d e8 be	89 26 80	0 0a X···w··I	P V····&·	
> Ethernet II, Src: VMware 9d:e8:be (	(00:50:56:9d:e8:b	e), Dst: Cisco b9:7	7:0e (58:97:b	d:b9:77:0e	) 0010	00 00 81 00 00	66 08 00	45 00 00 54	4 00 12 40	0 00 ·····f·	· E · · T · ·@	
✓ VN-Tag					0020	40 01 4d 9b c0	00 02 64	c6 33 64 64	4 08 00 90	e 67 @·M····	d · 3dd · · · ·	8
1	= Directi	ion: From Bridge			0030	00 18 01 5d e2	46 e9 62	00 00 00 00	0 c1 a6 00	c 00 ···]·F·I	o	·
.0	= Pointer	<pre>r: vif_id</pre>			0040	00 00 00 00 10	11 12 13	14 15 16 1	/ 18 19 18	a 10		
00 0000 0000 1010	= Destina	ation: 10			0050	10 10 1e 1f 20	21 22 23	24 25 26 2	7 28 29 20	d 20 ! i	7 3A& ()-	' I
0	= Looped:	:No 4			0000	20 20 20 21 50	51 52 55	34 33 30 31	/	,/012	3 4307	
0	= Reserve	ed: 0										
	= Version	n: 0										
0000 00	00 0000 = Source:	0										
Type: 802.1Q Virtual LAN (0x8100	)											
<ul> <li>802.1Q Virtual LAN, PRI: 0, DEI: 0</li> </ul>	, ID: 102											
000 = Priority:	Best Effort (defa	ault) (0)										
0 = DEI: Ineli	gible	3										
0000 0110 0110 = ID: 102												
Type: IPv4 (0x0800)												
> Internet Protocol Version 4, Src: 1	192.0.2.100, Dst:	198.51.100.100										
> Internet Control Message Protocol		2										
<					>							

Select the second packet, and check the key points:

- 1. Only ICMP echo request packets are captured. Each packet is captured and shown 2 times.
- 2. The original packet header is without the VLAN tag.
- 3. The internal switch inserts additional port VLAN tag **102** that identifies the ingress interface Ethernet1/2.

,	No. Time	Source D	Vestination	Protocol	Length	IP ID		IP TT	L Info							^
	1 2022-08-02 15:46:55.603277760	192.0.2.100 1	98.51.100.100	ICMP	108 1	0x0012 (	(18)	6	4 Echo	(ping)	request	id=0x0018,	seq=349/23809	, ttl=64	(no r	
	2 2022-08-02 15:46:55.603279688	192.0.2.100 1	98.51.100.100	ICMP	102	0x0012 (	(18)	6	4 Echo	(ping)	request	id=0x0018,	seq=349/23809	, ttl=64	(no r	
Г	3 2022-08-02 15:46:56.627139252	192.0.2.100 1	98.51.100.100	ICMP	108	0x00db (	(219)	6	4 Echo	(ping)	request	id=0x0018,	seq=350/24065	, ttl=64	(no r	
	4 2022-08-02 15:46:56.627140919	192.0.2.100 1	98.51.100.100	ICMP	102	0x00db (	(219)	6	4 Echo	(ping)	request	id=0x0018,	seq=350/24065	, ttl=64	(no r	
	5 2022-08-02 15:46:57.651185193	192.0.2.100 1	98.51.100.100	ICMP	108	0x01cb (	(459)	6	4 Echo	(ping)	request	id=0x0018,	seq=351/24321	, ttl=64	(no r	
Г	6 2022-08-02 15:46:57.651186787	192.0.2.100 1	98.51.100.100	ICMP	102	0x01cb (	(459)	6	4 Echo	(ping)	request	id=0x0018,	seq=351/24321	, ttl=64	(no r	
Г	7 2022-08-02 15:46:58.675153317	192.0.2.100 1	98.51.100.100	ICMP	108	0x01d6 (	(470)	6	4 Echo	(ping)	request	id=0x0018,	seq=352/24577	, ttl=64	(no r	
	8 2022-08-02 15:46:58.675154503	192.0.2.100 1	98.51.100.100	ICMP	102	0x01d6 (	(470)	6	4 Echo	(ping)	request	id=0x0018,	seq=352/24577	, ttl=64	(no r	
	9 2022-08-02 15:46:59.699152639	192.0.2.100 1	98.51.100.100	ICMP	108	0x01f4 (	(500)	6	4 Echo	(ping)	request	id=0x0018,	seq=353/24833	, ttl=64	(no r	
	10 2022-08-02 15:46:59.699153835	192.0.2.100 1	98.51.100.100	ICMP	102	0x01f4 (	(500)	6	4 Echo	(ping)	request	id=0x0018,	seq=353/24833	, ttl=64	(no r	
	11 2022-08-02 15:47:00.723142641	192.0.2.100 1	98.51.100.100	ICMP	108	0x01f9 (	(505)	6	4 Echo	(ping)	request	id=0x0018,	seq=354/25089	, ttl=64	(no r	
	12 2022-08-02 15:47:00.723144643	192.0.2.100 1	98.51.100.100	ICMP	102	0x01f9 (	(505)	6	4 Echo	(ping)	request	id=0x0018,	seq=354/25089	, ttl=64	(no r	
L	13 2022-08-02 15:47:01.747162204	192.0.2.100 1	98.51.100.100	ICMP	108	0x026e (	(622)	6	4 Echo	(ping)	request	id=0x0018,	seq=355/25345	, ttl=64	(no r	
	14 2022-08-02 15:47:01.747163783	192.0.2.100 1	98.51.100.100	ICMP	102	0x026e (	(622)	6	4 Echo	(ping)	request	id=0x0018,	seq=355/25345	, ttl=64	(no r	
	15 2022-08-02 15:47:02.771209952	192.0.2.100 1	98.51.100.100	ICMP	108	0x02bc (	(700)	6	4 Echo	(ping)	request	id=0x0018,	seq=356/25601	, ttl=64	(no r	
	16 2022-08-02 15:47:02.771211062	192.0.2.100 1	98.51.100.100	ICMP	102	0x02bc (	(700)	6	4 Echo	(ping)	request	id=0x0018,	seq=356/25601	, ttl=64	(no r	
н	17 2022-08-02 15:47:03.772258550	192.0.2.100 1	98.51.100.100	ICMP	108	0x032f (	(815)	6	4 Echo	(ping)	request	id=0x0018,	seq=357/25857	, ttl=64	(no r	
L	18 2022-08-02 15:47:03.772259724	192.0.2.100 1	98.51.100.100	ICMP	102	0x032f (	(815)	6	4 Echo	(ping)	request	id=0x0018,	seq=357/25857	, ttl=64	(no r	
	19 2022-08-02 15:47:04.791118519	192.0.2.100 1	98.51.100.100	ICMP	108	0x040f (	(1039)	6	4 Echo	(ping)	request	id=0x0018,	seq=358/26113	, ttl=64	(no r	
	20 2022-08-02 15:47:04.791119721	192.0.2.100 1	98.51.100.100	ICMP	102	0x040f (	(1039)	6	4 Echo	(ping)	request	id=0x0018,	seq=358/26113	, ttl=64	(no r	~
4	c														>	
	> Frame 2: 102 bytes on wire (816 bit	ts), 102 bytes capt	ured (816 bits) on	interface ca	pture u0 :	1, ie 000	00 <b>58</b>	97 bd b	9 77 0	e 00 50	56 9d e	8 be 81 00	00 66 X···w·	·P V····	٠f	
	> Ethernet II, Src: VMware 9d:e8:be (	(00:50:56:9d:e8:be)	, Dst: Cisco b9:77	:0e (58:97:bd	:b9:77:0e	) 001	10 08	00 45 0	0 00 5	4 00 12	40 00 4	10 01 4d 9b	c0 00 ··E··T	··· @·@·M·		
	802.10 Virtual LAN, PRI: 0, DEI: 0.	, ID: 102				002	20 02	64 c6 3	3 64 6	4 08 00	9e 67 0	0 18 01 5d	e2 46 ·d·3dd	····g····]	- F	
L	000 = Priority:	Best Effort (defaul	t) (0)			003	30 e9	62 00 0	0 00 0	0 c1 a6	0c 00 0	00 00 00 00	10 11 ·b····			
L	0 = DEI: Ineli	gible	3			004	40 12	13 14 1	5 16 1	7 18 19	1a 1b 1	c 1d 1e 1f	20 21			
L	0000 0110 0110 = ID: 102	-				005	50 22	23 24 2	5 26 2	7 28 29	2a 20 2	20 20 2e 2f	30 31 "#\$%&"	() *+,/	01	
Т	Type: IPv4 (0x0800)					006	50 32	55 54 3	5 36 3	<i>'</i>			234567			
	> Internet Protocol Version 4, Src: 1	192.0.2.100, Dst: 19	98.51.100.100													
	> Internet Control Message Protocol		2													
Т																

## Explanation

When a packet capture on a front interface is configured, the switch simultaneously captures each packet twice:

- After the insertion of the port VLAN tag.
- After the insertion of the VN tag.

In the order of operations, the VN tag is inserted at a later stage than the port VLAN tag insertion. But in the capture file, the packet with the VN tag is shown earlier than the packet with the port VLAN tag.

When a capture filter is applied only the packets that match the filter in the ingress direction are captured.

This table summarizes the task:

Task	Capture point	Internal port VLAN in captured packets	Direction	User filter	Captured traffic
Configure and verify a packet capture with a filter on the front interface Ethernet1/2	Ethernet1/2	102	Ingress only	Protocol: ICMP Source:192.0.2.100 Destination: 198.51.100.100	ICMP echo requests from host 192.0.2.100 to host 198.51.100.100

# **Collect Firepower 4100/9300 Internal Switch Capture Files**

## FCM

Perform these steps on FCM to collect internal switch capture files:

1. Click the **Disable Session** button to stop the active capture:

Overview	Interfaces	Logical Devices	Security Engine	Platforn	n Settings					System 1	ools He	lp admin
Capture Ses	ision Filter Li	st										
								C Refresh Capta	ure Session	Delete All Se	ssions	
	cap1	Drop Coun	t: 0	Operat	ional State: up	Buffer Size: 256 MB		Snap Length: 151	l8 Bytes			
Interface Na	ame	Filter			File Size (in bytes)	File Name	Device Name					
Ethernet1/2		None			34700	cap1-ethemet-1-2-0.pcap	ftd1		$\pm$			

2. Ensure the operational state is **DOWN - Session\_Admin\_Shut:** 

Overview	Interfaces	Logical Devices	Security Engine	Platform Settings					s	ystem	Tools	Help	admin
Capture Ses	sion Filter Lis	t											
								C Refresh Captu	re Session	Delete All	Sessions		
	cap1	Drop Count	t: 0	Operational State: DOWN - Sess	ion_Admin_Shut	Buffer Size: 256 MB		Snap Length: 151	8 Bytes			2	8 🖾
Interface Na	ime	Filter		File Size (in bytes)	F	ile Name	Device Name						
Ethernet1/2		None		218828	c	cap1-ethemet-1-2-0.pcap	ftd1		$\pm$				

3. Click **Download** to download the capture file:

Overview	Interfaces	Logical Devices	Security Engine	Platform Settings					System	Tools ⊦	lelp admin
Capture Se	ssion Fiter Li	st									
								Capture Session	Delete All S	Sessions	
	cap1	Drop Coun	t: 0	Operational State: DO	OWN - Session_Admin_Shut	Buffer Size: 256 MB		Snap Length: 1518 Bytes			/88
Interface I	lame	Filter		File Size (in l	bytes)	File Name	Device Name				
Ethernet1/2	2	None		218828		cap1-ethemet-1-2-0.pcap	ftd1	*			

In the case of port-channel interfaces, repeat this step for each member interface.

## **FXOS CLI**

Perform these steps on the FXOS CLI to collect capture files:

```
1. Stop the active capture:
```

<#root> 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: O Application Instance Identifier: ftd1 Application Name: ftd

2. Upload the capture file from the **local-mgmt** command scope:

<#root>

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:

In the case of port-channel interfaces, copy the capture file for each member interface.

## Guidelines, Limitations, and Best Practices for Internal Switch Packet Capture

For the guidelines and limitations related to Firepower 4100/9300 internal switch capture refer to the *Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide* or *Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*, chapter **Troubleshooting**, section **Packet Capture**.

This is the list of best practices based on the usage of packet capture in TAC cases:

- Be aware of guidelines and limitations.
- Capture packets on all port-channel member interfaces and analyze all capture files.
- Use capture filters.
- Consider the impact of NAT on packet IP addresses when a capture filter is configured.
- Increase or decrease the **Snap Len** that specifies frame size in case it differs from the default value of 1518 bytes. Shorter size results in an increased number of captured packets and vice versa.
- Adjust the **Buffer Size** as needed.
- Be aware of the **Drop Count** on FCM or FXOS CLI. Once the buffer size limit is reached, the drop count counter increases.
- Use the filter **!vntag** on Wireshark to display only packets without the VN-tag. This is useful to hide VN-tagged packets in the front interface packet capture files.
- Use the filter **frame.number&1** on Wireshark to display only odd frames. This is useful to hide duplicate packets in the backplane interface packet capture files.
- In the case of protocols like TCP, Wireshark by default applies colorization rules that display packets with specific conditions in different colors. In the case of internal switch captures due to duplicate packets in capture files, the packet can be colored and marked in a false-positive way. If you analyze packet capture files and apply any filter, then export the displayed packets to a new file and open the new file instead.

# **Configuration and Verification on Secure Firewall 3100/4200**

Unlike Firepower 4100/9300, the internal switch captures on the Secure Firewall 3100/4200 are configured on the application command line interface via the **capture** <**name> switch** command, where the **switch** option specifies that the captures are configured on the internal switch.

This is the **capture** command with the **switch** option:

<#root>

```
> 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>

General steps for packet capture configuration are as follows:

1. Specify an ingress interface:

Switch capture configuration accepts the ingress interface **nameif**. The user can specify data interfaces names, internal uplink, or the management interfaces:

<#root>
>
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

The Secure Firewall 4200 supports bidirectional captures. The default value is **ingress**, unless specified otherwise:

<#root>

>

capture capi switch interface inside direction

bothTo capture switch bi-directional trafficegressTo capture switch egressing trafficingressTo capture switch ingressing traffic

Additionall, the Secure Firewall 4245 has 2 internal data and 2 management uplink interfaces:

<#root>

>

capture capsw switch interface

eventing Name of interface Management1/2 in\_data\_uplink1 Capture packets on internal data uplink1 interface in\_data\_uplink2 Capture packets on internal data uplink2 interface in\_mgmt\_uplink1 Capture packets on internal mgmt uplink1 interface in\_mgmt\_uplink2 Capture packets on internal mgmt uplink1 interface management Name of interface Management1/1 2. Specify the ethernet frame EtherType. The default EtherType is IP. The **ethernet-type** option values specify the EtherType:

<#root>

>

```
capture capsw switch interface inside ethernet-type ?
```

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

3. Specify the match conditions. The capture **match** option specifies the match criteria:

<#root>

```
>
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-address filter
  mac
  nos
  ospf
  рср
  pim
  pptp
  sctp
  snp
           SPI value
  spi
  tcp
  udp
  <cr>
```

4. Specify other optional parameters such as the buffer size, the packet length, and so on.

5. Enable the capture. The command **no capture <name> switch stop** activates the capture:

<#root>

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

6. Verify the capture details:

- Administrative status is enabled, and operational status is up and active.
- Packet capture file size **Pcapsize** increases.
- The number of captured packets in the output of the **show capture** <**cap\_name**> is non-zero.
- Capture path **Pcapfile.** The captured packets are automatically saved in the /mnt/disk0/packet-capture/ folder.
- Capture conditions. The software automatically creates capture filters based on capture conditions.

<#root>

```
>
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 18838 Pcapsize: 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 00:00:00:00:00:00 Dest MAC: Src Port: 0 0 Dest Port: 0 Ethertype: 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. Stop the captures when needed:

<#root>

>

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 0 Drop Count: 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 24 Pcapsize: Filter: capsw-1-1 Packet Capture Filter Info capsw-1-1 Name: Protocol: 0 Ivlan: 0 Ovlan: 205 Src Ip: 0.0.0.0 Dest Ip: 0.0.0.0 Src Ipv6: :: Dest Ipv6: :: 00:00:00:00:00:00 Src MAC: Dest MAC: 00:00:00:00:00:00 Src Port: 0 0 Dest Port: 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. Collect the capture files. Perform the steps in the section **Collect Secure Firewall Internal Switch Capture Files**.

In Secure Firewall software version 7.4, the internal switch capture configuration is not supported on the FMC or FDM. In the case of ASA software version 9.18(1) and later, internal switch captures can be configured in ASDM versions 7.18.1.x and later.

These scenarios cover common use cases of Secure Firewall 3100/4200 internal switch captures.

# Packet Capture on a Physical or Port-channel Interface

Use the FTD or ASA CLI to configure and verify a packet capture on interface Ethernet1/1 or Portchannel1 interface. Both interfaces have the name of **inside**.

## Topology, packet flow, and the capture points

Secure Firewall 3100:



Secure Firewall 4200 with bidirectional captures:

	Chassis						
	Internal Switch		Security Module				
	Lth1/		FTD/ASA				
	RX						
192.0.2.100 ICMP echo-request	Eth1/2	Uplink	inside				
198.51.100.100			outside				

## Configuration

Perform these steps on ASA or FTD CLI to configure a packet capture on interface Ethernet1/1 or Portchannel1:

1. Verify the nameif:

<#root>

>

```
show nameif
```

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

<#root>

>

#### show nameif

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

#### 2. Create a capture session

- <#root>
- >

capture capsw switch interface inside

The Secure Firewall 4200 supports capture directionality:

<#root>

> capture capsw switch interface inside direction ?

both To capture switch bi-directional traffic egress To capture switch egressing traffic ingress To capture switch ingressing traffic

> capture capsw switch interface inside direction both

3. Enable the capture session:

#### <#root>

> no capture capsw switch stop

#### Verification

Verify the capture session name, administrative and operational state, interface slot, and identifier. Ensure the **Pcapsize** value in bytes increases and the number of captured packets is non-zero:

<#root> > 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 0.0.0.0 Src Ip: 0.0.0.0 Dest Ip: 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

Secure Firewal 4200:

<#root>

>

show cap 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

1
1
/mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
0

Direction: both

Drop: disable

Filter: capsw-1-1 Packet Capture Filter Info Name: capsw-1-1 Protocol: 0 0 Ivlan: Ovlan: 0 Src Ip: 0.0.0.0 Dest Ip: 0.0.0.0 Src Ipv6: :: Dest Ipv6: :: 00:00:00:00:00:00 Src MAC: Dest MAC: 00:00:00:00:00:00 Src Port: 0 Dest Port: 0 0 Ethertype: Total Physical breakout ports involved in Packet Capture: 0

Reading of capture file from disk is not supported

33 packet captured on disk using switch capture

capsw

enabled

1

up

yes

In the case of Port-channel1 the capture is configured on all member interfaces:

<#root>

> show capture capsw detail Packet Capture info Name: Session: Admin State: Oper State: Oper State Reason: Active Config Success: 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 Fi	lter 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
Dest MAC:	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 Fi	lter 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
Dest MAC:	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

The port-channel member interfaces can be verified in the FXOS **local-mgmt** command shell via the **show portchannel summary** command:

```
<#root>
connect fxos
firewall#
connect local-mgmt
firewall(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
_____
  Pol(U) Eth LACP Eth1/3(P) Eth1/4(P)
1
LACP KeepAlive Timer:
_____
   Channel PeerKeepAliveTimerFast
_____
1
   Po1(U)
         False
Cluster LACP Status:
_____
   Channel ClusterSpanned ClusterDetach ClusterUnitID ClusterSysID
_____
  Po1(U) False
                 False
                          0
                                 clust
1
```

To access the FXOS on ASA, run the **connect fxos admin** command. In the case of multi-context, run the command in the admin context.

## **Collect capture files**

Perform the steps in the section Collect Secure Firewall Internal Switch Capture Files.

#### Capture file analysis

Use a packet capture file reader application to open the capture files for Ethernet1/1. In this example, the packets capture on the Secure Firewall 3100 are analyzed. Select the first packet and check the key points:

- 1. Only ICMP echo request packets are captured.
- 2. The original packet header is without the VLAN tag.

No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info	^
<b>F</b>	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 r€
	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 r€
	6 2022-08-07 19:50:11.929144	192.0.2.100	198.51.100.100	ICMP	102	0x9b34 (39732)	64 Echo (ping) request	id=0x0034, seq=6/1536, ttl=64 (no r€
	7 2022-08-07 19:50:12.932943	192.0.2.100	198.51.100.100	ICMP	102	0x9b83 (39811)	64 Echo (ping) request	id=0x0034, seq=7/1792, ttl=64 (no r€
	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 r€
	9 2022-08-07 19:50:14.932004	192.0.2.100	198.51.100.100	ICMP	102	0x9c07 (39943)	64 Echo (ping) request	id=0x0034, seq=9/2304, ttl=64 (no re
	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 r
	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 r
	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 r
	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 r
	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 r
	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 r
	16 2022-08-07 19:50:21.940288	192.0.2.100	198.51.100.100	ICMP	102	0x9fe4 (40932)	64 Echo (ping) request	id=0x0034, seq=16/4096, ttl=64 (no r
	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 r
	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 r
<								, , , , , , , , , , , , , , , , , , , ,
	name 1: 102 butes on wire (816 hits)	102 hytes cant	ured (816 hits)			0000 bc e7 12	34 93 14 88 58 56 94 88	he as aa 45 aa
	thernet II Spc: Whore Odiegibe (00	, 102 bytes capt	Det: Cisco 34:02:	4 (hc:e7:12:3	4:02:14)	0010 00 54 9a	10 40 00 40 01 b3 9c c0	00 02 64 c6 33 ·T··@·@· ····d·3
	sternet Protocol Version 4 Spc: 103	0 2 100 Det: 1	09 51 100 100	14 (00.07.12.5	4.90.14)	0020 64 64 08	00 c6 91 00 34 00 01 61	17 f0 62 00 00 dd 4ab
	nternet Control Message Protocol	.0.2.100, 050. 1	56.51.100.100		2	0030 00 00 18	ec 08 00 00 00 00 00 10	11 12 13 14 15
٦Ľ	iter net control hessage Protocol					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	670000

Open the capture files for Portchannel1 member interfaces. Select the first packet and check the key points:

- 1. Only ICMP echo request packets are captured.
- 2. The original packet header is without the VLAN tag.

No	. Time	Source	Destination	Protocol	Length	IP 1D		IPTTL Info		^
C	1 2022-08-07 20:40:58.657533	192.0.2.100	198.51.100.100	ICMP	102	0x9296 (3	37526)	64 Echo (ping) request	id=0x0035, seq=1/256, ttl=64 (no re	s
	2 2022-08-07 20:40:59.658611	192.0.2.100	198.51.100.100	ICMP	102	0x9370 (3	37744)	64 Echo (ping) request	id=0x0035, seq=2/512, ttl=64 (no re	s
	3 2022-08-07 20:41:00.655662	192.0.2.100	198.51.100.100	ICMP	102	0x93f0 (3	37872)	64 Echo (ping) request	id=0x0035, seq=3/768, ttl=64 (no re	s
	4 2022-08-07 20:41:01.659749	192.0.2.100	198.51.100.100	ICMP	102	0x946f (3	37999)	64 Echo (ping) request	id=0x0035, seq=4/1024, ttl=64 (no r	e
	5 2022-08-07 20:41:02.660624	192.0.2.100	198.51.100.100	ICMP	102	0x94a4 (3	38052)	64 Echo (ping) request	id=0x0035, seq=5/1280, ttl=64 (no re	e
	6 2022-08-07 20:41:03.663226	192.0.2.100	198.51.100.100	ICMP	102	0x952d (3	38189)	64 Echo (ping) request	id=0x0035, seq=6/1536, ttl=64 (no r	e
	7 2022-08-07 20:41:04.661262	192.0.2.100	198.51.100.100	ICMP	102	0x958d (3	38285)	64 Echo (ping) request	id=0x0035, seq=7/1792, ttl=64 (no r	e
	8 2022-08-07 20:41:05.665955	192.0.2.100	198.51.100.100	ICMP	102	0x95d8 (3	38360)	64 Echo (ping) request	id=0x0035, seq=8/2048, ttl=64 (no r	e
	9 2022-08-07 20:41:06.666538	192.0.2.100	198.51.100.100	ICMP	102	0x964b (3	38475)	64 Echo (ping) request	id=0x0035, seq=9/2304, ttl=64 (no r	e
	10 2022-08-07 20:41:07.667298	192.0.2.100	198.51.100.100	ICMP	102	0x972b (3	38699)	64 Echo (ping) request	id=0x0035, seq=10/2560, ttl=64 (no r	r
	11 2022-08-07 20:41:08.670540	192.0.2.100	198.51.100.100	ICMP	102	0x980a (3	38922)	64 Echo (ping) request	id=0x0035, seq=11/2816, ttl=64 (no r	r
	12 2022-08-07 20:41:09.668278	192.0.2.100	198.51.100.100	ICMP	102	0x9831 (3	38961)	64 Echo (ping) request	id=0x0035, seq=12/3072, ttl=64 (no r	r
	13 2022-08-07 20:41:10.672417	192.0.2.100	198.51.100.100	ICMP	102	0x98a2 (3	39074)	64 Echo (ping) request	id=0x0035, seq=13/3328, ttl=64 (no	r
	14 2022-08-07 20:41:11.671369	192.0.2.100	198.51.100.100	ICMP	102	0x98f7 (3	39159)	64 Echo (ping) request	id=0x0035, seq=14/3584, ttl=64 (no r	r
	15 2022-08-07 20:41:12.675462	192.0.2.100	198.51.100.100	ICMP	102	0x99e4 (3	39396)	64 Echo (ping) request	id=0x0035, seq=15/3840, ttl=64 (no r	r
	16 2022-08-07 20:41:13.674903	192.0.2.100	198.51.100.100	ICMP	102	0x9a84 (3	39556)	64 Echo (ping) request	id=0x0035, seq=16/4096, ttl=64 (no r	r
	17 2022-08-07 20:41:14.674093	192.0.2.100	198.51.100.100	ICMP	102	0x9af3 (3	39667)	64 Echo (ping) request	id=0x0035, seq=17/4352, ttl=64 (no r	r
	18 2022-08-07 20:41:15.676904	192.0.2.100	198.51.100.100	ICMP	102	0x9b8e (3	39822)	64 Echo (ping) request	id=0x0035, seq=18/4608, ttl=64 (no	r ~
<									>	,
>	Frame 1: 102 bytes on wire (816 bits)	, 102 bytes capt	ured (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 02 64 c6 33 ·T··@·@· ····d·3	
>	Internet Protocol Version 4, Src: 192	.0.2.100, Dst: 1	98.51.100.100		-	0020	64 64 08	00 58 a8 00 35 00 01 4d	23 f0 62 00 00 dd · · X · · 5 · · M# · b · ·	
>	Internet Control Message Protocol				2	0030	00 00 9e	c8 04 00 00 00 00 00 10	11 12 13 14 15	
Ľ						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 2t 30	31 32 33 34 35 & ()*+,/012345	
						0060	30 37 55	22 22 22	670000	

## Explanation

The switch captures are configured on interfaces Ethernet1/1 or Portchannel1.

This table summarizes the task:

Task	Capture	Internal	Direction	Captured traffic
------	---------	----------	-----------	------------------

	point	filter		
Configure and verify a packet capture on interface Ethernet1/1	Ethernet1/1	None	Ingress only*	ICMP echo requests from host 192.0.2.100 to host 198.51.100.100
Configure and verify a packet capture on interface Portchannel1 with member interfaces Ethernet1/3 and Ethernet1/4	Ethernet1/3 Ethernet1/4	None	Ingress only*	ICMP echo requests from host 192.0.2.100 to host 198.51.100.100

\* Unlike 3100, the Secure Firewall 4200 supports **bidirectional** (ingress and egress) captures.

# Packet Capture on a Subinterface of a Physical or Port-channel Interface

Use the FTD or ASA CLI to configure and verify a packet capture on subinterfaces Ethernet1/1.205 or Portchannel1.205. Both subinterfaces have the name if **inside**.

## Topology, packet flow, and the capture points

Secure Firewall 3100:



Secure Firewall 4200:

	Chassis			
	Internal Switch		Security Module	
	Eth1113		FTD/ASA	
192.0.2.100 ICMP echo-request	Eth1/2	Uplink	inside	
198.51.100.100			outside	

# Configuration

Perform these steps on ASA or FTD CLI to configure a packet capture on interface Ethernet1/1 or Portchannel1:

1. Verify the nameif:

<#root>		
>		
show nameif		
Interface	Name	Security
Ethernet1/1.205	inside	0
Ethernet1/2	outside	0
Management1/1	diagnostic	0
<#root>		
>		
show nameif		
Interface	Name	Security
Port-channel1.205	inside	0

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

2. Create a capture session:
```
capture capsw switch interface inside
```

The Secure Firewall 4200 supports capture directionality:

<#root>

>

```
> capture capsw switch interface inside direction ?
```

both To capture switch bi-directional traffic egress To capture switch egressing traffic ingress To capture switch ingressing traffic

> capture capsw switch interface inside direction both

3. Enable the capture session:

<#root>

> no capture capsw switch stop

## Verification

Verify the capture session name, administrative and operational state, interface slot, and identifier. Ensure the **Pcapsize** value in bytes increases and the number of captured packets is non-zero:

<#root>	
>	
show capture capsw de	etail
Packet Capture info	
Name:	capsw
Session:	1
Admin State:	enabled
Admin State:	enabled
Admin State: Oper State:	enabled up
Admin State: Oper State:	enabled up
Admin State: Oper State: Oper State Reason:	enabled up Active
Admin State: Oper State: Oper State Reason:	enabled up Active
Admin State: Oper State: Oper State Reason: Config Success:	enabled up Active yes

Append Flag: Session Mem Usage: Session Pcap Snap Error Code: Drop Count:	overwrite 256 Len: 1518 O O
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 Filte	r Info
Name:	capsw-1-1
Protocol: Ivlan:	0 0
Ovlan:	205
Cre Tri	
Dest In:	
Src Tpy6:	::
Dest Ipv6:	
Src MAC:	00:00:00:00:00
Dest MAC:	00:00:00:00:00
Src Port:	0
Dest Port:	0
Ethertype:	0
Total Physical break	out ports involved in Packet Capture: 0

46 packets captured on disk using switch capture

Reading of capture file from disk is not supported

In this case, a filter with outer VLAN **Ovlan=205** is created and applied to the interface.

In the case of Port-channel1 the capture with a filter **Ovlan=205** is configured on all member interfaces:

<#root>

>

#### show capture capsw detail

### Packet Capture info

Name:	capsw
Session:	1
Admin State:	enabled
Oper State:	up
Oper State Reason:	Active
Config Success: Config Fail Reason Append Flag: Session Mem Usage: Session Pcap Snap Error Code: Drop Count:	yes : overwrite 256 Len: 1518 0 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 Filte Name: Protocol: Ivlan:	r Info capsw-1-4 0 0
Ovlan:	205
Src Ip: Dest Ip: Src Ipv6: Dest Ipv6: Src MAC:	0.0.0.0 0.0.0.0 :: :: 00:00:00:00:00:00

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
Name:	
Protocol:	Capsw-1-3
Tylan:	
ivian.	
Ovlan:	205
Src Ip:	0.0.0.0
Dest Ip:	0.0.0.0
Src Ipv6:	
Dest Ipv6:	::
Src MAC:	
Src Port:	0
Dest Port	0
Ethertype:	0
Total Physical break	out ports involved in Packet Capture: 0
49 packet captured o	n disk using switch capture
Reading of conturn f	tile from dick is not supported
Reading of Capture i	
The port-channel mer	ber interfaces can be verified in the EXOS local-mont command shell via the show
nortchannel summar	v command:
r Summu	J
<#root>	

>

connect fxos

… firewall#

connect local-mgmt

firewall(local-mgmt)#

show portchannel summary

Flags I - I s - S S - S U - U M - N	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	Туре	Protocol	Member P	orts					
1	Pol(U)	Eth	LACP	Eth1/3(P	) Eth1/4()	?)				
LACP	KeepAlive	Timer:								
	Channel	PeerKeepAliv	eTimerFas	t 						
1	Po1(U)	False								
Cluster LACP Status:										
	Channel	ClusterSpann	ed Clust	erDetach	ClusterUnit	ID ClusterSysID				
1	Po1(U)	False	Fal	 se	0	clust				

To access the FXOS on ASA, run the **connect fxos admin** command. In the case of multi-context, run this command in the admin context.

### **Collect capture files**

Perform the steps in the section Collect Secure Firewall Internal Switch Capture Files.

### Capture file analysis

Use a packet capture file reader application to open the capture files for Ethernet1/1.205. In this example, the packets capture on the Secure Firewall 3100 are analyzed. Select the first packet and check the key points:

- 1. Only ICMP echo request packets are captured.
- 2. The original packet header has VLAN tag **205**.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info	^
E.	1 2022-08-07 21:21:01.607187	192.0.2.100	198.51.100.100	ICMP	106	0x411f (16671)	64 Echo (ping) request	id=0x0037, seq=1/256, ttl=64 (no res
	2 2022-08-07 21:21:02.609418	192.0.2.100	198.51.100.100	ICMP	106	0x413a (16698)	64 Echo (ping) request	id=0x0037, seq=2/512, ttl=64 (no res
	3 2022-08-07 21:21:03.610671	192.0.2.100	198.51.100.100	ICMP	106	0x421a (16922)	64 Echo (ping) request	id=0x0037, seq=3/768, ttl=64 (no res
	4 2022-08-07 21:21:04.609160	192.0.2.100	198.51.100.100	ICMP	106	0x426c (17004)	64 Echo (ping) request	id=0x0037, seq=4/1024, ttl=64 (no re
	5 2022-08-07 21:21:05.609409	192.0.2.100	198.51.100.100	ICMP	106	0x4310 (17168)	64 Echo (ping) request	id=0x0037, seq=5/1280, ttl=64 (no re
	6 2022-08-07 21:21:06.611847	192.0.2.100	198.51.100.100	ICMP	106	0x43df (17375)	64 Echo (ping) request	id=0x0037, seq=6/1536, ttl=64 (no re
	7 2022-08-07 21:21:07.616688	192.0.2.100	198.51.100.100	ICMP	106	0x44d3 (17619)	64 Echo (ping) request	id=0x0037, seq=7/1792, ttl=64 (no re
	8 2022-08-07 21:21:08.618023	192.0.2.100	198.51.100.100	ICMP	106	0x4518 (17688)	64 Echo (ping) request	id=0x0037, seq=8/2048, ttl=64 (no re
	9 2022-08-07 21:21:09.619326	192.0.2.100	198.51.100.100	ICMP	106	0x453d (17725)	64 Echo (ping) request	id=0x0037, seq=9/2304, ttl=64 (no re
	10 2022-08-07 21:21:10.616696	192.0.2.100	198.51.100.100	ICMP	106	0x462b (17963)	64 Echo (ping) request	id=0x0037, seq=10/2560, ttl=64 (no r
	11 2022-08-07 21:21:11.621629	192.0.2.100	198.51.100.100	ICMP	106	0x4707 (18183)	64 Echo (ping) request	id=0x0037, seq=11/2816, ttl=64 (no r
	12 2022-08-07 21:21:12.619309	192.0.2.100	198.51.100.100	ICMP	106	0x474b (18251)	64 Echo (ping) request	id=0x0037, seq=12/3072, ttl=64 (no r
	13 2022-08-07 21:21:13.620168	192.0.2.100	198.51.100.100	ICMP	106	0x4781 (18305)	64 Echo (ping) request	id=0x0037, seq=13/3328, ttl=64 (no r
	14 2022-08-07 21:21:14.623169	192.0.2.100	198.51.100.100	ICMP	106	0x4858 (18520)	64 Echo (ping) request	id=0x0037, seq=14/3584, ttl=64 (no r
	15 2022-08-07 21:21:15.622497	192.0.2.100	198.51.100.100	ICMP	106	0x4909 (18697)	64 Echo (ping) request	id=0x0037, seq=15/3840, ttl=64 (no r
	16 2022-08-07 21:21:16.626226	192.0.2.100	198.51.100.100	ICMP	106	0x490b (18699)	64 Echo (ping) request	id=0x0037, seq=16/4096, ttl=64 (no r
	17 2022-08-07 21:21:17.629363	192.0.2.100	198.51.100.100	ICMP	106	0x4932 (18738)	64 Echo (ping) request	id=0x0037, seq=17/4352, ttl=64 (no r
	18 2022-08-07 21:21:18.626651	192.0.2.100	198.51.100.100	ICMP	106	0x4a05 (18949)	64 Echo (ping) request	id=0x0037, seq=18/4608, ttl=64 (no r 🗸
<								>
>	Frame 1: 106 bytes on wire (848 bits	), 106 bytes cap	tured (848 bits)			0000 bc e7	12 34 9a 14 00 50 56 9d e8	be 81 00 00 cd ···4···P V·····
>	Ethernet II, Src: VMware 9d:e8:be (0	0:50:56:9d:e8:be	), Dst: Cisco 34:9a	:14 (bc:e7:	12:34:9a:14)	0010 08 00	45 00 00 54 41 1f 40 00 40	01 0c 8e c0 00 ··E··TA·@·@·····
$\sim$	802.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 205				0020 02 64	c6 33 64 64 08 00 06 67 00	37 00 01 b0 2c ·d·3dd·· ·g·7···,
ш	000 Be Priority: Be	est Effort (defa	ult) (0)			0030 f0 62	00 00 00 00 8e fe 03 00 00	00 00 00 10 11 ·b·····
	0 = DEI: Ineligi	ible				0040 12 13	14 15 16 17 18 19 1a 1b 1c	1d 1e 1f 20 21
	0000 1100 1101 = ID: 205				-	0050 22 23	24 25 26 27 28 29 2a 2b 2c	2d 2e 2f 30 31 "#\$%&'() "+,/01
	Type: IPv4 (0x0800)				2	0000 32 33	34 35 36 37 55 55 55 55	23456700 00
	Trailer: 55555555							
>	Internet Protocol Version 4, Src: 19	2.0.2.100, Dst:	198.51.100.100					
>	Internet Control Message Protocol							

Open the capture files for Portchannel1 member interfaces. Select the first packet and check the key points:

- 1. Only ICMP echo request packets are captured.
- 2. The original packet header has VLAN tag 205.

No.	Time	Source	Destination	Protocol	Length	IP II	)		1	IP TTL	Info								^
-	1 2022-08-07 21:21:01.607187	192.0.2.100	198.51.100.100	ICMP	106	0x4	111f (	16671)		64	Echo	(ping)	request	id=0x0037	, seq=	1/256, t	tl=64 (	no res	
	2 2022-08-07 21:21:02.609418	192.0.2.100	198.51.100.100	ICMP	106	0x4	13a (	16698)	)	64	Echo	(ping)	request	id=0x0037	, seq=	2/512, t	tl=64 (	no res	
	3 2022-08-07 21:21:03.610671	192.0.2.100	198.51.100.100	ICMP	106	0x4	121a (	16922)		64	Echo	(ping)	request	id=0x0037	, seq=	3/768, t	tl=64 (	no res	
	4 2022-08-07 21:21:04.609160	192.0.2.100	198.51.100.100	ICMP	106	0x4	126c (	17004)		64	Echo	(ping)	request	id=0x0037	, seq=	4/1024,	ttl=64	(no re	
	5 2022-08-07 21:21:05.609409	192.0.2.100	198.51.100.100	ICMP	106	0x4	1310 (	17168)		64	Echo	(ping)	request	id=0x0037	, seq=	5/1280,	ttl=64	(no re	
	6 2022-08-07 21:21:06.611847	192.0.2.100	198.51.100.100	ICMP	106	0x4	13df (	17375)	1	64	Echo	(ping)	request	id=0x0037	, seq=	6/1536,	ttl=64	(no re	
	7 2022-08-07 21:21:07.616688	192.0.2.100	198.51.100.100	ICMP	106	0x4	14d3 (	17619)		64	Echo	(ping)	request	id=0x0037	, seq=	7/1792,	ttl=64	(no re	
	8 2022-08-07 21:21:08.618023	192.0.2.100	198.51.100.100	ICMP	106	0x4	1518 (	17688)		64	Echo	(ping)	request	id=0x0037	, seq=	8/2048,	ttl=64	(no re	
	9 2022-08-07 21:21:09.619326	192.0.2.100	198.51.100.100	ICMP	106	0x4	153d (	17725)		64	Echo	(ping)	request	id=0x0037	, seq=	9/2304,	ttl=64	(no re	
	10 2022-08-07 21:21:10.616696	192.0.2.100	198.51.100.100	ICMP	106	0x4	162b (	17963)		64	Echo	(ping)	request	id=0x0037	, seq=	10/2560,	ttl=64	(no r	
	11 2022-08-07 21:21:11.621629	192.0.2.100	198.51.100.100	ICMP	106	0x4	1707 (	18183)		64	Echo	(ping)	request	id=0x0037	, seq=	11/2816,	ttl=64	(no r	
	12 2022-08-07 21:21:12.619309	192.0.2.100	198.51.100.100	ICMP	106	0x4	174b (	18251)		64	Echo	(ping)	request	id=0x0037	, seq=	12/3072,	ttl=64	(no r	
	13 2022-08-07 21:21:13.620168	192.0.2.100	198.51.100.100	ICMP	106	0x4	1781 (	18305)		64	Echo	(ping)	request	id=0x0037	, seq=	13/3328,	ttl=64	(no r	
	14 2022-08-07 21:21:14.623169	192.0.2.100	198.51.100.100	ICMP	106	0x4	1858 (	18520)		64	Echo	(ping)	request	id=0x0037	, seq=	14/3584,	ttl=64	(no r	
	15 2022-08-07 21:21:15.622497	192.0.2.100	198.51.100.100	ICMP	106	0x4	1909 (	18697)		64	Echo	(ping)	request	id=0x0037	, seq=	15/3840,	ttl=64	(no r	
	16 2022-08-07 21:21:16.626226	192.0.2.100	198.51.100.100	ICMP	106	0x4	190b (	18699)		64	Echo	(ping)	request	id=0x0037	, seq=	16/4096,	ttl=64	(no r	
	17 2022-08-07 21:21:17.629363	192.0.2.100	198.51.100.100	ICMP	106	0x4	1932 (	18738)		64	Echo	(ping)	request	id=0x0037	, seq=	17/4352,	ttl=64	(no r	
	18 2022-08-07 21:21:18.626651	192.0.2.100	198.51.100.100	ICMP	106	0x4	1a05 (	18949)		64	Echo	(ping)	request	id=0x0037	, seq=	18/4608,	ttl=64	(no r	~
<																		>	
>	Frame 1: 106 bytes on wire (848 bits	), 106 bytes capt	ured (848 bits)				0000	bc e7	12	34 98	14 6	0 50	56 9d e8	be 81 00 0	0 cd	4	P V · · · ·		
>	Ethernet II, Src: VMware 9d:e8:be (@	0:50:56:9d:e8:be)	, Dst: Cisco 34:9a:	14 (bc:e7:12:3	34:9a:14)	1	0010	08 00	45	00 00	54 4	1 1f	40 00 40	01 0c 8e d	0 00	· · E · · T/	A- @.@		
$\sim$	802.10 Virtual LAN, PRI: 0, DEI: 0,	ID: 205	-				0020	02 64	c6	33 64	64 6	8 00	06 67 00	37 00 01 b	@ 2c	·d·3dd	·· ·g·7·	···,	
	000 B	est Effort (defaul	lt) (0)				0030	fØ 62	00	00 00	00 8	e fe	03 00 00	00 00 00 1	0 11	·b····		• • •	
	0 = DEI: Inelig	ible					0040	12 13	14	15 16	17 1	8 19	1a 1b 1c	1d 1e 1f 2	0 21			- 1	
	0000 1100 1101 = ID: 205				-		0050	22 23	24	25 26	27 2	8 29	2a 2b 2c	2d 2e 2f 3	0 31	"#\$%&`(	() "+,	/01	
	Type: IPv4 (0x0800)				2		0000	32 33	34	35 36	37 5	5 55	55 55			2345670	00 00		
	Trailer: 5555555																		
>	Internet Protocol Version 4, Src: 19	2.0.2.100, Dst: 1	98.51.100.100																
>	Internet Control Message Protocol																		
	0					- 11													

## Explanation

The switch captures are configured on subinterfaces Ethernet1/1.205 or Portchannel1.205 with a filter that matches outer VLAN 205.

This table summarizes the task:

Task	Capture point	Internal filter	Direction	Captured traffic
Configure and verify a packet capture on subinterface Ethernet1/1.205	Ethernet1/1	Outer VLAN 205	Ingress only*	ICMP echo requests from host 192.0.2.100 to host 198.51.100.100

Configure and verify a packet capture on subinterface Portchannel1.205 with member interfaces Ethernet1/3 and Ethernet1/4	Ethernet1/3 Ethernet1/4	Outer VLAN 205	Ingress only*	ICMP echo requests from host 192.0.2.100 to host 198.51.100.100
---	----------------------------	-------------------	------------------	---

\* Unlike 3100, the Secure Firewall 4200 supports **bidirectional** (ingress and egress) captures.

## **Packet Capture on Internal Interfaces**

The Secure Firewall 3100 has 2 internal interfaces:

- in\_data\_uplink1 connects the application to the internal switch.
- **in\_mgmt\_uplink1** provides a dedicated packet path for management connections, such as SSH to the management interface, or the management connection, also known as the sftunnel, between the FMC and the FTD.

The Secure Firewall 4200 has up to 4 internal interfaces:

- in\_data\_uplink1 and in\_data\_uplink2 (4245 only) these interfaces connect the application to the internal switch. In the case of 4245, the packets are load balance across the 2 uplink interfaces.
- **in\_mgmt\_uplink1** and **in\_mgmt\_uplink2** these interfaces provide a dedicated packet path for management connections, such as SSH to the management interface, or the management connection, also known as the sftunnel, between the FMC and the FTD. The Secure Firewall 4200 supports 2 managemet interfaces.

## Task 1

Use the FTD or ASA CLI to configure and verify a packet capture on the uplink interface in\_data\_uplink1.

## Topology, packet flow, and the capture points

Secure Firewall 3100:



Secure Firewall 4200:

	Chassis							
	Internal Switch	Security Module						
	E	FTD/ASA						
192.0.2.100 ICMP echo-reques	t آn_data_upl	link1						
198.51.100.100								

## Configuration

Perform these steps on ASA or FTD CLI to configure a packet capture on interface in\_data\_uplink1:

1. Create a capture session:

<#root>

>

capture capsw switch interface in\_data\_uplink1

The Secure Firewall 4200 supports capture directionality:

<#root>

```
> capture capsw switch interface in_data_uplink1 direction ?
```

both To capture switch bi-directional traffic egress To capture switch egressing traffic ingress To capture switch ingressing traffic

> capture capsw switch interface in\_data\_uplink1 direction both

2.Enable the capture session:

<#root>

> no capture capsw switch stop

## Verification

Verify the capture session name, administrative and operational state, interface slot, and identifier. Ensure the **Pcapsize** value in bytes increases and the number of captured packets is non-zero:

<#root>

> 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: :: 00:00:00:00:00:00 Src MAC: 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

In this case, a capture is created on the interface with an internal ID **18** which is the in\_data\_uplink1 interface on the Secure Firewall 3130. The **show portmanager switch status** command in the FXOS **local-mgmt** command shell shows the interface IDs:

<#root>

>

...

connect fxos

firewall#

connect local-mgmt

firewall(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

To access the FXOS on ASA, run the **connect fxos admin** command. In the case of multi-context, run this command in the admin context.

## **Collect capture files**

Perform the steps in the section Collect Secure Firewall Internal Switch Capture Files.

## Capture file analysis

Use a packet capture file reader application to open the capture files for interface in\_data\_uplink1. In this example, the packets capture on the Secure Firewall 3100 are analyzed.

Check the key point - in this case, ICMP echo request and echo reply packets are captured. These are the packets sent from the application to the internal switch.

No.	Time		4	Source	Destination	Protocol	Length	IP ID		_	IP TTU	Info								^
	1 2022-08-07	22:40:06.685606	1	192.0.2.100	198.51.100.100	ICMP	102	0x4d93	(1985	9)	64	1 Echo	(ping)	request	id=0x003a,	seq=33	/8448,	ttl=64	(repl	
4	2 2022-08-07	22:40:06.685615		198.51.100.100	192.0.2.100	ICMP	102	0x6cdc	(2786	(8)	64	1 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	Øx4de8	(1994	4)	64	1 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	(2808	(2)	64	1 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	(2018	(8)	64	4 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	(2809	5)	64	4 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	(2026	i9)	64	1 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	(2828	(8)	64	1 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	(2040	)1)	64	1 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	(2837	3)	64	4 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	(2048	(8)	64	4 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	(2847	5)	64	1 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	(2066	i4)	64	1 Echo	(ping)	request	id=0x003a,	seq=39	/9984,	ttl=64	(repl	
	14 2022-08-07	22:40:12.697209		198.51.100.100	192.0.2.100	ICMP	102	0x6fd7	(2863	1)	64	1 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	(2086	(8)	64	4 Echo	(ping)	request	id=0x003a,	seq=40	/10240,	ttl=64	(rep	
	16 2022-08-07	22:40:13.697327		198.51.100.100	192.0.2.100	ICMP	102	0x703e	(2873	(4)	64	4 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	(2095	2)	64	4 Echo	(ping)	request	id=0x003a,	seq=41	/10496,	ttl=64	(rep	
	18 2022-08-07	22:40:14.698518		198.51.100.100	192.0.2.100	ICMP	102	0x70dd	(2889	3)	64	1 Echo	(ping)	reply	id=0x003a,	seq=41	/10496,	ttl=64	(rec	~
<																			>	
>	Frame 1: 102 byte	s on wire (816 bit	ts)	, 102 bytes captu	ured (816 bits)			000	00	50 56	9d (	7 50	oc e7	12 34 9a	15 08 00 4	600	PV · · P ·	4	• E •	
>	Ethernet II, Src:	Cisco 34:9a:15 (	bc:	e7:12:34:9a:15),	Dst: VMware 9d:e7:	50 (00:50:56:9	d:e7:50)	001	00	54 4d	93 4	00 00	40 01	00 1a c0	00 02 64 c	33	- TM - @ - @		d-3	
>	Internet Protocol	Version 4, Src:	192	.0.2.100, Dst: 19	98.51.100.100			002	9 64	64 08	00 7	f 15	00 3a	00 21 39	3f f0 62 0	) 00 (	d · · · · bt	· 19? · 1	b	
>	Internet Control	Message Protocol						003	90	00 8b	1a (	95 00	00 00	00 00 10	11 12 13 14	15				
								004	16	17 18	19 1	la 1b	1c 1d	1e 1f 20	21 22 23 24	25		· · · 174	#\$%	
								005	26	27 28	29 2	2a 2b :	2C 2d	2e 2† 30	31 32 33 34	35 8	x () *+,	/012	345	
								006	36	37 55	55 3	5 55					370000			

### Explanation

When a switch capture on the uplink interface is configured, only packets sent from the application to the internal switch are captured. Packets sent to the application are not captured.

This table summarizes the task:

Task	Capture point	Internal filter	Direction	Captured traffic
Configure and verify a packet	in_data_uplink1	None	Ingress	ICMP echo requests from host

capture on the uplink interface in_data_uplink1		only*	192.0.2.100 to host 198.51.100.100
			ICMP echo replies from host 198.51.100.100 to host 192.0.2.100

\* Unlike 3100, the Secure Firewall 4200 supports **bidirectional** (ingress and egress) captures.

## Task 2

Use the FTD or ASA CLI to configure and verify a packet capture on the uplink interface **in\_mgmt\_uplink1.** Only the packets of management plane connections are captured.

## Topology, packet flow, and the capture points

Secure Firewall 3100:



Secure Firewall 4200:



## Configuration

Perform these steps on ASA or FTD CLI to configure a packet capture on interface in\_mgmt\_uplink1:

1. Create a capture session:

<#root>

>

capture capsw switch interface in\_mgmt\_uplink1

The Secure Firewall 4200 supports capture directionality:

<#root>

> capture capsw switch interface in\_mgmt\_uplink1 direction ?

both To capture switch bi-directional traffic egress To capture switch egressing traffic ingress To capture switch ingressing traffic

> capture capsw switch interface in\_mgmt\_uplink1 direction both

2. Enable the capture session:

<#root>

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

#### Verification

Verify the capture session name, administrative and operational state, interface slot, and identifier. Ensure the **Pcapsize** value in bytes increases and the number of captured packets is non-zero:

<#root>
> 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 Pcan Snap	len: 1518
Error Code:	0
Drop Count:	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: 1	37248
Filter:	capsw-1-19
Packet Capture Filte	r Info
Name:	capsw-1-19
Protocol:	0
Ivlan:	0
Ovlan:	0
Src Ip:	0.0.0
Dest Ip:	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 break	out ports involved in Packet Capture: O
281 packets captured	on disk using switch capture
Reading of capture f	ile from disk is not supported

In this case, a capture is created on the interface with an internal ID 19 which is the **in\_mgmt\_uplink1** interface on the Secure Firewall 3130. The **show portmanager switch status** command in the FXOS **local-mgmt** command shell shows the interface IDs:

<#root>

>

connect fxos

#### firewall#

...

#### connect local-mgmt

#### firewall(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	Un	256	Full	None	link-Un
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

To access the FXOS on ASA, run the **connect fxos admin** command. In the case of multi-context, run this command in the admin context.

## **Collect capture files**

Perform the steps in the section Collect Secure Firewall Internal Switch Capture Files.

## **Capture file analysis**

Use a packet capture file reader application to open the capture files for interface **in\_mgmt\_uplink1**. In this example, the packets capture on the Secure Firewall 3100 are analyzed.

Check the key point - in this case only the packets from the management IP address 192.0.2.200 are shown. Examples are SSH, Sftunnel or ICMP echo reply packets. These are the packets sent from the application management interface to the network through the internal switch.

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 (4	7056)	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 (4	7057)	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	Øxb7d2 (4	7058)	64 Application Data	
199 2022-08-07 23:21:45.928772	192.0.2.200	192.0.2.100	ICMP	78	0xbd48 (4	8456)	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 (1	9095)	64 Application Data	
201 2022-08-07 23:21:45.949027	192.0.2.200	192.0.2.101	TCP	70	0x4a98 (1	9096)	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 (1	9097)	64 Application Data	
203 2022-08-07 23:21:46.019899	192.0.2.200	192.0.2.101	TLSv1.2	96	0x4a9a (1	9098)	64 Application Data	
204 2022-08-07 23:21:46.019903	192.0.2.200	192.0.2.101	TCP	70	0x4a9b (1	9099)	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 (1	9100)	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 (4	7059)	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	Øxbd9e (4	8542)	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	Øxbdf2 (4	8626)	64 Echo (ping) reply id=0x0001, seq=4541/48401, ttl=64	
209 2022-08-07 23:21:48.406312	192.0.2.200	192.0.2.101	TCP	70	0x4a9d (1	9101)	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 (1	9102)	64 Application Data	
211 2022-08-07 23:21:48.994386	192.0.2.200	192.0.2.100	ICMP	78	0xbe48 (4	8712)	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	Øxbea6 (4	8806)	64 Echo (ping) reply id=0x0001, seq=4543/48913, ttl=64	
213 2022-08-07 23:21:50.140167	192.0.2.200	192.0.2.101	TCP	1518	0xb7d4 (4	7060)	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 (4	7061)	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 (4	7062)	64 Application Data	
216 2022-08-07 23:21:51.015884	192.0.2.200	192.0.2.100	ICMP	78	Øxbec1 (4	8833)	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 (4	7063)	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 (4	8898)	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 (4	8985)	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 (4	4340)	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 (4	4341)	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 (1	9103)	64 Application Data	
223 2022-08-07 23:21:54.102899	192.0.2.200	192.0.2.100	ICMP	78	0xbf63 (4	8995)	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 (1	9104)	64 8305 → 58885 [ACK] Seq=23407 Ack=26424 Win=4116 Len=0 TSv	
105 1011 00 07 12:11:55 126700	103 0 3 300	103 0 3 100	TCMD	70	avhfc1 (A	0000)	64 Echo (ning) conly id-avagat con-4640/60102 ++1-64	ř
> Frame 1: 747 bytes on wire (5976 bits	s), 747 bytes capt	ured (5976 bit	(5)		0000	a4 53 0e 11	1 38 2a bc e7 12 34 9a 00 08 00 45 00 ·S··8*···4····E·	î
> Ethernet II, Src: Cisco_34:9a:00 (bc	:e7:12:34:9a:00),	Dst: Cisco_11:	:38:2a (a4:53:0e:11	:38:2a)	0010	02 09 48 30	1 40 00 40 05 58 54 C0 00 02 C8 C0 00 ···J=@·@· n·····	
> Internet Protocol Version 4, Src: 19	2.0.2.200, Dst: 19	2.0.2.101			0020	10 14 27 6	00 00 01 01 02 03 00 05 00 04 00 18 ··· e q.·.g. ····k···	
> Transmission Control Protocol, Src Po	ort: 8305, Dst Por	rt: 58885, Seq:	: 1, Ack: 1, Len: 6	77	0040	3d 41 17 0	3 03 02 a0 22 6a 01 e0 ff cc 98 f9 af =A" j	
> Transport Layer Security					0050	07 40 75 19	a4 d5 df 64 d8 fe 66 8e 9b cc 8d 2f @udf/	
					0060	92 b2 1a 64	e7 20 36 03 8e 48 02 5a 7c 85 30 d4 ····d· 6· ·H·Z 0·	
					0070	fa c0 a8 56	5 b8 ad a7 7e 19 3a c1 9c 4b 57 0e e0 ····V···~ ·:··KW··	
					0080	be ef 95 22	2 84 c1 c1 9d 9f 24 78 b4 15 1c 44 0e ····"···· ·\$x···D·	
					0090	ea cb 43 90	e 1f fd a7 70 75 e5 6b a4 f8 2b ee 47 ···C····p u·k··+·G	
					00a0	21 86 73 81	b1 e1 b5 c6 57 e3 a8 46 0e cb 26 b7 /·s···· W··F··&·	
					0050	50 c7 e3 09	9 54 13 C1 11 26 d9 87 ea 51 3d 20 08 [T&Q= .	
					0000	10 TO CD TS	9 4T 91 98 56 80 15 1/ 55 68 6T 50 840	~
								_

## Explanation

When a switch capture on the management uplink interface is configured, only ingress packets sent from the application management interface are captured. Packets destined for the application management interface are not captured.

This table summarizes the task:

Task	Capture point	Internal filter	Direction	Captured traffic
Configure and verify a packet capture on the management uplink interface	in_mgmt_uplink1	None	Ingress only* (from the management interface to the network through the internal switch)	ICMP echo replies from FTD management IP address 192.0.2.200 to host 192.0.2.100 Sftunnel from FTD management IP address 192.0.2.200 to FMC IP address 192.0.2.101 SSH from FTD management IP address 192.0.2.200 to host 192.0.2.100

\* Unlike 3100, the Secure Firewall 4200 supports bidirectional (ingress and egress) captures.

## **Packet Capture Filters**

Internal switch packet capture filters are configured the same way as the data plane captures. Use the **ethernet-type** and **match** options to configure filters.

## Configuration

Perform these steps on ASA or FTD CLI to configure a packet capture with a filter that matches ARP frames or ICMP packets from host 198.51.100.100 on interface Ethernet1/1:

1. Verify the nameif:

<#root>		
>		
show nameif		
Interface	Name	Security
Ethernet1/1	inside	0
Ethernet1/2	outside	0
Management1/1	diagnostic	0

#### 2. Create a capture session for ARP or ICMP:

```
<#root>
```

>

capture capsw switch interface inside ethernet-type arp

<#root>

> capture capsw switch interface inside match icmp 198.51.100.100

## Verification

Verify the capture session name and the filter. The Ethertype value is **2054** in decimal and **0x0806** in hexadecimal:

<#root>

>

show capture capsw detail

Packet Capture info Name: capsw Session: 1 disabled Admin State: 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
Dest Ip:	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 O packet captured on disk using switch capture Reading of capture file from disk is not supported

This is the verification of the filter for ICMP. IP protocol 1 is the ICMP:

<#root>

> 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: :: 00:00:00:00:00:00 Src MAC: Dest MAC: 00:00:00:00:00:00 Src Port: 0 Dest Port: 0 0 Ethertype:

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

## **Collect Secure Firewall Internal Switch Capture Files**

Use ASA or FTD CLI to collect internal switch capture files. On FTD, the capture file can also be exported via the CLI **copy** command to destinations reachable via the data or diagnostic interfaces.

Alternatively, the file can be copied to **/ngfw/var/common** in expert mode and downloaded from FMC via the **File Download** option.

In the case of port-channel interfaces ensure to collect packet capture files from all member interfaces.

### ASA

Perform these steps on to collect internal switch capture files on ASA CLI:

1. Stop the capture:

<#root>

asa#

capture capsw switch stop

2. Verify the capture session is stopped and note the capture file name.

<#root>

asa#

show capture capsw detail

Packet Capture info

Name:	capsw
Session:	1

Admin State: disabled

Oper State: down

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 0 Ivlan: Ovlan: 0 Src Ip: 0.0.0.0 0.0.0.0 Dest Ip: Src Ipv6: :: Dest Ipv6: :: 00:00:00:00:00:00 Src MAC: 00:00:00:00:00:00 Dest MAC: Src Port: 0 Dest Port: 0 0 Ethertype: 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. Use the CLI copy command to export the file to remote destinations:

<#root>

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: smb: startup-config system: tftp:	Copy to scp: file system Copy to smb: file system Copy to startup configuration Copy to system: file system Copy to tftp: file system							
a	sa#								
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 progressC									
139826 bytes copied in 0.532 secs									

## FTD

Perform these steps to collect internal switch capture files on FTD CLI and copy them to servers reachable via data or diagnostic interfaces:

1. Go to diagnostic CLI:

<#root>

>

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. Stop the capture:

<#root>

firepower#

capture capi switch stop

3. Verify the capture session is stopped and note the capture file name:

<#root>

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: :: 00:00:00:00:00:00 Src MAC: Dest MAC: 00:00:00:00:00:00 Src Port: 0 0 Dest Port: 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. Use the CLI copy command to export the file to remote destinations.

#### <#root>

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

Perform these steps on to collect capture files from FMC via the File Download option:

1. Stop the capture:

<#root>

>

capture capsw switch stop

2. Verify the capture session is stopped and note the file name and full capture file path:

<#root>

>

show capture capsw detail

### Packet Capture info

Name:	capsw						
Session:	1						
56551011.	1						
Admin State:	disabled						
Oper State:	down						
Oper State Reason	: Session Admin Shut						
	·····						
Config Success:	yes						
Config Fail Reaso	on:						
Append Flag:	overwrite						
Session Mem Usage: 256							
Session Pcap Snap	) Len: 1518						
Error Code: 0							
Drop Count:	0						
Total Physical port	s involved in Packet Canture: 1						
focul injoicul port							
Physical port:							
Slot Id:	1						
Port Id:	1						
Baanfilo	(mpt/digk0/pagkot_gapturo/gagg_1_gapgu_atherpot_1_1_0_pgap						
rcapille.	/mic/disk0/packet-capture/sess-i-capsw-ethernet-i-i-v.pcap						
Pcapsize:	139826						
Filter:	capsw-1-1						
Packet Canture Filt	ar Info						
Name:	capsw-1-1						
Protocol:	0						
Tvlan:	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						
Dest MAC:	00:00:00:00:00						
Src Port:	0						
Dest Port:	0						
Ethertype:	0						
Total Physical brea	akout ports involved in Packet Capture: 0						
386 packets captured on disk using switch capture							

Reading of capture file from disk is not supported

3. Go to expert mode and switch to root mode:

>

#### expert

admin@firepower:~\$

sudo su

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

### 4. Copy the capture file to /ngfw/var/common/:

#### <#root>

```
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 -1 /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. On FMC choose **Devices > File Download**:



6. Choose the FTD, provide the capture file name, and click **Download**:

Firewall Management Center Devices / Troubleshoot / File Download	Overview	Analysis	Policies	Devices	Objects	Integration	Depl	loy	۹	¢	¢ (	) la	ab_domain \ <b>admin ▼</b>	cisco SECU	RE
									Threa	at Defe	nse Cl	. I	Packet Capture	Packet Tracer	
		Device FPR3100- File	1	Ť											
		sess-1-ca	psw-ethernet	-1-1-0.pcap											
		Back Download													

## Guidelines, Limitations, and Best Practices for Internal Switch Packet Capture

Guidelines and limitations:

- Multiple switch capture configuration sessions are supported, but only 1 switch capture session can be active at a time. An attempt to enable 2 or more capture sessions results in an error "ERROR: Failed to enable session, as limit of maximum 1 active packet capture sessions reached".
- An active switch capture cannot be deleted.
- Switch captures cannot be read on the application. The user must export the files.
- Certain data plane capture options such as **dump**, **decode**, **packet-number**, **trace**, and others are not supported for switch captures.
- In the case of multi-context ASA, the switch captures on data interfaces are configured in user contexts. The switch captures on interfaces in\_data\_uplink1, and in\_mgmt\_uplink1 are supported only in the admin context.

This is the list of best practices based on the usage of packet capture in TAC cases:

- Be aware of guidelines and limitations.
- Use capture filters.
- Consider the impact of NAT on packet IP addresses when a capture filter is configured.
- Increase or decrease the **packet-length** that specifies frame size, in case it differs from the default value of 1518 bytes. Shorter size results in an increased number of captured packets and vice versa.
- Adjust the **buffer** size as needed.
- Be aware of the **Drop Count** in the output of the **show cap <cap\_name> detail** command. Once the buffer size limit is reached, the drop count counter increases.

# **Related Information**

- <u>Firepower 4100/9300 Chassis Manager and FXOS CLI Configuration Guides</u>
- <u>Cisco Secure Firewall 3100 Getting Started Guide</u>
- <u>Cisco Firepower 4100/9300 FXOS Command Reference</u>