

配置並驗證安全防火牆和Firepower內部交換機捕獲

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[系統架構高級概述](#)

[內部交換機操作的高級概述](#)

[封包流程和擷取點](#)

[Firepower 4100/9300上的配置和驗證](#)

[物理或埠通道介面上的資料包捕獲](#)

[背板介面上的封包擷取](#)

[應用和應用埠上的資料包捕獲](#)

[物理或埠通道介面的子介面上的資料包捕獲](#)

[封包擷取過濾器](#)

[收集Firepower 4100/9300內部交換機捕獲檔案](#)

[內部交換器封包擷取准則、限制和最佳實踐](#)

[安全防火牆3100上的配置和驗證](#)

[物理或埠通道介面上的資料包捕獲](#)

[物理或埠通道介面的子介面上的資料包捕獲](#)

[內部介面上的資料包捕獲](#)

[封包擷取過濾器](#)

[收集Secure Firewall 3100內部交換機捕獲檔案](#)

[內部交換器封包擷取准則、限制和最佳實踐](#)

[相關資訊](#)

簡介

本檔案介紹Firepower的組態和驗證，以及Secure Firewall內部交換器擷取。

必要條件

需求

基礎產品知識、捕獲分析。

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

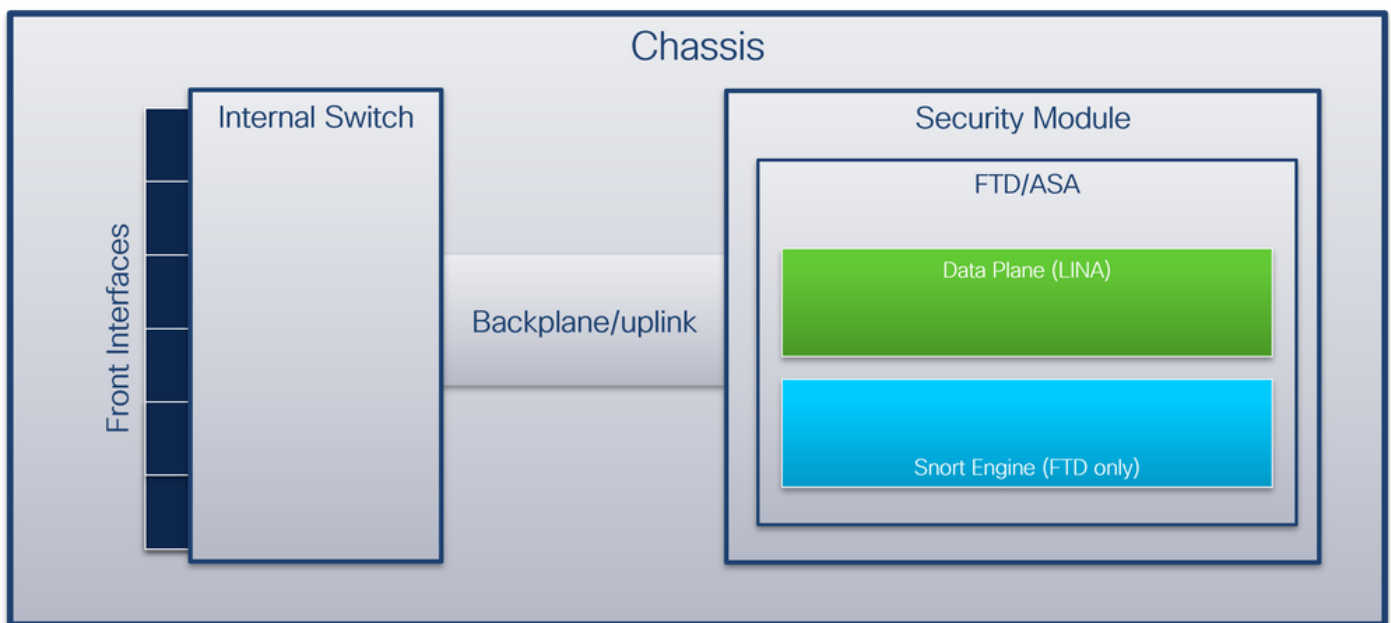
本文中的資訊係根據以下軟體和硬體版本：

- 安全防火牆31xx
- Firepower 41xx
- Firepower 93xx
- 思科安全可擴充作業系統(FXOS)2.12.0.x
- 思科安全防火牆威脅防禦(FTD)7.2.0.x
- 思科安全防火牆管理中心(FMC)7.2.0.x
- 思科安全防火牆裝置管理員(FDM)7.2.0.x
- 調適型安全裝置(ASA)9.18(1)x
- 調適型安全裝置裝置管理器(ASDM)7.18.1.x
- Wireshark 3.6.7(<https://www.wireshark.org/download.html>)

背景資訊

系統架構高級概述

從資料包流的角度，可以直觀顯示Firepower 4100/9300和安全防火牆3100的架構，如下圖所示：



機箱包括以下元件：

- **內部交換器** — 將資料包從網路轉發到應用，反之亦然。內部交換機連線到位於內建介面模組或外部網路模組上的**前介面**，並連線到外部裝置，例如交換機。前端介面的示例包括Ethernet 1/1、Ethernet 2/4等。「前沿」並不是一個強有力的技術定義。在本文檔中，它用於區分連線到外部裝置的介面與背板或上行鏈路介面。
- **背板或上行鏈路** — 將安全模組(SM)連線到內部交換機的內部介面。下表顯示Firepower 4100/9300上的背板介面和安全防火牆3100上的上行鏈路介面：

平台

支援的安全模組數量

背板/上行鏈路介面

對映的應用程式介

SM1:

Internal-Data0/0

Firepower 4100 (Firepower 4110/4112除外)	1	Ethernet1/9 Ethernet1/10	Internal-Data0/1
Firepower 4110/4112	1	Ethernet1/9	Internal-Data0/0 Internal-Data0/0 Internal-Data0/1
Firepower 9300	3	SM1: Ethernet1/9 Ethernet1/10 SM2: Ethernet1/11 Ethernet1/12 SM3: Ethernet1/13 Ethernet1/14	Internal-Data0/0 Internal-Data0/1 Internal-Data0/0 Internal-Data0/1 Internal-Data0/0 Internal-Data0/1
安全防火牆3100	1	SM1:in_data_uplink1	Internal-Data0/1

如果每個模組有2個背板介面，則內部交換機和模組上的應用通過2個介面執行流量負載均衡。

- **安全模組、安全引擎或刀片** — 安裝應用（例如FTD或ASA）的模組。Firepower 9300最多支援3個安全模組。
- **對映應用介面** — 應用（例如FTD或ASA）將背板或上行鏈路介面對映到內部介面。換句話說，背板或上行鏈路介面在應用程式中作為內部介面可見。

使用**show interface detail**命令驗證內部介面：

```
> 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
```

內部交換機操作的高級概述

Firepower 4100/9300

為了做出轉發決策，內部交換機使用介面VLAN標籤或埠VLAN標籤，以及虛擬網路標籤（VN標籤）。

內部交換機使用埠VLAN標籤來標識介面。交換器將連線埠VLAN標籤插入到前介面上的每個輸入封包中。VLAN標籤由系統自動配置，不能手動更改。可以在fxos命令shell中檢查標籤值：

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

version 5.0(3)N2(4.120)

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

VN標籤也由內部交換機插入，用於轉發資料包到應用。它由系統自動配置，不能手動更改。

埠VLAN標籤和VN標籤與應用程式共用。應用程式將各自的出口介面VLAN標籤和VN標籤插入到每個資料包中。當背板介面上的內部交換器接收到來自該應用的封包時，交換器讀取輸出介面VLAN標籤和VN標籤，識別該應用和輸出介面，去除連線埠VLAN標籤和VN標籤，並將封包轉送到網路。

安全防火牆3100

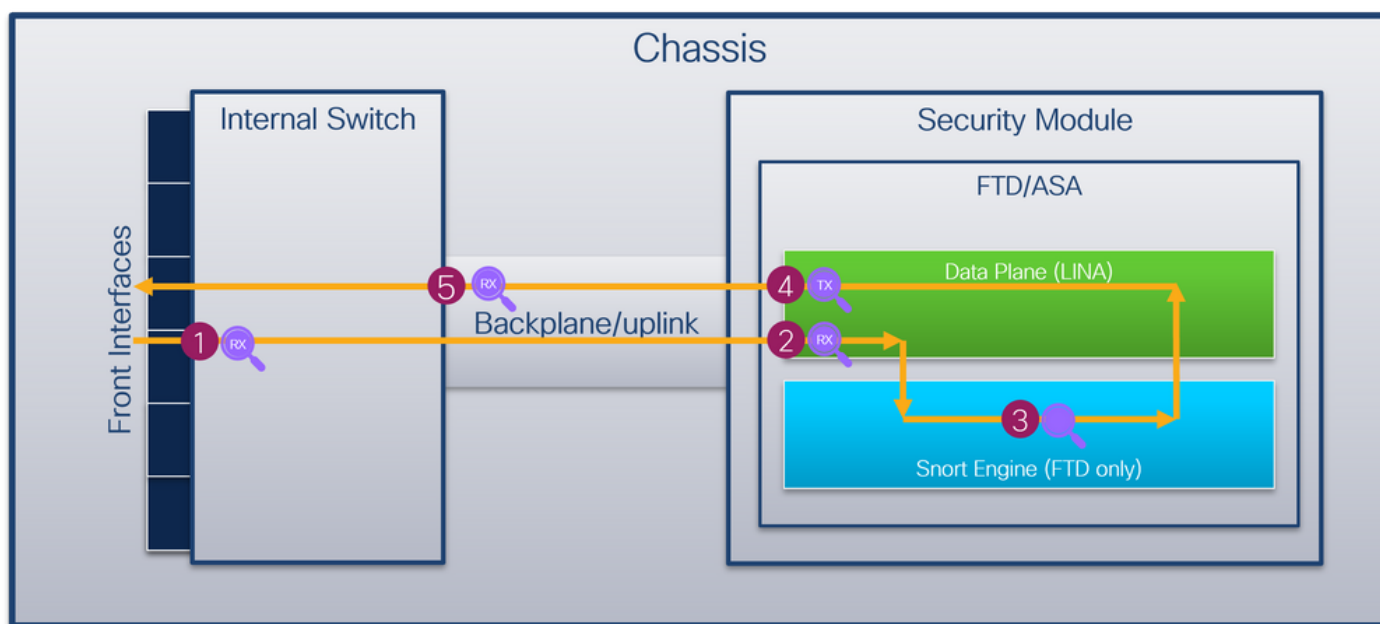
與Firepower 4100/9300一樣，內部交換機使用埠VLAN標籤來標識介面。

埠VLAN標籤與應用程式共用。應用程式將各自的出口介面VLAN標籤插入到每個資料包中。當上行鏈路介面上的內部交換機收到來自應用的資料包時，交換機讀取出口介面VLAN標籤，標識出口介面，去除埠VLAN標籤，並將資料包轉發到網路。

封包流程和擷取點

Firepower 4100/9300和安全防火牆3100防火牆支援內部交換機介面上的資料包捕獲。

下圖顯示機箱和應用程式內資料包路徑上的資料包捕獲點：



捕獲點包括：

1. 內部交換器正面介面輸入擷取點。前端介面是連線到對等裝置（如交換機）的任何介面。
2. 資料平面介面輸入擷取點
3. Snort捕獲點
4. 資料平面介面出口捕獲點
5. 內部交換器背板或上行鏈路輸入擷取點。背板或上行鏈路介面將內部交換機連線到應用。

內部交換器僅支援輸入介面擷取。也就是說，只能捕獲從網路或ASA/FTD應用接收的資料包。不支援輸出資料包捕獲。

上的組態和驗證 Firepower 4100/9300

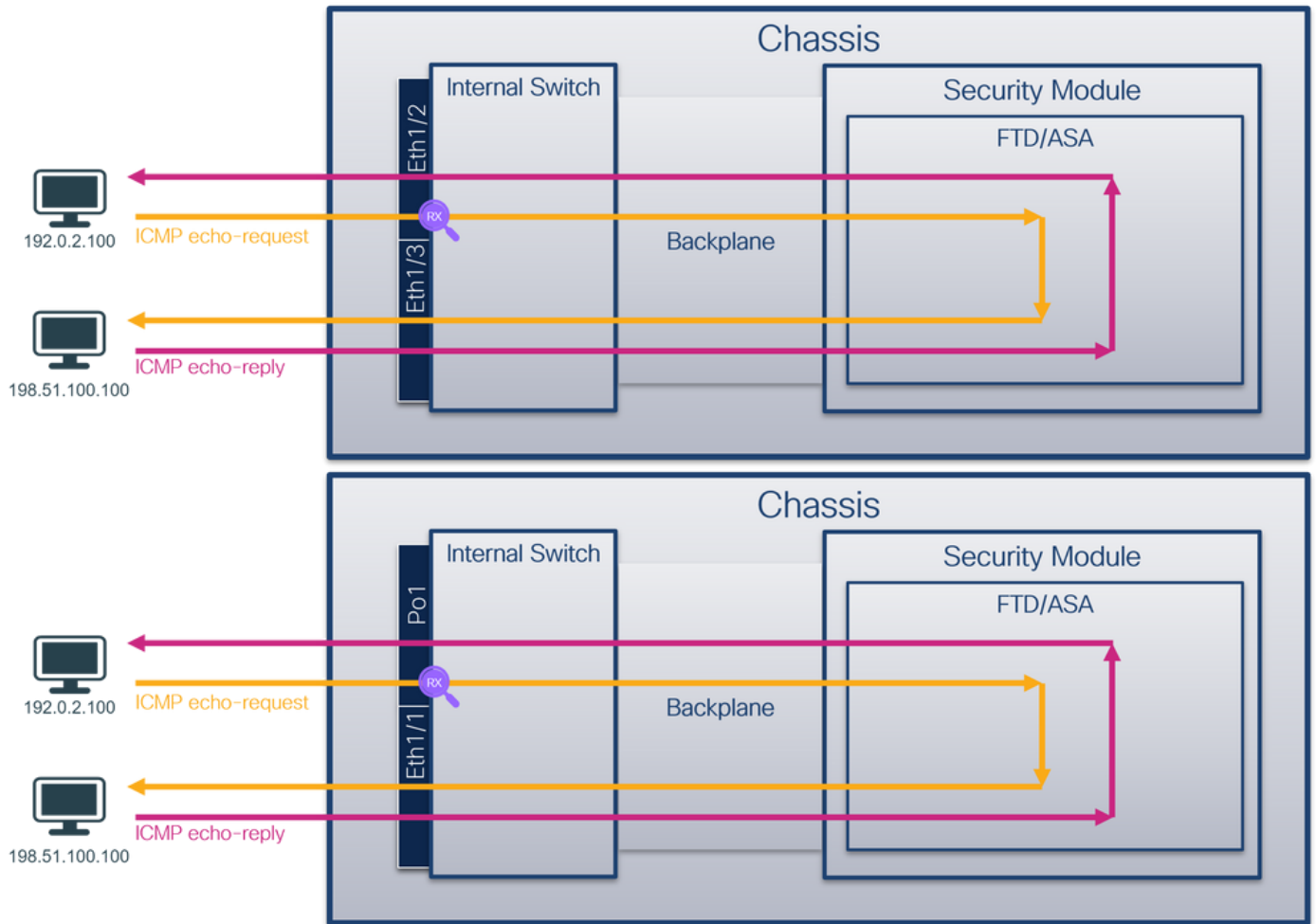
Firepower 4100/9300內部交換機捕獲可在FCM上的Tools > Packet Capture中配置，或在FXOS CLI的scope packet-capture中配置。有關資料包捕獲選項的說明，請參閱Cisco Firepower 4100/9300 FXOS機箱管理器配置指南或Cisco Firepower 4100/9300 FXOS CLI配置指南一章故障排除一節資料包捕獲。

這些情景包括Firepower 4100/9300內部交換機捕獲的常見使用案例。

物理或埠通道介面上的資料包捕獲

使用FCM和CLI在介面Ethernet1/2或Portchannel1介面上配置和驗證資料包捕獲。如果是埠通道介面，請確保選擇所有物理成員介面。

拓撲、資料包流和捕獲點

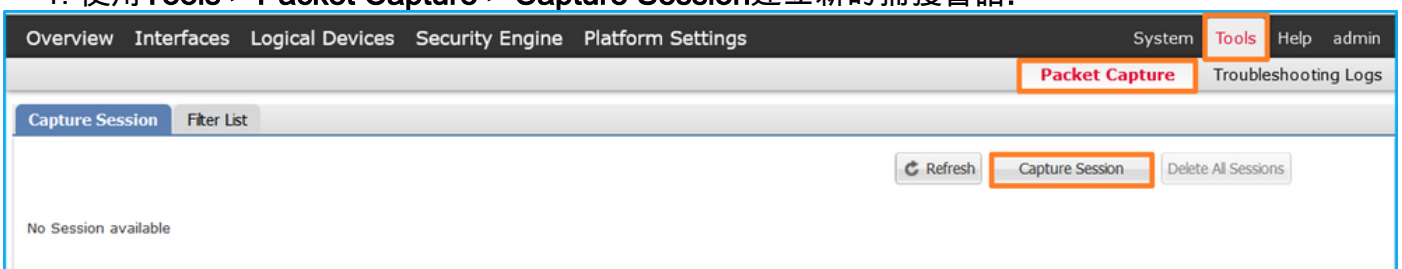


組態

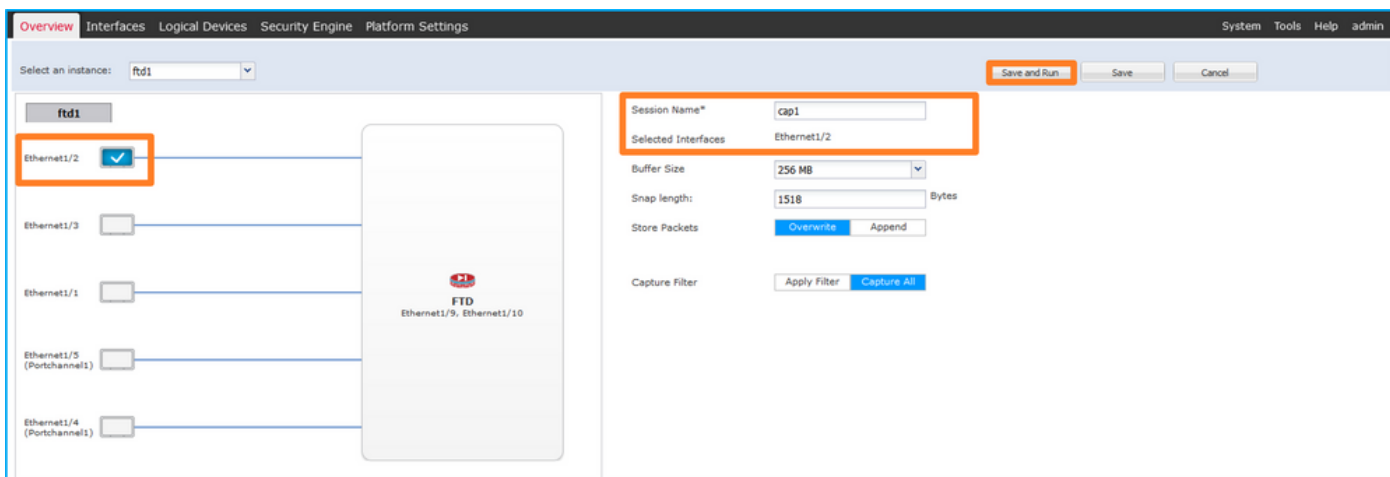
FCM

按照FCM上的以下步驟在介面Ethernet1/2或Portchannel1上配置資料包捕獲：

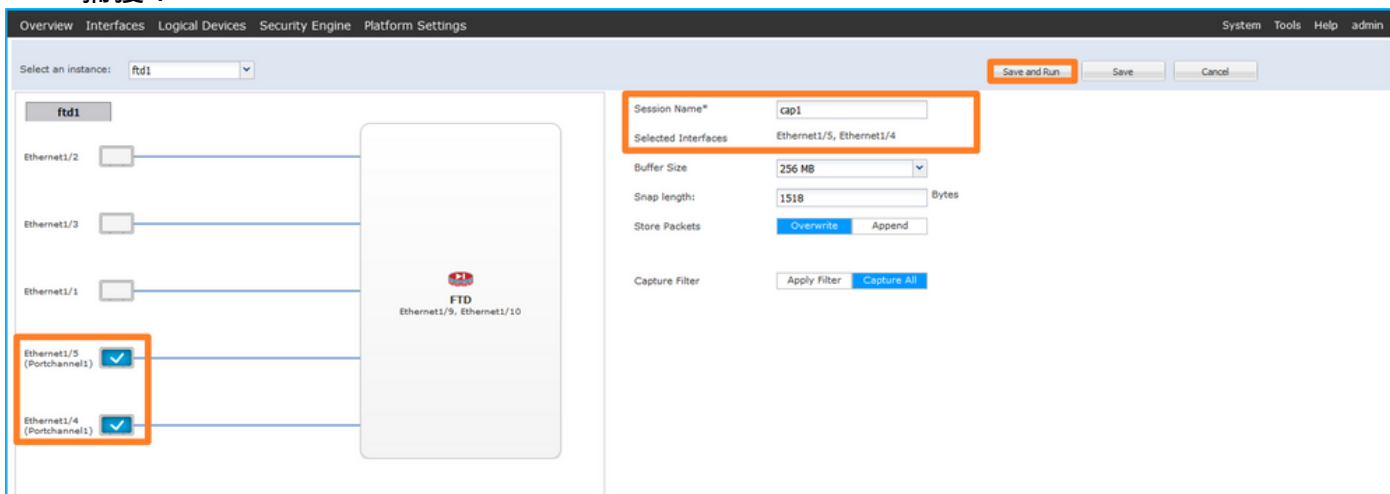
1. 使用Tools > Packet Capture > Capture Session建立新的捕獲會話:



2. 選擇介面Ethernet1/2，提供會話名稱，然後按一下儲存並運行以啟用捕獲：



3. 如果是埠通道介面，請選擇所有物理成員介面，提供會話名稱，然後按一下儲存並運行以啟用捕獲：



FXOS CLI

在FXOS CLI上執行以下步驟，在介面Ethernet1/2或Portchannel1上配置資料包捕獲：

1. 標識應用程式型別和識別符號：

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

2. 對於埠通道介面，請標識其成員介面：

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

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

3. 建立捕獲會話：

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

對於埠通道介面，為每個成員介面配置單獨的捕獲：

```
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 #
```

驗證

FCM

確認Interface Name，確保Operational Status為up，並確認File Size（以位元組為單位）增加：

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/2	None	28632	cap1-ethernet-1-2-0.pcap	ftd1

具有成員介面Ethernet1/4和Ethernet1/5的Portchannel1:

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/5	None	160	cap1-ethernet-1-5-0.pcap	ftd1
Ethernet1/4	None	85000	cap1-ethernet-1-4-0.pcap	ftd1

FXOS CLI

驗證scope packet-capture中的捕獲詳細資訊：

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

Traffic Monitoring Session:

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

Physical ports involved in Packet Capture:

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

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

```
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

收集捕獲檔案

按照收集Firepower 4100/9300內部交換機捕獲檔案一節中的步驟操作。

捕獲檔案分析

使用資料包捕獲檔案讀取器應用程式開啟Ethernet1/2的捕獲檔案。選擇第一個資料包並檢查要點：

1. 僅捕獲ICMP回應請求資料包。捕獲每個資料包並顯示2次。
2. 原始資料包報頭沒有VLAN標籤。
3. 內部交換器插入識別輸入介面Ethernet1/2的其他連線埠VLAN標籤102。
4. 內部交換機插入一個附加VN標籤。

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-07-13 06:23:58.285080930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found!)
2	2022-07-13 06:23:58.285082858	192.0.2.100	198.51.100.100	ICMP	102	0x9dec (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found!)
3	2022-07-13 06:23:59.309048886	192.0.2.100	198.51.100.100	ICMP	108	0x9ed0 (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found!)
4	2022-07-13 06:23:59.309193731	192.0.2.100	198.51.100.100	ICMP	102	0x9ed0 (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found!)
5	2022-07-13 06:24:00.333054190	192.0.2.100	198.51.100.100	ICMP	108	0xf20 (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	0xf20 (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	0xf2d (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	0xf2d (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	0xf88 (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	0xf88 (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!)


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

選擇第二個資料包並檢查要點：

1. 僅捕獲ICMP回應請求資料包。捕獲每個資料包並顯示2次。
2. 原始資料包報頭沒有VLAN標籤。
3. 內部交換器插入識別輸入介面Ethernet1/2的其他連線埠VLAN標籤102。

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-07-13 06:23:58.285088930	192.0.2.100	198.51.100.100	ICMP	108	0x90dc (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found)
2	2022-07-13 06:23:58.285088288	192.0.2.100	198.51.100.100	ICMP	102	0x90dc (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found)
3	2022-07-13 06:23:59.309048886	192.0.2.100	198.51.100.100	ICMP	108	0x9e0d (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found)
4	2022-07-13 06:23:59.309193731	192.0.2.100	198.51.100.100	ICMP	102	0x9e0d (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found)
5	2022-07-13 06:24:00.333054190	192.0.2.100	198.51.100.100	ICMP	108	0xf20 (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	0xf20 (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	0xf2d (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	0xf2d (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	0xf88 (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	0xf88 (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 06:24:11.597086627	192.0.2.100	198.51.100.100	ICMP	108	0xa349 (41801)	64	Echo (ping) request id=0x001a, seq=20/5120, ttl=64 (no response found)
28	2022-07-13 06:24:11.597088170	192.0.2.100	198.51.100.100	ICMP	102	0xa349 (41801)	64	Echo (ping) request id=0x001a, seq=20/5120, ttl=64 (no response found)
29	2022-07-13 06:24:12.621061022	192.0.2.100	198.51.100.100	ICMP	108	0xa3dc (41948)	64	Echo (ping) request id=0x001a, seq=21/5376, ttl=64 (no response found)

Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture_u0_1, id 0
 Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102

000. = Priority: Best Effort (default) (0)
 ...0 = DEI: Ineligible
 ... 0000 0110 0110 = ID: 102
 Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100

Internet Control Message Protocol

開啟Portchannel1成員介面的捕獲檔案。選擇第一個封包並檢查要點：

1. 僅捕獲ICMP回應請求資料包。捕獲每個資料包並顯示2次。
2. 原始資料包報頭沒有VLAN標籤。
3. 內部交換器插入一個額外的連線埠VLAN標籤1001，用於識別輸入介面Portchannel1。
4. 內部交換機插入一個附加VN標籤。

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

Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_3, id 0
 Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: a2:76:f2:00:00:25 (a2:76:f2:00:00:25)

VN-Tag

1.... = Direction: From Bridge
 .0.. = Pointer: vif_id
 ..00 0000 0101 0100 = Destination: 84
 = Looped: No
 ...0.. = Reserved: 0
 = Version: 0
 ... 0000 0000 0000 = Source: 0
 Type: 802.1Q Virtual LAN (0x8100)

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1001

000. = Priority: Best Effort (default) (0)
 ...0 = DEI: Ineligible
 ... 0011 1110 1001 = ID: 1001
 Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100

Internet Control Message Protocol

選擇第二個資料包並檢查要點：

1. 僅捕獲ICMP回應請求資料包。捕獲每個資料包並顯示2次。
2. 原始資料包報頭沒有VLAN標籤。
3. 內部交換器插入一個額外的連線埠VLAN標籤1001，用於識別輸入介面Portchannel1。

No.	Time	Source	Destination	Protocol	Length	P ID	P TTL	Info
1	2022-08-05 23:07:31.865872877	192.0.2.100	198.51.100.100	ICMP	108	0x322e (12846)	64	Echo (ping) request id=0x002d, seq=245/62720, ttl=64 (nc
2	2022-08-05 23:07:31.865875131	192.0.2.100	198.51.100.100	ICMP	102	0x322e (12846)	64	Echo (ping) request id=0x002d, seq=245/62720, ttl=64 (nc
3	2022-08-05 23:07:32.867144598	192.0.2.100	198.51.100.100	ICMP	108	0x32b9 (12985)	64	Echo (ping) request id=0x002d, seq=246/62976, ttl=64 (nc
4	2022-08-05 23:07:32.867145852	192.0.2.100	198.51.100.100	ICMP	102	0x32b9 (12985)	64	Echo (ping) request id=0x002d, seq=246/62976, ttl=64 (nc
5	2022-08-05 23:07:33.881902485	192.0.2.100	198.51.100.100	ICMP	108	0x32d8 (13016)	64	Echo (ping) request id=0x002d, seq=247/63232, ttl=64 (nc
6	2022-08-05 23:07:33.881904191	192.0.2.100	198.51.100.100	ICMP	102	0x32d8 (13016)	64	Echo (ping) request id=0x002d, seq=247/63232, ttl=64 (nc
7	2022-08-05 23:07:34.883049425	192.0.2.100	198.51.100.100	ICMP	108	0x3373 (13171)	64	Echo (ping) request id=0x002d, seq=248/63488, ttl=64 (nc
8	2022-08-05 23:07:34.883051649	192.0.2.100	198.51.100.100	ICMP	102	0x3373 (13171)	64	Echo (ping) request id=0x002d, seq=248/63488, ttl=64 (nc
9	2022-08-05 23:07:35.883478016	192.0.2.100	198.51.100.100	ICMP	108	0x3427 (13351)	64	Echo (ping) request id=0x002d, seq=249/63744, ttl=64 (nc
10	2022-08-05 23:07:35.883479190	192.0.2.100	198.51.100.100	ICMP	102	0x3427 (13351)	64	Echo (ping) request id=0x002d, seq=249/63744, ttl=64 (nc
11	2022-08-05 23:07:36.889741625	192.0.2.100	198.51.100.100	ICMP	108	0x34de (13534)	64	Echo (ping) request id=0x002d, seq=250/64000, ttl=64 (nc
12	2022-08-05 23:07:36.889742853	192.0.2.100	198.51.100.100	ICMP	102	0x34de (13534)	64	Echo (ping) request id=0x002d, seq=250/64000, ttl=64 (nc
13	2022-08-05 23:07:37.913770117	192.0.2.100	198.51.100.100	ICMP	108	0x354c (13644)	64	Echo (ping) request id=0x002d, seq=251/64256, ttl=64 (nc
14	2022-08-05 23:07:37.913772219	192.0.2.100	198.51.100.100	ICMP	102	0x354c (13644)	64	Echo (ping) request id=0x002d, seq=251/64256, ttl=64 (nc
15	2022-08-05 23:07:38.937829879	192.0.2.100	198.51.100.100	ICMP	108	0x3602 (13826)	64	Echo (ping) request id=0x002d, seq=252/64512, ttl=64 (nc
16	2022-08-05 23:07:38.937831215	192.0.2.100	198.51.100.100	ICMP	102	0x3602 (13826)	64	Echo (ping) request id=0x002d, seq=252/64512, ttl=64 (nc
17	2022-08-05 23:07:39.961786128	192.0.2.100	198.51.100.100	ICMP	108	0x366d (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	0x366d (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 captured (816 bits) on interface capture_u0_3, i
> Ethernet II, Src: VMWare 9d:e8:be (00:50:56:9d:e8:be), Dst: a2:76:f2:00:00:25 (a2:76:f2:00:00:25)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1001
000. .... = Priority: Best Effort (default) (0)
...0 .... = DEI: Ineligible
.... 0011 1110 1001 = ID: 1001
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
Internet Control Message Protocol
  
```

說明

在前端介面上設定封包擷取時，交換器會同時擷取每個封包兩次：

- 插入埠VLAN標籤之後。
- 在插入VN標籤之後。

按照操作順序，VN標籤插入的時間比埠VLAN標籤插入的時間晚。但是在擷取檔案中，含有VN標籤的封包會比含有連線埠VLAN標籤的封包顯示得更早。

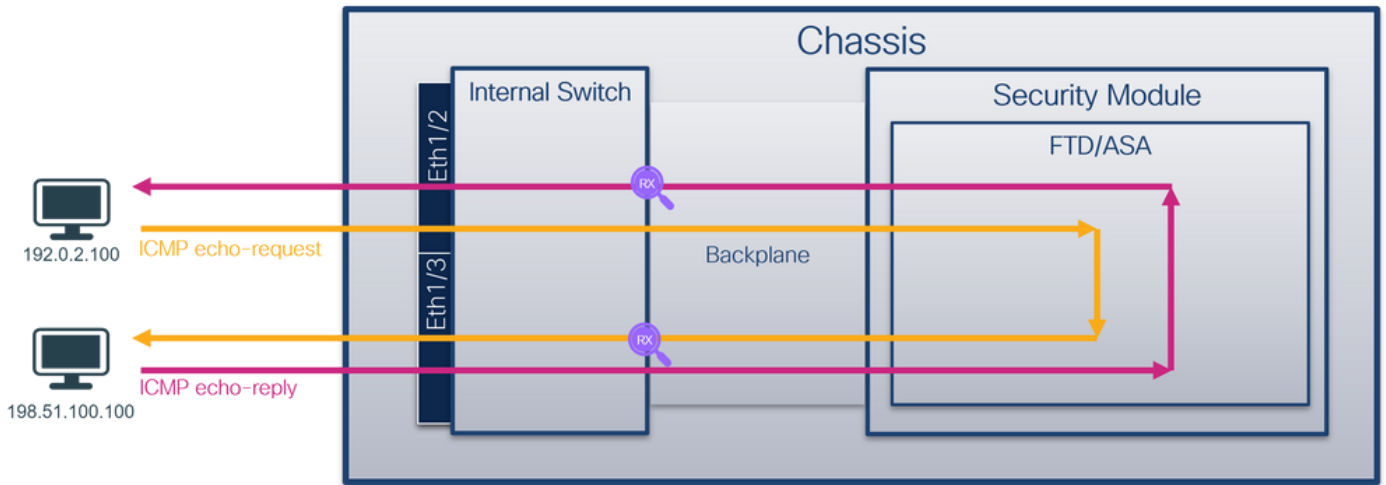
此表概述了任務：

工作	捕獲點	捕獲資料包中的內部埠VLAN	方向	捕獲的流量
在介面Ethernet1/2上配置並檢驗資料包捕獲	Ethernet1/2	102	僅限輸入	從主機192.0.2.100到主機198.51.100.100的ICMP回應請求
在介面Portchannel1上配置並檢驗帶有成員介面Ethernet1/4和Ethernet1/5的資料包捕獲	Ethernet1/4 Ethernet1/5	1001	僅限輸入	從主機192.0.2.100到主機198.51.100.100的ICMP回應請求

背板介面上的封包擷取

使用FCM和CLI配置和驗證背板介面上的資料包捕獲。

拓撲、資料包流和捕獲點

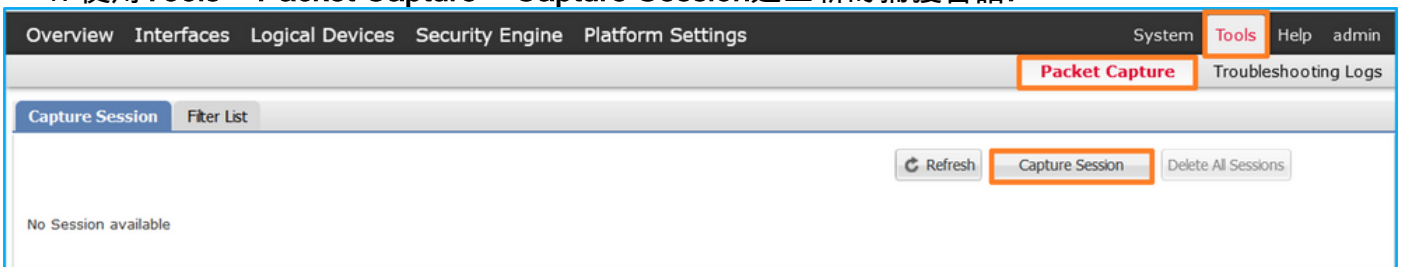


組態

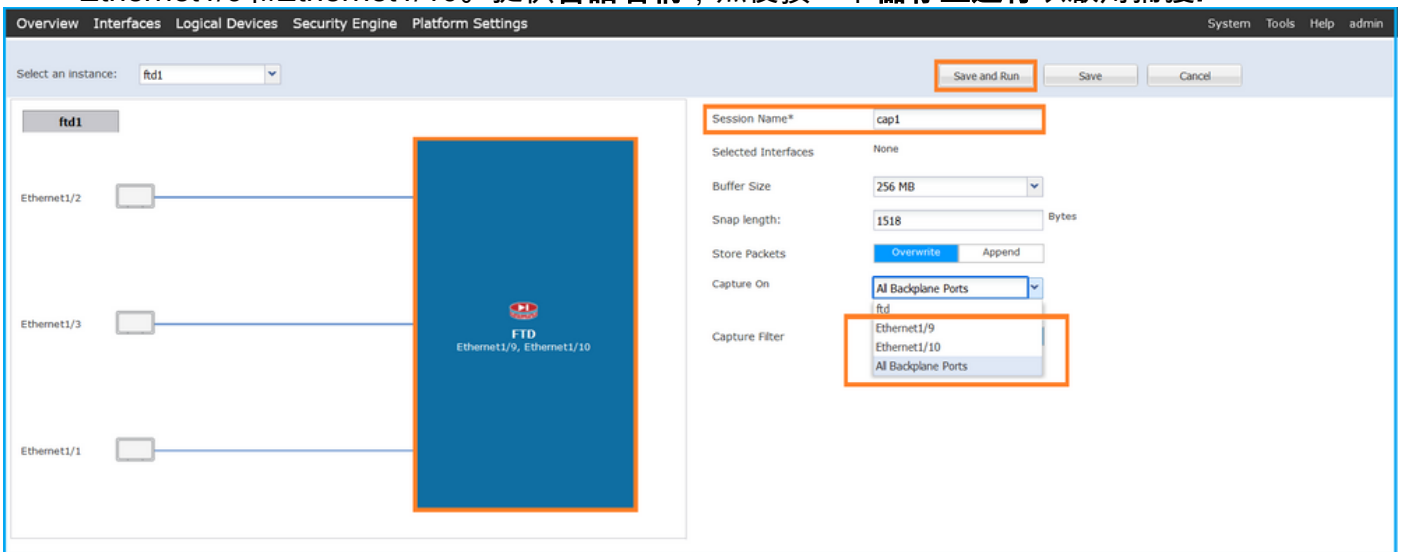
FCM

按照FCM上的以下步驟配置背板介面上的資料包捕獲：

1. 使用Tools > Packet Capture > Capture Session建立新的捕獲會話：



2. 若要擷取所有背板介面上的封包，請從下拉式清單中選擇應用程式，然後選擇Capture On(擷取在所有背板連線埠)。或者，選擇特定的背板介面。在這種情況下，可以提供背板介面Ethernet1/9和Ethernet1/10。提供會話名稱，然後按一下儲存並運行以啟用捕獲：



FXOS CLI

按照FXOS CLI上的以下步驟配置背板介面上的資料包捕獲：

1. 標識應用程式型別和識別符號：

```

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

```

2. 建立捕獲會話：

```

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 #

```

驗證

FCM

確認Interface Name，確保Operational Status為up，並確認File Size（以位元組為單位）增加：

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/10	None	194352	cap1-ethernet-1-10-0.pcap	ftd1
Ethernet1/9	None	286368	cap1-ethernet-1-9-0.pcap	ftd1

FXOS CLI

驗證scope packet-capture中的捕獲詳細資訊：

```

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

收集捕獲檔案

按照**收集Firepower 4100/9300內部交換機捕獲檔案**一節中的步驟操作。

捕獲檔案分析

使用資料包捕獲檔案讀取器應用程式開啟捕獲檔案。如果有一個以上的背板介面，請確保開啟每個背板介面的所有捕獲檔案。在這種情況下，封包會在背板介面Ethernet1/9上擷取。

選擇第一個和第二個資料包，並檢查要點：

1. 捕獲每個ICMP回應請求資料包並顯示兩次。
2. 原始資料包報頭沒有VLAN標籤。
3. 內部交換器插入識別輸出介面Ethernet1/3的其他連線埠VLAN標籤103。
4. 內部交換機插入一個附加VN標籤。

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-07-14 20:20:36.513854256	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (no response found!)
2	2022-07-14 20:20:36.513857289	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (reply in 3)
3	2022-07-14 20:20:36.514117394	198.51.100.100	192.0.2.100	ICMP	108	0xc2c2 (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 2)
4	2022-07-14 20:20:36.514119312	198.51.100.100	192.0.2.100	ICMP	108	0xc2c2 (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64
5	2022-07-14 20:20:37.537723822	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040)	64	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (no response found!)
6	2022-07-14 20:20:37.537726588	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040)	64	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (reply in 7)
7	2022-07-14 20:20:37.538046165	198.51.100.100	192.0.2.100	ICMP	108	0xc9b9 (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 6)
8	2022-07-14 20:20:37.538048311	198.51.100.100	192.0.2.100	ICMP	108	0xc9b9 (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64
9	2022-07-14 20:20:38.561776064	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (no response found!)
10	2022-07-14 20:20:38.561778310	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (reply in 11)
11	2022-07-14 20:20:38.562048288	198.51.100.100	192.0.2.100	ICMP	108	0xc4c4 (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 10)
12	2022-07-14 20:20:38.562050333	198.51.100.100	192.0.2.100	ICMP	108	0xc4c4 (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64
13	2022-07-14 20:20:39.585677043	192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366)	64	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (no response found!)
14	2022-07-14 20:20:39.585678455	192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366)	64	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (reply in 15)
15	2022-07-14 20:20:39.585936554	198.51.100.100	192.0.2.100	ICMP	108	0xcdbd (52621)	64	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64 (request in 14)
16	2022-07-14 20:20:39.585937900	198.51.100.100	192.0.2.100	ICMP	108	0xcdbd (52621)	64	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64
17	2022-07-14 20:20:40.609804804	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (23419)	64	Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (no response found!)
18	2022-07-14 20:20:40.610179685	198.51.100.100	192.0.2.100	ICMP	108	0xcdbf (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64 (request in 18)
19	2022-07-14 20:20:40.610181944	198.51.100.100	192.0.2.100	ICMP	108	0xcdbf (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64
20	2022-07-14 20:20:41.633805153	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (no response found!)
21	2022-07-14 20:20:41.633806997	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (reply in 23)
22	2022-07-14 20:20:41.634084102	198.51.100.100	192.0.2.100	ICMP	108	0xc3e6 (52790)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64 (request in 22)
23	2022-07-14 20:20:41.634085368	198.51.100.100	192.0.2.100	ICMP	108	0xc3e6 (52790)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64
24	2022-07-14 20:20:42.657799988	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (no response found!)
25	2022-07-14 20:20:42.657711660	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (reply in 27)
26	2022-07-14 20:20:42.657980675	198.51.100.100	192.0.2.100	ICMP	108	0xc649 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64 (request in 26)
27	2022-07-14 20:20:42.657981971	198.51.100.100	192.0.2.100	ICMP	108	0xc649 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64
28	2022-07-14 20:20:43.681736697	192.0.2.100	198.51.100.100	ICMP	108	0x5c52 (23634)	64	Echo (ping) request id=0x0001, seq=22/5632, ttl=64 (no response found!)
29	2022-07-14 20:20:43.681736697	192.0.2.100	198.51.100.100	ICMP	108	0x5c52 (23634)	64	Echo (ping) request id=0x0001, seq=22/5632, ttl=64 (no response found!)

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

```

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

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 103
000. .... = Priority: Best Effort (default) (0)
...0 .. = DEI: Ineligible
... 0000 0110 0111 = ID: 103
Type: IPv4 (0x0800)

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

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

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-07-14 20:20:36.513854256	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (no response found!)
2	2022-07-14 20:20:36.513857289	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (reply in 3)
3	2022-07-14 20:20:36.514117394	198.51.100.100	192.0.2.100	ICMP	108	0xc2c2 (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 2)
4	2022-07-14 20:20:36.514119312	198.51.100.100	192.0.2.100	ICMP	108	0xc2c2 (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64
5	2022-07-14 20:20:37.537723822	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040)	64	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (no response found!)
6	2022-07-14 20:20:37.537726588	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040)	64	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (reply in 7)
7	2022-07-14 20:20:37.538046165	198.51.100.100	192.0.2.100	ICMP	108	0xc9b9 (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 6)
8	2022-07-14 20:20:37.538048311	198.51.100.100	192.0.2.100	ICMP	108	0xc9b9 (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64
9	2022-07-14 20:20:38.561776064	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (no response found!)
10	2022-07-14 20:20:38.561778310	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (reply in 11)
11	2022-07-14 20:20:38.562048288	198.51.100.100	192.0.2.100	ICMP	108	0xc4c4 (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 10)
12	2022-07-14 20:20:38.562050333	198.51.100.100	192.0.2.100	ICMP	108	0xc4c4 (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64
13	2022-07-14 20:20:39.585677043	192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366)	64	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (no response found!)
14	2022-07-14 20:20:39.585678455	192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366)	64	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (reply in 15)
15	2022-07-14 20:20:39.585936554	198.51.100.100	192.0.2.100	ICMP	108	0xcdbd (52621)	64	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64 (request in 14)
16	2022-07-14 20:20:39.585937900	198.51.100.100	192.0.2.100	ICMP	108	0xcdbd (52621)	64	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64
17	2022-07-14 20:20:40.609804804	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (23419)	64	Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (no response found!)
18	2022-07-14 20:20:40.610179685	198.51.100.100	192.0.2.100	ICMP	108	0xcdbf (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64 (request in 18)
19	2022-07-14 20:20:40.610181944	198.51.100.100	192.0.2.100	ICMP	108	0xcdbf (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64
20	2022-07-14 20:20:41.633805153	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (no response found!)
21	2022-07-14 20:20:41.633806997	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (reply in 23)
22	2022-07-14 20:20:41.634084102	198.51.100.100	192.0.2.100	ICMP	108	0xc3e6 (52790)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64 (request in 22)
23	2022-07-14 20:20:41.634085368	198.51.100.100	192.0.2.100	ICMP	108	0xc3e6 (52790)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64
24	2022-07-14 20:20:42.657799988	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (no response found!)
25	2022-07-14 20:20:42.657711660	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (reply in 27)
26	2022-07-14 20:20:42.657980675	198.51.100.100	192.0.2.100	ICMP	108	0xc649 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64 (request in 26)
27	2022-07-14 20:20:42.657981971	198.51.100.100	192.0.2.100	ICMP	108	0xc649 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64
28	2022-07-14 20:20:43.681736697	192.0.2.100	198.51.100.100	ICMP	108	0x5c52 (23634)	64	Echo (ping) request id=0x0001, seq=22/5632, ttl=64 (no response found!)
29	2022-07-14 20:20:43.681736697	192.0.2.100	198.51.100.100	ICMP	108	0x5c52 (23634)	64	Echo (ping) request id=0x0001, seq=22/5632, ttl=64 (no response found!)

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

```

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

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 103
000. .... = Priority: Best Effort (default) (0)
...0 .. = DEI: Ineligible
... 0000 0110 0111 = ID: 103
Type: IPv4 (0x0800)

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

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

選擇第三個和第四個資料包，並檢查要點：

1. 捕獲每個ICMP回應應答並顯示2次。
2. 原始資料包報頭沒有VLAN標籤。
3. 內部交換器插入識別輸出介面Ethernet1/2的其他連線埠VLAN標籤102。
4. 內部交換機插入一個附加VN標籤。

The image shows a Wireshark packet capture of ICMP Echo (ping) traffic. The packet list pane shows 29 packets. Packet 3 is highlighted in red, indicating it is the selected packet. The packet details pane shows the following layers:

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

說明

在背板介面上設定封包擷取時，交換器會同時擷取每個封包兩次。在這種情況下，內部交換器會收到安全模組上應用程式已使用連線埠VLAN標籤和VN標籤標籤的封包。VLAN標籤標識內部機箱用於將資料包轉發到網路的輸出介面。ICMP回應請求資料包中的VLAN標籤103將Ethernet1/3標識為輸出介面，而ICMP回應應答資料包中的VLAN標籤102將Ethernet1/2標識為輸出介面。在將資料包轉發到網路之前，內部交換機會刪除VN標籤和內部介面VLAN標籤。

此表概述了任務：

工作	捕獲點	捕獲資料包中的內部埠 VLAN	方向	捕獲的流量
配置並檢驗背板介面上的資料包捕獲	背板介面	102 103	僅限輸入	從主機192.0.2.100到主機198.51.100.100的ICMP回應請求 從主機198.51.100.100到主機192.0.2.100的ICMP回應應答

應用和應用埠上的資料包捕獲

應用或應用埠資料包捕獲始終配置在背板介面上，如果使用者指定應用捕獲方向，則還會配置在前端介面上。

主要有2個使用案例：

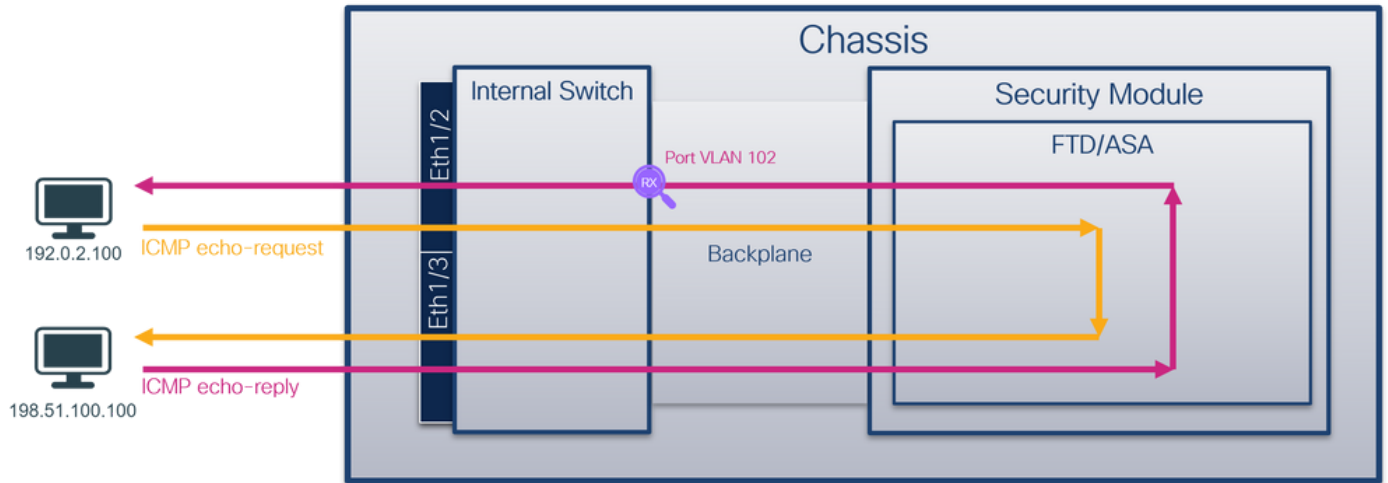
- 為離開特定前介面的資料包配置背板介面上的資料包捕獲。例如，為離開介面Ethernet1/2的封包在背板介面Ethernet1/9上設定封包擷取。
- 在特定正面介面和背板介面上配置同時資料包捕獲。例如，為離開介面Ethernet1/2的封包在介面Ethernet1/2和背板介面Ethernet1/9上設定同時封包擷取。

本節涵蓋這兩種使用情形。

任務1

使用FCM和CLI在背板介面上設定和驗證封包擷取。捕獲將應用埠Ethernet1/2標識為輸出介面的資料包。在此案例中，會擷取ICMP回覆。

拓撲、資料包流和捕獲點

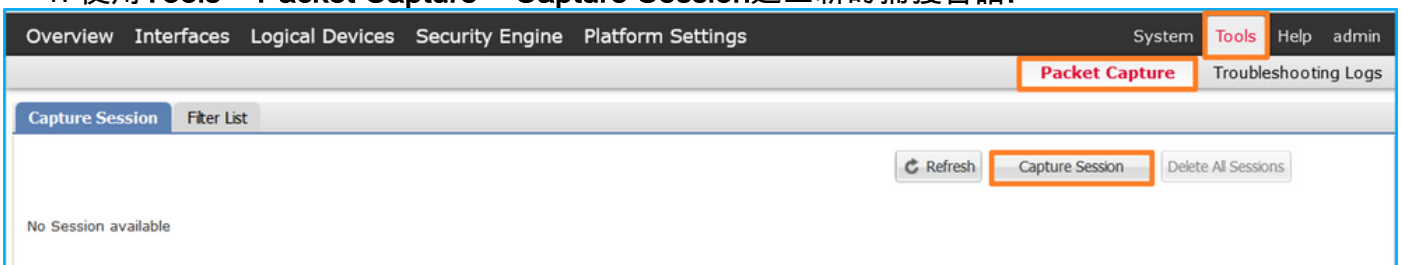


組態

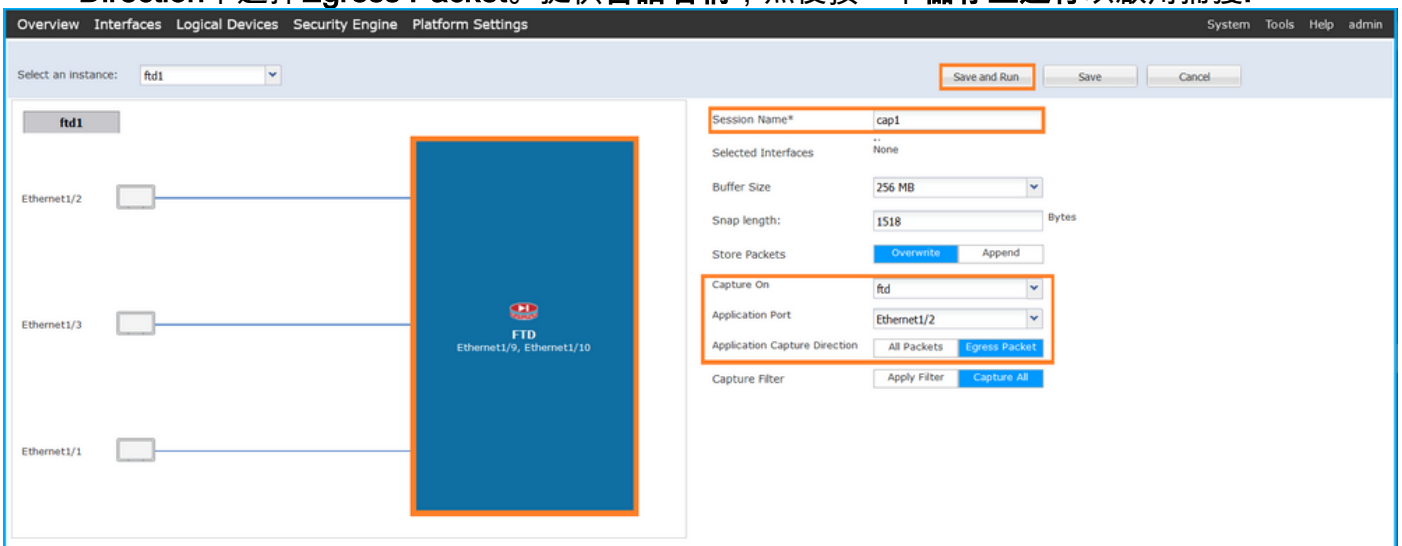
FCM

按照FCM上的以下步驟在FTD應用程式和應用連線埠Ethernet1/2上設定封包擷取：

1. 使用Tools > Packet Capture > Capture Session建立新的捕獲會話：



2. 在Application Port下拉選單中選擇application， Ethernet1/2， 然後在Application Capture Direction中選擇Egress Packet。提供會話名稱， 然後按一下儲存並運行以啟用捕獲：



FXOS CLI

按照FXOS CLI上的以下步驟配置背板介面上的資料包捕獲：

1. 標識應用程式型別和識別符號：

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

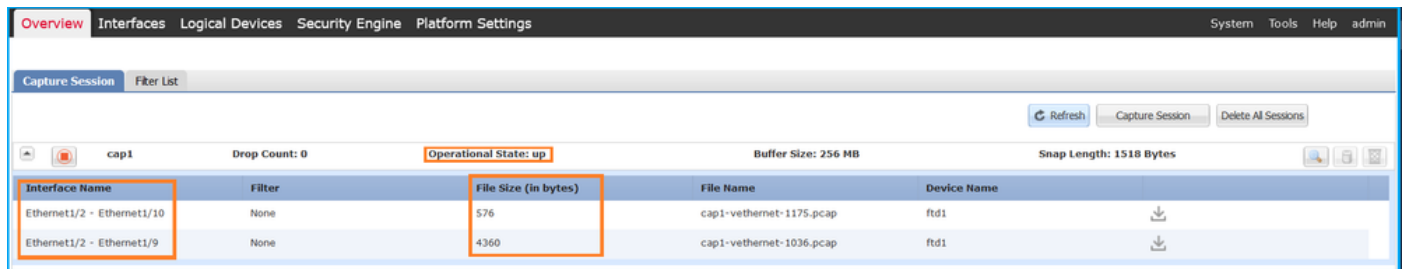
2. 建立捕獲會話：

```
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 #
```

驗證

FCM

確認Interface Name，確保Operational Status為up，並確認File Size (以位元組為單位) 增加：



Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/2 - Ethernet1/10	None	576	cap1-ve-ethernet-1175.pcap	ftd1
Ethernet1/2 - Ethernet1/9	None	4360	cap1-ve-ethernet-1036.pcap	ftd1

FXOS CLI

驗證scope packet-capture中的捕獲詳細資訊：

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

Traffic Monitoring Session:

```
Packet Capture Session Name: cap1
Session: 1
Admin State: Enabled
Oper State: Up
Oper State Reason: Active
Config Success: Yes
Config Fail Reason:
Append Flag: Overwrite
```

Session Mem Usage: 256 MB
Session Pcap Snap Len: 1518 Bytes
Error Code: 0
Drop Count: 0

Application ports involved in Packet Capture:

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

Application ports resolved to:

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

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

收集捕獲檔案

按照收集Firepower 4100/9300內部交換機捕獲檔案一節中的步驟操作。

捕獲檔案分析

使用資料包捕獲檔案讀取器應用程式開啟捕獲檔案。如果有多個背板介面，請確保開啟每個背板介面的所有捕獲檔案。在這種情況下，封包會在背板介面Ethernet1/9上擷取。

選擇第一個和第二個資料包，並檢查要點：

1. 捕獲每個ICMP回應應答並顯示2次。
2. 原始資料包報頭沒有VLAN標籤。
3. 內部交換器插入識別輸出介面Ethernet1/2的其他連線埠VLAN標籤102。
4. 內部交換機插入一個附加VN標籤。

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 10:03:22.231237959	198.51.100.100	192.0.2.100	ICMP	108	0x42f8 (17144)	64	Echo (ping) reply
2	2022-08-01 10:03:22.231239747	198.51.100.100	192.0.2.100	ICMP	108	0x42f8 (17144)	64	Echo (ping) reply
3	2022-08-01 10:03:23.232244769	198.51.100.100	192.0.2.100	ICMP	108	0x4303 (17331)	64	Echo (ping) reply
4	2022-08-01 10:03:23.232247753	198.51.100.100	192.0.2.100	ICMP	108	0x43b3 (17331)	64	Echo (ping) reply
5	2022-08-01 10:03:24.234703981	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64	Echo (ping) reply
6	2022-08-01 10:03:24.234706751	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64	Echo (ping) reply
7	2022-08-01 10:03:25.258672449	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64	Echo (ping) reply
8	2022-08-01 10:03:25.258674861	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64	Echo (ping) reply
9	2022-08-01 10:03:26.282663169	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64	Echo (ping) reply
10	2022-08-01 10:03:26.282666183	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64	Echo (ping) reply
11	2022-08-01 10:03:27.306671694	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64	Echo (ping) reply
12	2022-08-01 10:03:27.306674378	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64	Echo (ping) reply
13	2022-08-01 10:03:28.330664677	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64	Echo (ping) reply
14	2022-08-01 10:03:28.330667153	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64	Echo (ping) reply
15	2022-08-01 10:03:29.354795931	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply
16	2022-08-01 10:03:29.354936706	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply
17	2022-08-01 10:03:30.378795204	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64	Echo (ping) reply
18	2022-08-01 10:03:30.378798172	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64	Echo (ping) reply
19	2022-08-01 10:03:31.402772217	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64	Echo (ping) reply
20	2022-08-01 10:03:31.402774775	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64	Echo (ping) reply
21	2022-08-01 10:03:32.426693254	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64	Echo (ping) reply
22	2022-08-01 10:03:32.426695691	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64	Echo (ping) reply

```

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

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

  802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
  000... .. = Priority: Best Effort (default) (0)
  ...0 .. = DEI: Ineligible
  ... 0000 0110 0110 = ID: 102
  Type: IPv4 (0x0800)

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

0000	00 50 56 9d e8 be 58 97	bd b9 77 0e 89 26 00 00	PV...X...M...&...
0010	00 0a 81 00 00 66 08 00	45 00 00 54 42 f8 00 00	...f...E...TB...
0020	40 01 4a b5 c6 33 64 64	c0 00 02 64 00 00 00 04	@J...3dd...d...
0030	00 12 00 01 dd a4 e7 62	00 00 00 00 e3 0d 09 00	...b... ..
0040	00 00 00 00 10 11 12 13	14 15 16 17 18 19 1a 1b
0050	1c 1d 1e 1f 20 21 22 23	24 25 26 27 28 29 2a 2b	... !"# \$%&'()*+...
0060	2c 2d 2e 2f 30 31 32 33	34 35 36 37	.../0123 4567

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 10:03:22.231237959	198.51.100.100	192.0.2.100	ICMP	108	0x42f8 (17144)	64	Echo (ping) reply
2	2022-08-01 10:03:22.231239747	198.51.100.100	192.0.2.100	ICMP	108	0x42f8 (17144)	64	Echo (ping) reply
3	2022-08-01 10:03:23.232244769	198.51.100.100	192.0.2.100	ICMP	108	0x4303 (17331)	64	Echo (ping) reply
4	2022-08-01 10:03:23.232247753	198.51.100.100	192.0.2.100	ICMP	108	0x43b3 (17331)	64	Echo (ping) reply
5	2022-08-01 10:03:24.234703981	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64	Echo (ping) reply
6	2022-08-01 10:03:24.234706751	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64	Echo (ping) reply
7	2022-08-01 10:03:25.258672449	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64	Echo (ping) reply
8	2022-08-01 10:03:25.258674861	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64	Echo (ping) reply
9	2022-08-01 10:03:26.282663169	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64	Echo (ping) reply
10	2022-08-01 10:03:26.282666183	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64	Echo (ping) reply
11	2022-08-01 10:03:27.306671694	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64	Echo (ping) reply
12	2022-08-01 10:03:27.306674378	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64	Echo (ping) reply
13	2022-08-01 10:03:28.330664677	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64	Echo (ping) reply
14	2022-08-01 10:03:28.330667153	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64	Echo (ping) reply
15	2022-08-01 10:03:29.354795931	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply
16	2022-08-01 10:03:29.354936706	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply
17	2022-08-01 10:03:30.378795204	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64	Echo (ping) reply
18	2022-08-01 10:03:30.378798172	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64	Echo (ping) reply
19	2022-08-01 10:03:31.402772217	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64	Echo (ping) reply
20	2022-08-01 10:03:31.402774775	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64	Echo (ping) reply
21	2022-08-01 10:03:32.426693254	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64	Echo (ping) reply
22	2022-08-01 10:03:32.426695691	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64	Echo (ping) reply

```

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

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

  802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
  000... .. = Priority: Best Effort (default) (0)
  ...0 .. = DEI: Ineligible
  ... 0000 0110 0110 = ID: 102
  Type: IPv4 (0x0800)

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

0000	00 50 56 9d e8 be 58 97	bd b9 77 0e 89 26 00 00	PV...X...M...&...
0010	00 0a 81 00 00 66 08 00	45 00 00 54 42 f8 00 00	...f...E...TB...
0020	40 01 4a b5 c6 33 64 64	c0 00 02 64 00 00 00 04	@J...3dd...d...
0030	00 12 00 01 dd a4 e7 62	00 00 00 00 e3 0d 09 00	...b... ..
0040	00 00 00 00 10 11 12 13	14 15 16 17 18 19 1a 1b
0050	1c 1d 1e 1f 20 21 22 23	24 25 26 27 28 29 2a 2b	... !"# \$%&'()*+...
0060	2c 2d 2e 2f 30 31 32 33	34 35 36 37	.../0123 4567

說明

在這種情況下，連線埠VLAN標籤為102的Ethernet1/2是ICMP回應回覆封包的輸出介面。

當在擷取選項中將應用擷取方向設定為Egress時，就會在輸入方向的背板介面上擷取乙太網路標頭中連線埠VLAN標號為102的封包。

此表概述了任務：

工作	捕獲點	捕獲資料包中的內部埠 VLAN	方向	捕獲的流量
----	-----	--------------------	----	-------

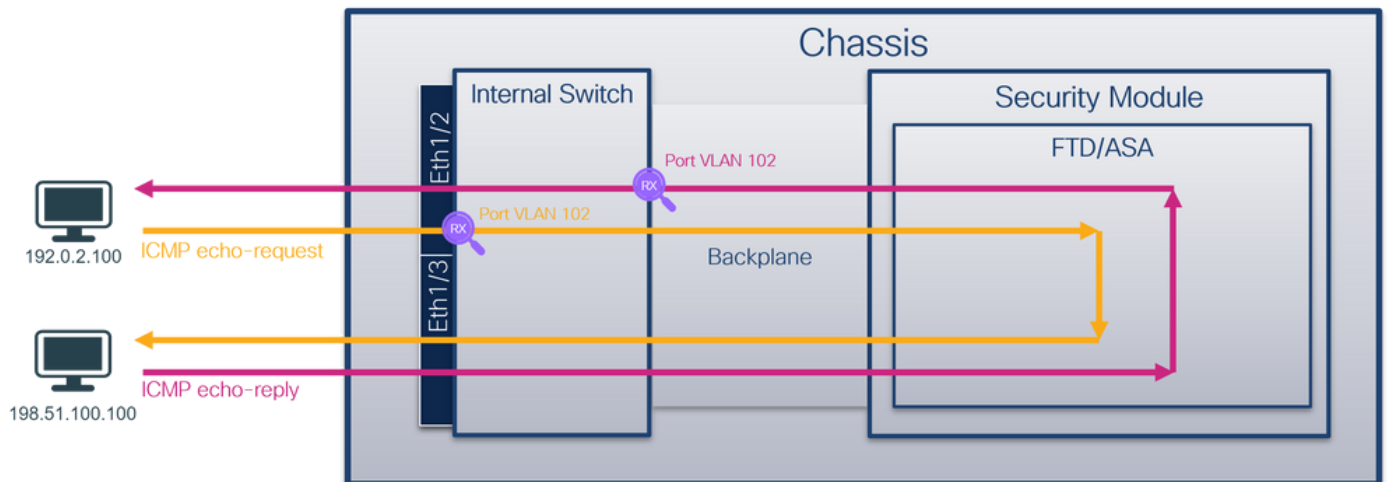
任務2

使用FCM和CLI在背板介面和正面介面Ethernet1/2上設定和驗證封包擷取。

同時捕獲資料包配置在：

- 前介面 — 捕獲介面Ethernet1/2上埠VLAN 102的資料包。捕獲的資料包是ICMP回應請求。
- 背板介面 — 擷取Ethernet1/2識別為輸出介面的封包或連線埠VLAN 102的封包。捕獲的資料包是ICMP回應應答。

拓撲、資料包流和捕獲點

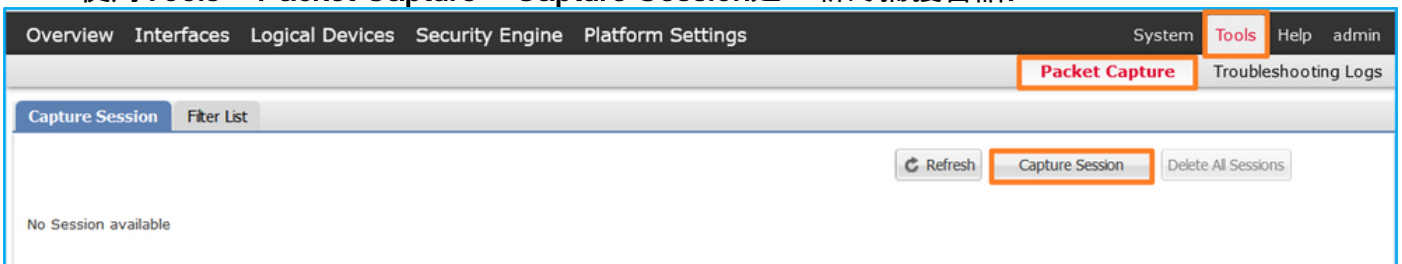


組態

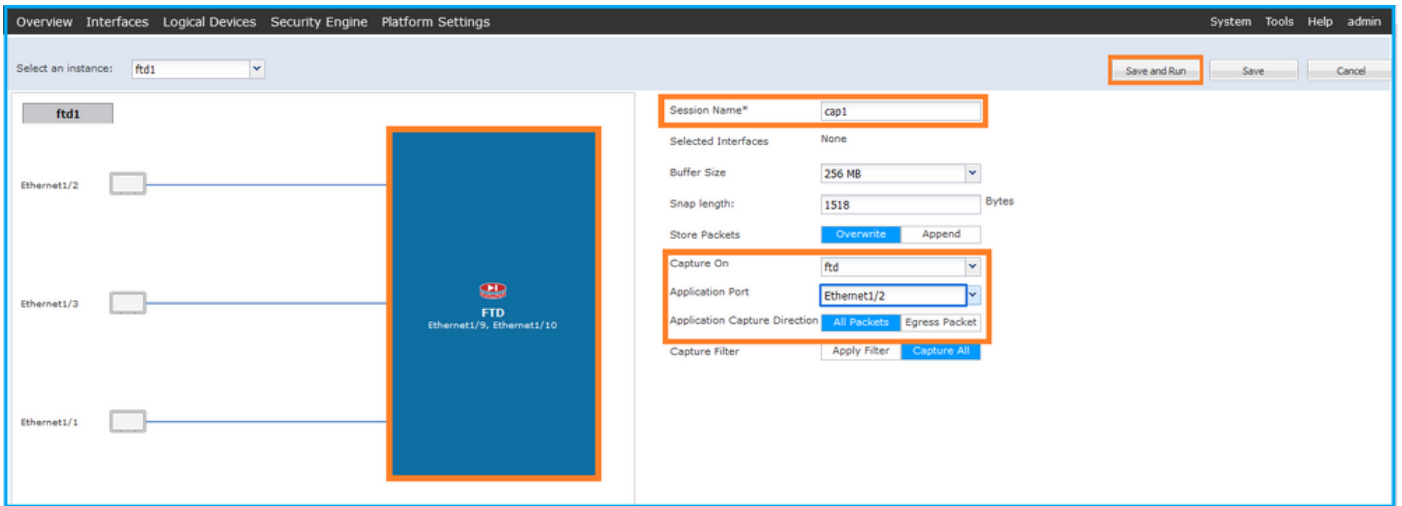
FCM

按照FCM上的以下步驟在FTD應用程式和應用連線埠Ethernet1/2上設定封包擷取：

1. 使用Tools > Packet Capture > Capture Session建立新的捕獲會話：



2. 在「Application Port」下拉式清單中選擇FTD應用程式Ethernet1/2，然後在「Application Capture Direction」中選擇All Packets。提供會話名稱，然後按一下儲存並運行以啟用捕獲：



FXOS CLI

按照FXOS CLI上的以下步驟配置背板介面上的資料包捕獲：

1. 標識應用程式型別和識別符號：

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

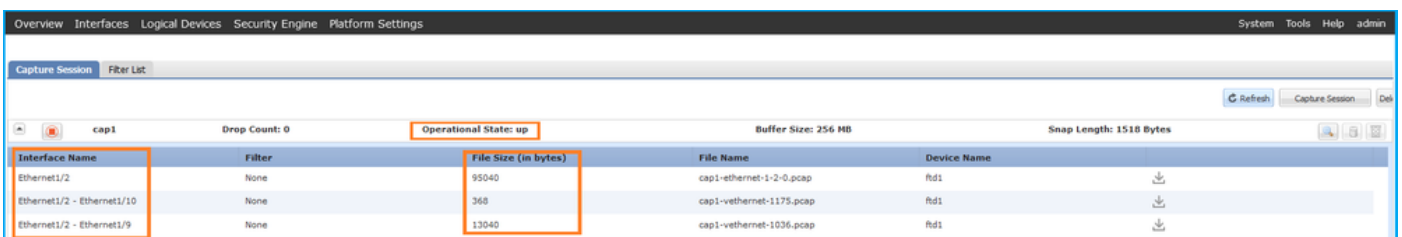
2. 建立捕獲會話：

```
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
```

驗證

FCM

確認Interface Name，確保Operational Status為up，並確認File Size（以位元組為單位）增加：



FXOS CLI

驗證scope packet-capture中的捕獲詳細資訊：

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

Traffic Monitoring Session:

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

Physical ports involved in Packet Capture:

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

Application ports involved in Packet Capture:

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

Application ports resolved to:

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

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

收集捕獲檔案

按照收集Firepower 4100/9300內部交換機捕獲檔案一節中的步驟操作。

捕獲檔案分析

使用資料包捕獲檔案讀取器應用程式開啟捕獲檔案。如果有多個背板介面，請確保開啟每個背板介面的所有捕獲檔案。 在這種情況下，封包會在背板介面Ethernet1/9上擷取。

開啟介面Ethernet1/2的擷取檔案，選擇第一個封包，並檢查要點：

1. 僅捕獲ICMP回應請求資料包。捕獲每個資料包並顯示2次。
2. 原始資料包報頭沒有VLAN標籤。
3. 內部交換器插入識別輸入介面Ethernet1/2的其他連線埠VLAN標籤102。
4. 內部交換機插入一個附加VN標籤。

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 11:33:19.070693081	192.0.2.100	198.51.100.100	ICMP	108	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
2	2022-08-01 11:33:19.070695347	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
3	2022-08-01 11:33:19.071217121	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
4	2022-08-01 11:33:19.071218458	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
5	2022-08-01 11:33:20.072036625	192.0.2.100	198.51.100.100	ICMP	102	0xc00a (49326)	64	Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found)
6	2022-08-01 11:33:20.072038399	192.0.2.100	198.51.100.100	ICMP	108	0xc00a (49326)	64	Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found)
7	2022-08-01 11:33:21.073266030	192.0.2.100	198.51.100.100	ICMP	108	0xc167 (49511)	64	Echo (ping) request id=0x0013, seq=3/768, ttl=64 (no response found)
8	2022-08-01 11:33:21.073268327	192.0.2.100	198.51.100.100	ICMP	102	0xc167 (49511)	64	Echo (ping) request id=0x0013, seq=3/768, ttl=64 (no response found)
9	2022-08-01 11:33:22.074576640	192.0.2.100	198.51.100.100	ICMP	108	0xc175 (49525)	64	Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found)
10	2022-08-01 11:33:22.074578010	192.0.2.100	198.51.100.100	ICMP	102	0xc175 (49525)	64	Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found)
11	2022-08-01 11:33:23.075779089	192.0.2.100	198.51.100.100	ICMP	108	0xc208 (49672)	64	Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found)
12	2022-08-01 11:33:23.075781513	192.0.2.100	198.51.100.100	ICMP	102	0xc208 (49672)	64	Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found)
13	2022-08-01 11:33:24.081839490	192.0.2.100	198.51.100.100	ICMP	108	0xc211 (49681)	64	Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found)
14	2022-08-01 11:33:24.081841386	192.0.2.100	198.51.100.100	ICMP	102	0xc211 (49681)	64	Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found)
15	2022-08-01 11:33:25.105806249	192.0.2.100	198.51.100.100	ICMP	108	0xc2e2 (49890)	64	Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found)
16	2022-08-01 11:33:25.105807895	192.0.2.100	198.51.100.100	ICMP	102	0xc2e2 (49890)	64	Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found)
17	2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	ICMP	108	0xc3b4 (50100)	64	Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found)
18	2022-08-01 11:33:26.129838114	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100)	64	Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found)
19	2022-08-01 11:33:27.153828653	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found)
20	2022-08-01 11:33:27.153830201	192.0.2.100	198.51.100.100	ICMP	102	0xc476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found)
21	2022-08-01 11:33:28.177847175	192.0.2.100	198.51.100.100	ICMP	108	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found)
22	2022-08-01 11:33:28.177849075	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found)
23	2022-08-01 11:33:29.201804760	192.0.2.100	198.51.100.100	ICMP	108	0xc578 (50552)	64	Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found)
24	2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	102	0xc578 (50552)	64	Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found)
25	2022-08-01 11:33:30.225834765	192.0.2.100	198.51.100.100	ICMP	108	0xc585 (50565)	64	Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found)
26	2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (50565)	64	Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found)
27	2022-08-01 11:33:31.249828955	192.0.2.100	198.51.100.100	ICMP	108	0xc618 (50712)	64	Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found)
28	2022-08-01 11:33:31.249831121	192.0.2.100	198.51.100.100	ICMP	102	0xc618 (50712)	64	Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found)
29	2022-08-01 11:33:32.273867960	192.0.2.100	198.51.100.100	ICMP	108	0xc64f (50767)	64	Echo (ping) request id=0x0013, seq=14/3584, ttl=64 (no response found)


```

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

選擇第二個資料包並檢查要點：

1. 僅捕獲ICMP回應請求資料包。捕獲每個資料包並顯示2次。
2. 原始資料包報頭沒有VLAN標籤。
3. 內部交換器插入識別輸入介面Ethernet1/2的其他連線埠VLAN標籤102。

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 11:33:19.070693081	192.0.2.100	198.51.100.100	ICMP	108	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found!)
2	2022-08-01 11:33:19.070695347	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found!)
3	2022-08-01 11:33:19.071217121	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found!)
4	2022-08-01 11:33:19.071218458	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found!)
5	2022-08-01 11:33:20.072036625	192.0.2.100	198.51.100.100	ICMP	108	0xc0ae (49326)	64	Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found!)
6	2022-08-01 11:33:20.072038390	192.0.2.100	198.51.100.100	ICMP	102	0xc0ae (49326)	64	Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found!)
7	2022-08-01 11:33:21.073266030	192.0.2.100	198.51.100.100	ICMP	108	0xc167 (49511)	64	Echo (ping) request id=0x0013, seq=3/768, ttl=64 (no response found!)
8	2022-08-01 11:33:21.073268327	192.0.2.100	198.51.100.100	ICMP	102	0xc167 (49511)	64	Echo (ping) request id=0x0013, seq=3/768, ttl=64 (no response found!)
9	2022-08-01 11:33:22.074576640	192.0.2.100	198.51.100.100	ICMP	108	0xc175 (49525)	64	Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found!)
10	2022-08-01 11:33:22.074578010	192.0.2.100	198.51.100.100	ICMP	102	0xc175 (49525)	64	Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found!)
11	2022-08-01 11:33:23.075799089	192.0.2.100	198.51.100.100	ICMP	108	0xc208 (49672)	64	Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found!)
12	2022-08-01 11:33:23.075781513	192.0.2.100	198.51.100.100	ICMP	102	0xc208 (49672)	64	Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found!)
13	2022-08-01 11:33:24.081839490	192.0.2.100	198.51.100.100	ICMP	108	0xc211 (49681)	64	Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found!)
14	2022-08-01 11:33:24.081841306	192.0.2.100	198.51.100.100	ICMP	102	0xc211 (49681)	64	Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found!)
15	2022-08-01 11:33:25.105806249	192.0.2.100	198.51.100.100	ICMP	108	0xc262 (49890)	64	Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found!)
16	2022-08-01 11:33:25.105807895	192.0.2.100	198.51.100.100	ICMP	102	0xc262 (49890)	64	Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found!)
17	2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	ICMP	108	0xc3b4 (50100)	64	Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found!)
18	2022-08-01 11:33:26.129838114	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100)	64	Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found!)
19	2022-08-01 11:33:27.153828653	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found!)
20	2022-08-01 11:33:27.153830201	192.0.2.100	198.51.100.100	ICMP	102	0xc476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found!)
21	2022-08-01 11:33:28.17847175	192.0.2.100	198.51.100.100	ICMP	108	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found!)
22	2022-08-01 11:33:28.17849075	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found!)
23	2022-08-01 11:33:29.201804760	192.0.2.100	198.51.100.100	ICMP	108	0xc578 (50552)	64	Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found!)
24	2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	102	0xc578 (50552)	64	Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found!)
25	2022-08-01 11:33:30.225834765	192.0.2.100	198.51.100.100	ICMP	108	0xc585 (50565)	64	Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found!)
26	2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (50565)	64	Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found!)
27	2022-08-01 11:33:31.249828955	192.0.2.100	198.51.100.100	ICMP	108	0xc618 (50712)	64	Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found!)
28	2022-08-01 11:33:31.249831121	192.0.2.100	198.51.100.100	ICMP	102	0xc618 (50712)	64	Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found!)
29	2022-08-01 11:33:32.273867960	192.0.2.100	198.51.100.100	ICMP	108	0xc64f (50767)	64	Echo (ping) request id=0x0013, seq=14/3584, ttl=64 (no response found!)

Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture_u0_1, id 0		0000	58 97 bd b9 77 0e 00 50	56 9d e8 be 81 00 00 66	X...w..P.V.....f
Ethernet II, Src: Vmware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)		0010	08 00 45 00 00 54 c0 09	40 00 40 01 8d a3 c0 00	..E..T...@.....
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102		0020	02 64 c6 33 64 04 08 00	8d 7c 00 13 00 01 f2 b9	.d.3dd...
0000..... = Priority: Best Effort (default) (0)		0030	e7 62 00 00 00 00 cb 7f	06 00 00 00 00 10 11	.b.....
...0..... = DEI: Ineligible		0040	12 13 14 15 16 17 18 19	1a 1c 1d 1e 1f 20 21
... 0000 0110 0110 = ID: 102		0050	22 23 24 25 26 27 28 29	2a 2b 2c 2d 2e 2f 30 31	"\$%&'()*+,-./01
Type: IPv4 (0x0800)		0060	32 33 34 35 36 37		234567
Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100					
Internet Control Message Protocol					

開啟介面Ethernet1/9的捕獲檔案，選擇第一個和第二個資料包，並檢查要點：

1. 捕獲每個ICMP回應應答並顯示2次。
2. 原始資料包報頭沒有VLAN標籤。
3. 內部交換器插入識別輸出介面Ethernet1/2的其他連線埠VLAN標籤102。
4. 內部交換機插入一個附加VN標籤。

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 11:33:19.071512698	198.51.100.100	192.0.2.100	ICMP	108	0x4f27 (20263)	64	Echo (ping) reply id=0x0013, seq=1/256, ttl=64
2	2022-08-01 11:33:19.071514882	198.51.100.100	192.0.2.100	ICMP	108	0x4f27 (20263)	64	Echo (ping) reply id=0x0013, seq=1/256, ttl=64
3	2022-08-01 11:33:20.072677302	198.51.100.100	192.0.2.100	ICMP	108	0x4ffb (20475)	64	Echo (ping) reply id=0x0013, seq=2/512, ttl=64
4	2022-08-01 11:33:20.072679384	198.51.100.100	192.0.2.100	ICMP	108	0x4ffb (20475)	64	Echo (ping) reply id=0x0013, seq=2/512, ttl=64
5	2022-08-01 11:33:21.073913640	198.51.100.100	192.0.2.100	ICMP	108	0x50ac (20652)	64	Echo (ping) reply id=0x0013, seq=3/768, ttl=64
6	2022-08-01 11:33:21.073915690	198.51.100.100	192.0.2.100	ICMP	108	0x50ac (20652)	64	Echo (ping) reply id=0x0013, seq=3/768, ttl=64
7	2022-08-01 11:33:22.075239381	198.51.100.100	192.0.2.100	ICMP	108	0x513e (20798)	64	Echo (ping) reply id=0x0013, seq=4/1024, ttl=64
8	2022-08-01 11:33:22.075241491	198.51.100.100	192.0.2.100	ICMP	108	0x513e (20798)	64	Echo (ping) reply id=0x0013, seq=4/1024, ttl=64
9	2022-08-01 11:33:23.076447152	198.51.100.100	192.0.2.100	ICMP	108	0x51c9 (20937)	64	Echo (ping) reply id=0x0013, seq=5/1280, ttl=64
10	2022-08-01 11:33:23.076449303	198.51.100.100	192.0.2.100	ICMP	108	0x51c9 (20937)	64	Echo (ping) reply id=0x0013, seq=5/1280, ttl=64
11	2022-08-01 11:33:24.082407896	198.51.100.100	192.0.2.100	ICMP	108	0x528e (21134)	64	Echo (ping) reply id=0x0013, seq=6/1536, ttl=64
12	2022-08-01 11:33:24.082410099	198.51.100.100	192.0.2.100	ICMP	108	0x528e (21134)	64	Echo (ping) reply id=0x0013, seq=6/1536, ttl=64
13	2022-08-01 11:33:25.106382424	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64	Echo (ping) reply id=0x0013, seq=7/1792, ttl=64
14	2022-08-01 11:33:25.106384549	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64	Echo (ping) reply id=0x0013, seq=7/1792, ttl=64
15	2022-08-01 11:33:26.130437851	198.51.100.100	192.0.2.100	ICMP	108	0x53a6 (21414)	64	Echo (ping) reply id=0x0013, seq=8/2048, ttl=64
16	2022-08-01 11:33:26.130440320	198.51.100.100	192.0.2.100	ICMP	108	0x53a6 (21414)	64	Echo (ping) reply id=0x0013, seq=8/2048, ttl=64
17	2022-08-01 11:33:27.154398212	198.51.100.100	192.0.2.100	ICMP	108	0x5446 (21574)	64	Echo (ping) reply id=0x0013, seq=9/2304, ttl=64
18	2022-08-01 11:33:27.154400198	198.51.100.100	192.0.2.100	ICMP	108	0x5446 (21574)	64	Echo (ping) reply id=0x0013, seq=9/2304, ttl=64
19	2022-08-01 11:33:28.178469866	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64	Echo (ping) reply id=0x0013, seq=10/2560, ttl=64
20	2022-08-01 11:33:28.178471810	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64	Echo (ping) reply id=0x0013, seq=10/2560, ttl=64
21	2022-08-01 11:33:29.202395869	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21748)	64	Echo (ping) reply id=0x0013, seq=11/2816, ttl=64
22	2022-08-01 11:33:29.202398067	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21748)	64	Echo (ping) reply id=0x0013, seq=11/2816, ttl=64
23	2022-08-01 11:33:30.226398735	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64	Echo (ping) reply id=0x0013, seq=12/3072, ttl=64
24	2022-08-01 11:33:30.226401017	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64	Echo (ping) reply id=0x0013, seq=12/3072, ttl=64
25	2022-08-01 11:33:31.250387808	198.51.100.100	192.0.2.100	ICMP	108	0x55f2 (22002)	64	Echo (ping) reply id=0x0013, seq=13/3328, ttl=64
26	2022-08-01 11:33:31.250389971	198.51.100.100	192.0.2.100	ICMP	108	0x55f2 (22002)	64	Echo (ping) reply id=0x0013, seq=13/3328, ttl=64
27	2022-08-01 11:33:32.274416011	198.51.100.100	192.0.2.100	ICMP	108	0x5660 (22112)	64	Echo (ping) reply id=0x0013, seq=14/3584, ttl=64
28	2022-08-01 11:33:32.274418229	198.51.100.100	192.0.2.100	ICMP	108	0x5660 (22112)	64	Echo (ping) reply id=0x0013, seq=14/3584, ttl=64
29	2022-08-01 11:33:33.298397657	198.51.100.100	192.0.2.100	ICMP	108	0x56e7 (22247)	64	Echo (ping) reply id=0x0013, seq=15/3840, ttl=64

Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0		0000	00 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:e8:be (00:50:56:9d:e8:be)		0010	00 00 81 00 00 00 00 00	45 00 00 54 4f 27 00 00f..E..T...@.....
VLAN-Tag		0020	40 01 3e 86 c6 33 64 64	c0 00 02 64 00 00 95 7c	@...3dd...d...
0..... = Direction: To Bridge		0030	00 13 00 01 f2 b9 e7 62	00 00 00 00 cb 7f 06 00b.....
..0..... = Pointer: vif_id		0040	00 00 00 00 10 11 12 13	14 15 16 17 18 19 1a 1b
...0000 0000 0000..... = Destination: 0		0050	1c 1d 1e 1f 20 21 22 23	24 25 26 27 28 29 2a 2bl"#\$%&'()*+,-./01234567
...0..... = Looped: No		0060	2c 2d 2e 2f 30 31 32 33	34 35 36 37	
...0..... = Reserved: 0					
...0..... = Version: 0					
... 0000 0000 1010 = Source: 10					
Type: 802.1Q Virtual LAN (0x8100)					
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102					
0000..... = Priority: Best Effort (default) (0)					
...0..... = DEI: Ineligible					
... 0000 0110 0110 = ID: 102					
Type: IPv4 (0x0800)					
Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100					
Internet Control Message Protocol					

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 11:33:19.071512698	198.51.100.100	192.0.2.100	ICMP	108	0x4f27 (20263)	64	Echo (ping) reply id=0x0013, seq=1/256, ttl=64
2	2022-08-01 11:33:19.07514882	198.51.100.100	192.0.2.100	ICMP	108	0x4f27 (20263)	64	Echo (ping) reply id=0x0013, seq=1/256, ttl=64
3	2022-08-01 11:33:20.072677302	198.51.100.100	192.0.2.100	ICMP	108	0x4ff0 (20475)	64	Echo (ping) reply id=0x0013, seq=2/512, ttl=64
4	2022-08-01 11:33:20.072679384	198.51.100.100	192.0.2.100	ICMP	108	0x4ffb (20475)	64	Echo (ping) reply id=0x0013, seq=2/512, ttl=64
5	2022-08-01 11:33:21.073913640	198.51.100.100	192.0.2.100	ICMP	108	0x50ac (20652)	64	Echo (ping) reply id=0x0013, seq=3/768, ttl=64
6	2022-08-01 11:33:21.073915690	198.51.100.100	192.0.2.100	ICMP	108	0x50ac (20652)	64	Echo (ping) reply id=0x0013, seq=3/768, ttl=64
7	2022-08-01 11:33:22.075239381	198.51.100.100	192.0.2.100	ICMP	108	0x513e (20798)	64	Echo (ping) reply id=0x0013, seq=4/1024, ttl=64
8	2022-08-01 11:33:22.075241491	198.51.100.100	192.0.2.100	ICMP	108	0x513e (20798)	64	Echo (ping) reply id=0x0013, seq=4/1024, ttl=64
9	2022-08-01 11:33:23.076447152	198.51.100.100	192.0.2.100	ICMP	108	0x51c9 (20937)	64	Echo (ping) reply id=0x0013, seq=5/1280, ttl=64
10	2022-08-01 11:33:23.076449303	198.51.100.100	192.0.2.100	ICMP	108	0x51c9 (20937)	64	Echo (ping) reply id=0x0013, seq=5/1280, ttl=64
11	2022-08-01 11:33:24.082407896	198.51.100.100	192.0.2.100	ICMP	108	0x528e (21134)	64	Echo (ping) reply id=0x0013, seq=6/1536, ttl=64
12	2022-08-01 11:33:24.082410099	198.51.100.100	192.0.2.100	ICMP	108	0x528e (21134)	64	Echo (ping) reply id=0x0013, seq=6/1536, ttl=64
13	2022-08-01 11:33:25.106382424	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64	Echo (ping) reply id=0x0013, seq=7/1792, ttl=64
14	2022-08-01 11:33:25.106384549	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64	Echo (ping) reply id=0x0013, seq=7/1792, ttl=64
15	2022-08-01 11:33:26.130437851	198.51.100.100	192.0.2.100	ICMP	108	0x53a6 (21414)	64	Echo (ping) reply id=0x0013, seq=8/2048, ttl=64
16	2022-08-01 11:33:26.130440320	198.51.100.100	192.0.2.100	ICMP	108	0x53a6 (21414)	64	Echo (ping) reply id=0x0013, seq=8/2048, ttl=64
17	2022-08-01 11:33:27.154398212	198.51.100.100	192.0.2.100	ICMP	108	0x5446 (21574)	64	Echo (ping) reply id=0x0013, seq=9/2304, ttl=64
18	2022-08-01 11:33:27.154400198	198.51.100.100	192.0.2.100	ICMP	108	0x5446 (21574)	64	Echo (ping) reply id=0x0013, seq=9/2304, ttl=64
19	2022-08-01 11:33:28.178469866	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64	Echo (ping) reply id=0x0013, seq=10/2560, ttl=64
20	2022-08-01 11:33:28.178471810	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64	Echo (ping) reply id=0x0013, seq=10/2560, ttl=64
21	2022-08-01 11:33:29.202395869	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21740)	64	Echo (ping) reply id=0x0013, seq=11/2816, ttl=64
22	2022-08-01 11:33:29.202398067	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21740)	64	Echo (ping) reply id=0x0013, seq=11/2816, ttl=64
23	2022-08-01 11:33:30.226398735	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64	Echo (ping) reply id=0x0013, seq=12/3072, ttl=64
24	2022-08-01 11:33:30.226401817	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64	Echo (ping) reply id=0x0013, seq=12/3072, ttl=64
25	2022-08-01 11:33:31.250387808	198.51.100.100	192.0.2.100	ICMP	108	0x55f2 (22002)	64	Echo (ping) reply id=0x0013, seq=13/3328, ttl=64
26	2022-08-01 11:33:31.250389971	198.51.100.100	192.0.2.100	ICMP	108	0x55f2 (22002)	64	Echo (ping) reply id=0x0013, seq=13/3328, ttl=64
27	2022-08-01 11:33:32.274416011	198.51.100.100	192.0.2.100	ICMP	108	0x5660 (22112)	64	Echo (ping) reply id=0x0013, seq=14/3584, ttl=64
28	2022-08-01 11:33:32.274418229	198.51.100.100	192.0.2.100	ICMP	108	0x5660 (22112)	64	Echo (ping) reply id=0x0013, seq=14/3584, ttl=64
29	2022-08-01 11:33:33.298397657	198.51.100.100	192.0.2.100	ICMP	108	0x56e7 (22247)	64	Echo (ping) reply id=0x0013, seq=15/3840, ttl=64


```

> Frame 2: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
> Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VMware 9d:e8:be (00:50:56:9d:e8:be)
  > VN-Tag
    0... .. = Direction: To Bridge
    .0... .. = Pointer: vif_id
    ..00 0000 0000 0000 .. = Destination: 0
    ..0... .. = Looped: No
    ..0... .. = Reserved: 0
    ..00 .. = Version: 0
    ..0000 0000 1010 = Source: 10
    Type: 802.1Q Virtual LAN (0x8100)
  > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
    000... .. = Priority: Best Effort (default) (0)
    ..0... .. = DEI: Ineligible
    ... 0000 0110 0110 = ID: 102
    Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100
  > Internet Control Message Protocol
  
```

說明

如果選擇All Packets in the Application Capture Direction選項，則會配置與所選應用埠 Ethernet1/2相關的2個同時資料包捕獲：前介面Ethernet1/2上的捕獲和選定背板介面上的捕獲。

在前端介面上設定封包擷取時，交換器會同時擷取每個封包兩次：

- 插入埠VLAN標籤之後。
- 在插入VN標籤之後。

按照操作順序，VN標籤插入的時間比埠VLAN標籤插入的時間晚。但是在擷取檔案中，含有VN標籤的封包會比含有連線埠VLAN標籤的封包顯示得更早。在本範例中，ICMP回應請求封包中的VLAN標籤102將Ethernet1/2識別為輸入介面。

在背板介面上設定封包擷取時，交換器會同時擷取每個封包兩次。內部交換器接收安全模組上應用程式已使用連線埠VLAN標籤和VN標籤標籤的封包。埠VLAN標籤標識內部機箱用於將資料包轉發到網路的輸出介面。在本例中，ICMP回應回覆封包中的VLAN標籤102將Ethernet1/2識別為輸出介面。

在將資料包轉發到網路之前，內部交換機會刪除VN標籤和內部介面VLAN標籤。

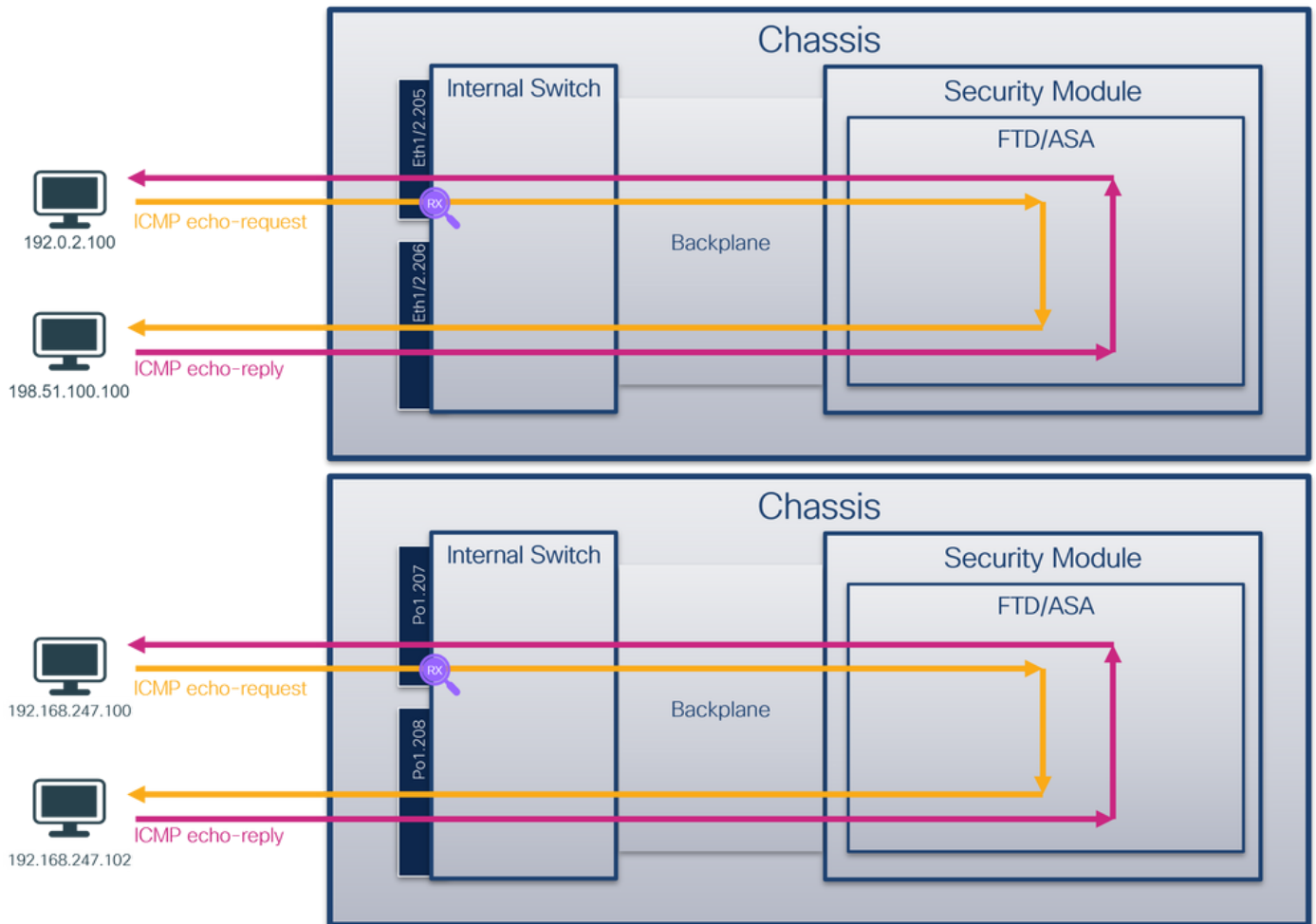
此表概述了任務：

工作	捕獲點	捕獲資料包中的內部埠VLAN	方向	捕獲的流量
配置並檢驗應用程式和應用程式埠Ethernet1/2上的捕獲	背板介面	102	僅限輸入	從主機198.51.100.100到主機192.0.2.100的ICMP回應應答
	Interface Ethernet1/2	102	僅限輸入	從主機192.0.2.100到主機198.51.100.100的ICMP回應請求

物理或埠通道介面的子介面上的資料包捕獲

使用FCM和CLI在子介面Ethernet1/2.205或埠通道子介面Portchannel1.207上配置並驗證資料包捕獲。僅在容器模式下對於FTD應用程式才支援子介面和子介面上的捕獲。在此案例中，在Ethernet1/2.205和Portchannel1.207上設定封包擷取。

拓撲、資料包流和捕獲點

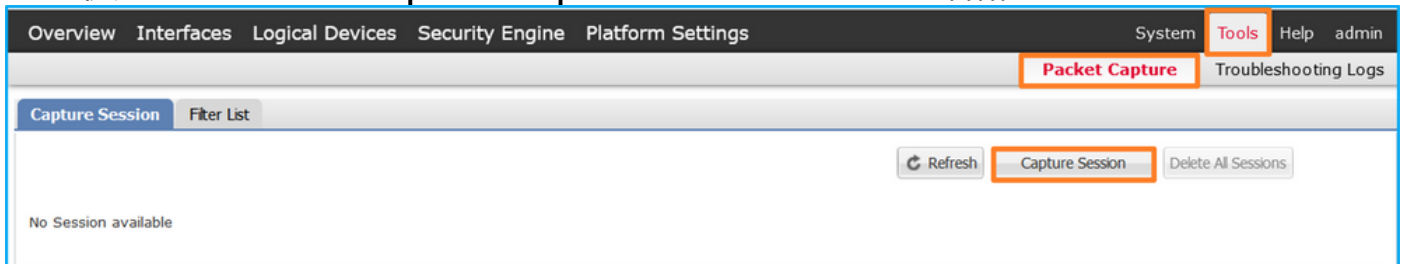


組態

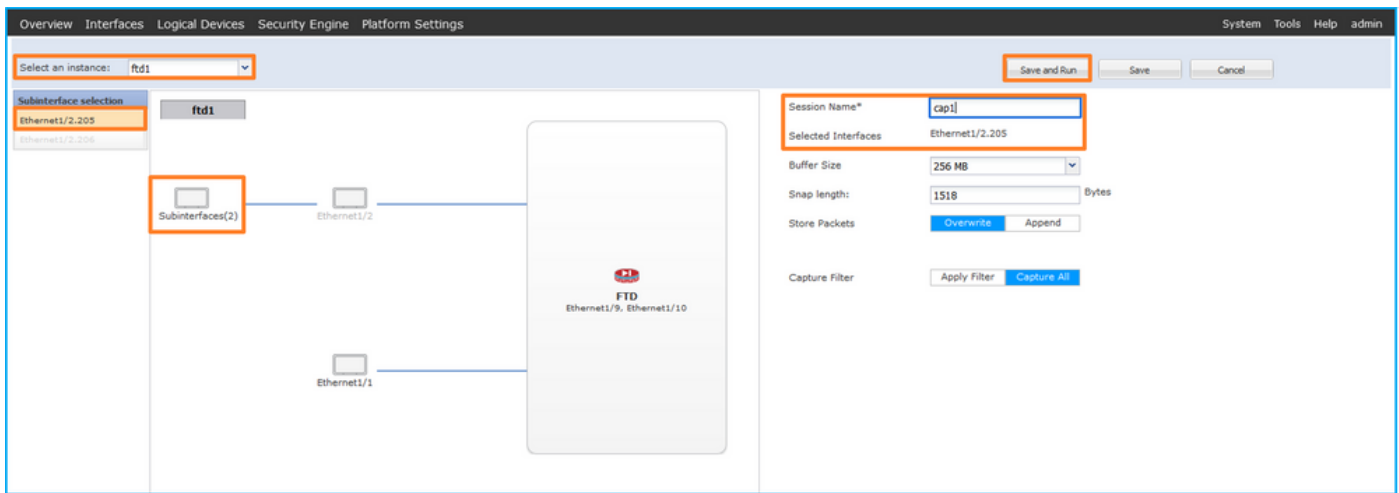
FCM

按照FCM上的以下步驟在FTD應用程式和應用連線埠Ethernet1/2上設定封包擷取：

1. 使用Tools > Packet Capture > Capture Session建立新的捕獲會話：



2. 選擇特定的應用程式例項ftd1（子介面Ethernet1/2.205），提供會話名稱，然後按一下Save and Run啟用捕獲：



3. 在連線埠通道子介面的情況下，由於Cisco錯誤ID [CSCVq33119](#)子介面在FCM中不可見。使用FXOS CLI在埠通道子介面上配置捕獲。

FXOS CLI

在FXOS CLI上執行以下步驟，在子介面Ethernet1/2.205和Portchannel1.207上配置資料包捕獲：

1. 標識應用程式型別和識別符號：

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

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version
ftd	ftd1	1	Enabled	Online	7.2.0.82	7.2.0.82
Container	No	RP20	Not Applicable	None		
ftd	ftd2	1	Enabled	Online	7.2.0.82	7.2.0.82
Container	No	RP20	Not Applicable	None		

2. 對於埠通道介面，請標識其成員介面：

```
firepower# connect fxos
<output skipped>
firepower (fxos) # show port-channel summary
```

Flags: D - Down P - Up in port-channel (members)
 I - Individual H - Hot-standby (LACP only)
 s - Suspended r - Module-removed
 S - Switched R - Routed
 U - Up (port-channel)
 M - Not in use. Min-links not met

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

3. 建立捕獲會話：

```
firepower# scope packet-capture
firepower /packet-capture # create session cap1
firepower /packet-capture/session* # create phy-port Eth1/2
firepower /packet-capture/session/phy-port* # set app ftd
```

```

firepower /packet-capture/session/phy-port* # set app-identifier ftd1
firepower /packet-capture/session/phy-port* # set subinterface 205
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # enable
firepower /packet-capture/session* # commit
firepower /packet-capture/session #

```

對於埠通道子介面，請為每個埠通道成員介面建立一個資料包捕獲：

```

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

```

驗證

FCM

確認Interface Name，確保Operational Status為up，並確認File Size（以位元組為單位）增加：

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/2.205	None	233992	cap1-ethernet-1-2-0.pcap	ftd1

在FXOS CLI上配置的埠通道子介面捕獲也在FCM上可見；但是，無法對其進行編輯：

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

驗證scope packet-capture中的捕獲詳細資訊：

```

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

```

Traffic Monitoring Session:

Packet Capture Session Name: cap1

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

Physical ports involved in Packet Capture:

Slot Id: 1
Port Id: 2
Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap
Pcapsize: 9324 bytes

Filter:

Sub Interface: 205
Application Instance Identifier: ftd1
Application Name: ftd

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

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

Traffic Monitoring Session:

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

Physical ports involved in Packet Capture:

Slot Id: 1
Port Id: 3
Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-3-0.pcap
Pcapsize: 160 bytes

Filter:

Sub Interface: 207
Application Instance Identifier: ftd1
Application Name: ftd

Slot Id: 1

Port Id: 4

Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-4-0.pcap
Pcapsize: 624160 bytes

Filter:

Sub Interface: 207
Application Instance Identifier: ftd1
Application Name: ftd

收集捕獲檔案

按照收集Firepower 4100/9300內部交換機捕獲檔案一節中的步驟操作。

捕獲檔案分析

使用資料包捕獲檔案讀取器應用程式開啟捕獲檔案。選擇第一個封包並檢查要點：

1. 僅捕獲ICMP回應請求資料包。捕獲每個資料包並顯示2次。
2. 原始資料包報頭的VLAN標籤為205。
3. 內部交換器插入識別輸入介面Ethernet1/2的其他連線埠VLAN標籤102。
4. 內部交換機插入一個附加VN標籤。

Frame 1: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface capture_u0_1, id 0
Ethernet II, Src: VMware 9d:e8:be (08:50:56:9d:e8:be), Dst: a2:76:f2:00:00:1b (a2:76:f2:00:00:1b)

VLAN-Tag
1. = Direction: From Bridge
0. = Pointer: vif_id
..00 0000 0101 0100 = Destination: 84
..... = Looped: No
..... = Reserved: 0
..... = Version: 0
..... 0000 0000 0000 = Source: 0
Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
000. = Priority: Best Effort (default) (0)
...0 = DEI: Ineligible
... 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
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
Internet Control Message Protocol

選擇第二個資料包並檢查要點：

1. 僅捕獲ICMP回應請求資料包。捕獲每個資料包並顯示2次。
2. 原始資料包報頭的VLAN標籤為205。

Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture_u0_1, id 0
Ethernet II, Src: VMware 9d:e8:be (08:50:56:9d:e8:be), Dst: a2:76:f2:00:00:1b (a2:76:f2:00:00:1b)

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 205
000. = Priority: Best Effort (default) (0)
...0 = DEI: Ineligible
... 0000 1100 1101 = ID: 205
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
Internet Control Message Protocol

現在開啟Portchannel1.207的捕獲檔案。選擇第一個資料包並檢查要點

1. 僅捕獲ICMP回應請求資料包。捕獲每個資料包並顯示2次。
2. 原始資料包報頭具有VLAN標籤207。
3. 內部交換器插入一個額外的連線埠VLAN標籤1001，用於識別輸入介面Portchannel1。
4. 內部交換機插入一個附加VN標籤。

No.	Time	Source	Destination	Protocol	Length	IP ID	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
2	2022-08-04 08:18:24.572550073	192.168.247.100	192.168.247.102	ICMP	128	0x609e (24734)	255	Echo (ping) request
3	2022-08-04 08:18:24.573286630	192.168.247.100	192.168.247.102	ICMP	128	0x609f (24735)	255	Echo (ping) request
4	2022-08-04 08:18:24.573287640	192.168.247.100	192.168.247.102	ICMP	128	0x609f (24735)	255	Echo (ping) request
5	2022-08-04 08:18:24.573795748	192.168.247.100	192.168.247.102	ICMP	128	0x60a0 (24736)	255	Echo (ping) request
6	2022-08-04 08:18:24.573795748	192.168.247.100	192.168.247.102	ICMP	128	0x60a0 (24736)	255	Echo (ping) request
7	2022-08-04 08:18:24.574368638	192.168.247.100	192.168.247.102	ICMP	128	0x60a1 (24737)	255	Echo (ping) request
8	2022-08-04 08:18:24.574368638	192.168.247.100	192.168.247.102	ICMP	128	0x60a1 (24737)	255	Echo (ping) request
9	2022-08-04 08:18:24.574914512	192.168.247.100	192.168.247.102	ICMP	128	0x60a2 (24738)	255	Echo (ping) request
10	2022-08-04 08:18:24.574914512	192.168.247.100	192.168.247.102	ICMP	128	0x60a2 (24738)	255	Echo (ping) request
11	2022-08-04 08:18:24.575442569	192.168.247.100	192.168.247.102	ICMP	128	0x60a3 (24739)	255	Echo (ping) request
12	2022-08-04 08:18:24.575442569	192.168.247.100	192.168.247.102	ICMP	128	0x60a3 (24739)	255	Echo (ping) request
13	2022-08-04 08:18:24.575918119	192.168.247.100	192.168.247.102	ICMP	128	0x60a4 (24740)	255	Echo (ping) request
14	2022-08-04 08:18:24.575919057	192.168.247.100	192.168.247.102	ICMP	128	0x60a4 (24740)	255	Echo (ping) request
15	2022-08-04 08:18:24.576407671	192.168.247.100	192.168.247.102	ICMP	128	0x60a5 (24741)	255	Echo (ping) request
16	2022-08-04 08:18:24.576408585	192.168.247.100	192.168.247.102	ICMP	128	0x60a5 (24741)	255	Echo (ping) request
17	2022-08-04 08:18:24.576885643	192.168.247.100	192.168.247.102	ICMP	128	0x60a6 (24742)	255	Echo (ping) request
18	2022-08-04 08:18:24.576885643	192.168.247.100	192.168.247.102	ICMP	128	0x60a6 (24742)	255	Echo (ping) request
19	2022-08-04 08:18:24.577394328	192.168.247.100	192.168.247.102	ICMP	128	0x60a7 (24743)	255	Echo (ping) request
20	2022-08-04 08:18:24.577395234	192.168.247.100	192.168.247.102	ICMP	128	0x60a7 (24743)	255	Echo (ping) request
21	2022-08-04 08:18:24.577987632	192.168.247.100	192.168.247.102	ICMP	128	0x60a8 (24744)	255	Echo (ping) request
22	2022-08-04 08:18:24.577989290	192.168.247.100	192.168.247.102	ICMP	128	0x60a8 (24744)	255	Echo (ping) request
23	2022-08-04 08:18:24.578448781	192.168.247.100	192.168.247.102	ICMP	128	0x60a9 (24745)	255	Echo (ping) request
24	2022-08-04 08:18:24.578449900	192.168.247.100	192.168.247.102	ICMP	128	0x60a9 (24745)	255	Echo (ping) request
25	2022-08-04 08:18:24.578900043	192.168.247.100	192.168.247.102	ICMP	128	0x60aa (24746)	255	Echo (ping) request
26	2022-08-04 08:18:24.578900097	192.168.247.100	192.168.247.102	ICMP	128	0x60aa (24746)	255	Echo (ping) request
27	2022-08-04 08:18:24.579426962	192.168.247.100	192.168.247.102	ICMP	128	0x60ab (24747)	255	Echo (ping) request

```
> Frame 1: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface capture_u0_3, id 0
  Ethernet II, Src: Cisco d6:ec:00 (00:17:df:d6:ec:00), Dst: a2:76:f2:00:00:1c (a2:76:f2:00:00:1c)

  VLAN-Tag
  1. .... = Direction: From Bridge
  .0. .... = Pointer: vif id
  ..00 0000 0011 1101 .... = Destination: 61
  .... = Looped: No
  .... = Reserved: 0
  .... = Version: 0
  .... = Source: 0
  Type: 802.1Q Virtual LAN (0x8100)

  802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1001
  000. .... = Priority: Best Effort (default) (0)
  ...0 .... = DEI: Ineligible
  .... 0011 1110 1001 = ID: 1001
  Type: 802.1Q Virtual LAN (0x8100)

  802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 207
  000. .... = Priority: Best Effort (default) (0)
  ...0 .... = DEI: Ineligible
  .... 0000 1100 1111 = ID: 207
  Type: IPv4 (0x0800)

  Internet Protocol Version 4, Src: 192.168.247.100, Dst: 192.168.247.102
  Internet Control Message Protocol
```

選擇第二個資料包並檢查要點：

1. 僅捕獲ICMP回應請求資料包。捕獲每個資料包並顯示2次。
2. 原始資料包報頭的VLAN標籤為207。

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
2	2022-08-04 08:18:24.572550073	192.168.247.100	192.168.247.102	ICMP	128	0x609e (24734)	255	Echo (ping) request

```
> Frame 2: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface capture_u0_3, id 0
  Ethernet II, Src: Cisco d6:ec:00 (00:17:df:d6:ec:00), Dst: a2:76:f2:00:00:1c (a2:76:f2:00:00:1c)

  802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 207
  000. .... = Priority: Best Effort (default) (0)
  ...0 .... = DEI: Ineligible
  .... 0000 1100 1111 = ID: 207
  Type: IPv4 (0x0800)

  Internet Protocol Version 4, Src: 192.168.247.100, Dst: 192.168.247.102
  Internet Control Message Protocol
```

說明

在前端介面上設定封包擷取時，交換器會同時擷取每個封包兩次：

- 插入埠VLAN標籤之後。
- 在插入VN標籤之後。

按照操作順序，VN標籤插入的時間比埠VLAN標籤插入的時間晚。但是在擷取檔案中，含有VN標籤的封包會比含有連線埠VLAN標籤的封包顯示得更早。此外，對於子介面，在捕獲檔案中，第二個資料包不包含埠VLAN標籤。

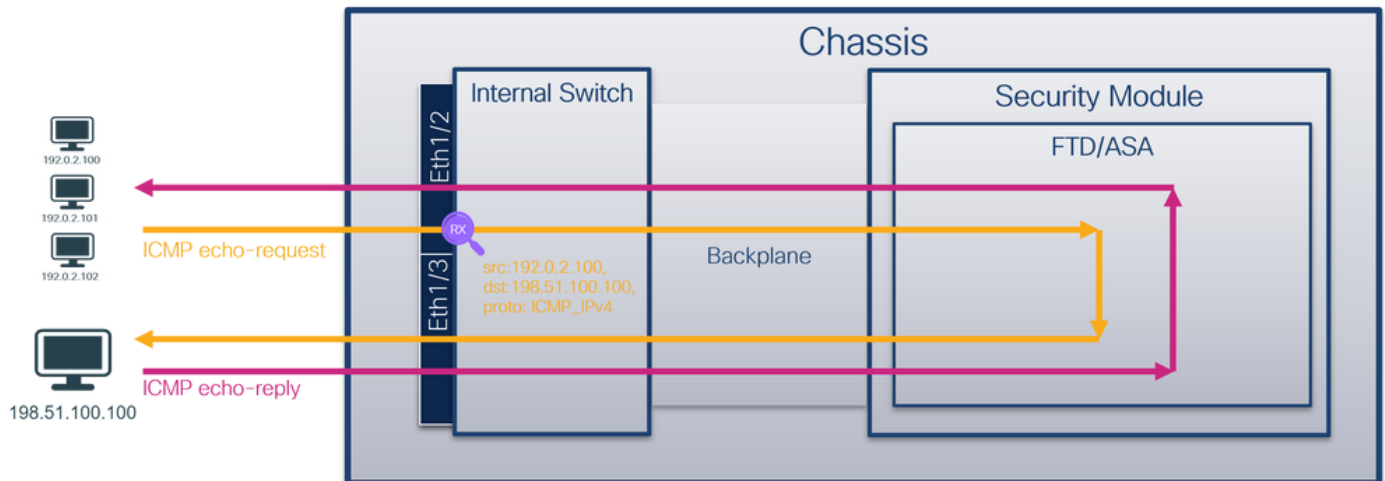
此表概述了任務：

工作	捕獲點	捕獲資料包中的內部埠VLAN	方向	捕獲的流量
在子介面 Ethernet1/2.205 上配置並檢驗資料包捕獲	Ethernet1/2.205	102	僅限輸入	從主機 192.0.2.100 到主機 198.51.100.100 的 ICMP 回應請求
在成員介面 Ethernet1/3 和 Ethernet1/4 的 Portchannel1 子介面上配置並檢驗資料包捕獲	Ethernet1/3 Ethernet1/4	1001	僅限輸入	從 192.168.207.100 到主機 192.168.207.102 的 ICMP 回應請求

封包擷取過濾器

使用 FCM 和 CLI 在帶有過濾器的介面 Ethernet1/2 上配置和驗證資料包捕獲。

拓撲、資料包流和捕獲點

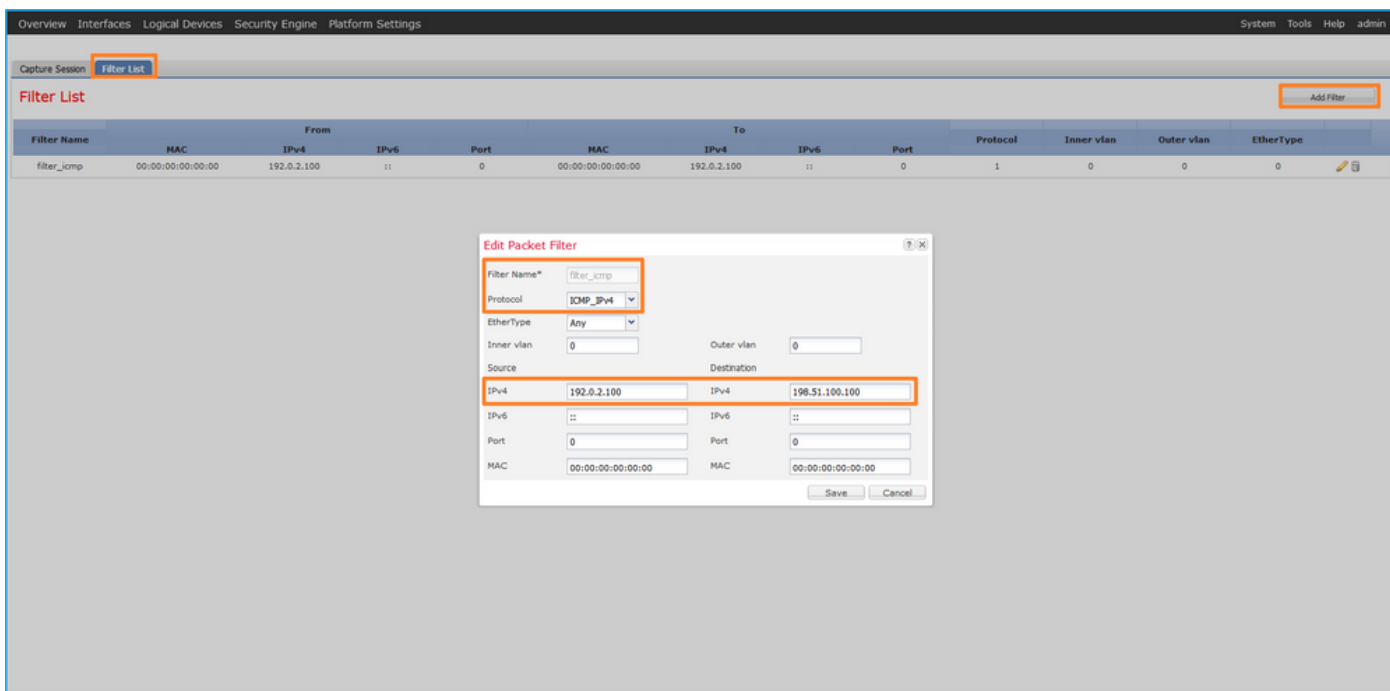


組態

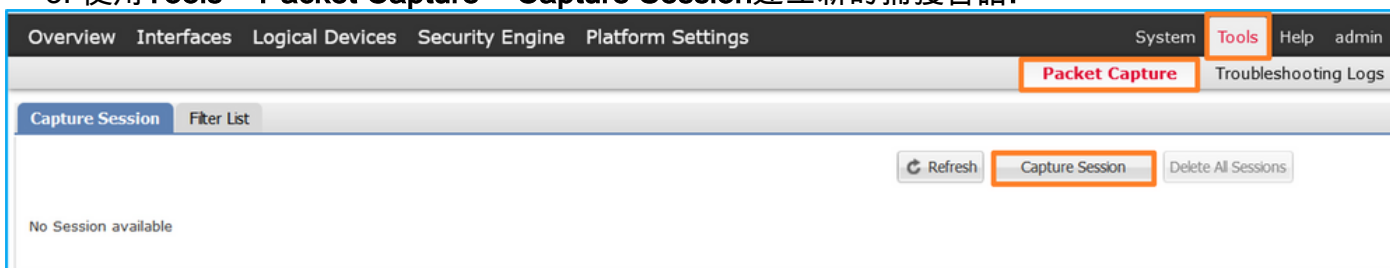
FCM

按照 FCM 上的以下步驟，為從主機 192.0.2.100 到主機 198.51.100.100 的 ICMP 回應請求資料包配置捕獲過濾器，並將其應用於介面 Ethernet1/2 上的資料包捕獲：

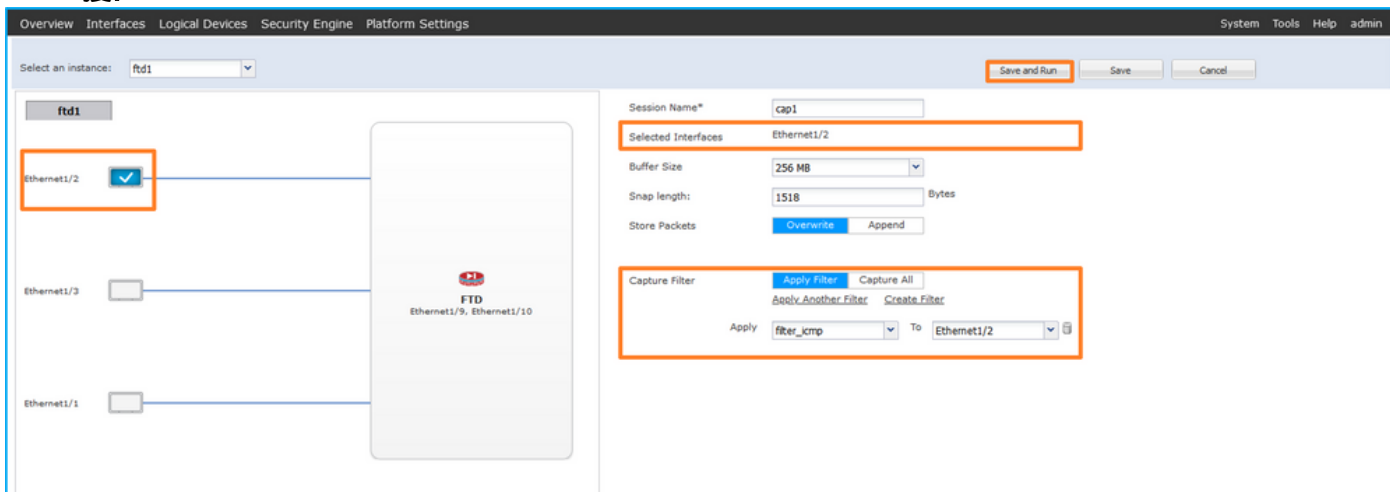
1. 使用 Tools > Packet Capture > Filter List > Add Filter 建立捕獲過濾器。
2. 指定過濾器名稱、協定、源 IPv4 和目標 IPv4，然後按一下儲存：



3. 使用Tools > Packet Capture > Capture Session建立新的捕獲會話:



4. 選擇Ethernet1/2，提供Session Name，應用捕獲過濾器，然後按一下Save and Run以啟用捕獲:



FXOS CLI

按照FXOS CLI上的以下步驟配置背板介面上的資料包捕獲：

1. 標識應用程式型別和識別符號：

```
firepower# scope ssa
firepower /ssa# show app-instance
App Name      Identifier Slot ID      Admin State Oper State      Running Version Startup Version
```

Deploy Type Turbo Mode Profile Name Cluster State Cluster Role

ftd	ftd1	1	Enabled	Online	7.2.0.82	7.2.0.82
Native	No		Not Applicable	None		

2. 在<https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>中標識IP協定編號。在這種情況下，ICMP協定編號為1。

3. 建立捕獲會話：

2.

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

驗證

FCM

確認Interface Name，確保Operational Status為up，並確認File Size（以位元組為單位）增加：

Filter Name	MAC	From			To			Protocol	Inner vlan	Outer vlan	EtherType
		IPv4	IPv6	Port	IPv4	IPv6	Port				
filter_icmp	00:00:00:00:00:00	192.0.2.100	::	0	198.51.100.100	::	0	1	0	0	0

在Tools > Packet Capture > Capture Session中驗證介面名稱、Filter，確保Operational Status為up，且File Size（以位元組為單位）增加：

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/2	filter_icmp	84340	cap1-ethernet-1-2-0.pcap	ftd1

FXOS CLI

驗證scope packet-capture中的捕獲詳細資訊：

```
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
```

收集捕獲檔案

按照**收集Firepower 4100/9300內部交換機捕獲檔案**一節中的步驟操作。

捕獲檔案分析

使用資料包捕獲檔案讀取器應用程式開啟捕獲檔案。選擇第一個資料包並檢查要點

1. 僅捕獲ICMP回應請求資料包。捕獲每個資料包並顯示2次。
2. 原始資料包報頭沒有VLAN標籤。
3. 內部交換器插入識別輸入介面Ethernet1/2的其他連線埠VLAN標籤**102**。
4. 內部交換機插入一個附加VN標籤。

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


```

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

選擇第二個資料包，並檢查要點：

1. 僅捕獲ICMP回應請求資料包。捕獲每個資料包並顯示2次。
2. 原始資料包報頭沒有VLAN標籤。
3. 內部交換器插入識別輸入介面Ethernet1/2的其他連線埠VLAN標籤102。

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


```

> Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture_u0_1, i
> Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)
  802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
  000. .... = Priority: Best Effort (default) (0)
  ...0 .. = DEI: Ineligible
  .... 0000 0110 0110 = ID: 102
  Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
  > Internet Control Message Protocol
  
```

說明

在前端介面上設定封包擷取時，交換器會同時擷取每個封包兩次：

- 插入埠VLAN標籤之後。
- 在插入VN標籤之後。

按照操作順序，VN標籤插入的時間比埠VLAN標籤插入的時間晚。但是在擷取檔案中，含有VN標籤的封包會比含有連線埠VLAN標籤的封包顯示得更早。

應用擷取過濾器時，只會擷取與輸入方向中過濾器相符的封包。

此表概述了任務：

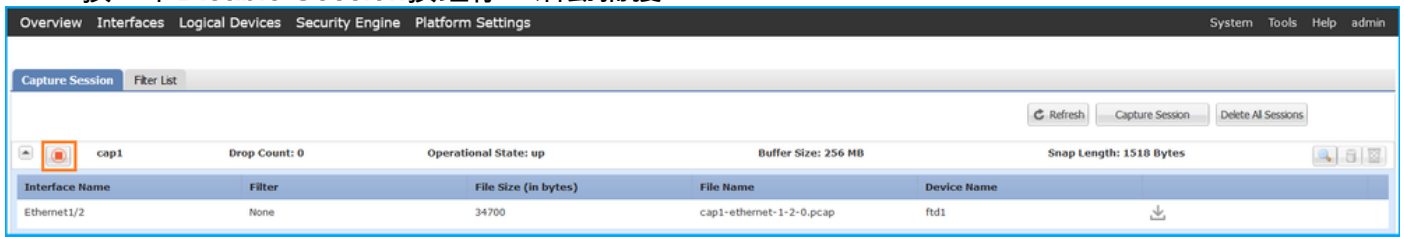
工作	捕獲點	捕獲資料包中的內部埠VLAN	方向	使用者篩選器	捕獲的流量
在前介面 Ethernet1/2上使用過濾器配置並檢驗資料包捕獲	Ethernet1/2	102	僅限輸入	通訊協定:ICMP 來源 : 192.0.2.100 目標 : 198.51.100.100	從主機192.0.2.100到主機198.51.100.100的ICMP回應

收集Firepower 4100/9300內部交換機捕獲檔案

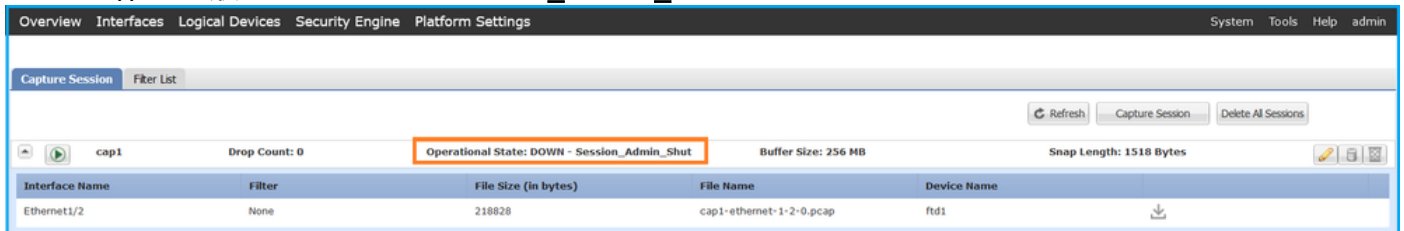
FCM

按照FCM上的以下步驟收集內部交換機捕獲檔案：

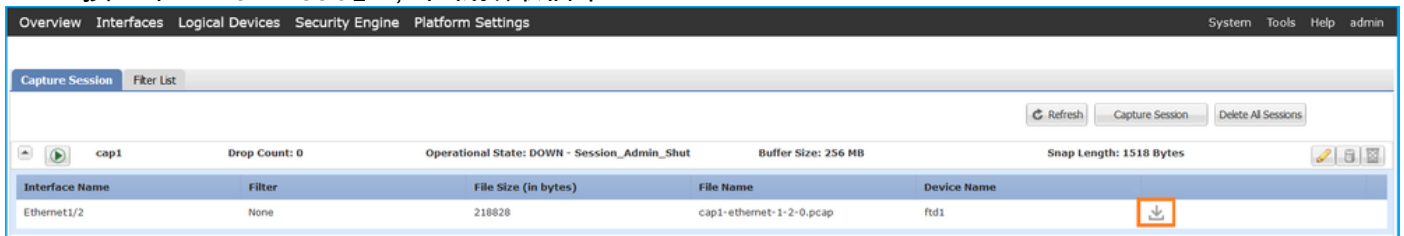
1. 按一下**Disable Session**按鈕停止活動捕獲：



2. 確保操作狀態為**DOWN - Session_Admin_Shut**:



3. 按一下「**Download**」，下載擷取檔案：



對於埠通道介面，對每個成員介面重複此步驟。

FXOS CLI

按照FXOS CLI上的以下步驟收集捕獲檔案：

1. 停止活動捕獲：

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

Traffic Monitoring Session:

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

Physical ports involved in Packet Capture:

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

2. 從local-mgmt命令範圍上傳捕獲檔案：

```
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:
```

對於埠通道介面，請為每個成員介面複製捕獲檔案。

指南、限制和最佳實踐 內部交換器 封包擷取

有關Firepower 4100/9300內部交換機捕獲的准則和限制，請參閱*Cisco Firepower 4100/9300 FXOS機箱管理器配置指南*或*Cisco Firepower 4100/9300 FXOS CLI配置指南*一章故障排除一節資料包捕獲。

以下是基於TAC案例中封包擷取使用方式的最佳實踐清單：

- 瞭解准則和限制。

- 捕獲所有埠通道成員介面上的資料包並分析所有捕獲檔案。
- 使用捕獲過濾器。
- 配置捕獲過濾器時，考慮NAT對資料包IP地址的影響。
- 增加或減少用於指定幀大小的**Snap Len**，以防其與1518位元組的預設值不同。更短的大小導致捕獲的資料包數量增加，反之亦然。
- 根據需要調整緩衝區大小。
- 請注意FCM或FXOS CLI上的**Drop Count**。一旦達到緩衝區大小限制，丟棄計數計數器就會增加。
- 在Wireshark上使用filter **!vntag**可僅顯示不帶VN標籤的資料包。這對於在前介面資料包捕獲檔案中隱藏VN標籤的資料包非常有用。
- 在Wireshark上使用filter **frame.number&1**僅顯示奇數幀。這對於隱藏背板介面資料包捕獲檔案中的重複資料包非常有用。
- 對於TCP等協定，Wireshark預設應用著色規則，以不同的顏色顯示具有特定條件的資料包。在由於捕獲檔案中的重複資料包而導致內部交換機捕獲的情況下，資料包可能會被塗色並以誤報方式標籤。如果分析資料包捕獲檔案並應用任何過濾器，則將顯示的資料包匯出到新檔案，然後開啟新檔案。

上的組態和驗證 安全防火牆3100

與Firepower 4100/9300不同，安全防火牆3100上的內部交換機捕獲通過**capture <name> switch**命令在應用程式命令列介面上配置，其中**switch**選項指定在內部交換機上配置捕獲。

以下是具有**switch**選項的**capture**命令：

```
> 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>
```

配置資料包捕獲的一般步驟如下：

1. 指定輸入介面：

交換器擷取組態接受輸入介面**nameif**。使用者可以指定資料介面名稱、內部上行鏈路或管理介面：

```
> capture capsw switch interface ?
Available interfaces to listen:
in_data_uplink1  Capture packets on internal data uplink1 interface
in_mgmt_uplink1  Capture packets on internal mgmt uplink1 interface
inside           Name of interface Ethernet1/1.205
```


management Name of interface Management1/1

2. 指定乙太網幀EtherType。預設EtherType為IP。ethernet-type選項值指定EtherType:

```
> capture caps w switch interface inside ethernet-type ?
802.1Q
<0-65535> Ethernet type
arp
ip
ip6
pppoed
pppoes
rarp
sgt
vlan
```

3. 指定匹配條件。capture match 選項指定匹配條件：

```
> capture caps w switch interface inside match ?
<0-255> Enter protocol number (0 - 255)
ah
eigrp
esp
gre
icmp
icmp6
igmp
igrp
ip
ipinip
ipsec
mac      Mac-address filter
nos
ospf
pcp
pim
pptp
sctp
snp
spi      SPI value
tcp
udp
<cr>
```

4. 指定其他可選引數，如緩衝區大小、資料包長度等。

5. 啟用捕獲。no capture <name> switch stop指令將啟用擷取:

```
> capture caps w switch interface inside match ip
>no capture caps w switch stop
```

6. 驗證捕獲詳細資訊：

- 管理狀態為**啟用**，操作狀態為**up**和**active**。
- 資料包捕獲檔案大小Pcapsize增加。
- show capture <cap_name>輸出中捕獲的資料包數量非零。
- 捕獲路徑Pcapfile。捕獲的資料包將自動儲存/mnt/disk0/packet-capture/檔案夾。
- 捕獲條件。軟體將根據捕獲條件自動建立捕獲過濾器。

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

```
>show capture capsw detail
```

```
Packet Capture info
```

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

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

```
Physical port:
```

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

```
Packet Capture Filter Info
```

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

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

```
0 packet captured on disk using switch capture
```

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

7. 必要時停止捕獲：

```
> capture capsw switch stop
```

```
>show capture capsw detail
```

```
Packet Capture info
```

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

Total Physical ports involved in Packet Capture: 1

Physical port:

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

Packet Capture Filter Info

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

Total Physical breakout ports involved in Packet Capture: 0

0 packet captured on disk using switch capture

Reading of capture file from disk is not supported

8. 收集捕獲檔案。按照收集安全防火牆3100內部交換機捕獲檔案一節中的步驟操作。

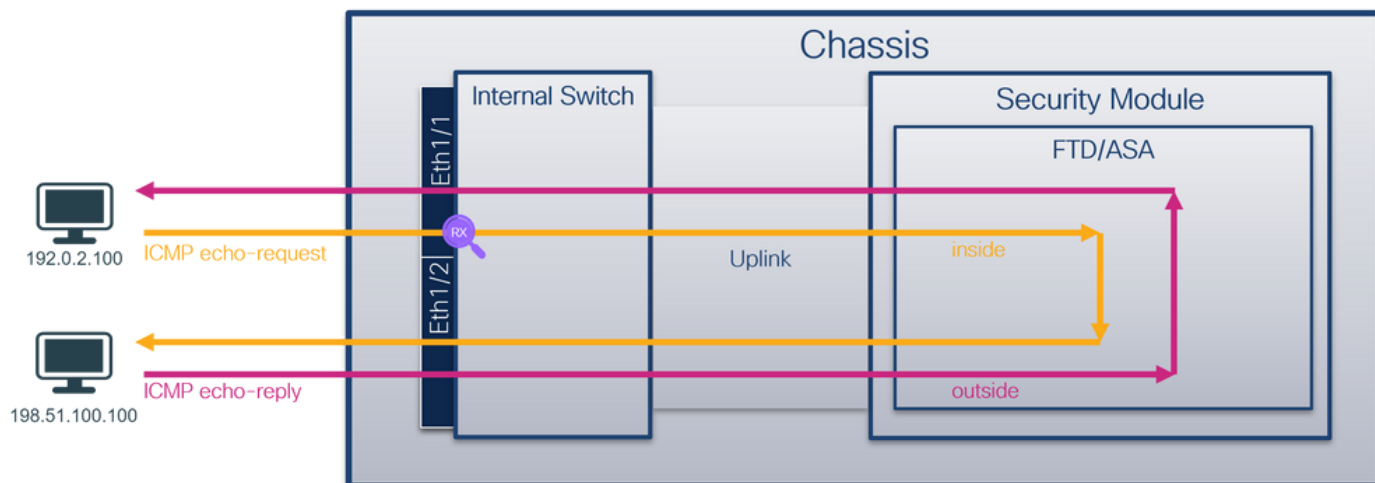
在版本7.2中，FMC或FDM不支援內部交換機捕獲配置。在ASA軟體版本9.18(1)及更高版本中，可以在ASDM版本7.18.1.x及更高版本中配置內部交換機捕獲。

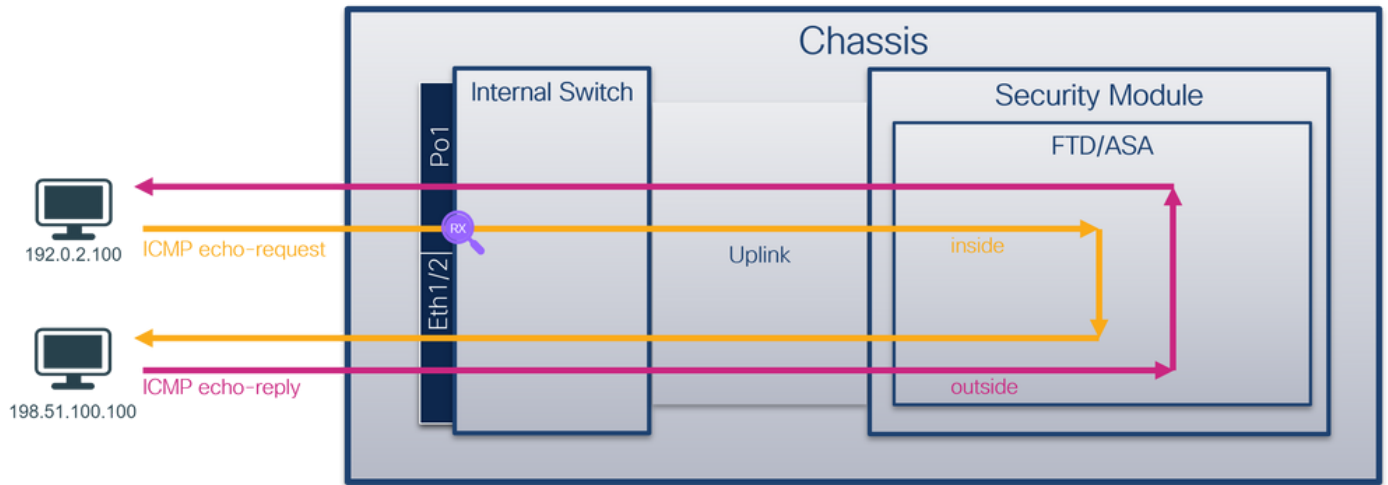
這些場景涵蓋安全防火牆3100內部交換機捕獲的常見使用案例。

物理或埠通道介面上的資料包捕獲

使用FTD或ASA CLI在介面Ethernet1/1或Portchannel1介面上配置和驗證資料包捕獲。兩個介面都具有nameif **inside**。

拓撲、資料包流和捕獲點





組態

在ASA或FTD CLI上執行以下步驟，在介面Ethernet1/1或Port-channel1上配置資料包捕獲：

1. 驗證nameif:

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

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

2. 建立捕獲會話：

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

3. 啟用捕獲會話：

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

驗證

驗證捕獲會話名稱、管理和操作狀態、介面插槽和識別符號。確保Pcapsize值（以位元組為單位）增加且捕獲的資料包數量非零：

```
> show capture capsw detail
Packet Capture info
  Name:          capsw
  Session:      1
  Admin State:  enabled
  Oper State:   up
  Oper State Reason: Active
  Config Success: yes
  Config Fail Reason:
  Append Flag:  overwrite
  Session Mem Usage: 256
```

Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0

Total Physical ports involved in Packet Capture: 1

Physical port:

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

Packet Capture Filter Info

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

Total Physical breakout ports involved in Packet Capture: 0

79 packets captured on disk using switch capture

Reading of capture file from disk is not supported

在Port-channel1的情況下，捕獲在所有成員介面上配置：

> **show capture capsw detail**

Packet Capture info

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

Total Physical ports involved in Packet Capture: 2

Physical port:

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

Packet Capture Filter Info

Name: capsw-1-4
Protocol: 0

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

Physical port:

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

Packet Capture Filter Info

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

Total Physical breakout ports involved in Packet Capture: 0

56 packet captured on disk using switch capture

Reading of capture file from disk is not supported

埠通道成員介面可以在FXOS local-mgmt命令外殼中通過show portchannel summary 命令進行驗證
:

> connect fxos

...

KSEC-FPR3100-1 connect local-mgmt

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

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

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

s - Suspended r - Module-removed

S - Switched R - Routed

U - Up (port-channel)

M - Not in use. Min-links not met

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

LACP KeepAlive Timer:

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

1 Po1 (U) False

Cluster LACP Status:

Channel ClusterSpanned ClusterDetach ClusterUnitID ClusterSysID

1 Po1 (U) False False 0 clust

要訪問ASA上的FXOS，請運行connect fxos admin 命令。在多情景的情況下，在管理情景中運行命令。

收集捕獲檔案

按照收集安全防火牆3100內部交換機捕獲檔案一節中的步驟操作。

捕獲檔案分析

使用資料包捕獲檔案讀取器應用程式開啟Ethernet1/1的捕獲檔案。選擇第一個資料包並檢查要點：

1. 僅捕獲ICMP回應請求資料包。
2. 原始資料包報頭沒有VLAN標籤。

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-07 19:50:06.925768	192.0.2.100	198.51.100.100	ICMP	102	0x9a10 (39440)	64	Echo (ping) request id=0x0034, seq=1/256, ttl=64 (no res
2	2022-08-07 19:50:07.921684	192.0.2.100	198.51.100.100	ICMP	102	0x9a3a (39482)	64	Echo (ping) request id=0x0034, seq=2/512, ttl=64 (no res
3	2022-08-07 19:50:08.924468	192.0.2.100	198.51.100.100	ICMP	102	0x9aa6 (39590)	64	Echo (ping) request id=0x0034, seq=3/768, ttl=64 (no res
4	2022-08-07 19:50:09.928484	192.0.2.100	198.51.100.100	ICMP	102	0x9afe (39678)	64	Echo (ping) request id=0x0034, seq=4/1024, ttl=64 (no re
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 re
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 re
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 re
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 re
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	0x9d6d (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

Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
 Ethernet II, Src: VMware_9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco_34:9a:14 (bc:e7:12:34:9a:14)
 Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
 Internet Control Message Protocol

開啟Portchannel1成員介面的捕獲檔案。選擇第一個封包並檢查要點：

1. 僅捕獲ICMP回應請求資料包。
2. 原始資料包報頭沒有VLAN標籤。

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-07 20:40:58.657533	192.0.2.100	198.51.100.100	ICMP	102	0x9296 (37526)	64	Echo (ping) request id=0x0035, seq=1/256, ttl=64 (no res
2	2022-08-07 20:40:59.658611	192.0.2.100	198.51.100.100	ICMP	102	0x9370 (37744)	64	Echo (ping) request id=0x0035, seq=2/512, ttl=64 (no res
3	2022-08-07 20:41:00.655662	192.0.2.100	198.51.100.100	ICMP	102	0x93f0 (37872)	64	Echo (ping) request id=0x0035, seq=3/768, ttl=64 (no res
4	2022-08-07 20:41:01.659749	192.0.2.100	198.51.100.100	ICMP	102	0x946f (37999)	64	Echo (ping) request id=0x0035, seq=4/1024, ttl=64 (no re
5	2022-08-07 20:41:02.660624	192.0.2.100	198.51.100.100	ICMP	102	0x94aa (38052)	64	Echo (ping) request id=0x0035, seq=5/1280, ttl=64 (no re
6	2022-08-07 20:41:03.663226	192.0.2.100	198.51.100.100	ICMP	102	0x952d (38189)	64	Echo (ping) request id=0x0035, seq=6/1536, ttl=64 (no re
7	2022-08-07 20:41:04.661262	192.0.2.100	198.51.100.100	ICMP	102	0x958d (38285)	64	Echo (ping) request id=0x0035, seq=7/1792, ttl=64 (no re
8	2022-08-07 20:41:05.665955	192.0.2.100	198.51.100.100	ICMP	102	0x95d8 (38360)	64	Echo (ping) request id=0x0035, seq=8/2048, ttl=64 (no re
9	2022-08-07 20:41:06.666538	192.0.2.100	198.51.100.100	ICMP	102	0x964b (38475)	64	Echo (ping) request id=0x0035, seq=9/2304, ttl=64 (no re
10	2022-08-07 20:41:07.667298	192.0.2.100	198.51.100.100	ICMP	102	0x972b (38699)	64	Echo (ping) request id=0x0035, seq=10/2560, ttl=64 (no r
11	2022-08-07 20:41:08.670540	192.0.2.100	198.51.100.100	ICMP	102	0x980a (38922)	64	Echo (ping) request id=0x0035, seq=11/2816, ttl=64 (no r
12	2022-08-07 20:41:09.668278	192.0.2.100	198.51.100.100	ICMP	102	0x9831 (38961)	64	Echo (ping) request id=0x0035, seq=12/3072, ttl=64 (no r
13	2022-08-07 20:41:10.672417	192.0.2.100	198.51.100.100	ICMP	102	0x98a2 (39074)	64	Echo (ping) request id=0x0035, seq=13/3328, ttl=64 (no r
14	2022-08-07 20:41:11.671369	192.0.2.100	198.51.100.100	ICMP	102	0x98f7 (39159)	64	Echo (ping) request id=0x0035, seq=14/3584, ttl=64 (no r
15	2022-08-07 20:41:12.675462	192.0.2.100	198.51.100.100	ICMP	102	0x99e4 (39396)	64	Echo (ping) request id=0x0035, seq=15/3840, ttl=64 (no r
16	2022-08-07 20:41:13.674993	192.0.2.100	198.51.100.100	ICMP	102	0x9a84 (39556)	64	Echo (ping) request id=0x0035, seq=16/4096, ttl=64 (no r
17	2022-08-07 20:41:14.674093	192.0.2.100	198.51.100.100	ICMP	102	0x9af3 (39667)	64	Echo (ping) request id=0x0035, seq=17/4352, ttl=64 (no r
18	2022-08-07 20:41:15.676904	192.0.2.100	198.51.100.100	ICMP	102	0x9b8e (39822)	64	Echo (ping) request id=0x0035, seq=18/4608, ttl=64 (no r

Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
 Ethernet II, Src: VMware_9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco_34:9a:2c (bc:e7:12:34:9a:2c)
 Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
 Internet Control Message Protocol

說明

交換器擷取是在介面Ethernet1/1或Portchannel1上設定的。

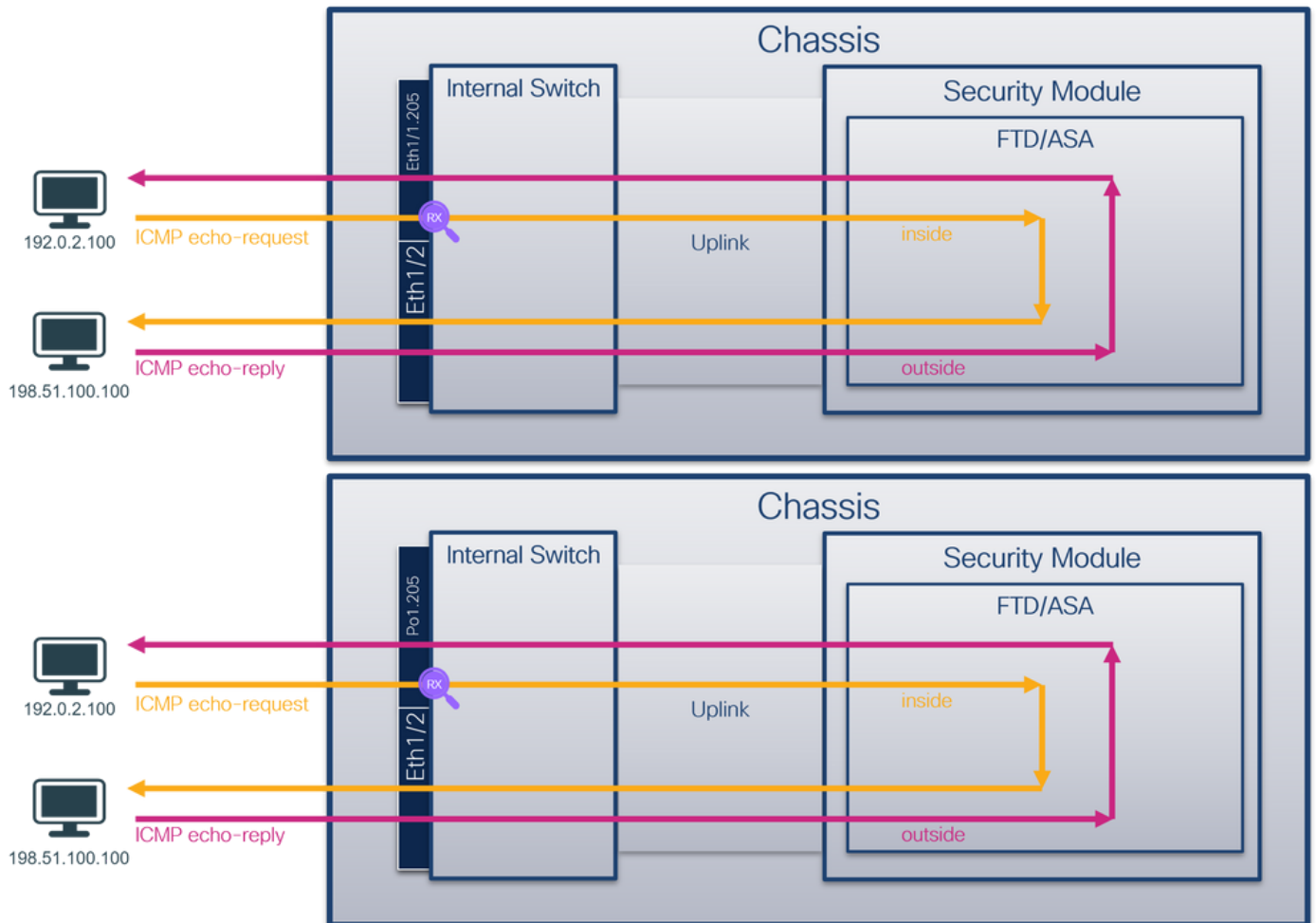
此表概述了任務：

工作	捕獲點	內部篩選器	方向	捕獲的流量
在介面Ethernet1/1上配置並檢驗資料包捕獲	Ethernet1/1	無	僅限輸入	從主機192.0.2.100到主機198.51.100.100的ICMP回應請求
在介面Portchannel1上配置並檢驗帶有成員介面Ethernet1/3和Ethernet1/4的資料包捕獲	Ethernet1/3 Ethernet1/4	無	僅限輸入	從主機192.0.2.100到主機198.51.100.100的ICMP回應請求

物理或埠通道介面的子介面上的資料包捕獲

使用FTD或ASA CLI在子介面Ethernet1/1.205或Portchannel1.205上配置和驗證資料包捕獲。兩個子介面都具有inside的nameif。

拓撲、資料包流和捕獲點



組態

在ASA或FTD CLI上執行以下步驟，在介面Ethernet1/1或Port-channel1上配置資料包捕獲：

1. 驗證nameif:

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

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

2. 建立捕獲會話：

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

3. 啟用捕獲會話：

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

驗證

驗證捕獲會話名稱、管理和操作狀態、介面插槽和識別符號。確保Pcapsize值（以位元組為單位）增加且捕獲的資料包數量非零：

```
> show capture capsw detail
```

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

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

```
Physical port:
```

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

```
Packet Capture Filter Info
```

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

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

Total Physical breakout ports involved in Packet Capture: 0

46 packets captured on disk using switch capture

Reading of capture file from disk is not supported

在此案例中，會建立一個外部VLAN Ovlan=205的篩選器，並將其套用至介面。

在Port-channel1的情況下，在所有成員介面上配置了過濾器Ovlan=205的捕獲：

> show capture capsw detail

Packet Capture info

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

Total Physical ports involved in Packet Capture: 2

Physical port:

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

Packet Capture Filter Info

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

Physical port:

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

Packet Capture Filter Info

```
Name:            capsw-1-3
```



```

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

```

Total Physical breakout ports involved in Packet Capture: 0

49 packet captured on disk using switch capture

Reading of capture file from disk is not supported

埠通道成員介面可以在FXOS local-mgmt命令外殼中通過show portchannel summary 命令進行驗證：

```
> connect fxos
```

```
...
```

```
KSEC-FPR3100-1 connect local-mgmt
```

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

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

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

```
s - Suspended   r - Module-removed
```

```
S - Switched   R - Routed
```

```
U - Up (port-channel)
```

```
M - Not in use. Min-links not met
```

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

LACP KeepAlive Timer:

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

Cluster LACP Status:

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

要訪問ASA上的FXOS，請運行connect fxos admin 命令。如果是多情景，請在管理情景中運行此命令。

收集捕獲檔案

按照收集安全防火牆3100內部交換機捕獲檔案一節中的步驟操作。

捕獲檔案分析

使用資料包捕獲檔案讀取器應用程式開啟Ethernet1/1.205的捕獲檔案。選擇第一個資料包並檢查要點：

1. 僅捕獲ICMP回應請求資料包。
2. 原始資料包報頭的VLAN標籤為205。

Wireshark capture showing ICMP Echo (ping) requests. The packet list shows 18 packets from 192.0.2.100 to 198.51.100.100. The packet details pane shows Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol. The raw packet bytes pane shows the hex and ASCII representation of the packet.

開啟Portchannel1成員介面的捕獲檔案。選擇第一個封包並檢查要點：

1. 僅捕獲ICMP回應請求資料包。
2. 原始資料包報頭的VLAN標籤為205。

Wireshark capture showing ICMP Echo (ping) requests. The packet list shows 18 packets from 192.0.2.100 to 198.51.100.100. The packet details pane shows Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol. The raw packet bytes pane shows the hex and ASCII representation of the packet.

說明

交換器擷取是在子介面Ethernet1/1.205或Portchannel1.205上設定的，且篩選條件與外部VLAN 205相符。

此表概述了任務：

工作	捕獲點	內部篩選器	方向	捕獲的流量
在子介面Ethernet1/1.205上配置並檢驗資料包捕獲	Ethernet 1/1	外部 VLAN 205	僅限輸 入	從主機192.0.2.100到主機 198.51.100.100的ICMP回應請求
在子介面Portchannel1.205 (成員介面Ethernet1/3和Ethernet1/4) 上配置並檢驗資料包捕獲	Ethernet 1/3 Ethernet 1/4	外部 VLAN 205	僅限輸 入	從主機192.0.2.100到主機 198.51.100.100的ICMP回應請求

內部介面上的資料包捕獲

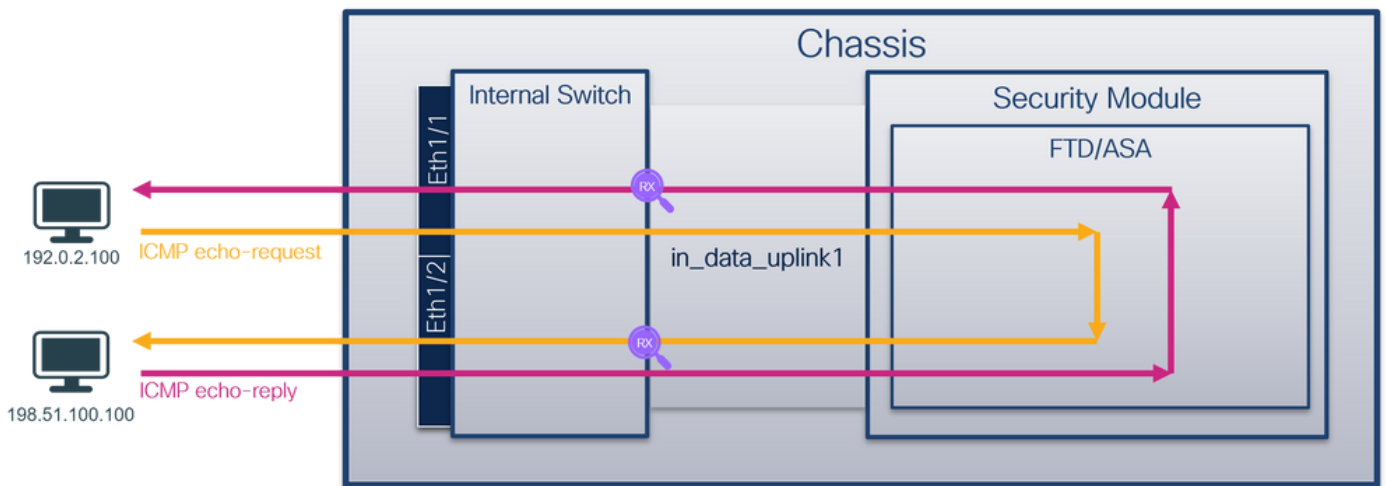
安全防火牆有2個內部介面：

- `in_data_uplink1` — 將應用程式連線到內部交換機。
- `in_mgmt_uplink1` — 為管理連線（例如到管理介面的SSH）或管理連線（也稱為FMC和FTD之間的sftunnel）提供專用資料包路徑。

任務1

使用FTD或ASA CLI在`in_data_uplink1`的上行鏈路介面上配置和驗證資料包捕獲。

拓撲、資料包流和捕獲點



組態

在ASA或FTD CLI上執行以下步驟，在`in_data_uplink1`介面上配置資料包捕獲：

1. 建立捕獲會話：

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

2. 啟用捕獲會話：

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

驗證

驗證捕獲會話名稱、管理和操作狀態、介面插槽和識別符號。確保Pcapsize值（以位元組為單位）增加且捕獲的資料包數量非零：

```
> show capture capsw detail
```

Packet Capture info

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

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

Total Physical ports involved in Packet Capture: 1

Physical port:

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

Packet Capture Filter Info

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

Total Physical breakout ports involved in Packet Capture: 0

66 packets captured on disk using switch capture

Reading of capture file from disk is not supported

在這種情況下，會在介面上使用內部ID 18建立捕獲，該內部ID是安全防火牆3130上的 in_data_uplink1 介面。FXOS local-mgmt 命令外殼中的 show portmanager switch status 命令會顯示 介面ID:

> connect fxos

...

KSEC-FPR3100-1 connect local-mgmt

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

Dev/Port	Mode	Link	Speed	Duplex	Loopback Mode	Port Manager
0/1	SGMII	Up	1G	Full	None	Link-Up
0/2	SGMII	Up	1G	Full	None	Link-Up
0/3	SGMII	Up	1G	Full	None	Link-Up
0/4	SGMII	Up	1G	Full	None	Link-Up
0/5	SGMII	Down	1G	Half	None	Mac-Link-Down
0/6	SGMII	Down	1G	Half	None	Mac-Link-Down
0/7	SGMII	Down	1G	Half	None	Mac-Link-Down
0/8	SGMII	Down	1G	Half	None	Mac-Link-Down
0/9	1000_BaseX	Down	1G	Full	None	Link-Down
0/10	1000_BaseX	Down	1G	Full	None	Link-Down
0/11	1000_BaseX	Down	1G	Full	None	Link-Down
0/12	1000_BaseX	Down	1G	Full	None	Link-Down
0/13	1000_BaseX	Down	1G	Full	None	Link-Down

0/14	1000_BaseX	Down	1G	Full	None	Link-Down
0/15	1000_BaseX	Down	1G	Full	None	Link-Down
0/16	1000_BaseX	Down	1G	Full	None	Link-Down
0/17	1000_BaseX	Up	1G	Full	None	Link-Up
0/18	KR2	Up	50G	Full	None	Link-Up
0/19	KR	Up	25G	Full	None	Link-Up
0/20	KR	Up	25G	Full	None	Link-Up
0/21	KR4	Down	40G	Full	None	Link-Down
0/22	n/a	Down	n/a	Full	N/A	Reset
0/23	n/a	Down	n/a	Full	N/A	Reset
0/24	n/a	Down	n/a	Full	N/A	Reset
0/25	1000_BaseX	Down	1G	Full	None	Link-Down
0/26	n/a	Down	n/a	Full	N/A	Reset
0/27	n/a	Down	n/a	Full	N/A	Reset
0/28	n/a	Down	n/a	Full	N/A	Reset
0/29	1000_BaseX	Down	1G	Full	None	Link-Down
0/30	n/a	Down	n/a	Full	N/A	Reset
0/31	n/a	Down	n/a	Full	N/A	Reset
0/32	n/a	Down	n/a	Full	N/A	Reset
0/33	1000_BaseX	Down	1G	Full	None	Link-Down
0/34	n/a	Down	n/a	Full	N/A	Reset
0/35	n/a	Down	n/a	Full	N/A	Reset
0/36	n/a	Down	n/a	Full	N/A	Reset

要訪問ASA上的FXOS，請運行connect fxos admin 命令。如果是多情景，請在管理情景中運行此命令。

收集捕獲檔案

按照收集安全防火牆3100內部交換機捕獲檔案一節中的步驟操作。

捕獲檔案分析

使用資料包捕獲檔案讀取器應用程式開啟in_data_uplink1介面的捕獲檔案。檢查關鍵點 — 在這種情況下，捕獲ICMP回應請求和回應應答資料包。這些是從應用程式傳送到內部交換機的資料包。

No.	Time	Source	Destination	Protocol	Length	IP ID	TTL	Info
1	2022-08-07 22:40:06.685606	192.0.2.100	198.51.100.100	ICMP	102	0x4d93 (19859)	64	Echo (ping) request id=0x003a, seq=33/8448, ttl=64 (req)
2	2022-08-07 22:40:06.685615	198.51.100.100	192.0.2.100	ICMP	102	0x6cdc (27868)	64	Echo (ping) reply id=0x003a, seq=33/8448, ttl=64 (repl)
3	2022-08-07 22:40:07.684219	192.0.2.100	198.51.100.100	ICMP	102	0x4de8 (19944)	64	Echo (ping) request id=0x003a, seq=34/8704, ttl=64 (req)
4	2022-08-07 22:40:07.689300	198.51.100.100	192.0.2.100	ICMP	102	0x6db2 (28082)	64	Echo (ping) reply id=0x003a, seq=34/8704, ttl=64 (repl)
5	2022-08-07 22:40:08.685736	192.0.2.100	198.51.100.100	ICMP	102	0x4edc (20188)	64	Echo (ping) request id=0x003a, seq=35/8960, ttl=64 (req)
6	2022-08-07 22:40:08.690806	198.51.100.100	192.0.2.100	ICMP	102	0x6dbf (28095)	64	Echo (ping) reply id=0x003a, seq=35/8960, ttl=64 (repl)
7	2022-08-07 22:40:09.690737	192.0.2.100	198.51.100.100	ICMP	102	0x4fd2 (20269)	64	Echo (ping) request id=0x003a, seq=36/9216, ttl=64 (req)
8	2022-08-07 22:40:09.690744	198.51.100.100	192.0.2.100	ICMP	102	0x6e00 (28288)	64	Echo (ping) reply id=0x003a, seq=36/9216, ttl=64 (repl)
9	2022-08-07 22:40:10.692266	192.0.2.100	198.51.100.100	ICMP	102	0x4fb1 (20401)	64	Echo (ping) request id=0x003a, seq=37/9472, ttl=64 (req)
10	2022-08-07 22:40:10.692272	198.51.100.100	192.0.2.100	ICMP	102	0x6ed5 (28373)	64	Echo (ping) reply id=0x003a, seq=37/9472, ttl=64 (repl)
11	2022-08-07 22:40:11.691159	192.0.2.100	198.51.100.100	ICMP	102	0x5008 (20488)	64	Echo (ping) request id=0x003a, seq=38/9728, ttl=64 (req)
12	2022-08-07 22:40:11.691166	198.51.100.100	192.0.2.100	ICMP	102	0x6f3b (28475)	64	Echo (ping) reply id=0x003a, seq=38/9728, ttl=64 (repl)
13	2022-08-07 22:40:12.692135	192.0.2.100	198.51.100.100	ICMP	102	0x50b8 (20664)	64	Echo (ping) request id=0x003a, seq=39/9984, ttl=64 (req)
14	2022-08-07 22:40:12.697209	198.51.100.100	192.0.2.100	ICMP	102	0x6fd7 (28631)	64	Echo (ping) reply id=0x003a, seq=39/9984, ttl=64 (repl)
15	2022-08-07 22:40:13.697320	192.0.2.100	198.51.100.100	ICMP	102	0x5184 (20868)	64	Echo (ping) request id=0x003a, seq=40/10240, ttl=64 (req)
16	2022-08-07 22:40:13.697327	198.51.100.100	192.0.2.100	ICMP	102	0x703e (28734)	64	Echo (ping) reply id=0x003a, seq=40/10240, ttl=64 (repl)
17	2022-08-07 22:40:14.698512	192.0.2.100	198.51.100.100	ICMP	102	0x51d8 (20952)	64	Echo (ping) request id=0x003a, seq=41/10496, ttl=64 (req)
18	2022-08-07 22:40:14.698518	198.51.100.100	192.0.2.100	ICMP	102	0x70dd (28893)	64	Echo (ping) reply id=0x003a, seq=41/10496, ttl=64 (repl)

> Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface in_data_uplink1 > Ethernet II, Src: Cisco_34:9a:15 (bc:e7:12:34:9a:15), Dst: VMware_9d:e7:50 (00:50:56:9d:e7:50) > Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100 > Internet Control Message Protocol		<pre> 0000 00 50 56 9d e7 50 bc e7 12 34 9a 15 08 00 45 00 .PV.P...4...E. 0010 00 54 4d 93 40 00 40 01 00 1a c0 00 02 64 c6 33 .TM:@:....d.3 0020 64 04 08 00 7f 15 00 30 00 21 39 3f f0 62 00 00 .dd...:19?b... 0030 00 00 8b 1a 05 00 00 00 00 00 10 11 12 13 14 15 . 0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 .!#\$% 0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 .&'()*+,-./012345 0060 36 37 55 55 55 55 .67UUUU </pre>
--	--	--

說明

當在上行鏈路介面上配置交換機捕獲時，僅捕獲從應用傳送到內部交換機的資料包。不會捕獲傳送到應用程式的資料包。

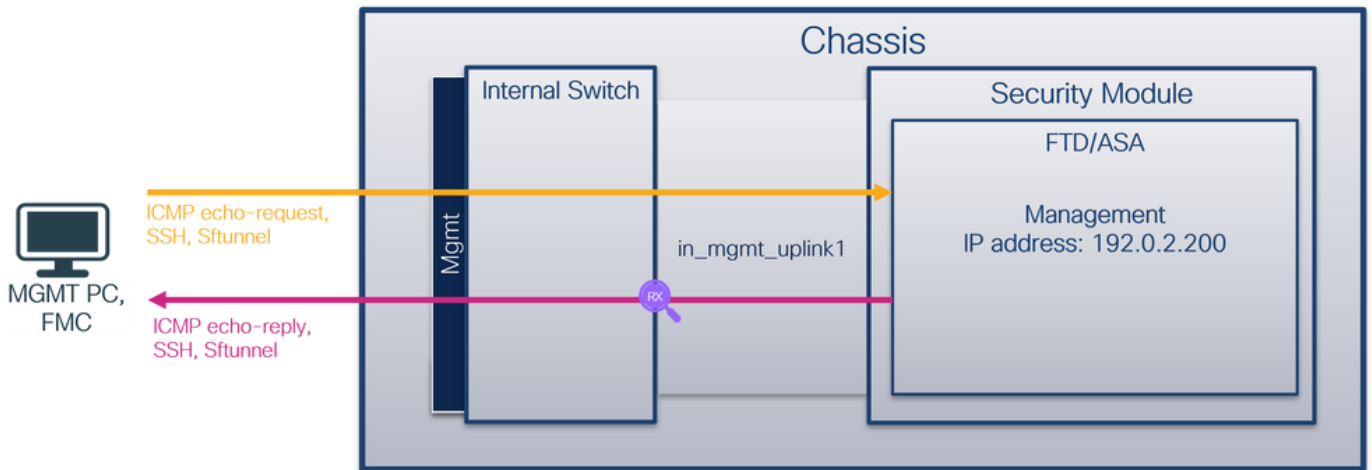
此表概述了任務：

工作	捕獲點	內部篩選器	方向	捕獲的流量
在in_data_uplink1的上行鏈路介面上配置並驗證資料包捕獲	in_data_uplink1	無	僅限輸入	從主機192.0.2.100到主機198.51.100.100的ICMP回應請求 從主機198.51.100.100到主機192.0.2.100的ICMP回應應答

任務2

使用FTD或ASA CLI在in_mgmt_uplink1的上行鏈路介面上配置和驗證資料包捕獲。僅捕獲管理平面連線的資料包。

拓撲、資料包流和捕獲點



組態

在ASA或FTD CLI上執行以下步驟，在in_mgmt_uplink1的介面上配置資料包捕獲：

1. 建立捕獲會話：

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

2. 啟用捕獲會話：

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

驗證

驗證捕獲會話名稱、管理和操作狀態、介面插槽和識別符號。確保Pcapsize值（以位元組為單位）增加且捕獲的資料包數量非零：

```
> show capture capsw detail
Packet Capture info
Name:          capsw
Session:       1
Admin State:   enabled
Oper State:    up
Oper State Reason: Active
Config Success:  yes
Config Fail Reason:
Append Flag:   overwrite
```

Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0

Total Physical ports involved in Packet Capture: 1

Physical port:

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

Packet Capture Filter Info

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

Total Physical breakout ports involved in Packet Capture: 0

281 packets captured on disk using switch capture

Reading of capture file from disk is not supported

在這種情況下，會在介面上使用內部ID 19建立擷取，該介面是安全防火牆3130上的 **in_mgmt_uplink1** 介面。FXOS local-mgmt命令外殼中的 **show portmanager switch status** 命令會顯示介面ID:

> **connect fxos**

...

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

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

Dev/Port	Mode	Link	Speed	Duplex	Loopback Mode	Port Manager
0/1	SGMII	Up	1G	Full	None	Link-Up
0/2	SGMII	Up	1G	Full	None	Link-Up
0/3	SGMII	Up	1G	Full	None	Link-Up
0/4	SGMII	Up	1G	Full	None	Link-Up
0/5	SGMII	Down	1G	Half	None	Mac-Link-Down
0/6	SGMII	Down	1G	Half	None	Mac-Link-Down
0/7	SGMII	Down	1G	Half	None	Mac-Link-Down
0/8	SGMII	Down	1G	Half	None	Mac-Link-Down
0/9	1000_BaseX	Down	1G	Full	None	Link-Down
0/10	1000_BaseX	Down	1G	Full	None	Link-Down
0/11	1000_BaseX	Down	1G	Full	None	Link-Down
0/12	1000_BaseX	Down	1G	Full	None	Link-Down
0/13	1000_BaseX	Down	1G	Full	None	Link-Down
0/14	1000_BaseX	Down	1G	Full	None	Link-Down
0/15	1000_BaseX	Down	1G	Full	None	Link-Down
0/16	1000_BaseX	Down	1G	Full	None	Link-Down
0/17	1000_BaseX	Up	1G	Full	None	Link-Up
0/18	KR2	Up	50G	Full	None	Link-Up

0/19	KR	Up	25G	Full	None	Link-Up
0/20	KR	Up	25G	Full	None	Link-Up
0/21	KR4	Down	40G	Full	None	Link-Down
0/22	n/a	Down	n/a	Full	N/A	Reset
0/23	n/a	Down	n/a	Full	N/A	Reset
0/24	n/a	Down	n/a	Full	N/A	Reset
0/25	1000_BaseX	Down	1G	Full	None	Link-Down
0/26	n/a	Down	n/a	Full	N/A	Reset
0/27	n/a	Down	n/a	Full	N/A	Reset
0/28	n/a	Down	n/a	Full	N/A	Reset
0/29	1000_BaseX	Down	1G	Full	None	Link-Down
0/30	n/a	Down	n/a	Full	N/A	Reset
0/31	n/a	Down	n/a	Full	N/A	Reset
0/32	n/a	Down	n/a	Full	N/A	Reset
0/33	1000_BaseX	Down	1G	Full	None	Link-Down
0/34	n/a	Down	n/a	Full	N/A	Reset
0/35	n/a	Down	n/a	Full	N/A	Reset
0/36	n/a	Down	n/a	Full	N/A	Reset

要訪問ASA上的FXOS，請運行connect fxos admin 命令。如果是多情景，請在管理情景中運行此命令。

收集捕獲檔案

請按照收集安全防火牆3100內部交換機捕獲檔案一節中的步驟操作。

捕獲檔案分析

使用資料包捕獲檔案讀取器應用程式開啟介面in_mgmt_uplink1的捕獲檔案。檢查關鍵點 — 在這種情況下，僅顯示來自管理IP地址192.0.2.200的資料包。例如SSH、Sftunnel或ICMP回應應答資料包。這些資料包是通過內部交換機從應用程式管理介面傳送到網路的。

The screenshot displays a network traffic capture tool interface. The top section shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, IP ID, and IP TTL. A red box highlights the Source and Destination columns, showing that all packets in the list originate from 192.0.2.200 and are destined for 192.0.2.101. The bottom section shows a detailed view of a selected packet (Frame 1: 747 bytes on wire), including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (TCP) details. The packet is identified as an Echo (ping) reply from 192.0.2.200 to 192.0.2.101.

說明

當在管理上行鏈路介面上配置交換機捕獲時，僅捕獲從應用管理介面傳送的輸入資料包。目的地為

應用程式管理介面的資料包不會被捕獲。

此表概述了任務：

工作	捕獲點	內部篩選器	方向	捕獲的流量
在管理上行鏈路介面上配置並驗證資料包捕獲	in_mgmt_uplink1	無	僅限輸入 (從管理介面通過內部交換機連線到網路)	從FTD管理IP位址192.0.2.200到主機192.0.2.100的ICMP回應應答 從FTD管理IP地址192.0.2.200到FMC IP地址192.0.2.101的SFTUNNEL 從FTD管理IP地址192.0.2.200到主機192.0.2.100的SSH

封包擷取過濾器

內部交換器封包擷取過濾器的設定方式與資料平面擷取相同。使用**ethernet-type**和**match**選項配置過濾器。

組態

在ASA或FTD CLI上執行以下步驟，使用與來自主機198.51.100.100的Ethernet1/1上的ARP幀或ICMP資料包匹配的過濾器配置資料包捕獲：

1. 驗證nameif:

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

2. 為ARP或ICMP建立捕獲會話：

```
> capture capsw switch interface inside ethernet-type arp
> capture capsw switch interface inside match icmp 198.51.100.100
```

驗證

驗證捕獲會話名稱和過濾器。Ethertype值為十進位制的**2054**，十六進位制的**0x0806**:

```
> 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: caps-1-1

Packet Capture Filter Info

Name: caps-1-1
Protocol: 0
Ivlan: 0
Ovlan: 0
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 2054

Total Physical breakout ports involved in Packet Capture: 0

0 packet captured on disk using switch capture

Reading of capture file from disk is not supported

這是對ICMP過濾器的驗證。IP通訊協定1是ICMP:

> **show capture caps detail**

Packet Capture info

Name: caps
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: caps-1-1

Packet Capture Filter Info

Name: caps-1-1
Protocol: 1
Ivlan: 0
Ovlan: 0
Src Ip: 198.51.100.100


```
Dest Ip:          0.0.0.0
Src Ipv6:         ::
Dest Ipv6:        ::
Src MAC:          00:00:00:00:00:00
Dest MAC:         00:00:00:00:00:00
Src Port:         0
Dest Port:        0
Ethertype:        0
```

Total Physical breakout ports involved in Packet Capture: 0

0 packets captured on disk using switch capture

Reading of capture file from disk is not supported

收集Secure Firewall 3100內部交換機捕獲檔案

使用ASA或FTD CLI收集內部交換機捕獲檔案。在FTD上，也可透過CLI `copy`指令將擷取檔案匯出到透過資料或診斷介面可達的目標。

或者，您也可以專家模式下將檔案複製到`/ngfw/var/common`，然後通過File Download選項從FMC下載。

對於埠通道介面，請確保從所有成員介面收集資料包捕獲檔案。

ASA

按照以下步驟在ASA CLI上收集內部交換機捕獲檔案：

1. 停止捕獲：

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

2. 驗證捕獲會話是否已停止，並記下捕獲檔名。

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

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

Total Physical ports involved in Packet Capture: 1

Physical port:

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

Packet Capture Filter Info

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

Total Physical breakout ports involved in Packet Capture: 0

886 packets captured on disk using switch capture

Reading of capture file from disk is not supported

3. 使用CLI **copy**命令將檔案匯出到遠端目標：

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

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

FTD

請依照以下步驟操作，收集FTD CLI上的內部交換器擷取檔案，並將其複製到透過資料或診斷介面連線的伺服器：

1. 前往診斷CLI:

```
> 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. 停止捕獲：

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

3. 驗證擷取作業階段是否已停止，並記下擷取檔案名稱：

```
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:             caps-1-1
```

```
Packet Capture Filter Info
```

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

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

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

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

4. 使用CLI copy命令將檔案匯出到遠端目標。

```
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
```

按照以下步驟，通過File Download選項從FMC收集捕獲文件：

1. 停止捕獲：

```
> capture capsw switch stop
```

2. 驗證捕獲會話是否已停止，並記下檔名和完整的捕獲檔案路徑：

```
> show capture capsw detail
```

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

Total Physical ports involved in Packet Capture: 1

Physical port:

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

Packet Capture Filter Info

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

Total Physical breakout ports involved in Packet Capture: 0

886 packets captured on disk using switch capture
Reading of capture file from disk is not supported

3. 前往專家模式並切換到根模式：

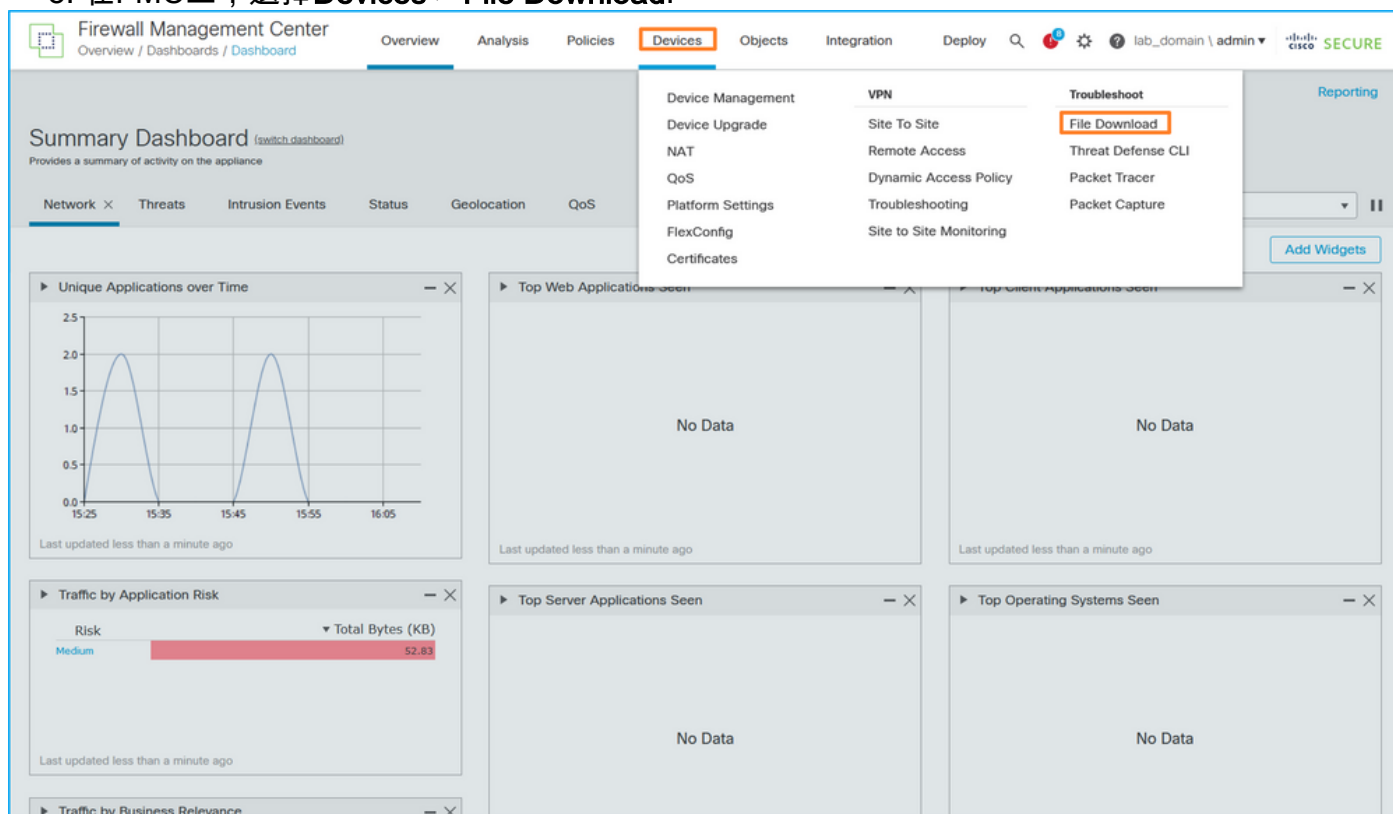
```
> expert
```

```
admin@firepower:~$ sudo su
root@firepower:/home/admin
```

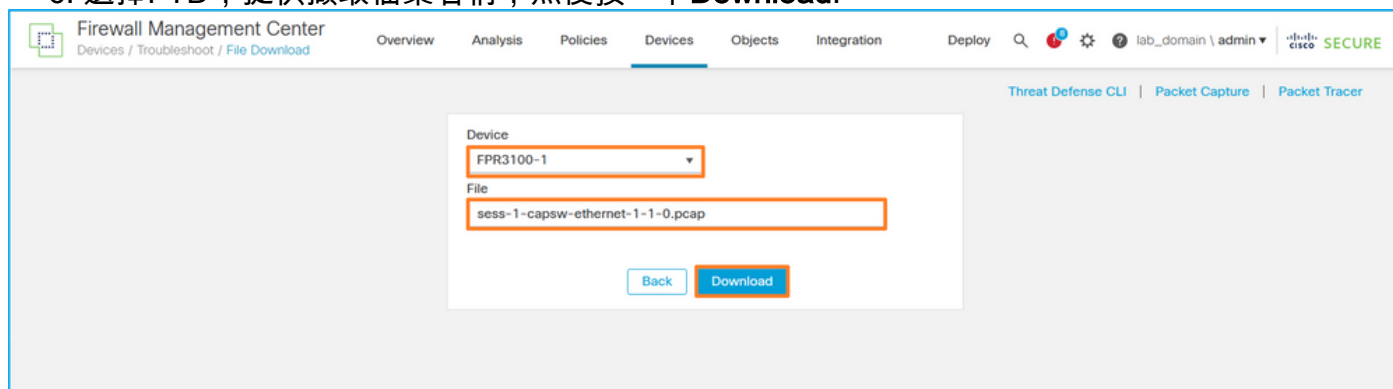
4. 將捕獲檔案複製到/ngfw/var/common/:

```
root@KSEC-FPR3100-1:/home/admin cp /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
/ngfw/var/common/
root@KSEC-FPR3100-1:/home/admin ls -l /ngfw/var/common/sess*
-rwxr-xr-x 1 root admin 139826 Aug  7 20:14 /ngfw/var/common/sess-1-capsw-ethernet-1-1-0.pcap
-rwxr-xr-x 1 root admin    24 Aug  6 21:58 /ngfw/var/common/sess-1-capsw-ethernet-1-3-0.pcap
```

5. 在FMC上，選擇Devices > File Download:



6. 選擇FTD，提供擷取檔案名稱，然後按一下Download:



內部交換器封包擷取准則、限制和最佳實踐

准則和限制：

- 支援多個交換機捕獲配置會話，但一次只能有一個交換機捕獲會話處於活動狀態。嘗試啟用2個或更多捕獲會話會導致錯誤「ERROR:無法啟用會話，因為已達到最大1個活動資料包捕獲會話的限制」。
- 無法刪除活動的交換機捕獲。
- 無法在應用程式上讀取交換機捕獲。使用者必須匯出檔案。
- 某些資料平面捕獲選項(如轉儲、解碼、資料包編號、跟蹤等)不支援交換機捕獲。

- 在多情景ASA中，資料介面上的交換機捕獲是在使用者情景中配置的。交換機在in_data_uplink1介面上捕獲，僅在管理上下文中支援in_mgmt_uplink1。

以下是基於TAC案例中封包擷取使用方式的最佳實踐清單：

- 瞭解准則和限制。
- 使用捕獲過濾器。
- 配置捕獲過濾器時，考慮NAT對資料包IP地址的影響。
- 增加或減少指定幀大小的packet-length，以防其與預設值1518位元組不同。更短的大小導致捕獲的資料包數量增加，反之亦然。
- 根據需要調整緩衝大小。
- 請注意show cap <cap_name> detail命令輸出中的Drop Count。一旦達到緩衝區大小限制，丟棄計數計數器就會增加。

相關資訊

- [Firepower 4100/9300機箱管理器和FXOS CLI配置指南](#)
- [Cisco Secure Firewall 3100入門指南](#)
- [Cisco Firepower 4100/9300 FXOS命令參考](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。