

配置和验证安全防火墙和Firepower内部交换机捕获

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[系统架构高级概述](#)

[内部交换机操作高级概述](#)

[数据包流和捕获点](#)

[Firepower 4100/9300的配置与验证](#)

[物理或端口通道接口上的数据包捕获](#)

[背板接口上的数据包捕获](#)

[应用和应用端口上的数据包捕获](#)

[物理或端口通道接口的子接口上的数据包捕获](#)

[数据包捕获过滤器](#)

[收集Firepower 4100/9300内部交换机捕获文件](#)

[内部交换机数据包捕获指南、限制和最佳实践](#)

[安全防火墙3100的配置与验证](#)

[物理或端口通道接口上的数据包捕获](#)

[物理或端口通道接口的子接口上的数据包捕获](#)

[内部接口上的数据包捕获](#)

[数据包捕获过滤器](#)

[收集安全防火墙3100内部交换机捕获文件](#)

[内部交换机数据包捕获指南、限制和最佳实践](#)

[相关信息](#)

简介

本文档介绍Firepower的配置和验证，以及安全防火墙内部交换机捕获。

先决条件

要求

产品基础知识、捕获分析。

使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

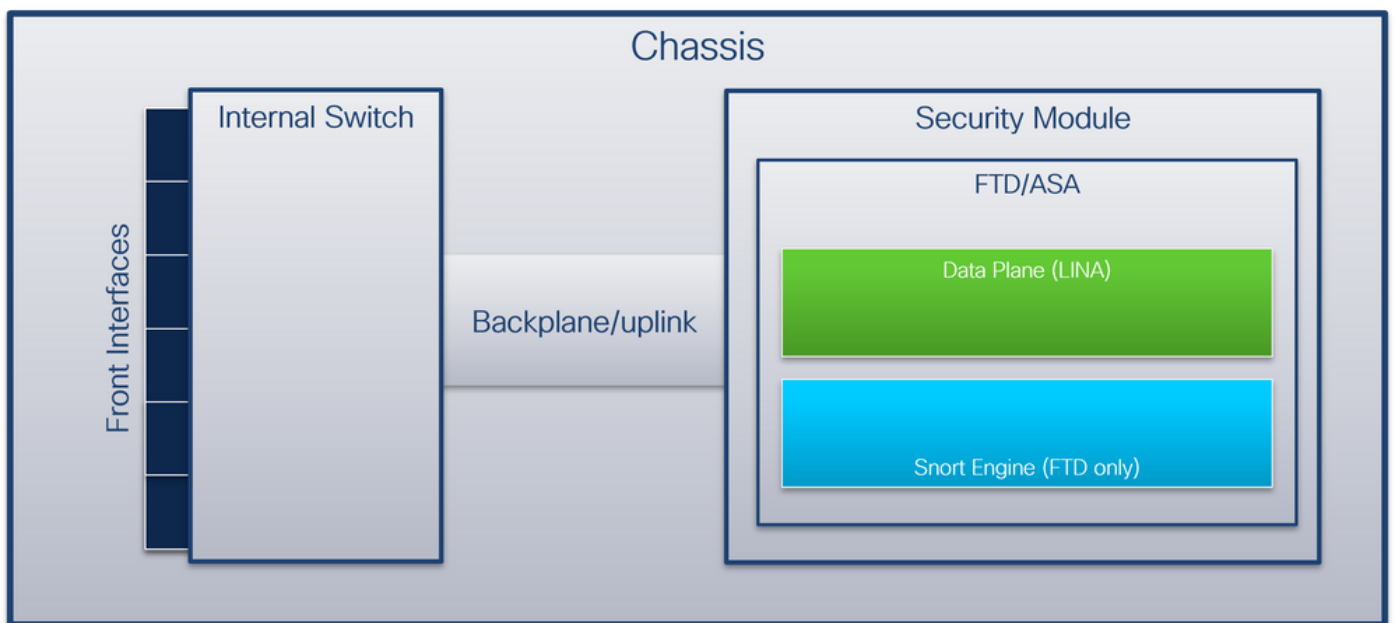
本文档中的信息基于以下软件和硬件版本：

- 安全防火墙31xx
- Firepower 41xx
- Firepower 93xx
- 思科安全可扩展操作系统(FXOS)2.12.0.x
- 思科安全防火墙威胁防御(FTD)7.2.0.x
- 思科安全防火墙管理中心(FMC)7.2.0.x
- 思科安全防火墙设备管理器(FDM)7.2.0.x
- 自适应安全设备(ASA)9.18(1)x
- 自适应安全设备设备管理器(ASDM)7.18.1.x
- Wireshark 3.6.7(<https://www.wireshark.org/download.html>)

背景信息

系统架构高级概述

从数据包流的角度，Firepower 4100/9300和安全防火墙3100的架构可视化，如下图所示：



机箱包括以下组件：

- **内部交换机** — 将数据包从网络转发到应用，反之亦然。内部交换机连接到位于内置接口模块或外部网络模块上的**前端接口**，并连接到外部设备，例如交换机。例如，Ethernet 1/1、Ethernet 2/4等等。“前线”不是一个严格的技术定义。在本文档中，它用于将连接到外部设备的接口与背板或上行链路接口区分开来。
- **背板或上行链路** — 将安全模块(SM)连接到内部交换机的内部接口。下表显示了Firepower 4100/9300上的背板接口和安全防火墙3100上的上行链路接口：

Platform	支持的安全模块数量	背板/上行链路接口	映射的应用接口
		SM1:	Internal-Data0/0

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

如果每个模块有2个背板接口，则内部交换机和模块上的应用在2个接口上执行流量负载均衡。

- **安全模块、安全引擎或刀片** — 安装FTD或ASA等应用的模块。Firepower 9300支持多达3个安全模块。
- **映射应用接口** — 应用（例如FTD或ASA）将背板或上行链路接口映射到内部接口。换句话说，背板或上行链路接口在应用中作为内部接口可见。

使用**show interface detail**命令验证内部接口：

```
> 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
```

内部交换机操作高级概述

Firepower 4100/9300

要做出转发决策，内部交换机使用**接口VLAN标记**或**端口VLAN标记**以及虚拟网络标记(VN-tag)。

内部交换机使用端口VLAN标记来标识接口。交换机将端口VLAN标记插入前接口上的每个入口数据包。VLAN标记由系统自动配置，不能手动更改。可以在fxos命令外壳中检查标记值：

```
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标记也由内部交换机插入，用于将数据包转发到应用。它由系统自动配置，不能手动更改。

端口VLAN标记和VN标记与应用共享。应用程序将各个出口接口VLAN标记和VN标记插入到每个数据包中。当背板接口上的内部交换机收到来自应用的数据包时，交换机读取出口接口VLAN标记和VN标记，识别应用和出口接口，剥离端口VLAN标记和VN标记，并将数据包转发到网络。

安全防火墙3100

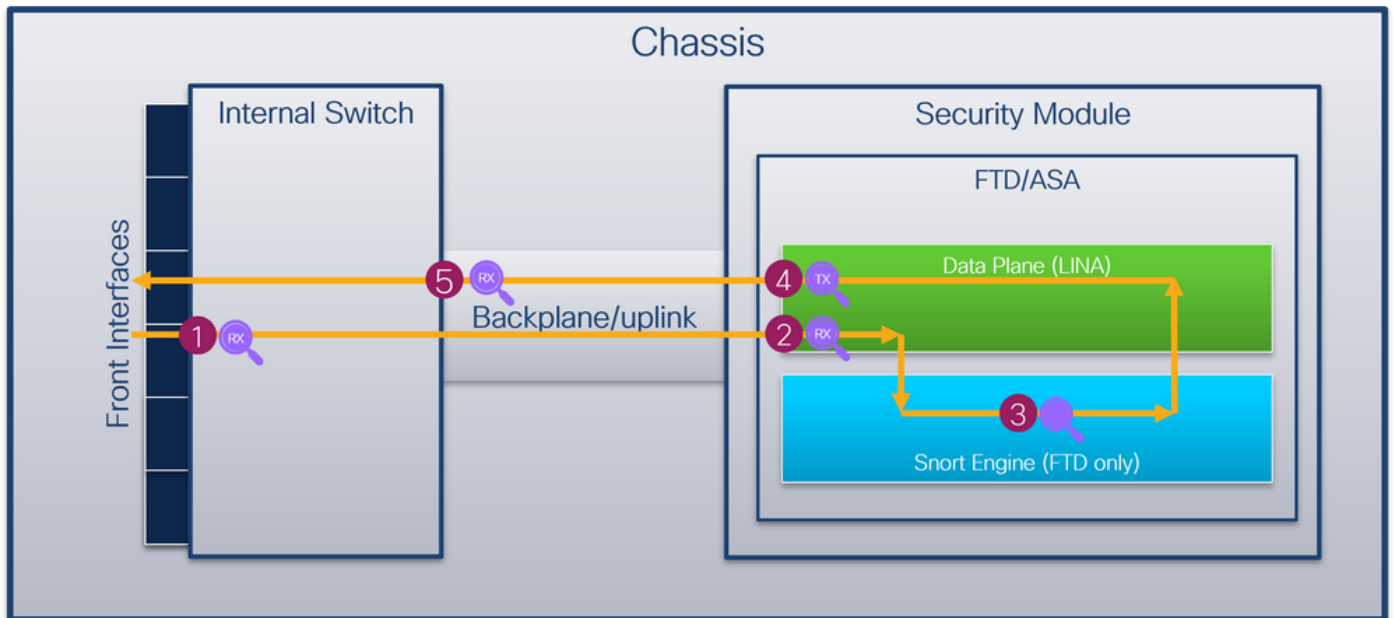
与Firepower 4100/9300类似，内部交换机使用端口VLAN标记来标识接口。

端口VLAN标记与应用共享。应用程序将各个出口接口VLAN标记插入到每个数据包中。当上行链路接口上的内部交换机收到来自应用的数据包时，交换机读取出口接口VLAN标记，识别出口接口，剥离端口VLAN标记，并将数据包转发到网络。

数据包流和捕获点

Firepower 4100/9300和安全防火墙3100防火墙支持内部交换机接口上的数据包捕获。

此图显示了机箱和应用程序内沿数据包路径的数据包捕获点：



捕获点包括：

1. 内部交换机前接口入口捕获点。前接口是连接到对等设备（例如交换机）的任何接口。
2. 数据平面接口入口捕获点
3. Snort捕获点
4. 数据平面接口出口捕获点
5. 内部交换机背板或上行链路入口捕获点。背板或上行链路接口将内部交换机连接到应用。

内部交换机仅支持入口接口捕获。也就是说，只能捕获从网络或ASA/FTD应用接收的数据包。不支持出口数据包捕获。

配置和验证 Firepower 4100/9300

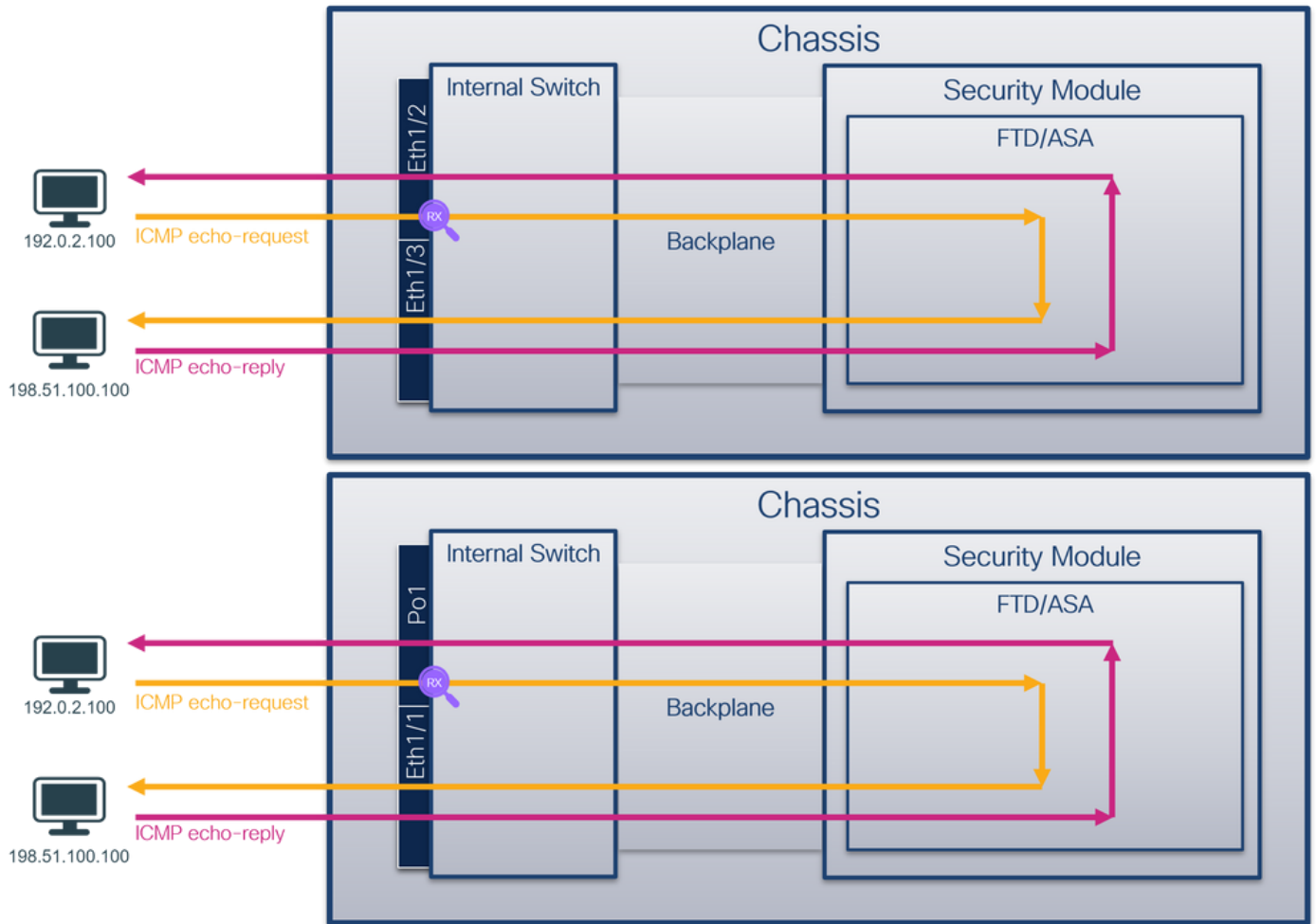
Firepower 4100/9300内部交换机捕获可以在FCM上的Tools > Packet Capture中配置，或在FXOS CLI中的scope packet-capture中配置。有关数据包捕获选项的说明，请参阅Cisco Firepower 4100/9300 FXOS机箱管理器配置指南或Cisco Firepower 4100/9300 FXOS CLI配置指南一章故障排除,数据包捕获一节。

这些场景包括Firepower 4100/9300内部交换机捕获的常见使用案例。

物理或端口通道接口上的数据包捕获

使用FCM和CLI在接口Ethernet1/2或Portchannel1接口上配置和验证数据包捕获。如果是端口通道接口，请确保选择所有物理成员接口。

拓扑、数据包流和捕获点

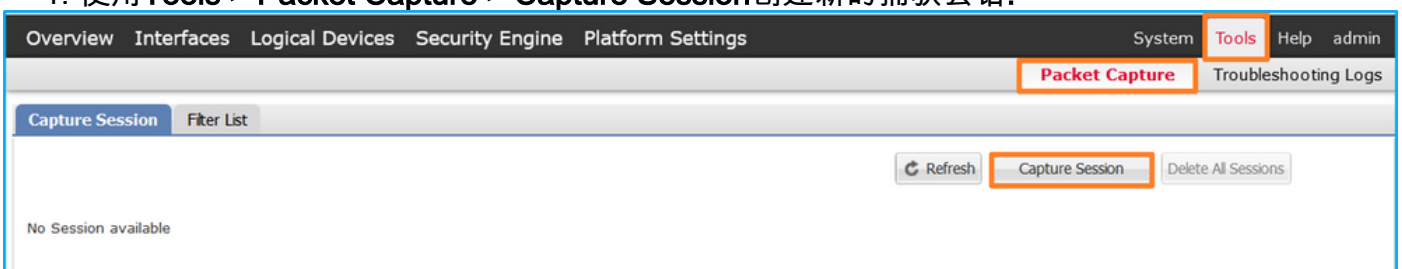


配置

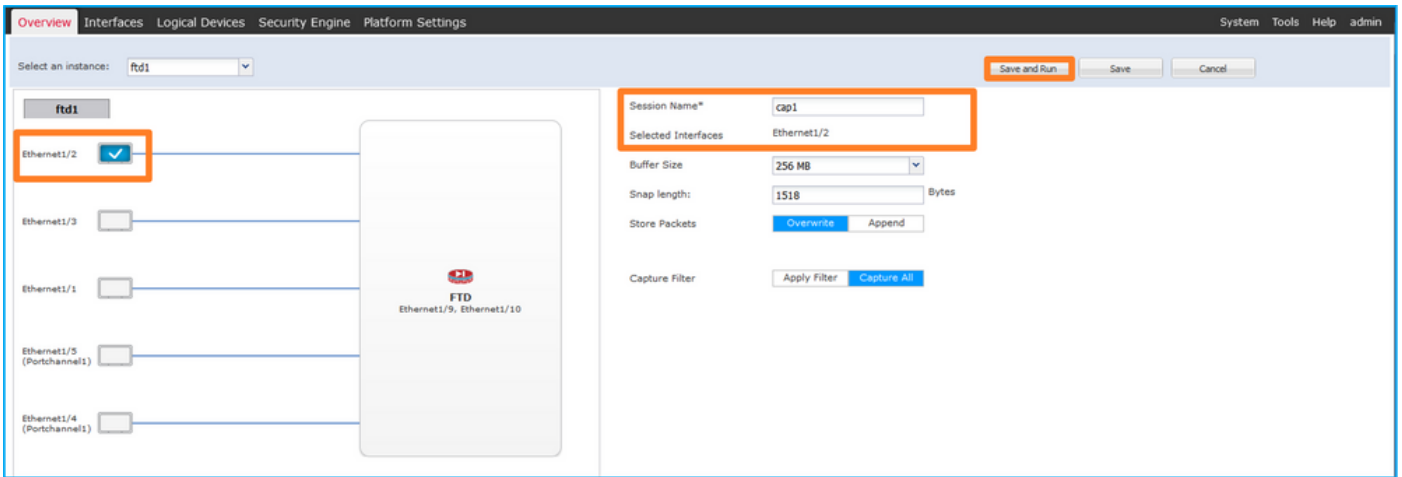
FCM

按照FCM上的以下步骤在接口Ethernet1/2或Portchannel1上配置数据包捕获：

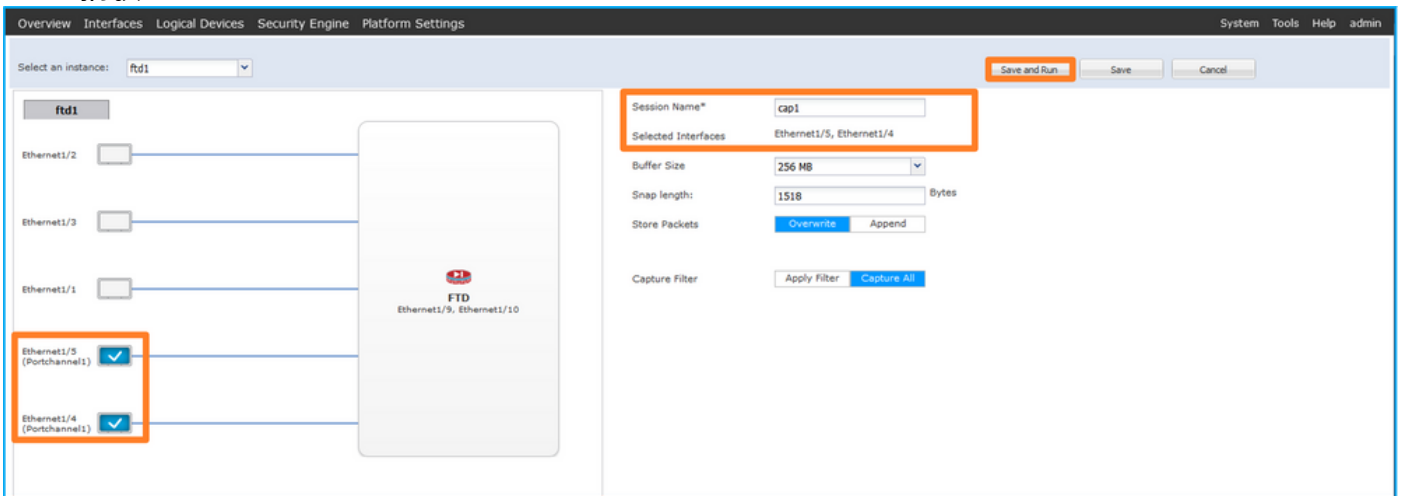
1. 使用Tools > Packet Capture > Capture Session创建新的捕获会话:



2. 选择接口Ethernet1/2，提供会话名称，然后单击保存并运行以激活捕获：



3. 如果是端口通道接口，请选择所有物理成员接口，提供会话名称，然后单击保存并运行以激活捕获：



FXOS CLI

在FXOS CLI上执行以下步骤，在接口Ethernet1/2或Portchannel1上配置数据包捕获：

1. 标识应用类型和标识符：

```
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. 对于端口通道接口，请标识其成员接口：

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

```

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

```

3. 创建捕获会话：

```

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 #

```

对于端口通道接口，为每个成员接口配置单独的捕获：

```

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 #

```

确认

FCM

验证Interface Name，确保Operational Status为up且File Size（以字节为单位）增加：

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

具有成员接口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

在scope packet-capture中验证捕获详细信息：


```
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具有成员接口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

收集捕获文件

按照收集Firepower 4100/9300内部交换机捕获文件部分中的步骤进行操作。

捕获文件分析

使用数据包捕获文件读取器应用程序打开Ethernet1/2的捕获文件。选择第一个数据包并检查要点：

1. 仅捕获ICMP回应请求数据包。捕获每个数据包并显示2次。
2. 原始数据包报头没有VLAN标记。
3. 内部交换机插入标识入口接口Ethernet1/2的额外端口VLAN标记102。
4. 内部交换机插入一个额外的VN标记。

The screenshot displays a network capture analysis tool interface. The top section shows a list of captured packets, with the first packet selected. The packet details are as follows:

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!)

The detailed view of the first packet shows the following headers:

- VN-Tag:** Direction: From Bridge; Pointer: vif_id; Destination: 10; Looped: No; Reserved: 0; Version: 0; Source: 0. Type: 802.1Q Virtual LAN (0x8100).
- 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102**
- Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100**
- Internet Control Message Protocol**

The packet data section shows the raw bytes of the ICMP Echo request.

选择第二个数据包并检查要点：

1. 仅捕获ICMP回应请求数据包。捕获每个数据包并显示2次。
2. 原始数据包报头没有VLAN标记。
3. 内部交换机插入标识入口接口Ethernet1/2的额外端口VLAN标记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 06:23:58.285088858	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!)

```

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 0100 = ID: 102
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
Internet Control Message Protocol
    
```

打开Portchannel1成员接口的捕获文件。选择第一个数据包并检查要点：

1. 仅捕获ICMP回应请求数据包。捕获每个数据包并显示2次。
2. 原始数据包报头没有VLAN标记。
3. 内部交换机插入标识入口接口Portchannel1的附加端口VLAN标记1001。
4. 内部交换机插入一个额外的VN标记。

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info
1	2022-08-05 23:07:31.865872877	192.0.2.100	198.51.100.100	ICMP	108	0x322e (12846)	64 Echo (ping) request id=0x002d, seq=245/62720, ttl=64 (nc)
2	2022-08-05 23:07:31.865875131	192.0.2.100	198.51.100.100	ICMP	102	0x322e (12846)	64 Echo (ping) request id=0x002d, seq=245/62720, ttl=64 (nc)
3	2022-08-05 23:07:32.867144598	192.0.2.100	198.51.100.100	ICMP	108	0x32b9 (12985)	64 Echo (ping) request id=0x002d, seq=246/62976, ttl=64 (nc)

```

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)
VLAN-Tag
  1. .... .. = Direction: From Bridge
  .0.. .... .. = Pointer: vif_id
  ..00 0000 0101 0100 .. .. = Destination: 84
  .. ... .. = 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: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
Internet Control Message Protocol
    
```

选择第二个数据包并检查要点：

1. 仅捕获ICMP回应请求数据包。捕获每个数据包并显示2次。
2. 原始数据包报头没有VLAN标记。
3. 内部交换机插入标识入口接口Portchannel1的附加端口VLAN标记1001。

说明

在前接口上配置数据包捕获后，交换机将同时捕获每个数据包两次：

- 插入端口VLAN标记之后。
- 在插入VN标记之后。

按照操作顺序，VN标记插入的时间晚于端口VLAN标记插入的时间。但是，在捕获文件中，带VN标记的数据包会比带端口VLAN标记的数据包更早显示。

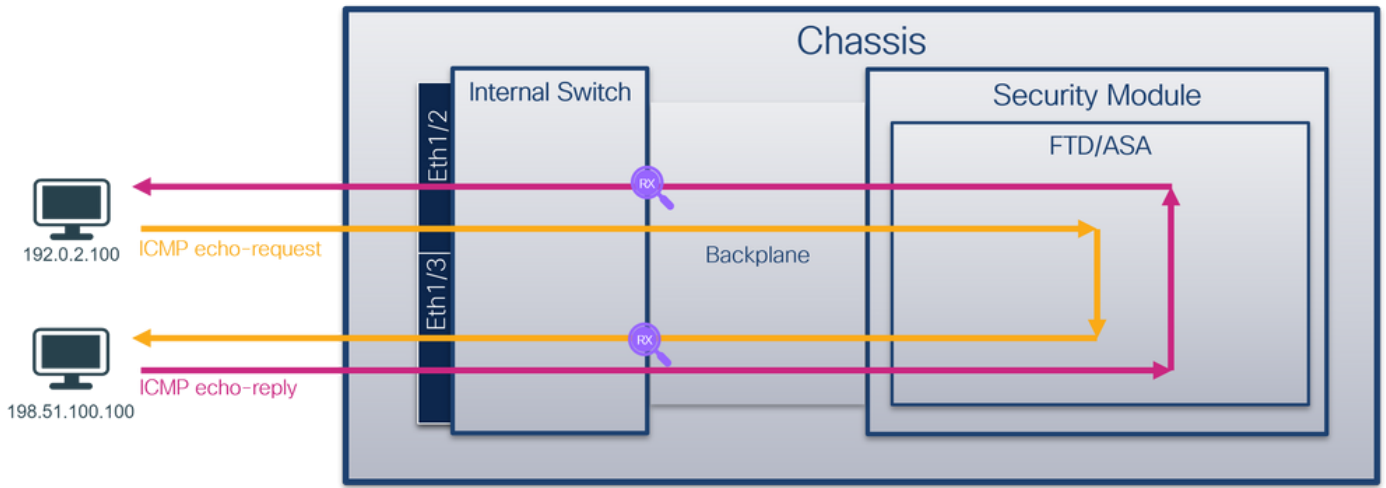
此表概述了任务：

任务	捕获点	捕获数据包中的内部端口VLAN	方向	捕获的流量
配置并检验以太网接口1/2上的数据包捕获	以太网1/2	102	仅限入口	从主机192.0.2.100到主机198.51.100.100的ICMP回应请求
在接口Portchannel1上配置并检验带有成员接口Ethernet1/4和Ethernet1/5的数据包捕获	Ethernet1/4 Ethernet1/5	1001	仅限入口	从主机192.0.2.100到主机198.51.100.100的ICMP回应请求

背板接口上的数据包捕获

使用FCM和CLI配置和验证背板接口上的数据包捕获。

拓扑、数据包流和捕获点

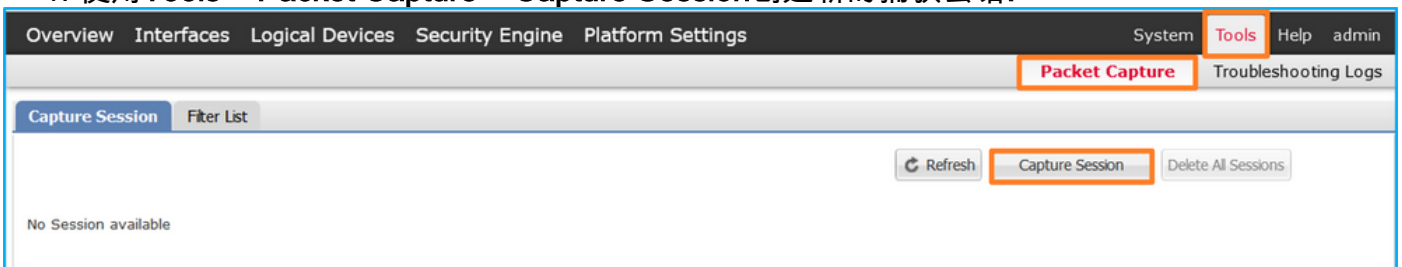


配置

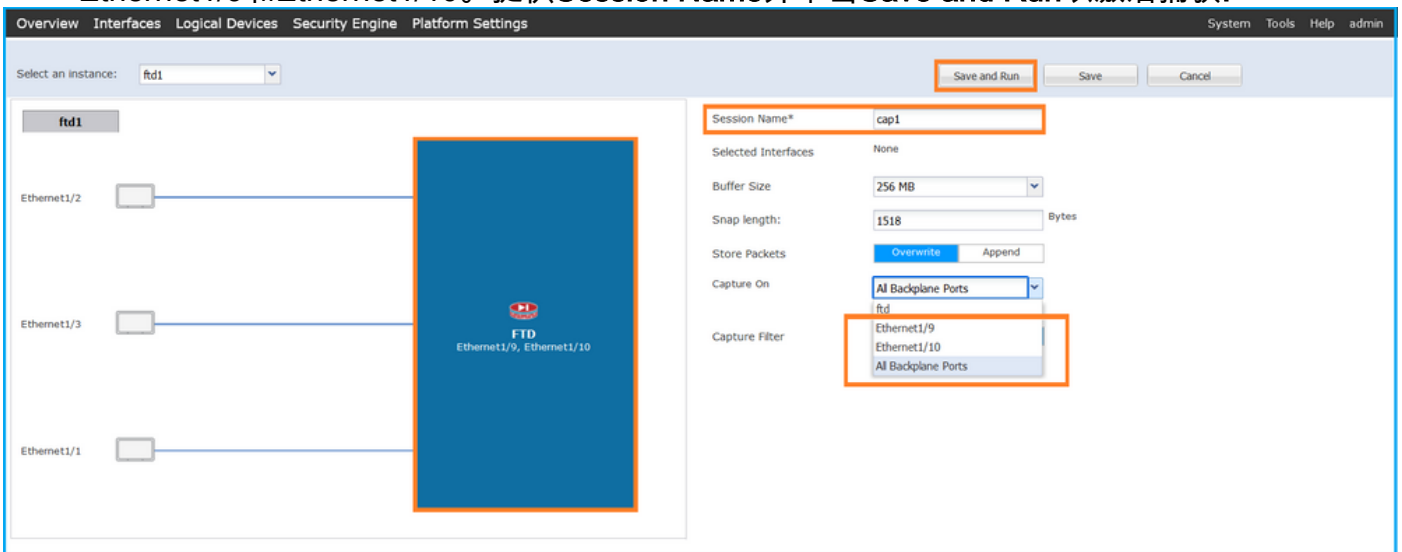
FCM

按照FCM上的以下步骤配置背板接口上的数据包捕获：

1. 使用Tools > Packet Capture > Capture Session创建新的捕获会话：



2. 要捕获所有背板接口上的数据包，请从下拉列表的Capture On中选择应用，然后选择All Backplane Ports。或者，选择特定的背板接口。在这种情况下，可以使用背板接口Ethernet1/9和Ethernet1/10。提供Session Name并单击Save and Run以激活捕获：



FXOS CLI

按照FXOS CLI上的以下步骤配置背板接口上的数据包捕获：

1. 标识应用类型和标识符：

```

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. 创建捕获会话：

```

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 #

```

确认

FCM

验证Interface Name，确保Operational Status为up且File Size（以字节为单位）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

在scope packet-capture中验证捕获详细信息：

```

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

收集捕获文件

按照**收集Firepower 4100/9300内部交换机捕获文件**部分中的步骤进行操作。

捕获文件分析

使用数据包捕获文件读取器应用程序打开捕获文件。如果有多个背板接口，请确保打开每个背板接口的所有捕获文件。在这种情况下，数据包在背板接口Ethernet1/9上捕获。

选择第一个和第二个数据包，并检查要点：

1. 捕获每个ICMP回应请求数据包并显示两次。
2. 原始数据包报头没有VLAN标记。
3. 内部交换机插入标识出口接口Ethernet1/3的额外端口VLAN标记**103**。
4. 内部交换机插入一个额外的VN标记。

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

4
 VN-Tag
 0..... = Direction: To Bridge
 .0..... = Pointer: vif_id
 ..00 0000 0000 0000 = Destination: 0
 = Looped: No
0..... = Reserved: 0
00 = Version: 0
0000 0000 1010 = Source: 10
 Type: 802.1Q Virtual LAN (0x8100)

3
 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)

2
 Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100
 Internet Control Message Protocol

说明

当在背板接口上配置了数据包捕获时，交换机将同时捕获每个数据包两次。在这种情况下，内部交换机接收安全模块上的应用已使用端口VLAN标记和VN标记标记的数据包。VLAN标记标识内部机箱用于将数据包转发到网络的出口接口。ICMP回应请求数据包中的VLAN标记103将Ethernet1/3标识为出口接口，而ICMP回应应答数据包中的VLAN标记102将Ethernet1/2标识为出口接口。在将数据包转发到网络之前，内部交换机会删除VN标记和内部接口VLAN标记。

此表概述了任务：

任务	捕获点	捕获数据包中的内部端口VLAN	方向	捕获的流量
配置和验证背板接口上的数据包捕获	背板接口	102 103	仅限入 口	从主机192.0.2.100到主机198.51.100.100的ICMP回应请求 从主机198.51.100.100到主机192.0.2.100的ICMP回应应答

应用和应用端口上的数据包捕获

如果用户指定应用捕获方向，则应用或应用端口数据包捕获始终在背板接口上配置，并在前接口上配置。

主要有2个使用案例：

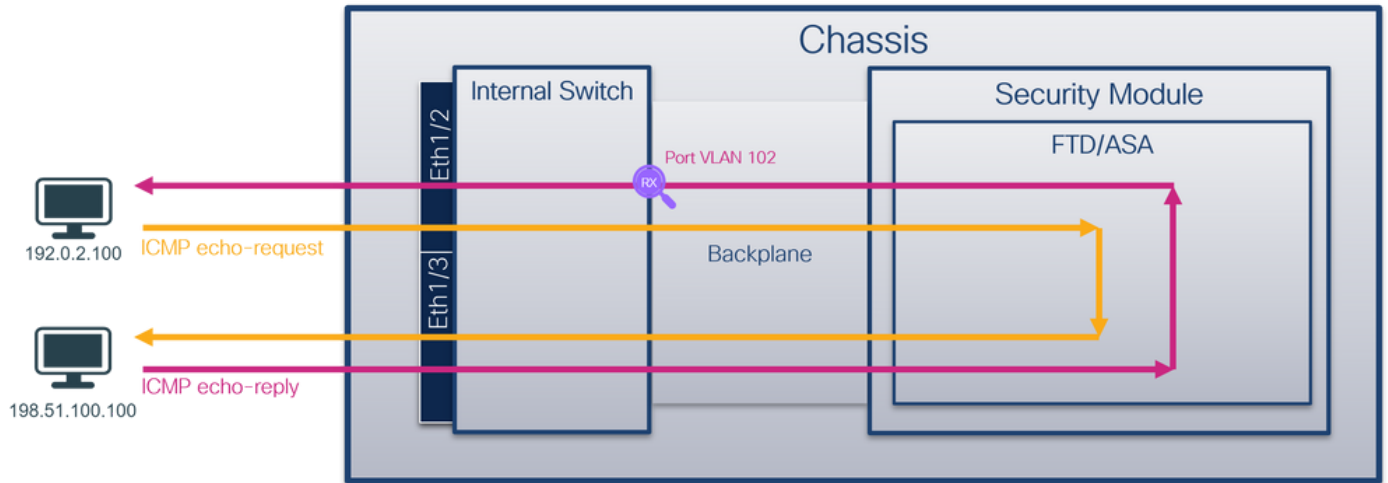
- 为离开特定前接口的数据包配置背板接口上的数据包捕获。例如，在背板接口Ethernet1/9上为离开接口Ethernet1/2的数据包配置数据包捕获。
- 在特定前接口和背板接口上配置同步数据包捕获。例如，在接口Ethernet1/2和背板接口Ethernet1/9上为离开接口Ethernet1/2的数据包配置同步数据包捕获。

本节介绍这两种使用案例。

任务1

使用FCM和CLI配置和验证背板接口上的数据包捕获。捕获应用端口Ethernet1/2被识别为出口接口的数据包。在本例中，捕获ICMP应答。

拓扑、数据包流和捕获点

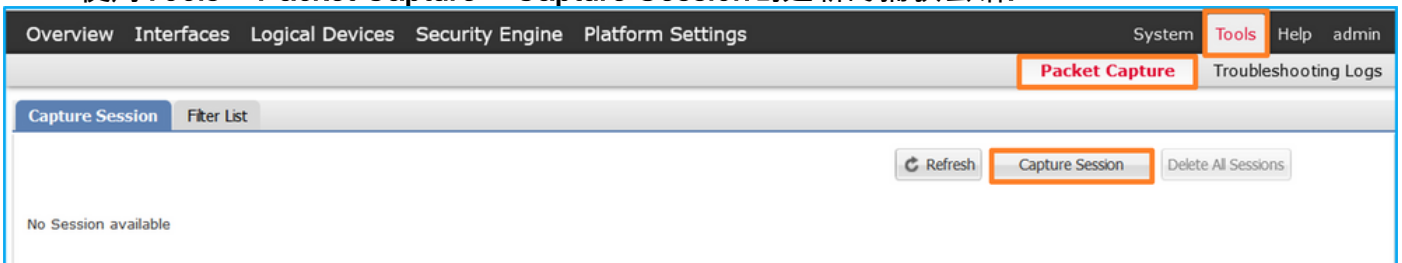


配置

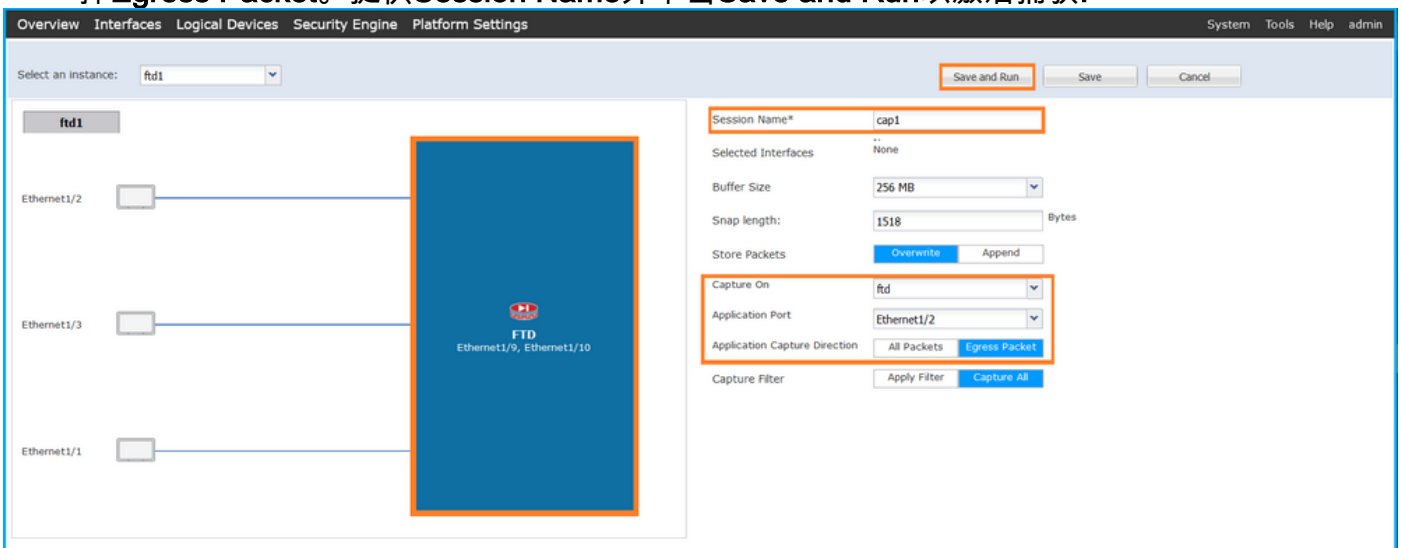
FCM

按照FCM上的以下步骤在FTD应用和应用端口Ethernet1/2上配置数据包捕获：

1. 使用Tools > Packet Capture > Capture Session创建新的捕获会话：



2. 在Application Port下拉列表中选择应用Ethernet1/2，然后在Application Capture Direction中选择Egress Packet。提供Session Name并单击Save and Run以激活捕获：



FXOS CLI

按照FXOS CLI上的以下步骤配置背板接口上的数据包捕获：

1. 标识应用类型和标识符：

```
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. 创建捕获会话：

```
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 #
```

确认

FCM

验证Interface Name，确保Operational Status为up且File Size（以字节为单位）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

在scope packet-capture中验证捕获详细信息：

```
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:

收集捕获文件

按照收集Firepower 4100/9300内部交换机捕获文件部分中的步骤进行操作。

捕获文件分析

使用数据包捕获文件读取器应用程序打开捕获文件。如果有多个背板接口，请确保打开每个背板接口的所有捕获文件。在这种情况下，数据包在背板接口Ethernet1/9上捕获。

选择第一个和第二个数据包，并检查要点：

1. 捕获每个ICMP回应应答并显示2次。
2. 原始数据包报头没有VLAN标记。
3. 内部交换机插入用于标识出口接口Ethernet1/2的其他端口VLAN标记102。
4. 内部交换机插入一个额外的VN标记。

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 10:03:29.354979593	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply
16	2022-08-01 10:03:29.3549936706	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)

```

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

```

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 10:03:22.231237959	198.51.100.100	192.0.2.100	ICMP	108	0x42f8 (17144)	64	Echo (ping) reply
2	2022-08-01 10:03:22.231239747	198.51.100.100	192.0.2.100	ICMP	108	0x42f8 (17144)	64	Echo (ping) reply
3	2022-08-01 10:03:23.232244769	198.51.100.100	192.0.2.100	ICMP	108	0x4303 (17331)	64	Echo (ping) reply
4	2022-08-01 10:03:23.232247753	198.51.100.100	192.0.2.100	ICMP	108	0x43b3 (17331)	64	Echo (ping) reply
5	2022-08-01 10:03:24.234703981	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64	Echo (ping) reply
6	2022-08-01 10:03:24.234706751	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64	Echo (ping) reply
7	2022-08-01 10:03:25.258672449	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64	Echo (ping) reply
8	2022-08-01 10:03:25.258674861	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64	Echo (ping) reply
9	2022-08-01 10:03:26.282663169	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64	Echo (ping) reply
10	2022-08-01 10:03:26.282666183	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64	Echo (ping) reply
11	2022-08-01 10:03:27.306671694	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64	Echo (ping) reply
12	2022-08-01 10:03:27.306674378	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64	Echo (ping) reply
13	2022-08-01 10:03:28.330664677	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64	Echo (ping) reply
14	2022-08-01 10:03:28.330667153	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64	Echo (ping) reply
15	2022-08-01 10:03:29.354979593	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply
16	2022-08-01 10:03:29.3549936706	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)

```

0... .. = Direction: To Bridge
.0... .. = Pointer: vif_id
..00 0000 0000 0000 .. = Destination: 0
... .. = Looped: No
... .. = Reserved: 0
... .. = Version: 0
... .. = 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

```

说明

在这种情况下，端口VLAN标记为102的Ethernet1/2是ICMP回应应答数据包的出口接口。

当在捕获选项中将应用捕获方向设置为Egress时，在入口方向的背板接口上捕获以太网报头中端口VLAN标记为102的数据包。

此表概述了任务：

任务	捕获点	捕获数据包中的内部端口VLAN	方向	捕获的流量

配置并验证应用和应用端口
Ethernet1/2上的捕获

背板接口

102

仅限入口 从主机198.51.100.100到主机
192.0.2.100的ICMP回应应答

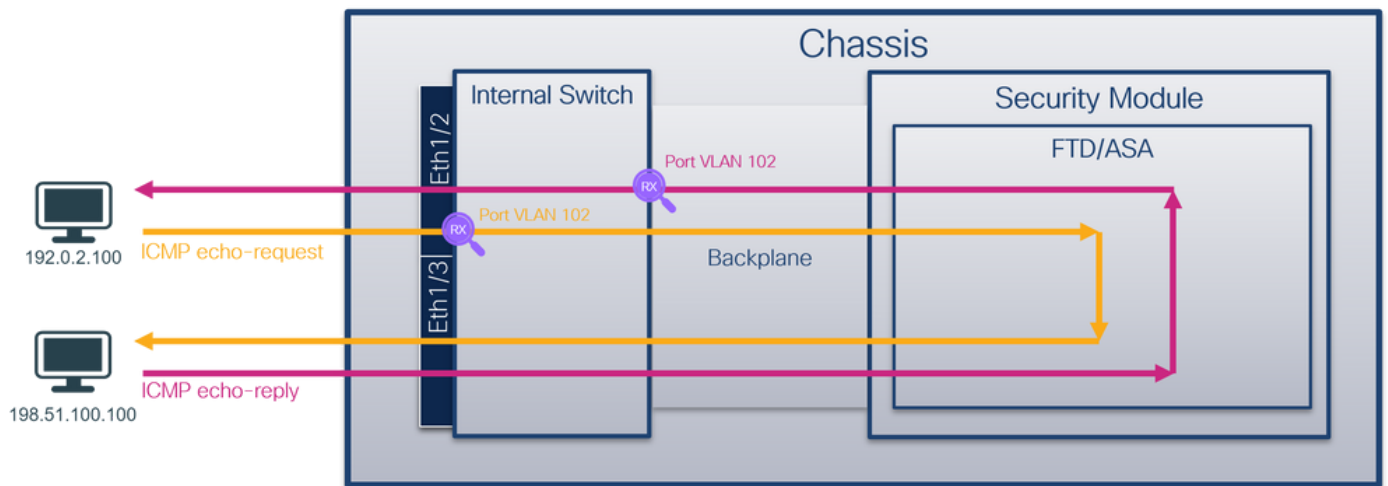
任务2

使用FCM和CLI配置并检验背板接口和前接口Ethernet1/2上的数据包捕获。

同时数据包捕获配置在：

- 前接口 — 捕获接口Ethernet1/2上端口VLAN 102的数据包。捕获的数据包是ICMP回应请求。
- 背板接口 — 捕获将Ethernet1/2标识为出口接口的数据包，或者捕获端口VLAN 102的数据包。捕获的数据包是ICMP回应应答。

拓扑、数据包流和捕获点

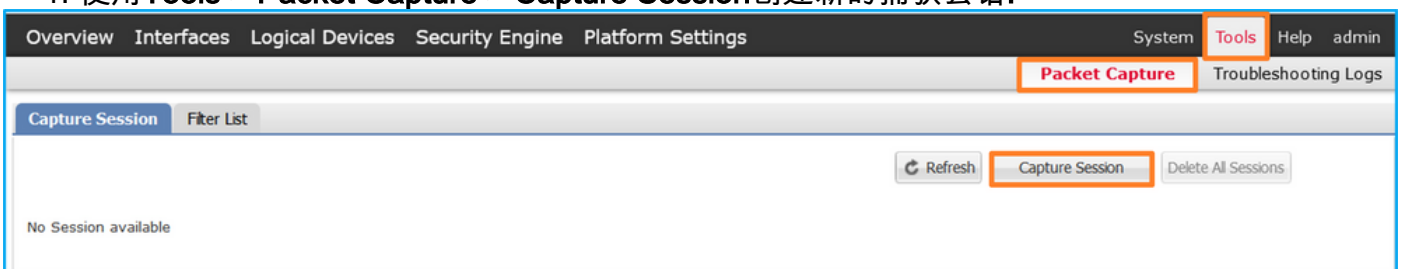


配置

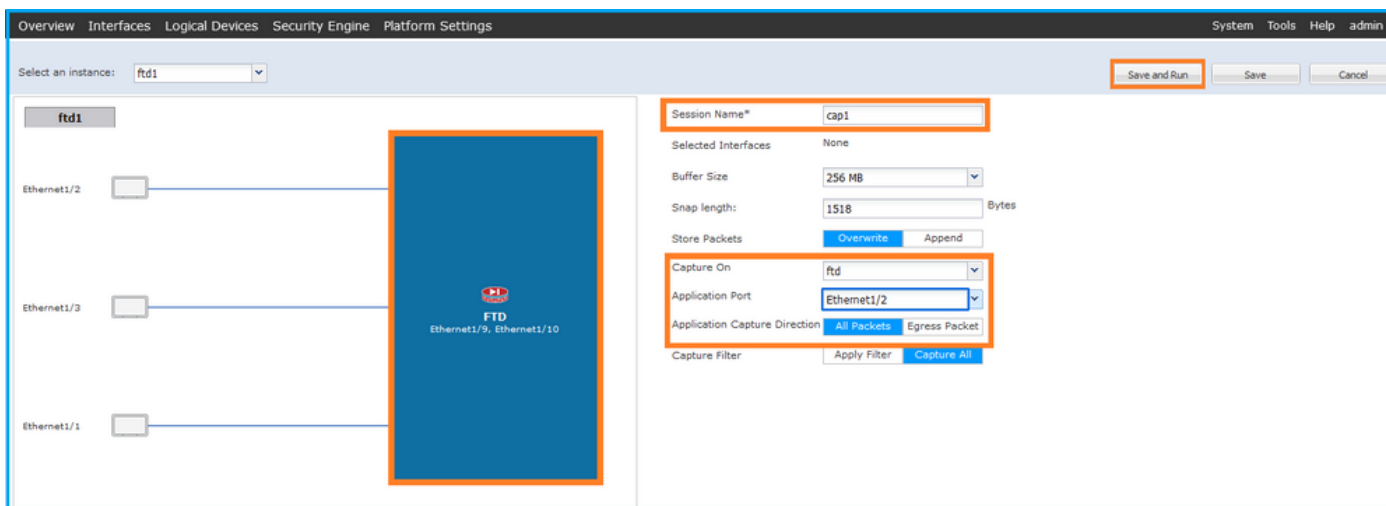
FCM

按照FCM上的以下步骤在FTD应用和应用端口Ethernet1/2上配置数据包捕获：

1. 使用Tools > Packet Capture > Capture Session创建新的捕获会话：



2. 在Application Port下拉列表中选择FTD应用Ethernet1/2，然后在Application Capture Direction中选择All Packets。提供Session Name并单击Save and Run以激活捕获：



FXOS CLI

按照FXOS CLI上的以下步骤配置背板接口上的数据包捕获：

1. 标识应用类型和标识符：

```
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. 创建捕获会话：

```
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
```

确认

FCM

验证Interface Name，确保Operational Status为up且File Size（以字节为单位）增加：

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

FXOS CLI

在scope packet-capture中验证捕获详细信息：

```
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:
```

收集捕获文件

按照收集Firepower 4100/9300内部交换机捕获文件部分中的步骤进行操作。

捕获文件分析

使用数据包捕获文件读取器应用程序打开捕获文件。如果有多个背板接口，请确保打开每个背板接口的所有捕获文件。在这种情况下，数据包在背板接口Ethernet1/9上捕获。

打开接口Ethernet1/2的捕获文件，选择第一个数据包，然后检查要点：

1. 仅捕获ICMP回应请求数据包。捕获每个数据包并显示2次。
2. 原始数据包报头没有VLAN标记。
3. 内部交换机插入标识入口接口Ethernet1/2的额外端口VLAN标记102。
4. 内部交换机插入一个额外的VN标记。

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 11:33:19.07069347	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	102	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
  
```

选择第二个数据包并检查要点：

1. 仅捕获ICMP回应请求数据包。捕获每个数据包并显示2次。
2. 原始数据包报头没有VLAN标记。
3. 内部交换机插入标识入口接口Ethernet1/2的额外端口VLAN标记102。

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 11:33:19.07152698	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	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 11:33:30.226401017	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 2: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
> Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VMware 9d:e8:be (00:50:56:9d:e8:be)
  0000  00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00  -PV...X...m...&...
  0010  00 0a 81 00 00 66 08 00 45 00 00 54 4f 27 00 00  -.....f...E...TO...
  0020  40 01 3e 86 c3 33 64 64 c0 00 02 64 00 00 95 7c  -@->...3dd...d...|
  0030  00 13 00 01 f2 b9 e7 62 00 00 00 00 cb 7f 06 00  -.....b.....
  0040  00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b  -.....
  0050  1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b  -.....l"*$%&'()*+
  0060  2c 2d 2e 2f 30 31 32 33 34 35 36 37              -,-./0123 4567
  
```



```

> VN-Tag
  0... .. = Direction: To Bridge
  .0... .. = Pointer: vif_id
  ..00 0000 0000 0000 .. = Destination: 0
  .. = Looped: No
  ..0... .. = 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 (0x0000)
  
```



```

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

说明

如果选择了Application Capture Direction中的All Packets，则配置与所选应用端口Ethernet1/2相关的2个同时数据包捕获：在前接口Ethernet1/2上捕获数据，在选定的背板接口上捕获数据。

在前接口上配置数据包捕获后，交换机将同时捕获每个数据包两次：

- 插入端口VLAN标记之后。
- 在插入VN标记之后。

按照操作顺序，VN标记插入的时间晚于端口VLAN标记插入的时间。但在捕获文件中，带有VN标记的数据包比带有端口VLAN标记的数据包更早显示。在本示例中，ICMP回应请求数据包中的VLAN标记102将Ethernet1/2标识为入口接口。

当在背板接口上配置了数据包捕获时，交换机将同时捕获每个数据包两次。内部交换机接收安全模块上的应用已使用端口VLAN标记和VN标记标记的数据包。端口VLAN标记标识内部机箱用于将数据包转发到网络的出口接口。在本示例中，ICMP回应应答数据包中的VLAN标记102将Ethernet1/2标识为出口接口。

在将数据包转发到网络之前，内部交换机会删除VN标记和内部接口VLAN标记。

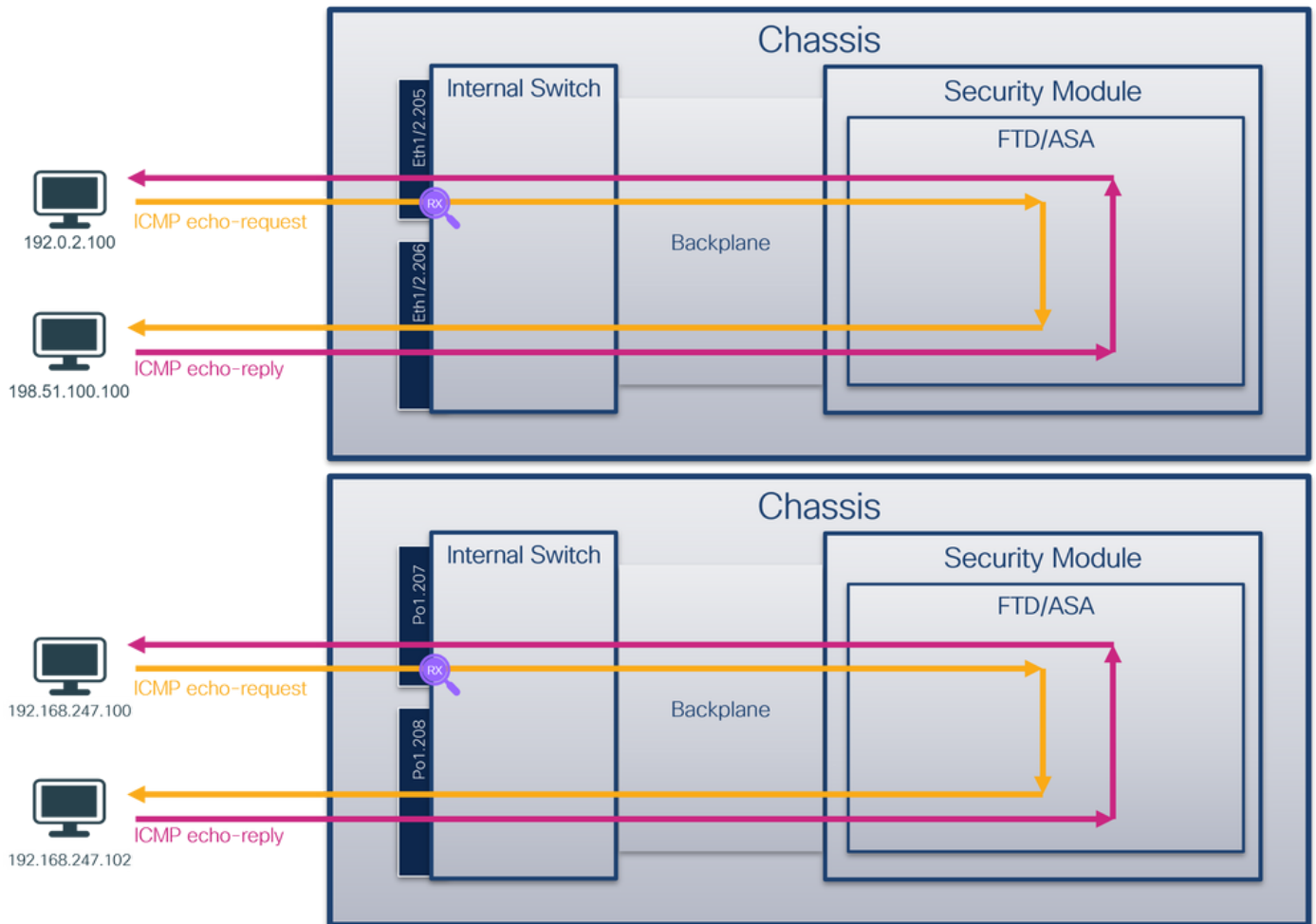
此表概述了任务：

任务	捕获点	捕获数据包中的内部端口VLAN	方向	捕获的流量
配置并验证应用和应用端口Ethernet1/2上的捕获	背板接口	102	仅限入口	从主机198.51.100.100到主机192.0.2.100的ICMP回应应答
	以太网接口1/2	102	仅限入口	从主机192.0.2.100到主机198.51.100.100的ICMP回应请求

物理或端口通道接口的子接口上的数据包捕获

使用FCM和CLI在子接口Ethernet1/2.205或端口通道子接口Portchannel1.207上配置和验证数据包捕获。仅容器模式中的FTD应用支持子接口和子接口捕获。在本例中，在Ethernet1/2.205和Portchannel1.207上配置了数据包捕获。

拓扑、数据包流和捕获点

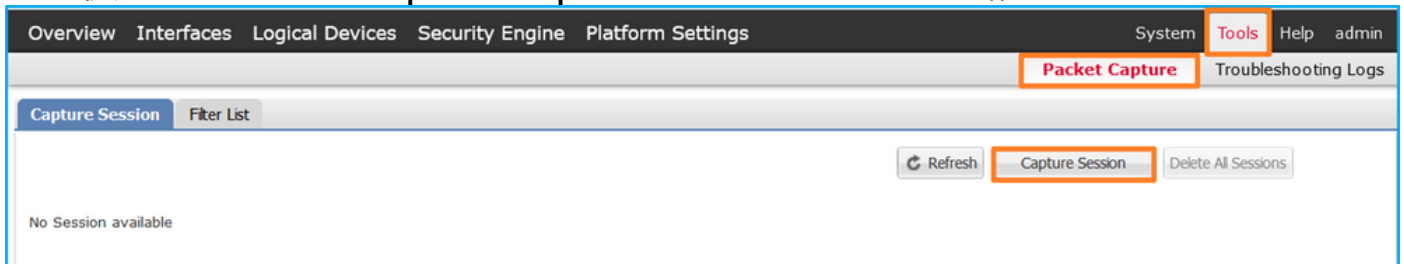


配置

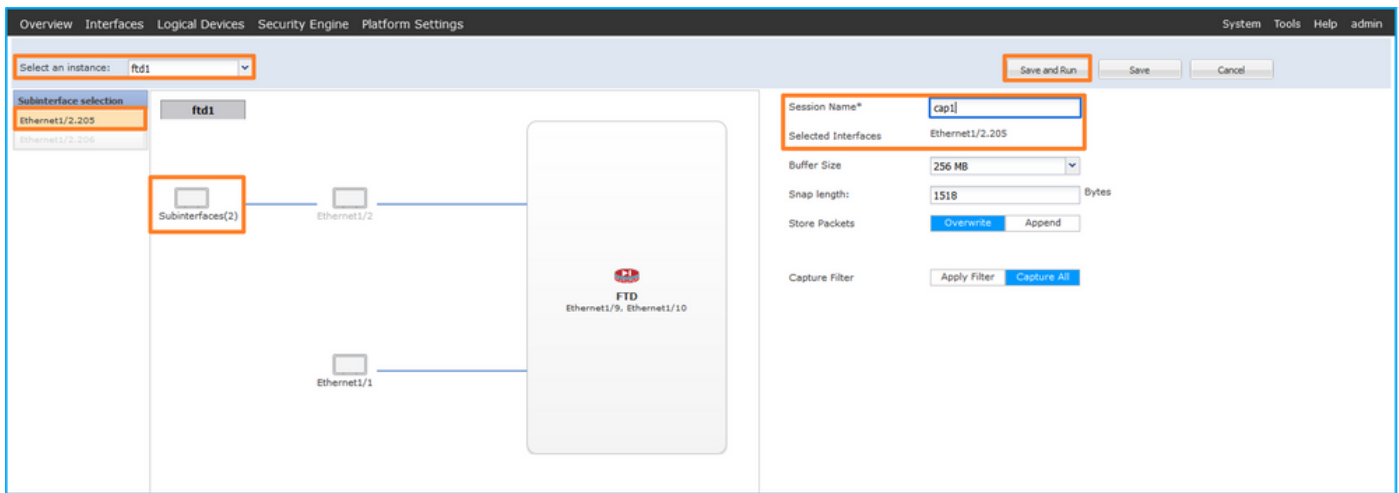
FCM

按照FCM上的以下步骤在FTD应用和应用端口Ethernet1/2上配置数据包捕获：

1. 使用Tools > Packet Capture > Capture Session创建新的捕获会话：



2. 选择特定应用实例ftd1（子接口Ethernet1/2.205），提供会话名称，然后单击Save and Run激活捕获：



3.对于端口通道子接口，由于Cisco Bug ID [CSCvq33119](#)子接口在FCM中不可见。使用FXOS CLI在端口通道子接口上配置捕获。

FXOS CLI

在FXOS CLI上执行以下步骤，在子接口Ethernet1/2.205和Portchannel1.207上配置数据包捕获：

1. 标识应用类型和标识符：

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

2. 对于端口通道接口，请标识其成员接口：

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

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

3. 创建捕获会话：

```
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 #

```

对于端口通道子接口，请为每个端口通道成员接口创建数据包捕获：

```

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 #

```

确认

FCM

验证Interface Name，确保Operational Status为up且File Size（以字节为单位）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上配置的端口通道子接口捕获也在FCM上可见；但是，不能对其进行编辑：

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

在scope packet-capture中验证捕获详细信息：

```

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具有成员接口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
```

收集捕获文件

按照收集Firepower 4100/9300内部交换机捕获文件部分中的步骤进行操作。

捕获文件分析

使用数据包捕获文件读取器应用程序打开捕获文件。选择第一个数据包并检查要点：

1. 仅捕获ICMP回应请求数据包。捕获每个数据包并显示2次。
2. 原始数据包报头的VLAN标记为205。
3. 内部交换机插入标识入口接口Ethernet1/2的额外端口VLAN标记102。
4. 内部交换机插入一个额外的VN标记。

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 (00:50:56:9d: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

选择第二个数据包并检查要点：

1. 仅捕获ICMP回应请求数据包。捕获每个数据包并显示2次。
2. 原始数据包报头的VLAN标记为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 (00:50:56:9d: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

现在打开Portchannel1.207的捕获文件。选择第一个数据包并检查要点

1. 仅捕获ICMP回应请求数据包。捕获每个数据包并显示2次。
2. 原始数据包报头的VLAN标记为207。
3. 内部交换机插入标识入口接口Portchannel1的附加端口VLAN标记1001。
4. 内部交换机插入一个额外的VN标记。

选择第二个数据包并检查要点：

1. 仅捕获ICMP回应请求数据包。捕获每个数据包并显示2次。
2. 原始数据包报头的VLAN标记为207。

说明

在前接口上配置数据包捕获后，交换机将同时捕获每个数据包两次：

- 插入端口VLAN标记之后。
- 在插入VN标记之后。

按照操作顺序，VN标记插入的时间晚于端口VLAN标记插入的时间。但在捕获文件中，带有VN标记的数据包比带有端口VLAN标记的数据包更早显示。此外，对于子接口，在捕获文件中，每个第二个数据包不包含端口VLAN标记。

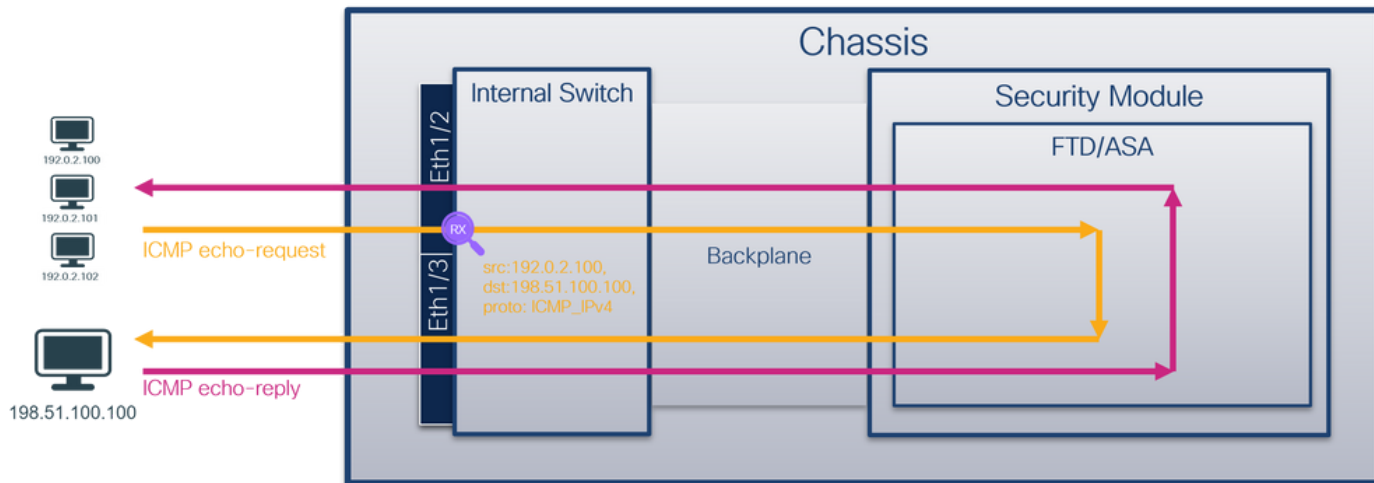
此表概述了任务：

任务	捕获点	捕获数据包中的内部端口VLAN	方向	捕获的流量
在子接口 Ethernet1/2.205 上配置并检验数据包捕获	以太网 1/2.205	102	仅限入口	从主机 192.0.2.100 到主机 198.51.100.100 的 ICMP 回应请求
在成员接口 Ethernet1/3 和 Ethernet1/4 的 Portchannel1 子接口上配置并检验数据包捕获	以太网 1/3 以太网 1/4	1001	仅限入口	从 192.168.207.100 到主机 192.168.207.102 的 ICMP 回应请求

数据包捕获过滤器

使用 FCM 和 CLI 配置和验证带有过滤器的接口 Ethernet1/2 上的数据包捕获。

拓扑、数据包流和捕获点

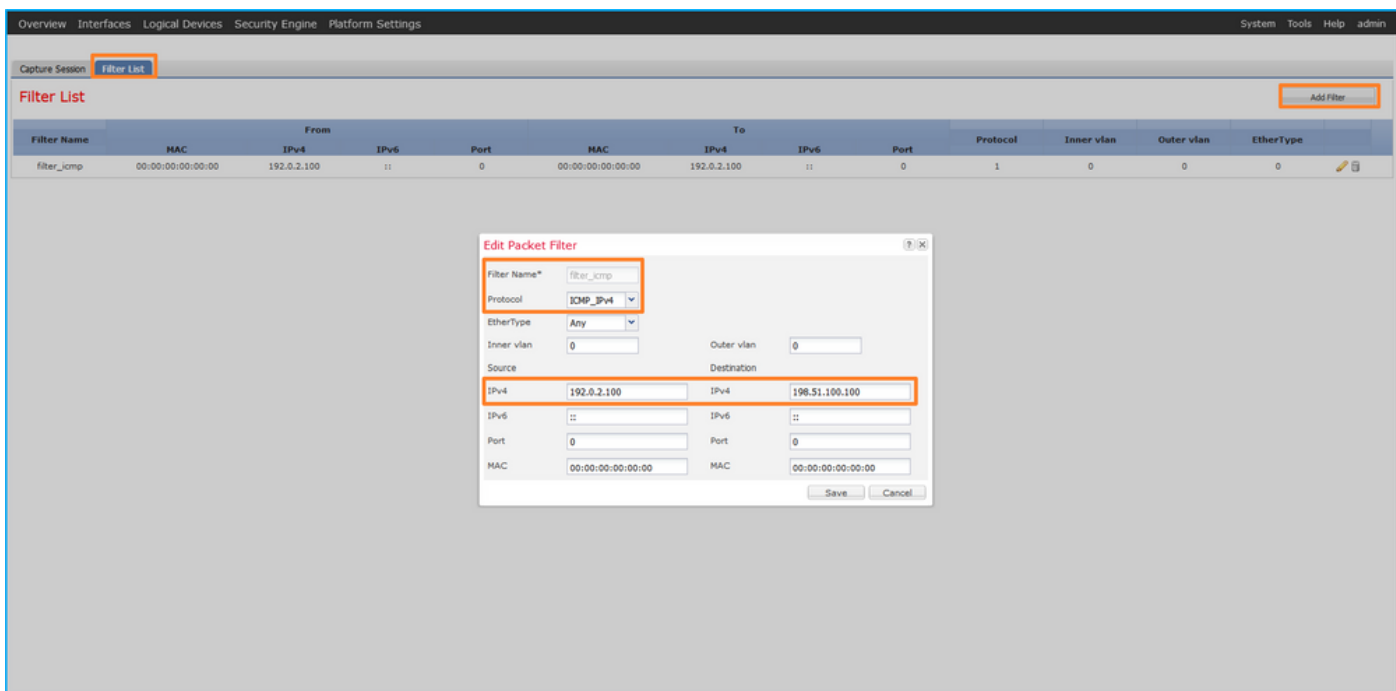


配置

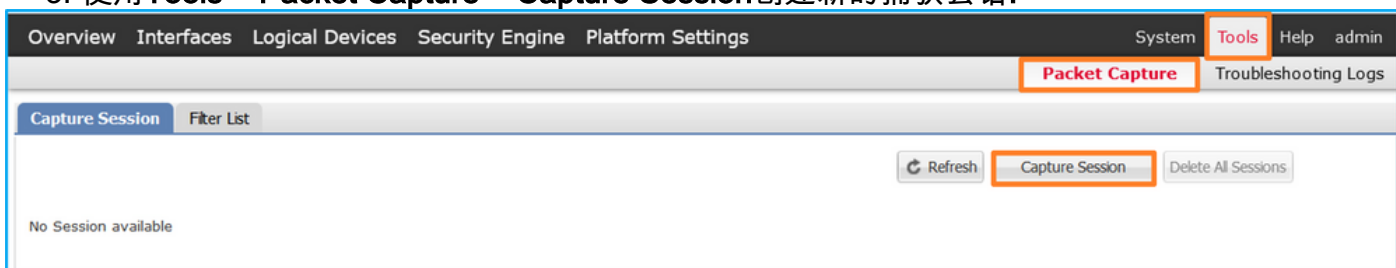
FCM

按照 FCM 上的以下步骤，为从主机 192.0.2.100 到主机 198.51.100.100 的 ICMP 回应请求数据包配置捕获过滤器，并将其应用于接口 Ethernet1/2 上的数据包捕获：

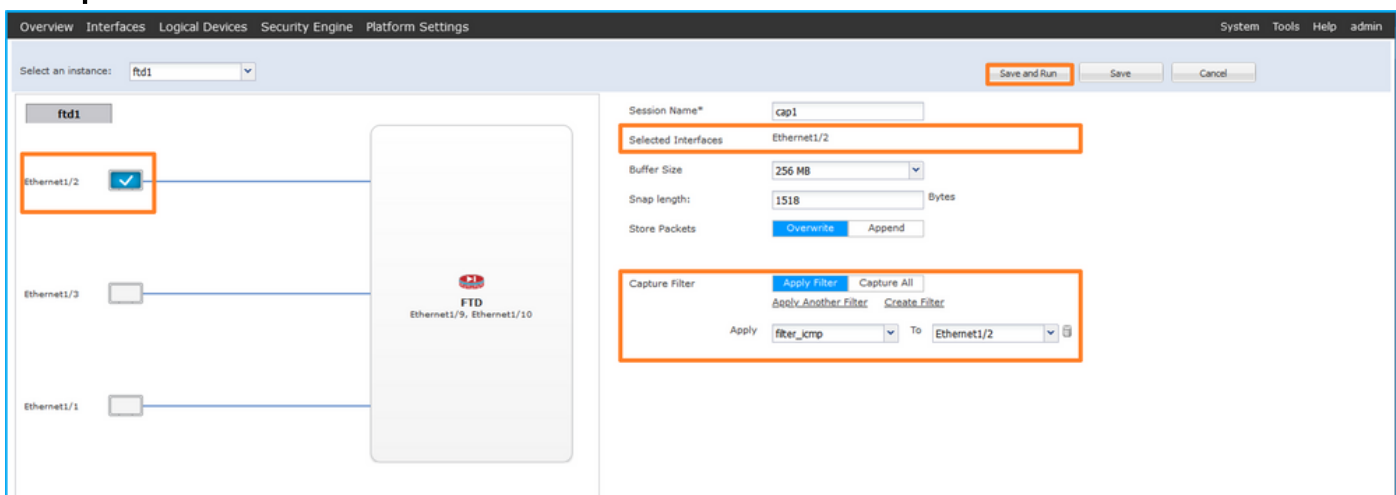
1. 使用 Tools > Packet Capture > Filter List > Add Filter 创建捕获过滤器。
2. 指定 Filter Name、Protocol、Source IPv4、Destination IPv4，然后单击 Save:



3. 使用Tools > Packet Capture > Capture Session创建新的捕获会话:



4. 选择Ethernet1/2，提供Session Name，应用捕获过滤器，然后单击Save and Run以激活捕获



FXOS CLI

按照FXOS CLI上的以下步骤配置背板接口上的数据包捕获：

1. 标识应用类型和标识符：

```
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>中确定IP协议编号。在本例中，ICMP协议编号为1。

3.创建捕获会话：

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 #
```

确认

FCM

验证Interface Name，确保Operational Status为up且File Size（以字节为单位）增加：

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

在Tools > Packet Capture > Capture Session中验证Interface Name(Filter)，确保Operational Status为up，且File Size（以字节为单位）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

在scope packet-capture中验证捕获详细信息：

```
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
```

收集捕获文件

按照**收集Firepower 4100/9300内部交换机捕获文件**部分中的步骤进行操作。

捕获文件分析

使用数据包捕获文件读取器应用程序打开捕获文件。选择第一个数据包并检查要点

1. 仅捕获ICMP回应请求数据包。捕获每个数据包并显示2次。
2. 原始数据包报头没有VLAN标记。
3. 内部交换机插入标识入口接口Ethernet1/2的额外端口VLAN标记**102**。
4. 内部交换机插入一个额外的VN标记。

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	102	0x01cb (459)	64	Echo (ping) request id=0x0018, seq=351/24321, ttl=64 (no r
7	2022-08-02 15:46:58.675153317	192.0.2.100	198.51.100.100	ICMP	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	102	0x01d6 (470)	64	Echo (ping) request id=0x0018, seq=352/24577, ttl=64 (no r
9	2022-08-02 15:46:59.699152639	192.0.2.100	198.51.100.100	ICMP	108	0x01f4 (500)	64	Echo (ping) request id=0x0018, seq=353/24833, ttl=64 (no r
10	2022-08-02 15:46:59.699153835	192.0.2.100	198.51.100.100	ICMP	102	0x01f4 (500)	64	Echo (ping) request id=0x0018, seq=353/24833, ttl=64 (no r
11	2022-08-02 15:47:00.723142641	192.0.2.100	198.51.100.100	ICMP	108	0x01f9 (505)	64	Echo (ping) request id=0x0018, seq=354/25089, ttl=64 (no r
12	2022-08-02 15:47:00.723144643	192.0.2.100	198.51.100.100	ICMP	102	0x01f9 (505)	64	Echo (ping) request id=0x0018, seq=354/25089, ttl=64 (no r
13	2022-08-02 15:47:01.747162204	192.0.2.100	198.51.100.100	ICMP	108	0x026e (622)	64	Echo (ping) request id=0x0018, seq=355/25345, ttl=64 (no r
14	2022-08-02 15:47:01.747163783	192.0.2.100	198.51.100.100	ICMP	102	0x026e (622)	64	Echo (ping) request id=0x0018, seq=355/25345, ttl=64 (no r
15	2022-08-02 15:47:02.771209952	192.0.2.100	198.51.100.100	ICMP	108	0x02bc (700)	64	Echo (ping) request id=0x0018, seq=356/25601, ttl=64 (no r
16	2022-08-02 15:47:02.771211062	192.0.2.100	198.51.100.100	ICMP	102	0x02bc (700)	64	Echo (ping) request id=0x0018, seq=356/25601, ttl=64 (no r
17	2022-08-02 15:47:03.772258550	192.0.2.100	198.51.100.100	ICMP	108	0x032f (815)	64	Echo (ping) request id=0x0018, seq=357/25857, ttl=64 (no r
18	2022-08-02 15:47:03.772259724	192.0.2.100	198.51.100.100	ICMP	102	0x032f (815)	64	Echo (ping) request id=0x0018, seq=357/25857, ttl=64 (no r
19	2022-08-02 15:47:04.791118519	192.0.2.100	198.51.100.100	ICMP	108	0x040f (1039)	64	Echo (ping) request id=0x0018, seq=358/26113, ttl=64 (no r
20	2022-08-02 15:47:04.791119721	192.0.2.100	198.51.100.100	ICMP	102	0x040f (1039)	64	Echo (ping) request id=0x0018, seq=358/26113, ttl=64 (no r


```

> Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_1, i
> Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)
  > VN-Tag
    1... .. = Direction: From Bridge
    .0.. .. = Pointer: vif_id
    ..00 0000 0000 1010 .. = Destination: 10
    .. = Looped: No
    .. = Reserved: 0
    ..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
  
```

选择第二个数据包，并检查要点：

1. 仅捕获ICMP回应请求数据包。捕获每个数据包并显示2次。
2. 原始数据包报头没有VLAN标记。
3. 内部交换机插入标识入口接口Ethernet1/2的额外端口VLAN标记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	102	0x01cb (459)	64	Echo (ping) request id=0x0018, seq=351/24321, ttl=64 (no r
7	2022-08-02 15:46:58.675153317	192.0.2.100	198.51.100.100	ICMP	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	102	0x01d6 (470)	64	Echo (ping) request id=0x0018, seq=352/24577, ttl=64 (no r
9	2022-08-02 15:46:59.699152639	192.0.2.100	198.51.100.100	ICMP	108	0x01f4 (500)	64	Echo (ping) request id=0x0018, seq=353/24833, ttl=64 (no r
10	2022-08-02 15:46:59.699153835	192.0.2.100	198.51.100.100	ICMP	102	0x01f4 (500)	64	Echo (ping) request id=0x0018, seq=353/24833, ttl=64 (no r
11	2022-08-02 15:47:00.723142641	192.0.2.100	198.51.100.100	ICMP	108	0x01f9 (505)	64	Echo (ping) request id=0x0018, seq=354/25089, ttl=64 (no r
12	2022-08-02 15:47:00.723144643	192.0.2.100	198.51.100.100	ICMP	102	0x01f9 (505)	64	Echo (ping) request id=0x0018, seq=354/25089, ttl=64 (no r
13	2022-08-02 15:47:01.747162204	192.0.2.100	198.51.100.100	ICMP	108	0x026e (622)	64	Echo (ping) request id=0x0018, seq=355/25345, ttl=64 (no r
14	2022-08-02 15:47:01.747163783	192.0.2.100	198.51.100.100	ICMP	102	0x026e (622)	64	Echo (ping) request id=0x0018, seq=355/25345, ttl=64 (no r
15	2022-08-02 15:47:02.771209952	192.0.2.100	198.51.100.100	ICMP	108	0x02bc (700)	64	Echo (ping) request id=0x0018, seq=356/25601, ttl=64 (no r
16	2022-08-02 15:47:02.771211062	192.0.2.100	198.51.100.100	ICMP	102	0x02bc (700)	64	Echo (ping) request id=0x0018, seq=356/25601, ttl=64 (no r
17	2022-08-02 15:47:03.772258550	192.0.2.100	198.51.100.100	ICMP	108	0x032f (815)	64	Echo (ping) request id=0x0018, seq=357/25857, ttl=64 (no r
18	2022-08-02 15:47:03.772259724	192.0.2.100	198.51.100.100	ICMP	102	0x032f (815)	64	Echo (ping) request id=0x0018, seq=357/25857, ttl=64 (no r
19	2022-08-02 15:47:04.791118519	192.0.2.100	198.51.100.100	ICMP	108	0x040f (1039)	64	Echo (ping) request id=0x0018, seq=358/26113, ttl=64 (no r
20	2022-08-02 15:47:04.791119721	192.0.2.100	198.51.100.100	ICMP	102	0x040f (1039)	64	Echo (ping) request id=0x0018, seq=358/26113, ttl=64 (no r


```

> Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture_u0_1, i
> 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
  
```

说明

在前接口上配置数据包捕获后，交换机将同时捕获每个数据包两次：

- 插入端口VLAN标记之后。
- 在插入VN标记之后。

按照操作顺序，VN标记插入的时间晚于端口VLAN标记插入的时间。但在捕获文件中，带有VN标记的数据包比带有端口VLAN标记的数据包更早显示。

当应用捕获过滤器时，只会捕获与入口方向过滤器匹配的数据包。

此表概述了任务：

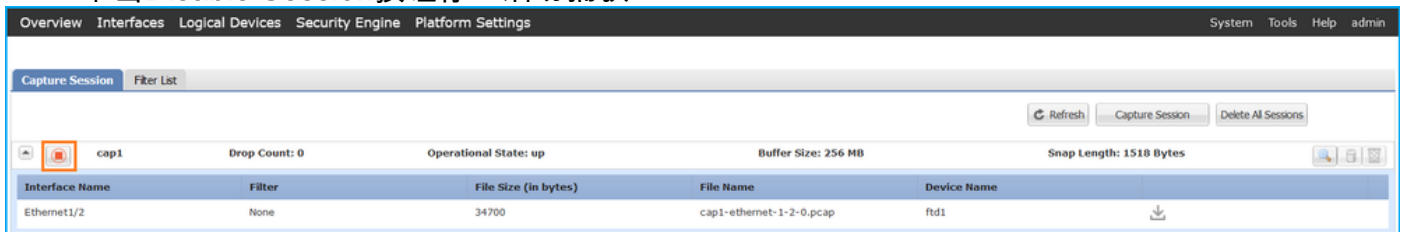
任务	捕获点	捕获数据包中的内部端口VLAN	方向	用户过滤器	捕获的流量
使用前接口 Ethernet1/2 上的过滤器配置并检验数据包捕获	以太网 1/2	102	仅限入口	协议：ICMP 源：192.0.2.100 目的地：198.51.100.1 00	从主机192.0.2.100到主机198.51.100.100的ICMP回应

收集Firepower 4100/9300内部交换机捕获文件

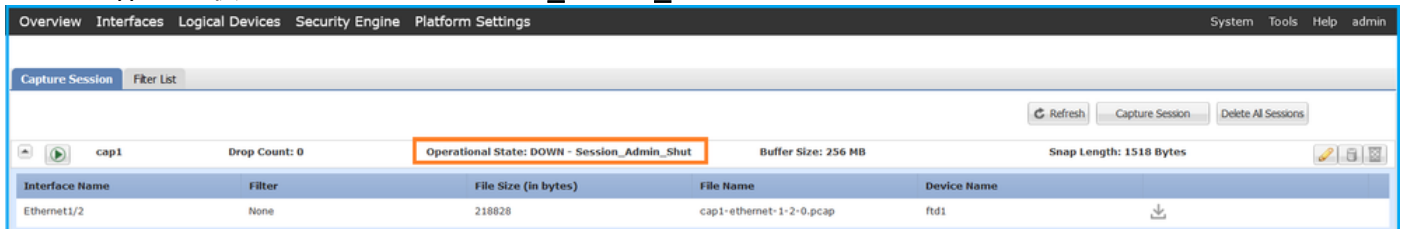
FCM

按照FCM上的以下步骤收集内部交换机捕获文件：

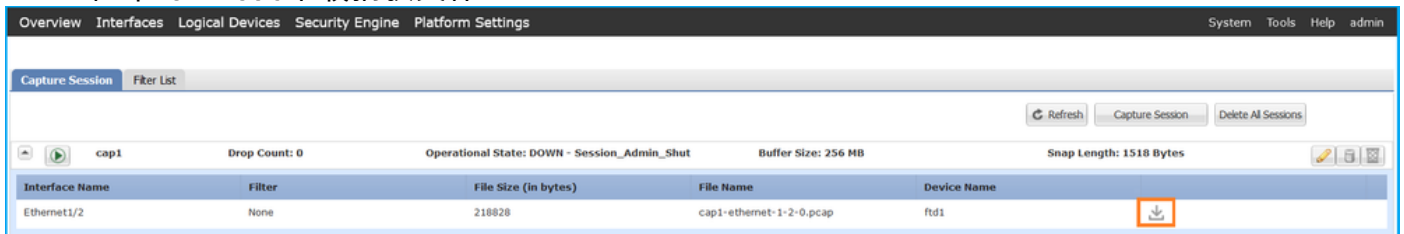
1. 单击Disable Session按钮停止活动捕获：



2. 确保运行状态为DOWN - Session_Admin_Shut:



3. 单击Download下载捕获文件：



对于端口通道接口，对每个成员接口重复此步骤。

FXOS CLI

在FXOS CLI上执行以下步骤以收集捕获文件：

1. 停止活动捕获：

```
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. 从local-mgmt命令范围上传捕获文件：

```
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:
```

对于端口通道接口，请为每个成员接口复制捕获文件。

指南、限制和最佳实践 内部交换机 数据包捕获

有关与Firepower 4100/9300内部交换机捕获相关的准则和限制，请参阅*Cisco Firepower 4100/9300 FXOS机箱管理器配置指南*或*Cisco Firepower 4100/9300 FXOS CLI配置指南*的故障排除部分数据包捕获部分。

这是基于TAC案例中数据包捕获使用情况的最佳实践列表：

- 了解准则和限制。

- 捕获所有端口通道成员接口上的数据包并分析所有捕获文件。
- 使用捕获过滤器。
- 配置捕获过滤器时，考虑NAT对数据包IP地址的影响。
- 增加或减少用于指定帧大小的**Snap Len**，以防其不同于默认值1518字节。更短的大小导致捕获的数据包数量增加，反之亦然。
- 根据需要调整缓冲区大小。
- 请注意FCM或FXOS CLI上的**Drop Count**。一旦达到缓冲区大小限制，丢弃计数计数器就会增加。
- 在Wireshark上使用filter **!vntag**可仅显示不带VN标记的数据包。这对于在前端接口数据包捕获文件中隐藏VN标记的数据包非常有用。
- 在Wireshark上使用filter **frame.number&1**仅显示奇数帧。这对于在背板接口数据包捕获文件中隐藏重复数据包非常有用。
- 对于TCP等协议，Wireshark默认应用着色规则，以不同颜色显示具有特定条件的数据包。如果由于捕获文件中存在重复的数据包而导致内部交换机捕获，则数据包可能会以误报的方式进行着色和标记。如果分析数据包捕获文件并应用任何过滤器，则将显示的数据包导出到新文件并打开新文件。

配置和验证 安全防火墙3100

与Firepower 4100/9300不同，安全防火墙3100上的内部交换机捕获通过**capture <name> switch**命令在应用命令行界面上配置，其中**switch**选项指定在内部交换机上配置捕获。

以下是带有**switch**选项的**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>
```

配置数据包捕获的一般步骤如下：

1. 指定入口接口：

交换机捕获配置接受入口接口**名称if**。用户可以指定数据接口名称、内部上行链路或管理接口：

```
> 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. 指定以太网帧EtherType。默认EtherType为IP。**ethernet-type**选项值指定EtherType:

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

3. 指定匹配条件。**capture match**选项指定匹配条件：

```
> 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. 指定其他可选参数，例如缓冲区大小、数据包长度等。

5. 启用捕获。**no capture <name> switch stop**命令会激活捕获:

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

6. 验证捕获详细信息：

- 管理状态为**enabled**，操作状态为**up**和**active**。
- 数据包捕获文件大小**Pcapsize**增加。
- **show capture <cap_name>**输出中捕获的数据包数量非零。
- 捕获路径**Pcapfile**。捕获的数据包会自动保存/mnt/disk0/packet-capture/文件夹。
- 捕获条件。软件根据捕获条件自动创建捕获过滤器。

```
> 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. 在需要时停止捕获：

```
> 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. 收集捕获文件。按照收集安全防火墙3100内部交换机捕获文件部分中的步骤进行操作。

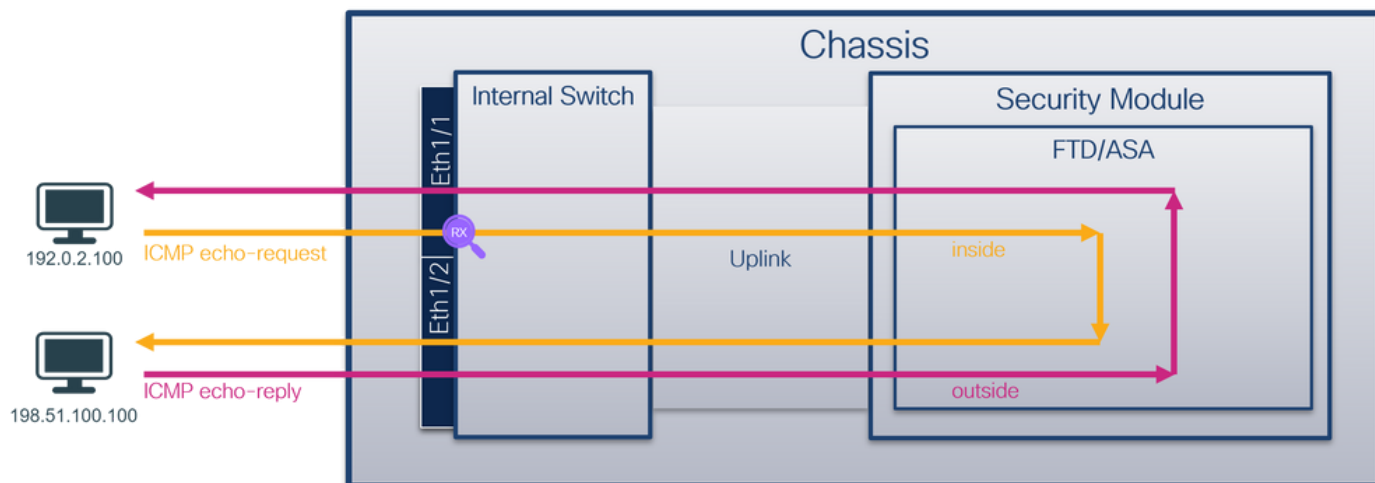
在版本7.2中，FMC或FDM不支持内部交换机捕获配置。对于ASA软件版本9.18(1)及更高版本，可以在ASDM版本7.18.1.x及更高版本中配置内部交换机捕获。

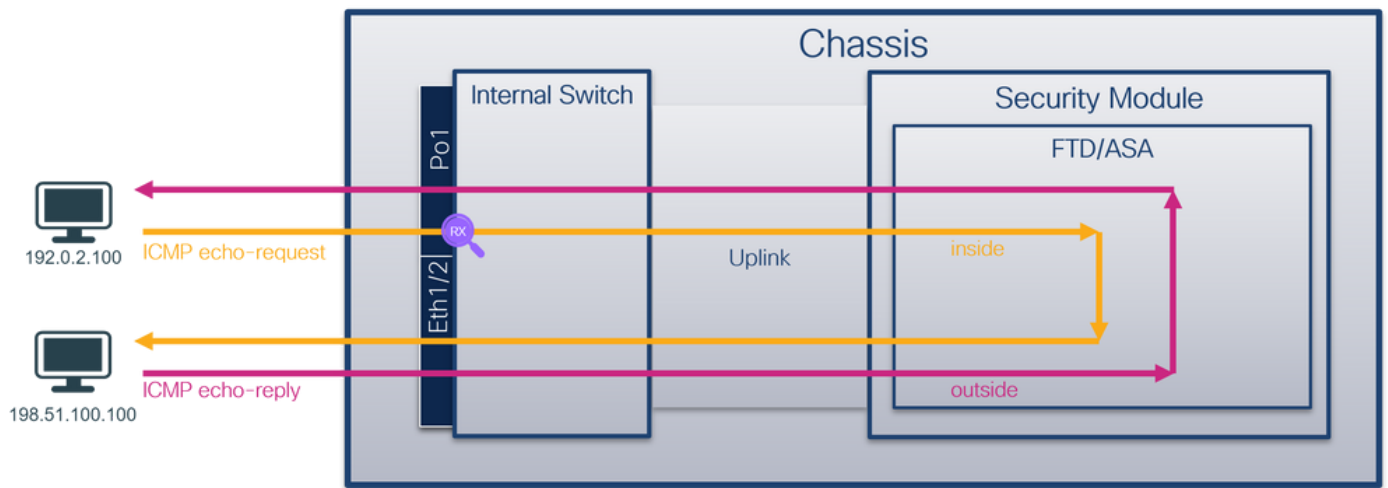
这些场景包括安全防火墙3100内部交换机捕获的常见使用案例。

物理或端口通道接口上的数据包捕获

使用FTD或ASA CLI在接口Ethernet1/1或Portchannel1接口上配置和验证数据包捕获。两个接口都有nameif **inside**。

拓扑、数据包流和捕获点





配置

在ASA或FTD CLI上执行以下步骤，在接口Ethernet1/1或Port-channel1上配置数据包捕获：

1. 验证名称：

```
> 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. 创建捕获会话：

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

3. 启用捕获会话：

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

确认

检验捕获会话名称、管理和运行状态、接口插槽和标识符。确保Pcapsize值增加，且捕获的数据包数量非零：

```
> 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

对于Port-channel1，捕获在所有成员接口上配置：

> **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

可以在FXOS local-mgmt命令外壳中通过show portchannel summary命令验证端口通道成员接口：

> 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

```

要访问ASA上的FXOS，请运行connect fxos admin命令。如果是多情景，请在管理情景中运行命令。

收集捕获文件

按照收集安全防火墙3100内部交换机捕获文件部分中的步骤进行操作。

捕获文件分析

使用数据包捕获文件读取器应用程序打开Ethernet1/1的捕获文件。选择第一个数据包并检查要点：

1. 仅捕获ICMP回应请求数据包。
2. 原始数据包报头没有VLAN标记。

The screenshot shows a packet capture analysis tool interface. The top table lists 18 ICMP Echo (ping) request packets. The selected packet (No. 1) has the following details:

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)

Below the table, the packet details are shown:

- 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

The hex dump shows the raw packet data, with the ICMP Echo request structure visible.

打开Portchannel1成员接口的捕获文件。选择第一个数据包并检查要点：

1. 仅捕获ICMP回应请求数据包。
2. 原始数据包报头没有VLAN标记。

The screenshot shows a packet capture analysis tool interface for a different capture. The top table lists 18 ICMP Echo (ping) request packets. The selected packet (No. 1) has the following details:

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)

Below the table, the packet details are shown:

- 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

The hex dump shows the raw packet data, with the ICMP Echo request structure visible.

说明

交换机捕获配置在接口Ethernet1/1或Portchannel1上。

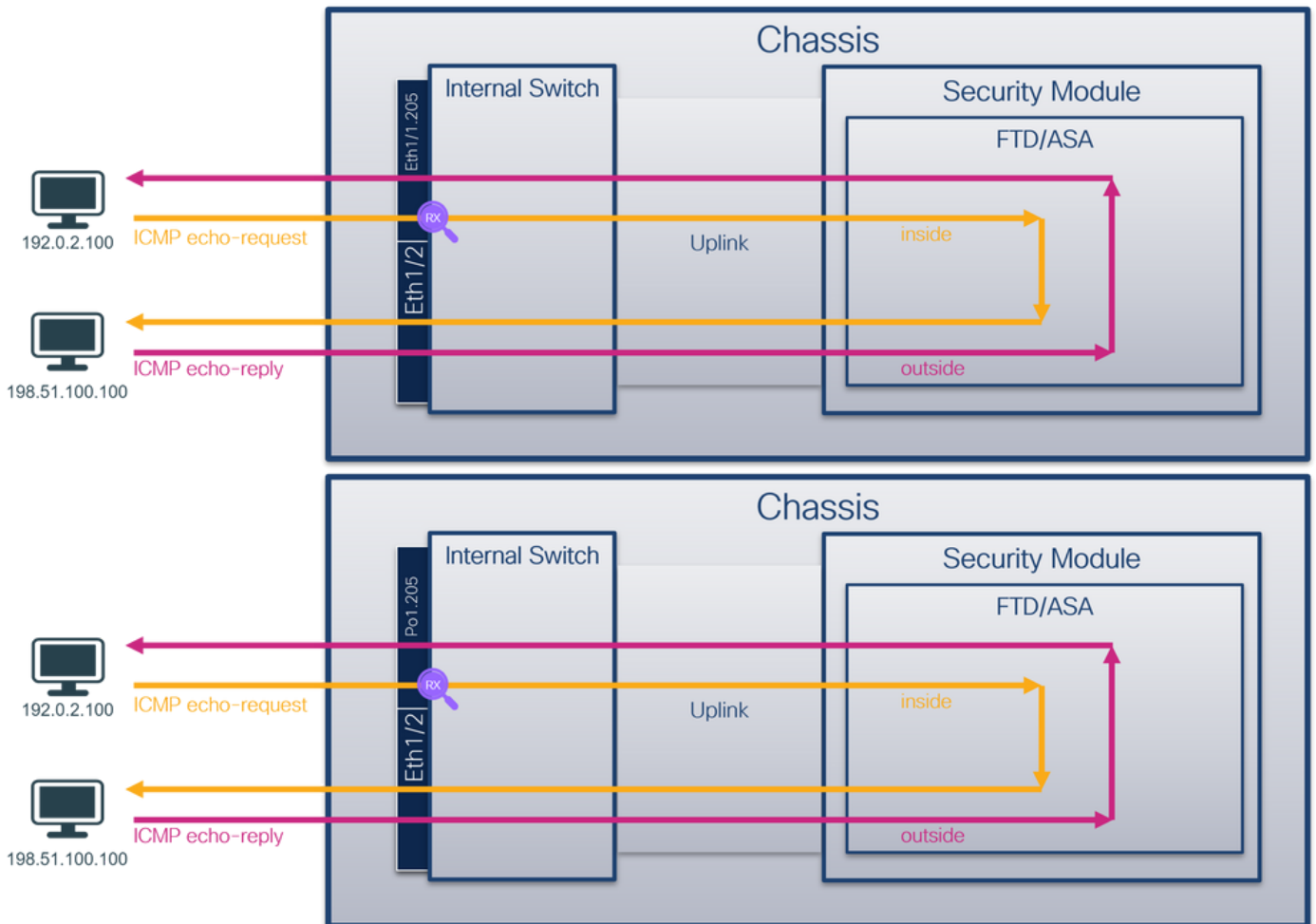
此表概述了任务：

任务	捕获点	内部过滤器	方向	捕获的流量
配置并检验以太网接口1/1上的数据包捕获	以太网1/1	无	仅限入口	从主机192.0.2.100到主机198.51.100.100的ICMP回应请求
在接口Portchannel1上配置并检验带有成员接口Ethernet1/3和Ethernet1/4的数据包捕获	以太网1/3 以太网1/4	无	仅限入口	从主机192.0.2.100到主机198.51.100.100的ICMP回应请求

物理或端口通道接口的子接口上的数据包捕获

使用FTD或ASA CLI在子接口Ethernet1/1.205或Portchannel1.205上配置和验证数据包捕获。两个子接口都具有inside名称。

拓扑、数据包流和捕获点



配置

在ASA或FTD CLI上执行以下步骤，在接口Ethernet1/1或Port-channel1上配置数据包捕获：

1. 验证名称：

```
> 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. 创建捕获会话：

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

3. 启用捕获会话：

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

确认

检验捕获会话名称、管理和运行状态、接口插槽和标识符。确保Pcapsize值增加，且捕获的数据包数量非零：

```
> 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

在这种情况下，会创建一个外部VLAN Ovlan=205的过滤器，并将其应用于接口。

对于Port-channel1，在所有成员接口上配置了带过滤器Ovlan=205的捕获：

> 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

可以在FXOS local-mgmt命令外壳中通过show portchannel summary命令验证端口通道成员接口：

```
> 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
```

要访问ASA上的FXOS，请运行connect fxos admin命令。如果是多情景，请在管理情景中运行此命令。

收集捕获文件

按照收集安全防火墙3100内部交换机捕获文件部分中的步骤进行操作。

捕获文件分析

使用数据包捕获文件读取器应用程序打开Ethernet1/1.205的捕获文件。选择第一个数据包并检查要点：

1. 仅捕获ICMP回应请求数据包。

2. 原始数据包报头的VLAN标记为205。

The screenshot displays a list of 18 ICMP Echo (ping) requests. Packet 1 is highlighted. The details pane for packet 1 shows:

- Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 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)
- 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)
 - Trailer: 55555555
- Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
- Internet Control Message Protocol

打开Portchannel1成员接口的捕获文件。选择第一个数据包并检查要点：

1. 仅捕获ICMP回应请求数据包。
2. 原始数据包报头的VLAN标记为205。

The screenshot displays a list of 18 ICMP Echo (ping) requests. Packet 1 is highlighted. The details pane for packet 1 shows:

- Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 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)
- 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)
 - Trailer: 55555555
- Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
- Internet Control Message Protocol

说明

交换机捕获在子接口Ethernet1/1.205或Portchannel1.205上配置，其过滤器匹配外部VLAN 205。

此表概述了任务：

任务	捕获点	内部过滤器	方向	捕获的流量
在子接口Ethernet1/1.205上配置并检验数据包捕获	以太网1/1	外部	仅限入	从主机192.0.2.100到主机198.51.100.100的ICMP回应请求
在子接口Portchannel1.205上配置并检验带有成员接口Ethernet1/3和Ethernet1/4的数据包捕获	以太网1/3 以太网1/4	外部	仅限入	从主机192.0.2.100到主机198.51.100.100的ICMP回应请求

内部接口上的数据包捕获

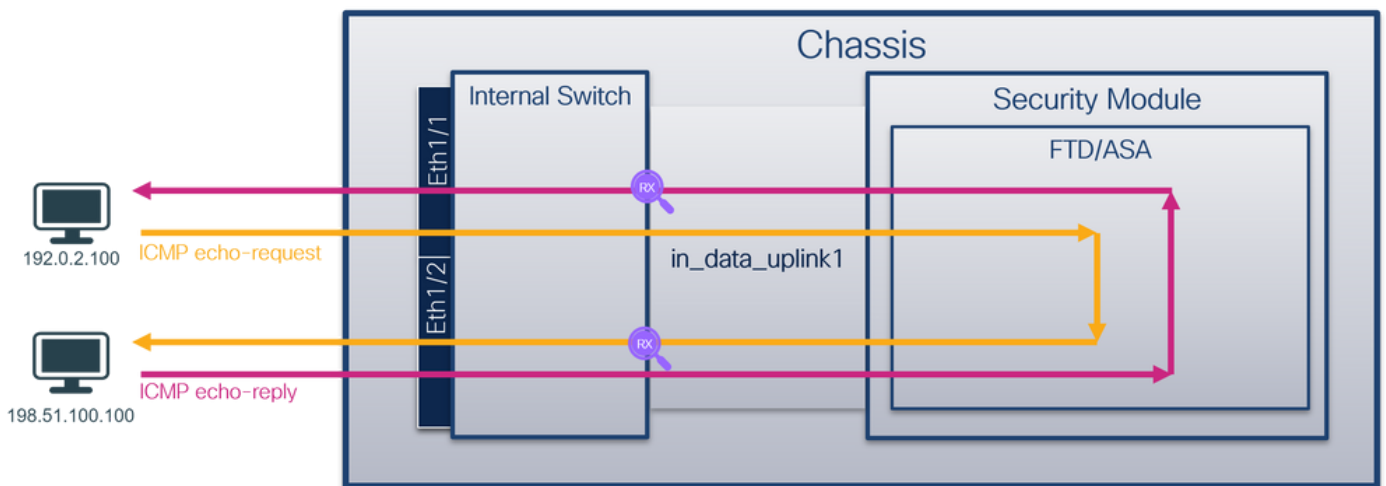
安全防火墙具有2个内部接口：

- **in_data_uplink1** — 将应用程序连接到内部交换机。
- **in_mgmt_uplink1** — 为管理连接（例如到管理接口的SSH）或管理连接（也称为FMC和FTD之间的sftunnel）提供专用数据包路径。

任务1

使用FTD或ASA CLI配置和验证上行链路接口in_data_uplink1上的数据包捕获。

拓扑、数据包流和捕获点



配置

在ASA或FTD CLI上执行以下步骤，在in_data_uplink1接口上配置数据包捕获：

1. 创建捕获会话：

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

2. 启用捕获会话：

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

确认

检验捕获会话名称、管理和运行状态、接口插槽和标识符。确保Pcapsize值增加，且捕获的数据包数量非零：

```
> 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

在这种情况下，使用内部ID 18在接口上创建捕获，该接口是安全防火墙3130上的in_data_uplink1接口。FXOS local-mgmt命令外壳中的show portmanager switch status命令显示接口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

要访问ASA上的FXOS，请运行connect fxos admin命令。如果是多情景，请在管理情景中运行此命令。

收集捕获文件

按照收集安全防火墙3100内部交换机捕获文件部分中的步骤进行操作。

捕获文件分析

使用数据包捕获文件读取器应用程序打开接口in_data_uplink1的捕获文件。检查关键点 — 在这种情况下，捕获的是ICMP回应请求和应答数据包。这些是从应用发送到内部交换机的数据包。

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	0x6e80 (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 64 08 00 7f 15 30 3a 00 21 39 3f f0 62 00 00 dd...:..!9?-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 !""\$%&'()*+,-./012345 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 55 55 67UUUU </pre>
--	--	--

说明

配置上行链路接口上的交换机捕获时，仅捕获从应用发送到内部交换机的数据包。不会捕获发送到应用的数据包。

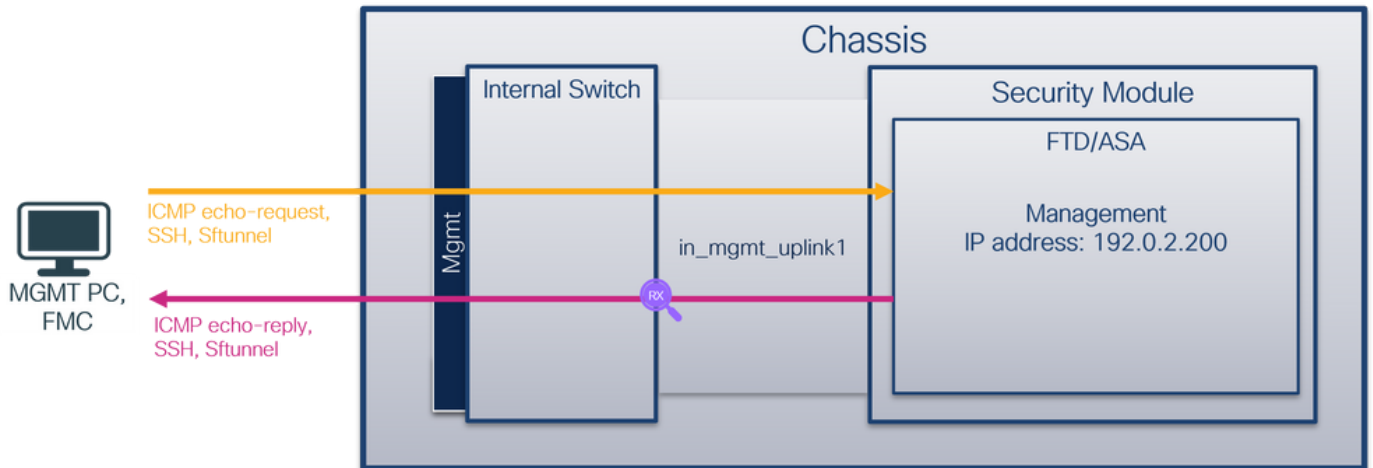
此表概述了任务：

任务	捕获点	内部过滤器	方向	捕获的流量
在in_data_uplink1的上行链路接口上配置 in_data_uplink1 并检验数据包捕获	in_data_uplink1	无	仅限入口	从主机192.0.2.100到主机198.51.100.100的ICMP回应请求 从主机198.51.100.100到主机

任务2

使用FTD或ASA CLI配置和验证上行链路接口in_mgmt_uplink1上的数据包捕获。仅捕获管理平面连接的数据包。

拓扑、数据包流和捕获点



配置

在ASA或FTD CLI上执行以下步骤，在in_mgmt_uplink1接口上配置数据包捕获：

1. 创建捕获会话：

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

2. 启用捕获会话：

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

确认

检验捕获会话名称、管理和运行状态、接口插槽和标识符。确保Pcapsize值增加，且捕获的数据包数量非零：

```
> 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

在这种情况下，使用内部ID 19在接口上创建捕获，该接口是安全防火墙3130上的 **in_mgmt_uplink1**接口。FXOS local-mgmt命令外壳中的**show portmanager switch status**命令显示接口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

要访问ASA上的FXOS，请运行connect fxos admin命令。如果是多情景，请在管理情景中运行此命令。

收集捕获文件

按照收集安全防火墙3100内部交换机捕获文件部分中的步骤进行操作。

捕获文件分析

使用数据包捕获文件读取器应用程序打开接口in_mgmt_uplink1的捕获文件。检查要点 — 在这种情况下，仅显示来自管理IP地址192.0.2.200的数据包。示例包括SSH、Sftunnel或ICMP回应应答数据包。这些是通过内部交换机从应用管理接口发送到网络的数据包。

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 packet with Source 192.0.2.200 and Destination 192.0.2.101 is highlighted. The bottom section shows a detailed view of a selected packet (Frame 1), including its structure: Ethernet II, Internet Protocol Version 4, and Transport Layer Security.

说明

当在管理上行链路接口上配置交换机捕获时，仅捕获从应用管理接口发送的入口数据包。不会捕获发往应用管理接口的数据包。

此表概述了任务：

任务	捕获点	内部过	方向	捕获的流量
----	-----	-----	----	-------

过滤器

配置并验证管理上行链路接口上的数据包捕获

in_mgmt_ 无
uplink1

仅限入口
(从管理接口通过内部交换机连接到网络)

从FTD管理IP地址192.0.2.200到主机192.0.2.100的ICMP回应应答
从FTD管理IP地址192.0.2.200到FMC IP地址192.0.2.101的Sftunnel
从FTD管理IP地址192.0.2.200到主机192.0.2.100的SSH

数据包捕获过滤器

内部交换机数据包捕获过滤器的配置方式与数据平面捕获相同。使用**ethernet-type**和**match**选项配置过滤器。

配置

在ASA或FTD CLI上执行以下步骤，配置数据包捕获和过滤器，该过滤器匹配来自接口Ethernet1/1上的主机198.51.100.100的ARP帧或ICMP数据包：

1. 验证名称：

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

2. 为ARP或ICMP创建捕获会话：

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

确认

验证捕获会话名称和过滤器。Ethertype值为十进制的**2054**和十六进制的**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

这是ICMP过滤器的验证。IP协议1是ICMP:

> **show capture caps-1-1 detail**

Packet Capture info

Name: caps-1-1
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

收集安全防火墙3100内部交换机捕获文件

使用ASA或FTD CLI收集内部交换机捕获文件。在FTD上，还可以通过CLI `copy`命令将捕获文件导出到通过数据或诊断接口可访问的目标。

或者，可在专家模式下将文件复制到`/ngfw/var/common`，并通过**File Download**选项从FMC下载。

对于端口通道接口，请确保从所有成员接口收集数据包捕获文件。

ASA

按照以下步骤在ASA CLI上收集内部交换机捕获文件：

1. 停止捕获：

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

2. 验证捕获会话是否已停止，并记下捕获文件名。

```
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命令将文件导出到远程目标：

```
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

按照以下步骤收集FTD CLI上的内部交换机捕获文件，并将其复制到通过数据或诊断接口可访问的服务器：

1. 转到诊断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. 停止捕获：

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

3. 验证捕获会话是否已停止，并记下捕获文件名：

```
firepower# show capture capsw detail
Packet Capture info
Name:          capsw
Session:       1
```

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

Total Physical ports involved in Packet Capture: 1

Physical port:

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

Packet Capture Filter Info

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

Total Physical breakout ports involved in Packet Capture: 0

886 packets captured on disk using switch capture

Reading of capture file from disk is not supported

4. 使用CLI copy命令将文件导出到远程目标。

```
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
```

按照以下步骤通过File Download选项从FMC收集捕获文件：

1. 停止捕获：

```
> capture capsw switch stop
```

2. 验证捕获会话是否已停止，并记下文件名和完整的捕获文件路径：

```
> 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. 转到专家模式并切换到根模式：

```
> expert
```

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

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

4. 将捕获文件复制到/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，选择Devices > File Download:

The screenshot shows the Cisco Firewall Management Center (FMC) interface. The 'Devices' menu is open, and 'File Download' is highlighted under the 'Troubleshoot' sub-menu. The main dashboard shows various widgets like 'Unique Applications over Time' and 'Traffic by Application Risk'.

6. 选择FTD，提供捕获文件名，然后单击Download:

The screenshot shows the Cisco Firewall Management Center (FMC) interface. The 'File Download' dialog is open, showing the 'Device' dropdown set to 'FPR3100-1' and the 'File' input field containing 'sess-1-capsw-ethernet-1-1-0.pcap'. The 'Download' button is highlighted.

内部交换机数据包捕获指南、限制和最佳实践

准则和限制：

- 支持多个交换机捕获配置会话，但一次只能有一个交换机捕获会话处于活动状态。尝试启用2个或更多捕获会话会导致错误“ERROR:无法启用会话，因为已达到最大1个活动数据包捕获会话的限制”。
- 无法删除活动的交换机捕获。
- 无法在应用程序上读取交换机捕获。用户必须导出文件。
- 交换机捕获不支持某些数据平面捕获选项，例如dump、decode、packet-number、trace等。
- 对于多情景ASA，交换机在数据接口上的捕获是在用户情景中配置的。只有管理情景支持交换机在in_data_uplink1和in_mgmt_uplink1接口上捕获。

这是基于TAC案例中数据包捕获使用情况的最佳实践列表：

- 了解准则和限制。
- 使用捕获过滤器。
- 配置捕获过滤器时，考虑NAT对数据包IP地址的影响。
- 增加或减少用于指定帧大小的`packet-length`，以防其与默认值1518字节不同。更短的大小导致捕获的数据包数量增加，反之亦然。
- 根据需要调整缓冲区大小。
- 请注意`show cap <cap_name> detail`命令输出中的Drop Count。一旦达到缓冲区大小限制，丢弃计数计数器就会增加。

相关信息

- [Firepower 4100/9300机箱管理器和FXOS CLI配置指南](#)
- [Cisco Secure Firewall 3100入门指南](#)
- [Cisco Firepower 4100/9300 FXOS命令参考](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。