配置和验证安全防火墙和Firepower内部交换机捕获

目录

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。

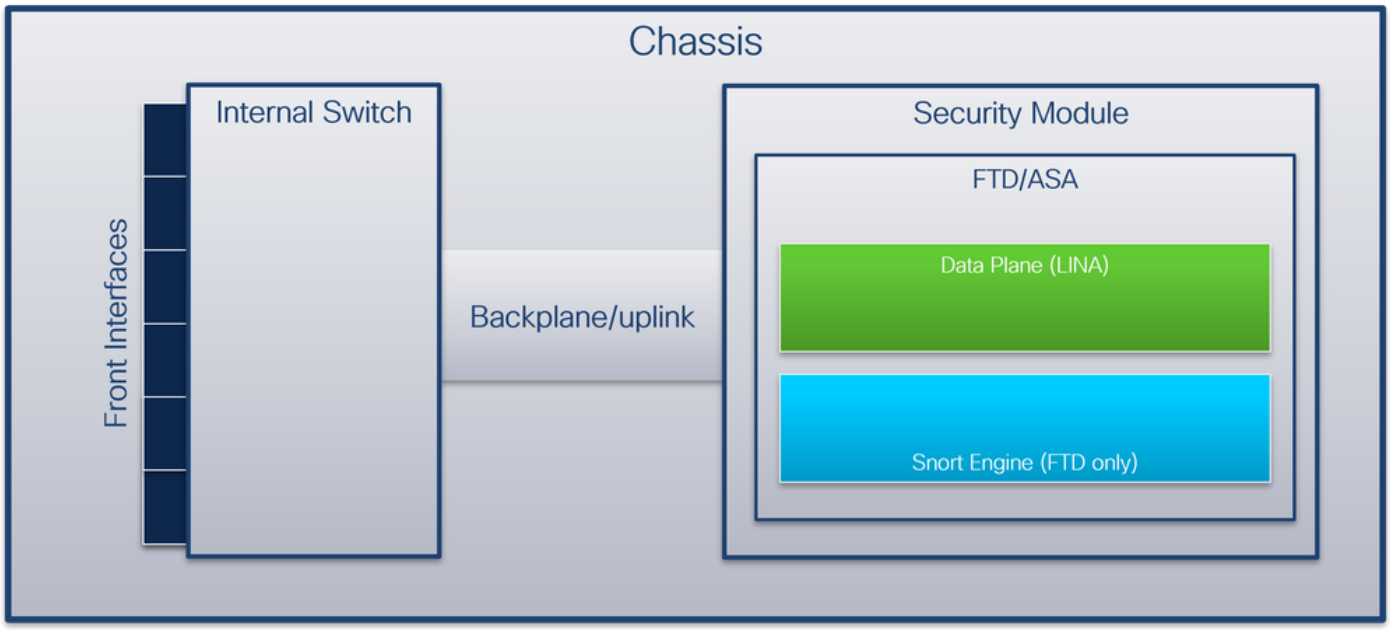
本文档中的信息基于以下软件和硬件版本：

- 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
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 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

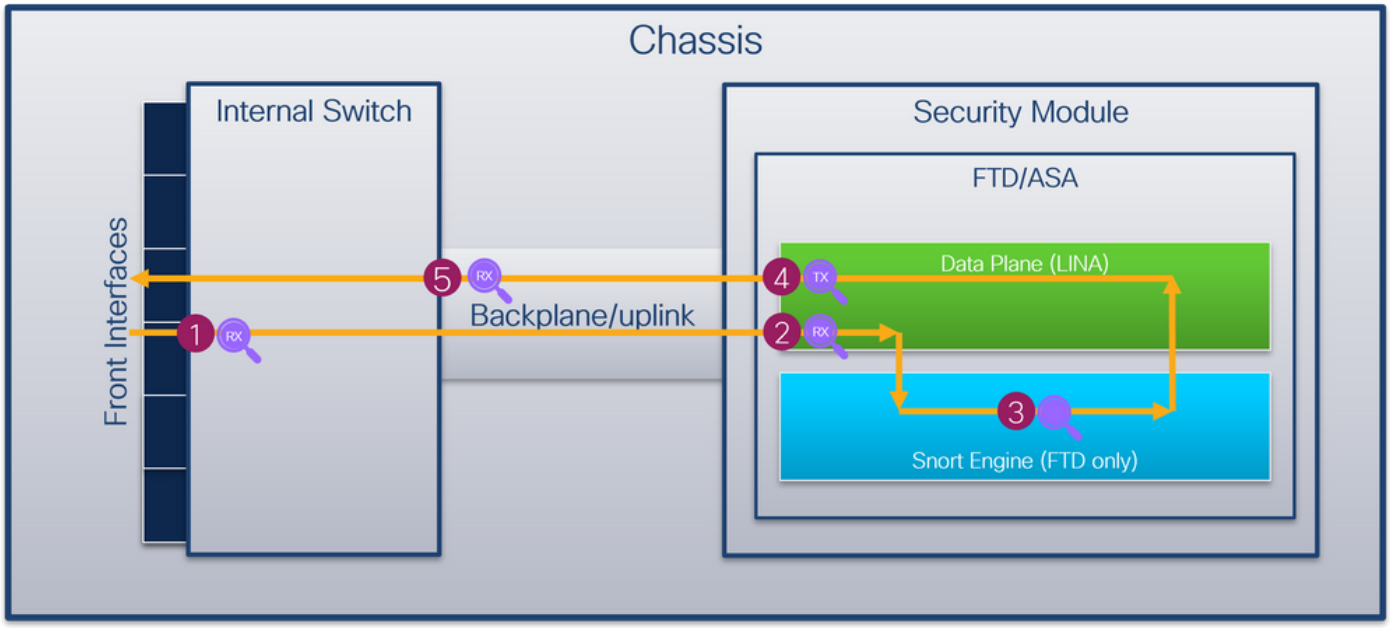
与Firepower 4100/9300类似，内部交换机使用端口VLAN标记来标识接口。

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

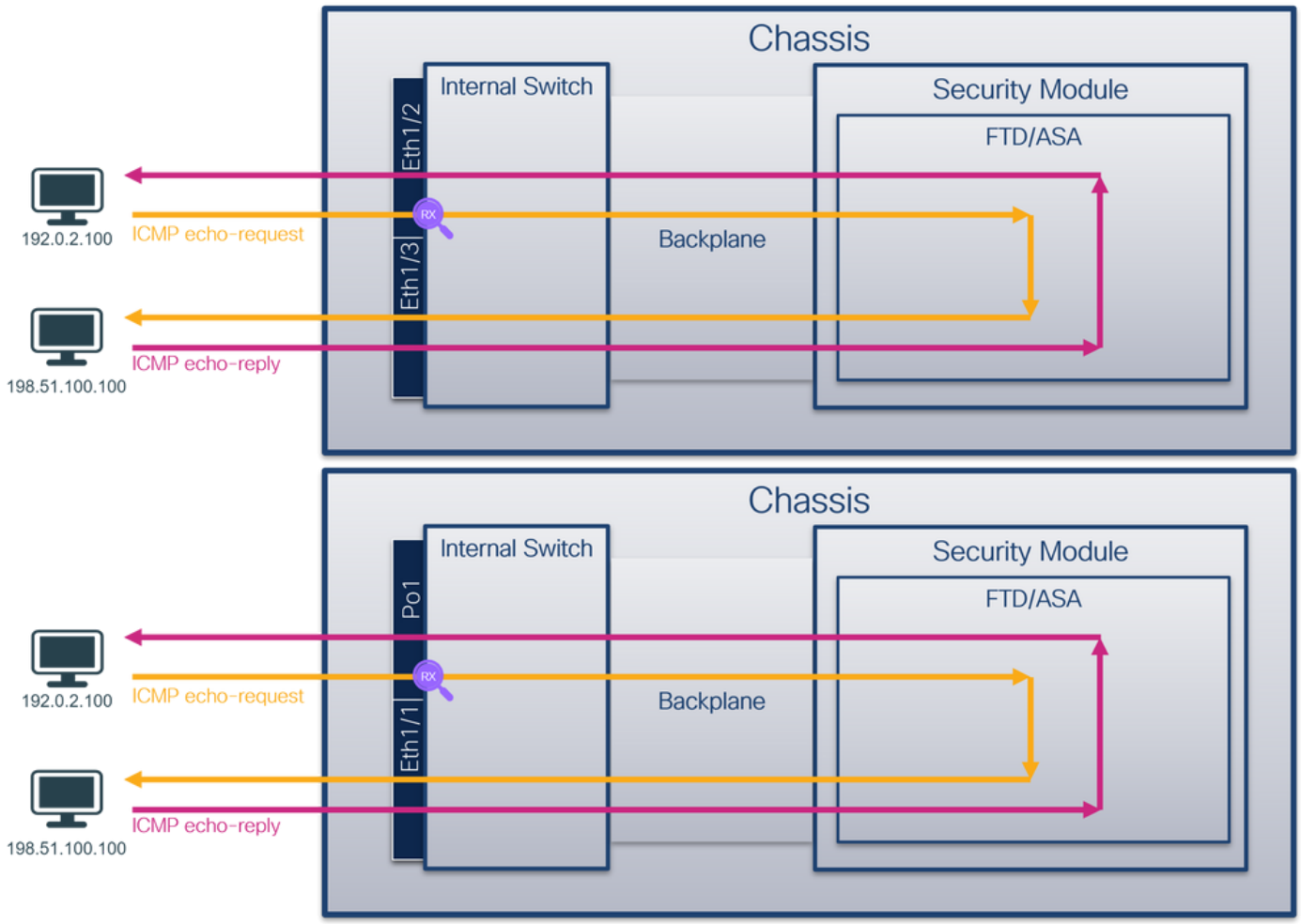
Firepower 4100/9300内部交换机捕获可以在FCM上的**Tools > Packet Capture**中配置，或在**FXOS CLI中的**scope packet-capture中配置。**有关数据包捕获选项的说明，请参阅***Cisco Firepower 4100/9300 FXOS机箱管理器配置指南*或*Cisco Firepower 4100/9300 FXOS CLI配置指南*一章*故障排除,数据包捕获*一节。

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

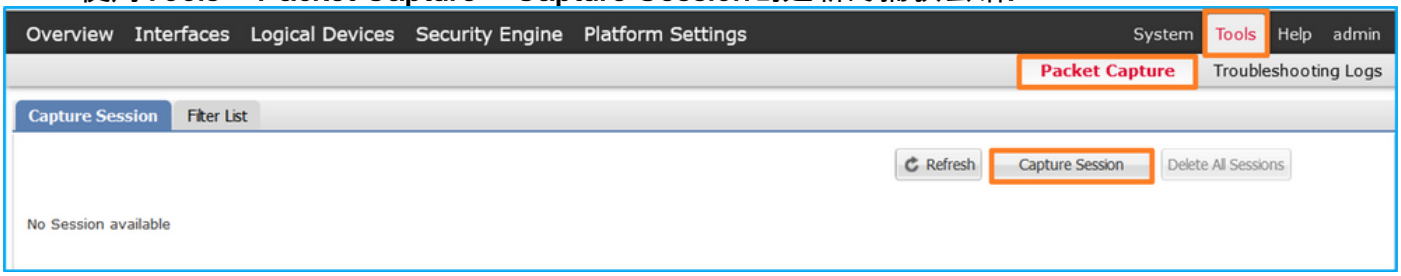


配置

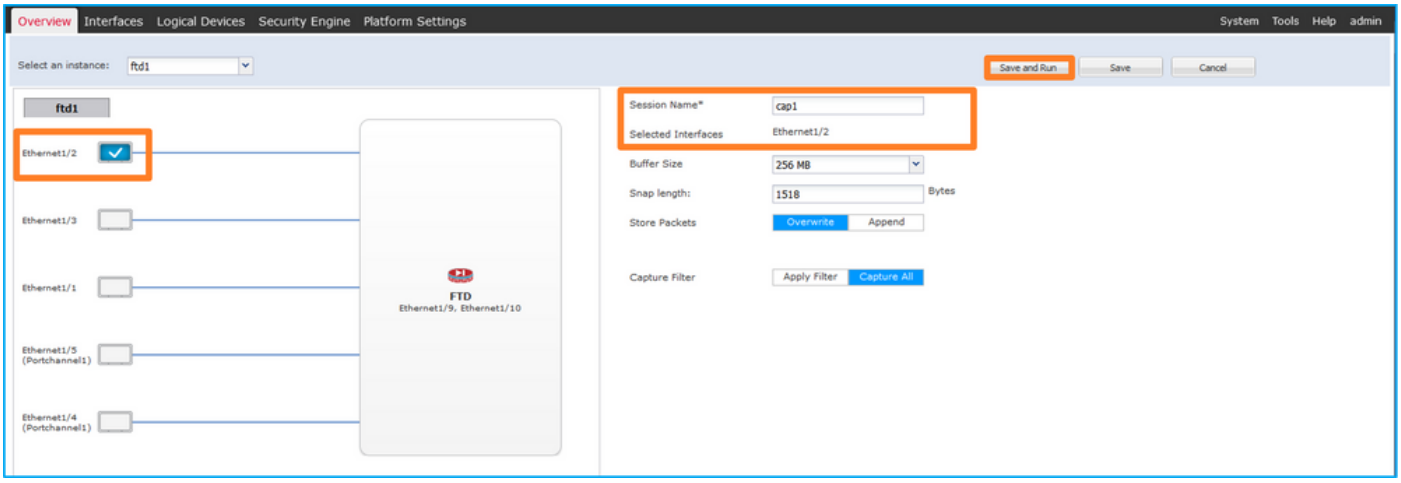
FCM

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

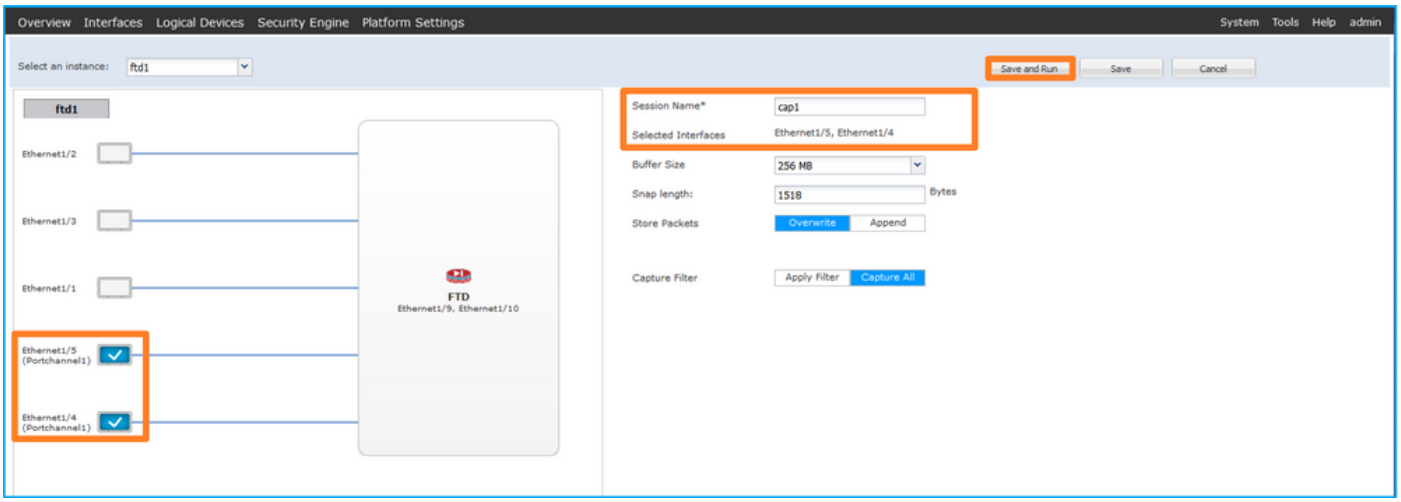
1. 使用**Tools > Packet Capture > Capture Session**创建新的捕获会话:



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 #
```

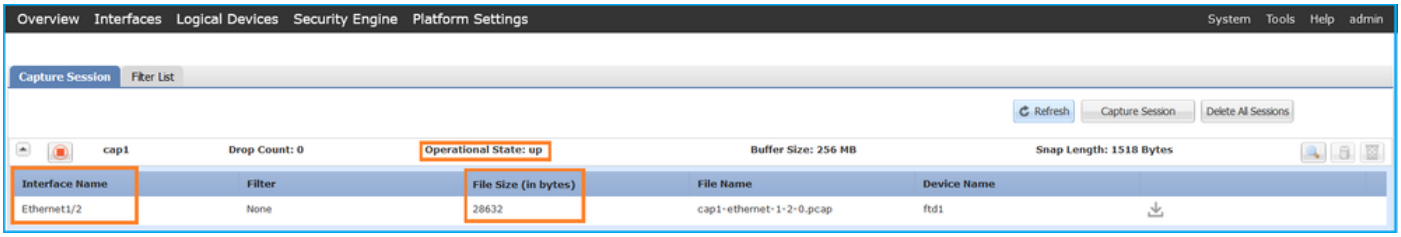
对于端口通道接口，为每个成员接口配置单独的捕获：

```
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 #
```

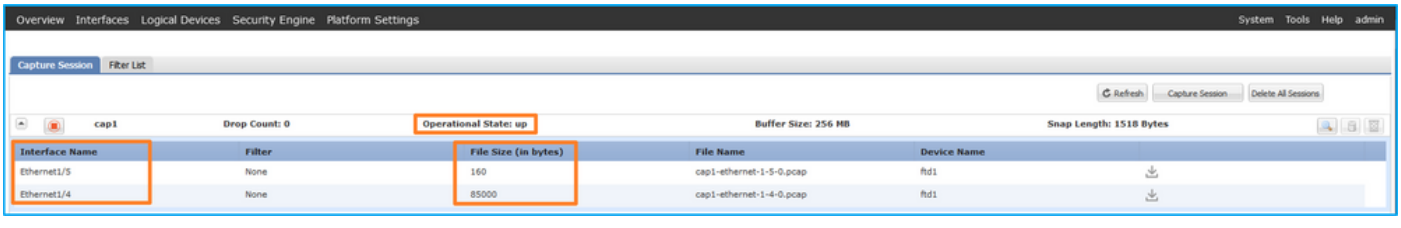
确认

FCM

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



具有成员接口Ethernet1/4和Ethernet1/5的Portchannel1:



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
```

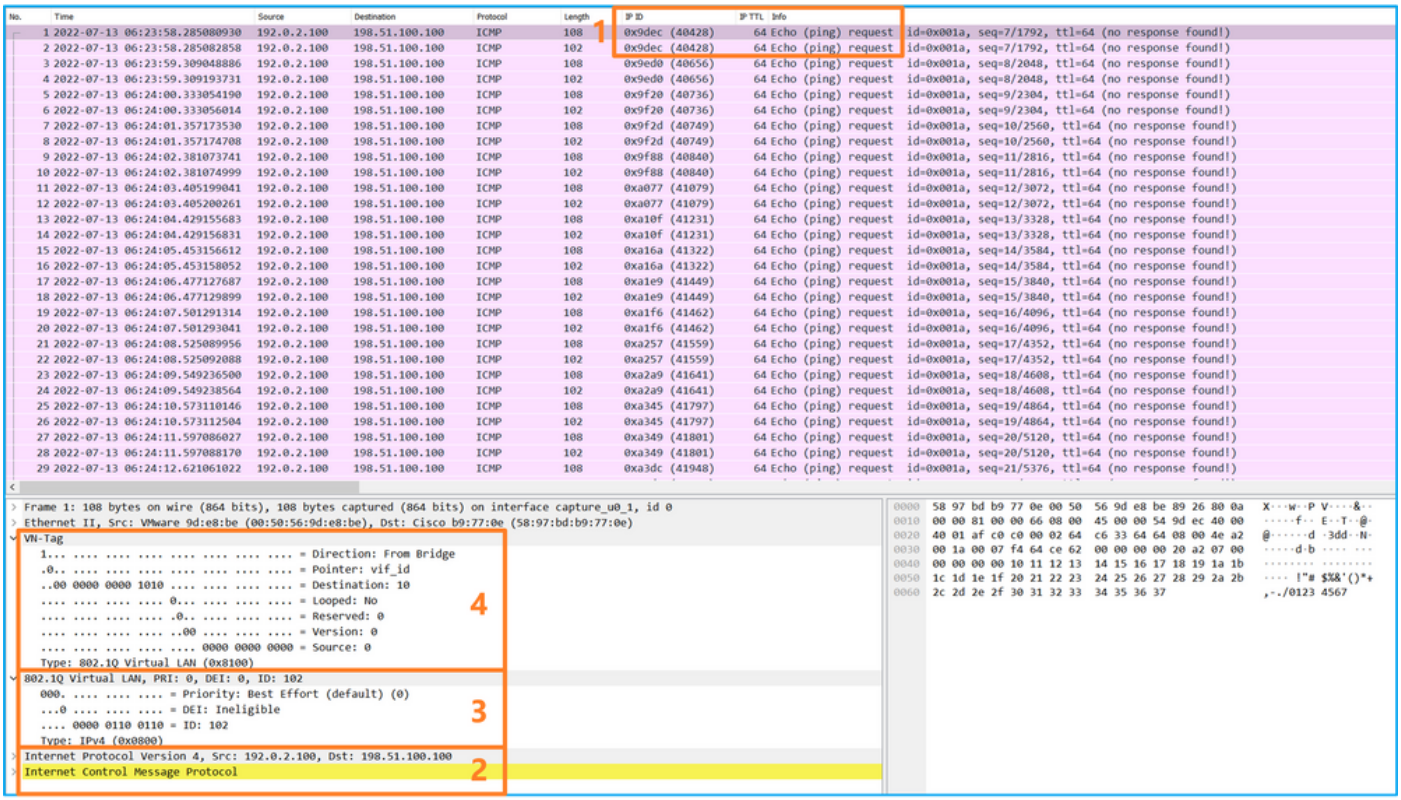
收集捕获文件

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

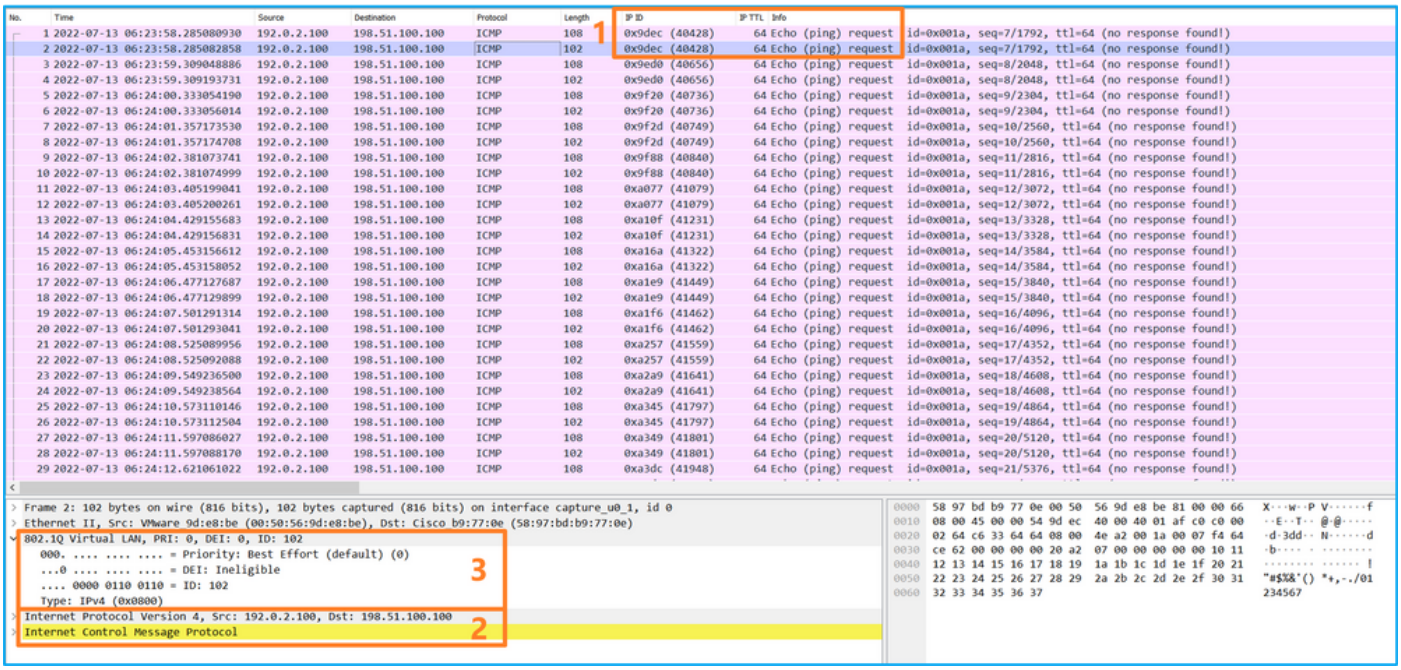
使用数据包捕获文件读取器应用程序打开Ethernet1/2的捕获文件。选择第一个数据包并检查要点：

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。



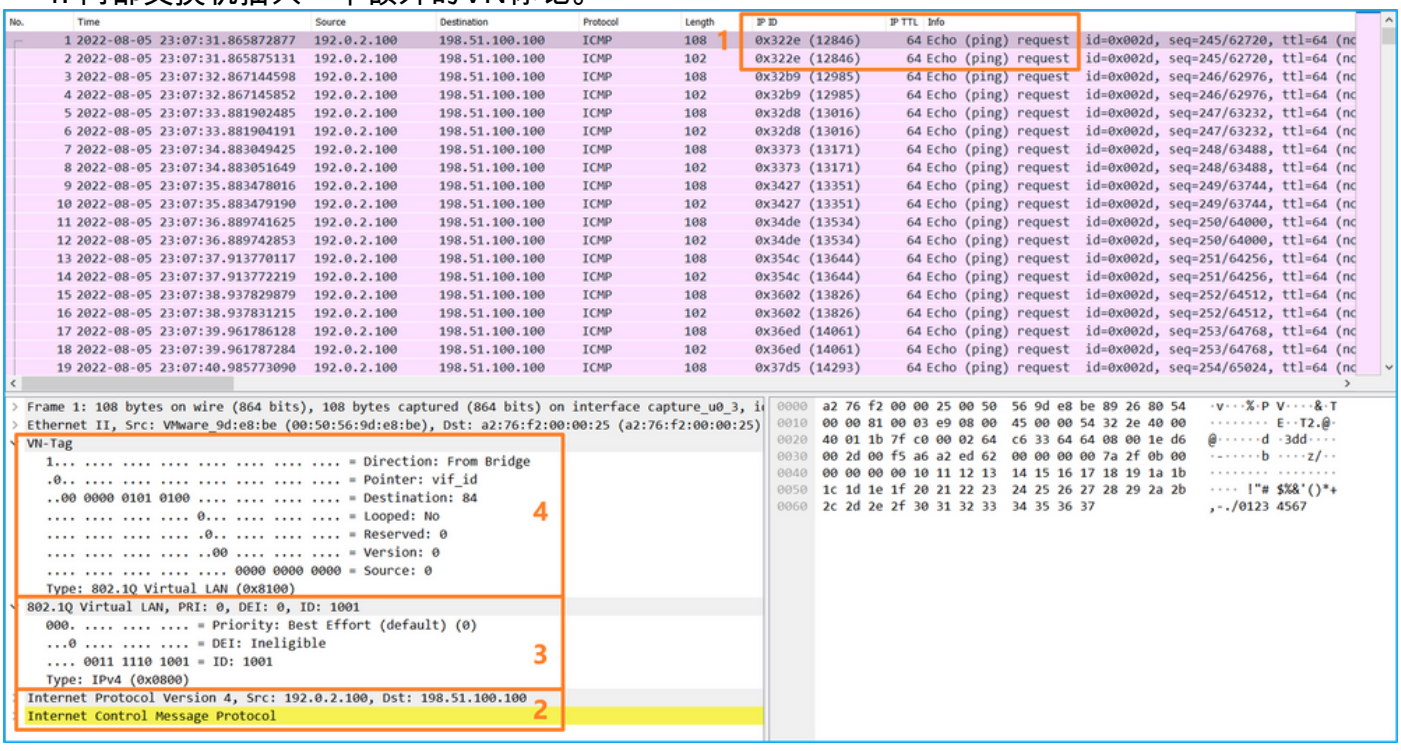
选择第二个数据包并检查要点：

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**。



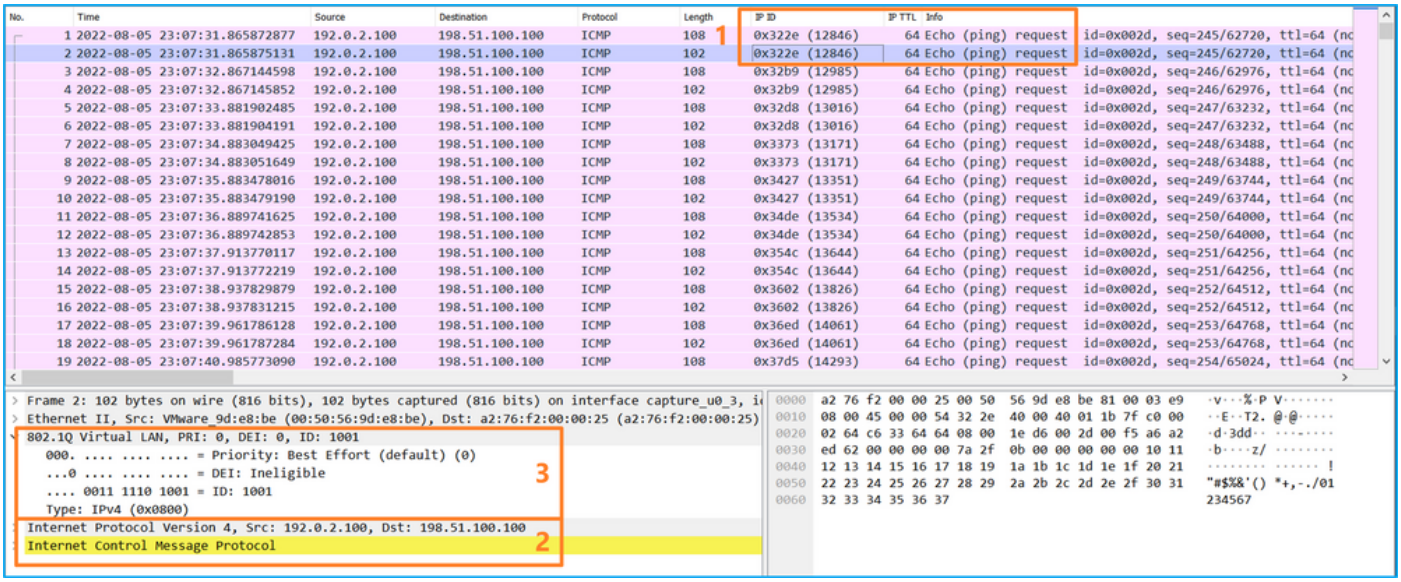
打开Portchannel1成员接口的捕获文件。选择第一个数据包并检查要点：

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。



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。

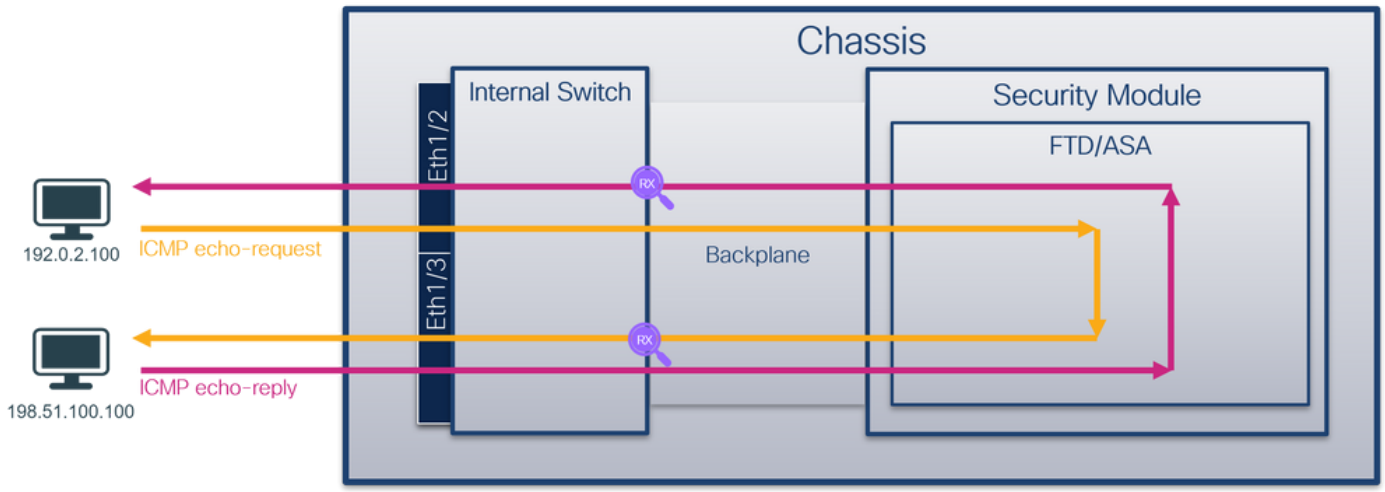
此表概述了任务：

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

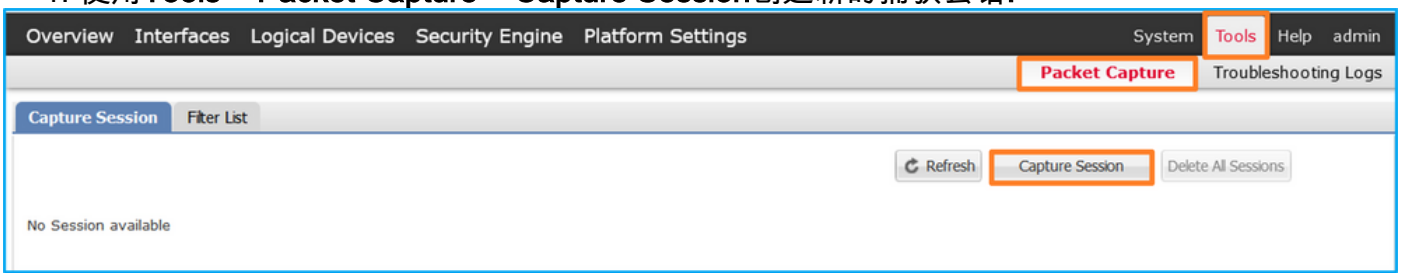


配置

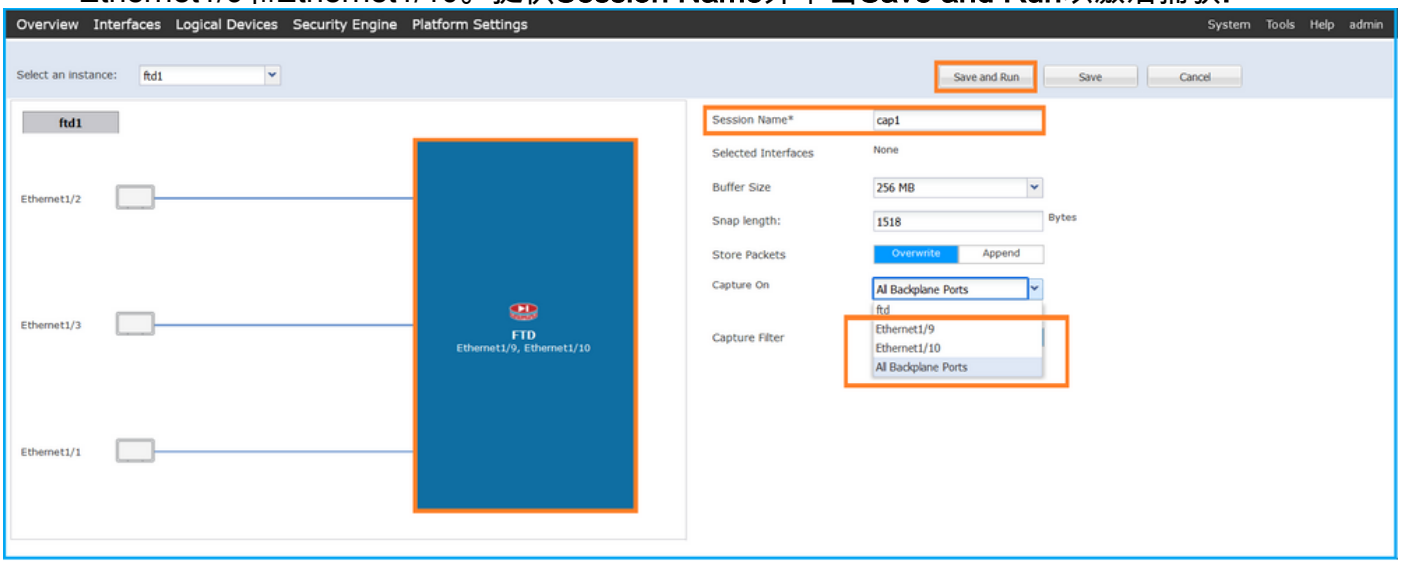
FCM

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
```

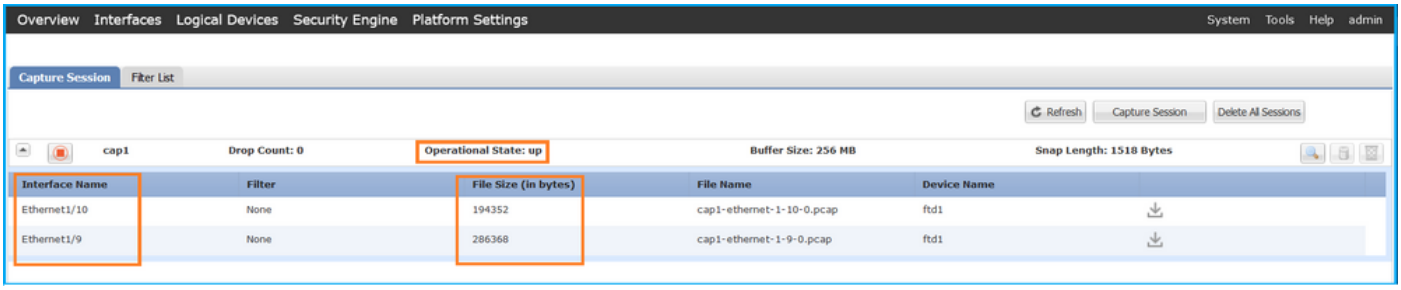
2. 创建捕获会话：

```
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：



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

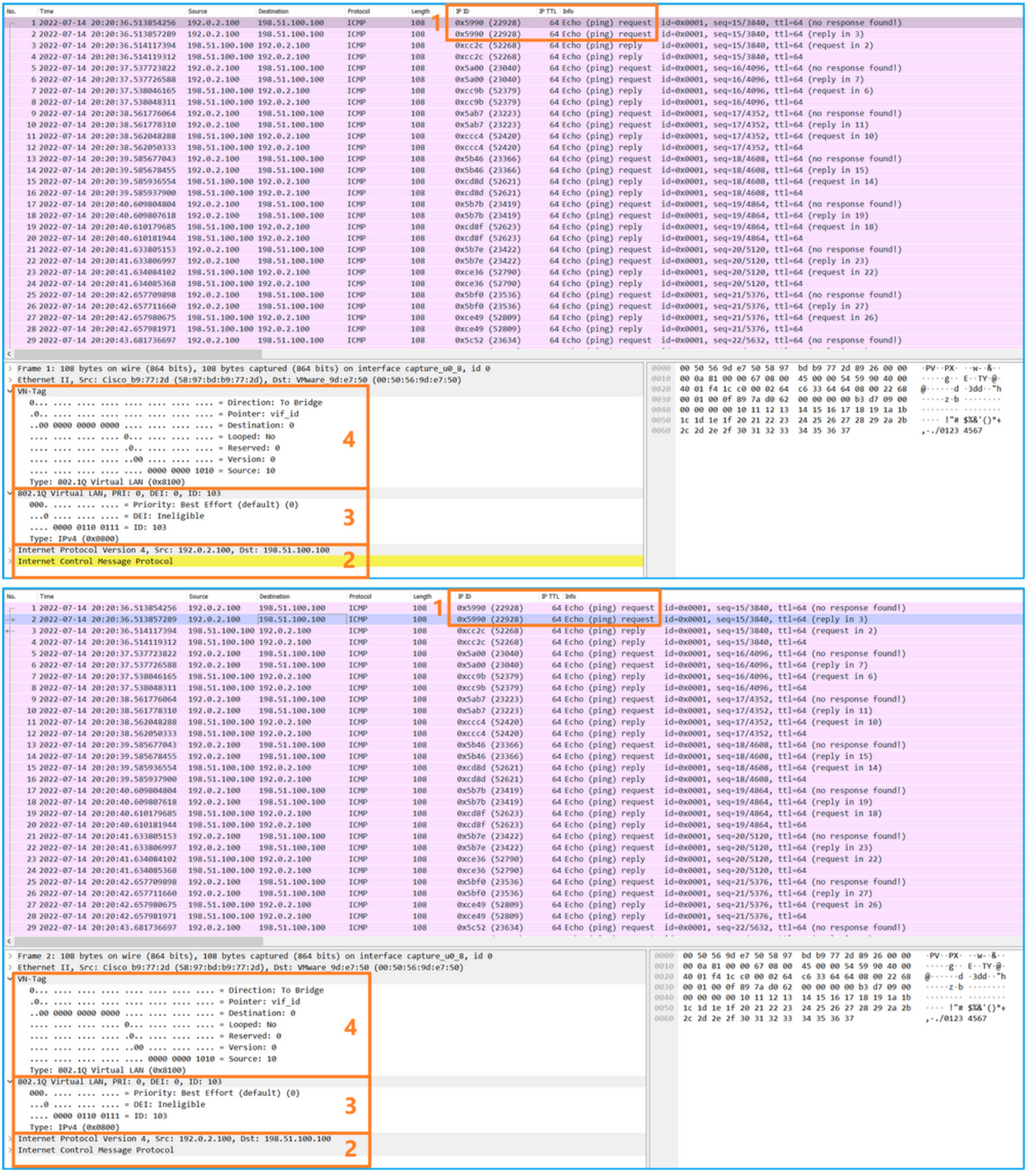
按照**收集Firepower 4100/9300内部交换机捕获文件**部分中的步骤进行操作。

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。

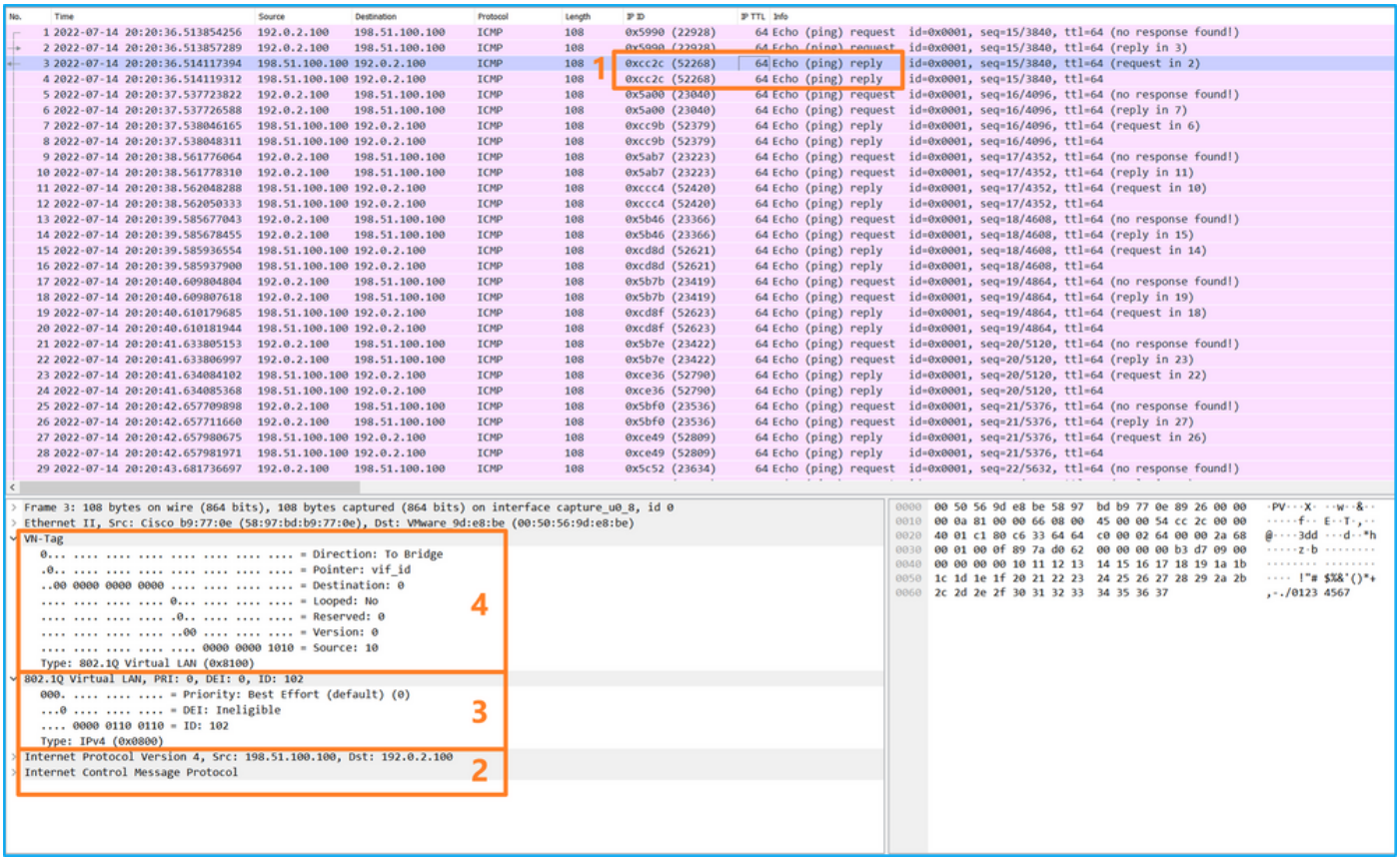
选择第一个和第二个数据包，并检查要点：

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。



选择第三个和第四个数据包，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。



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：

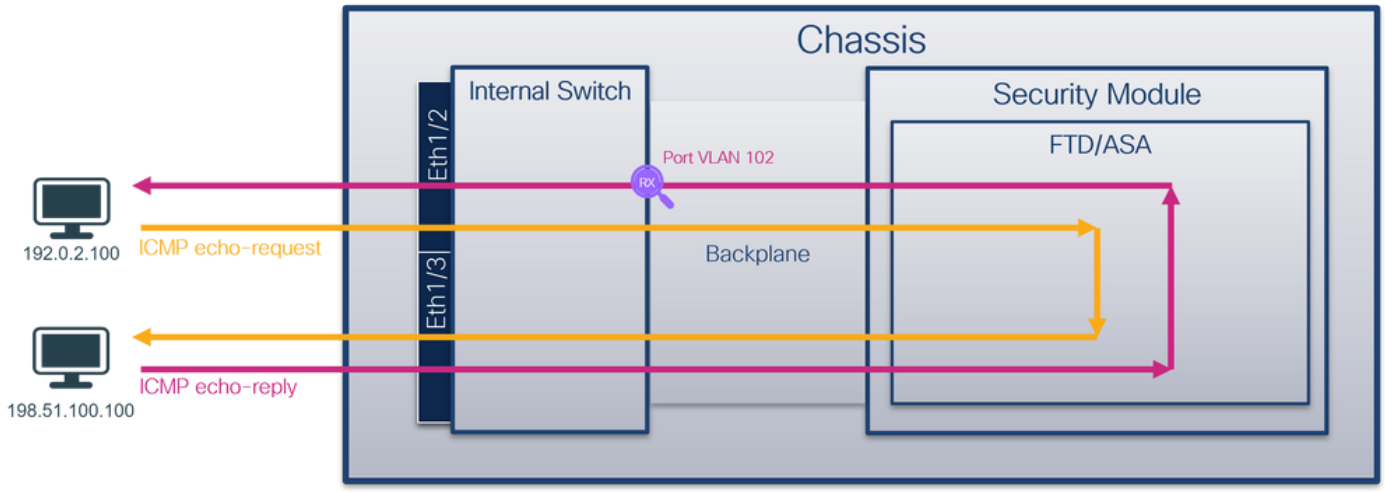
- 为离开特定前接口的数据包配置背板接口上的数据包捕获。例如，在背板接口Ethernet1/9上为离开接口Ethernet1/2的数据包配置数据包捕获。
- 在特定前接口和背板接口上配置同步数据包捕获。例如，在接口Ethernet1/2和背板接口Ethernet1/9上为离开接口Ethernet1/2的数据包配置同步数据包捕获。

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

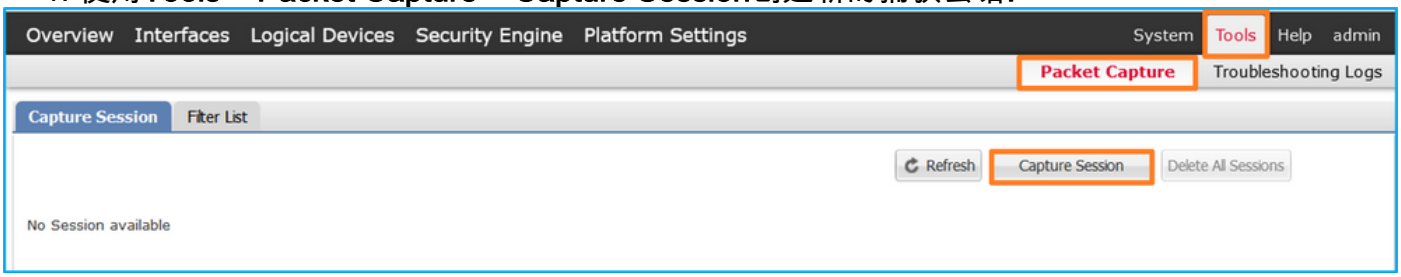


配置

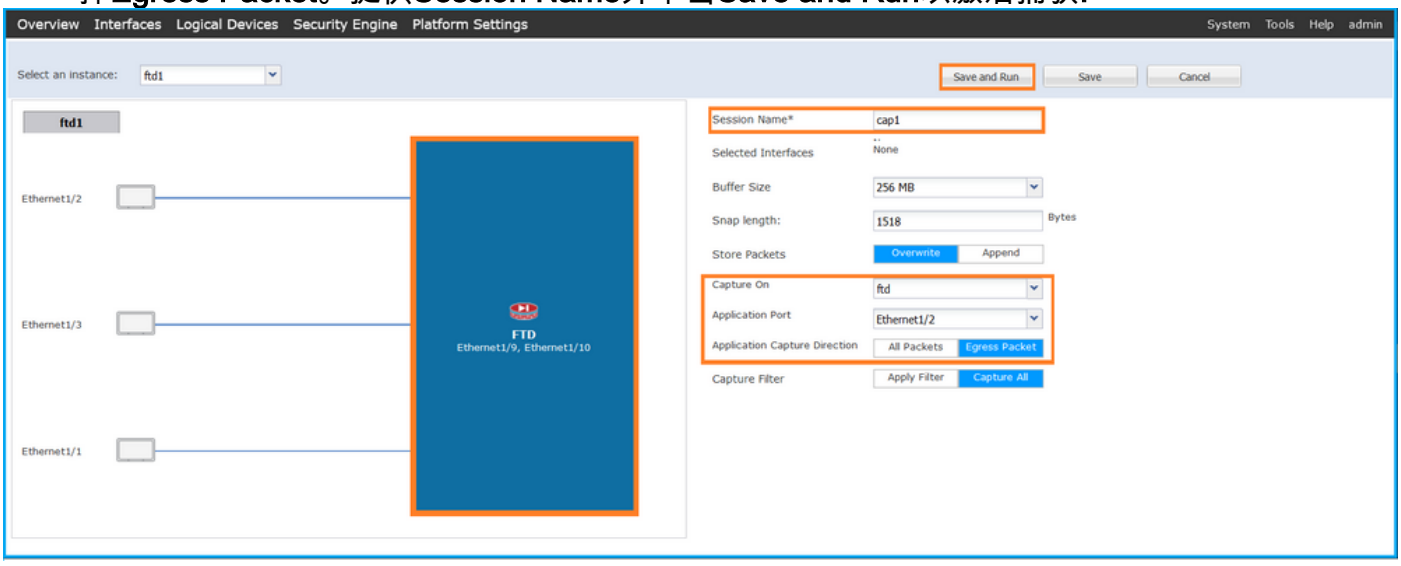
FCM

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
```

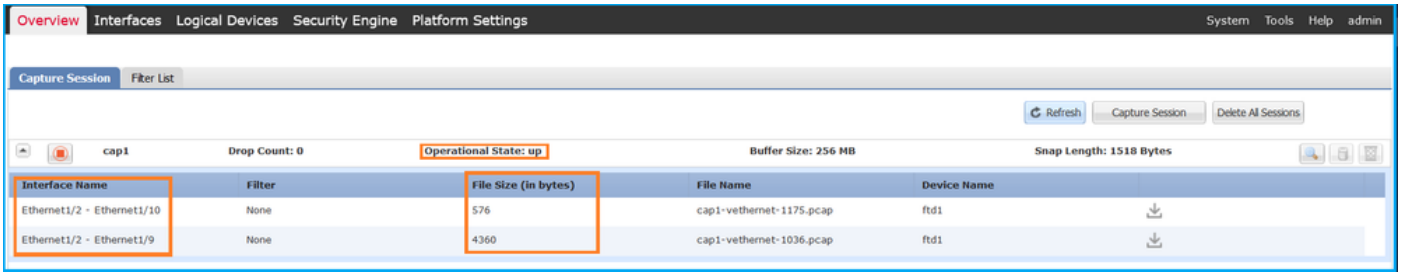
2. 创建捕获会话：

```
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：



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: l12
    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

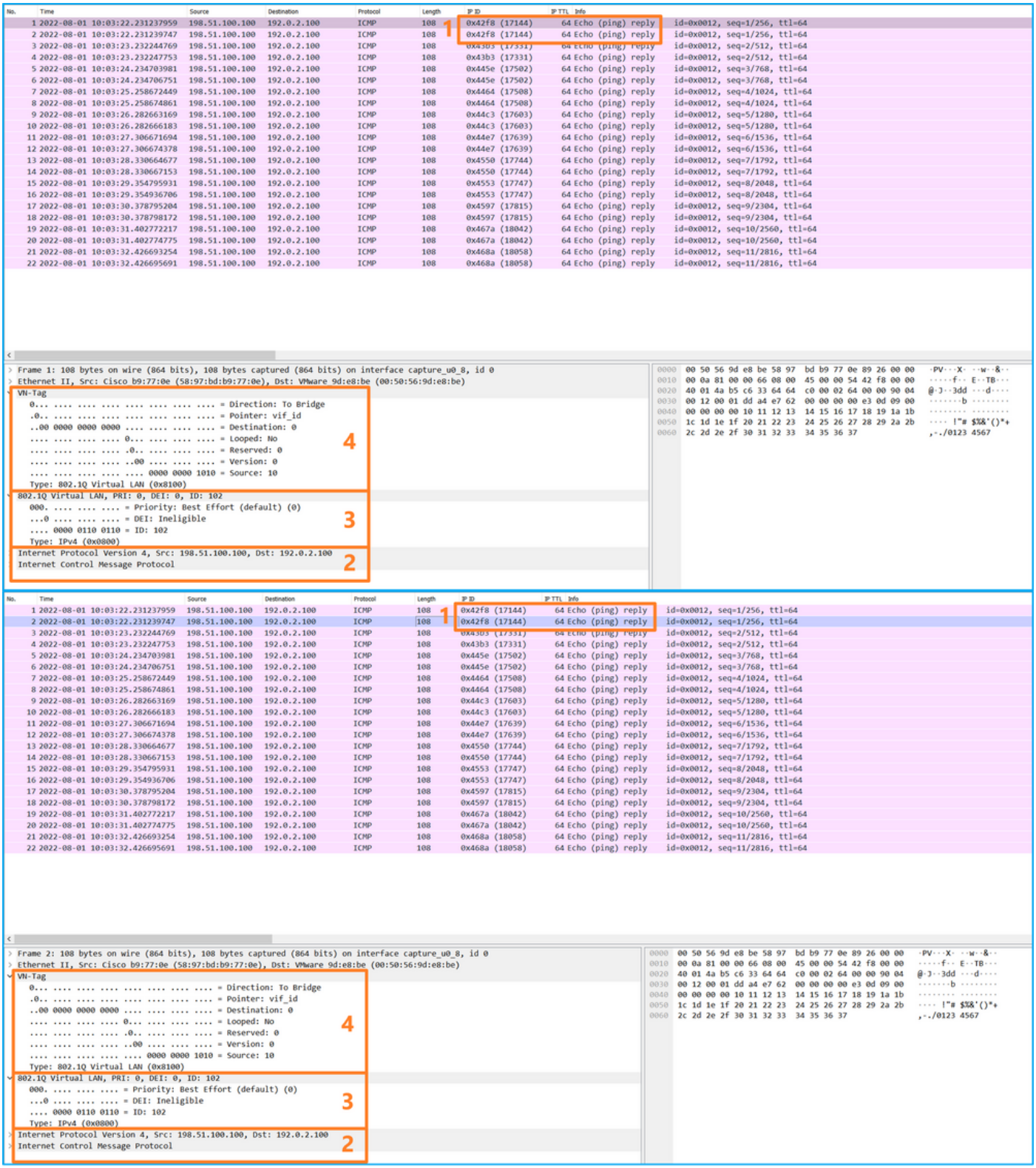
按照**收集Firepower 4100/9300内部交换机捕获文件**部分中的步骤进行操作。

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。



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

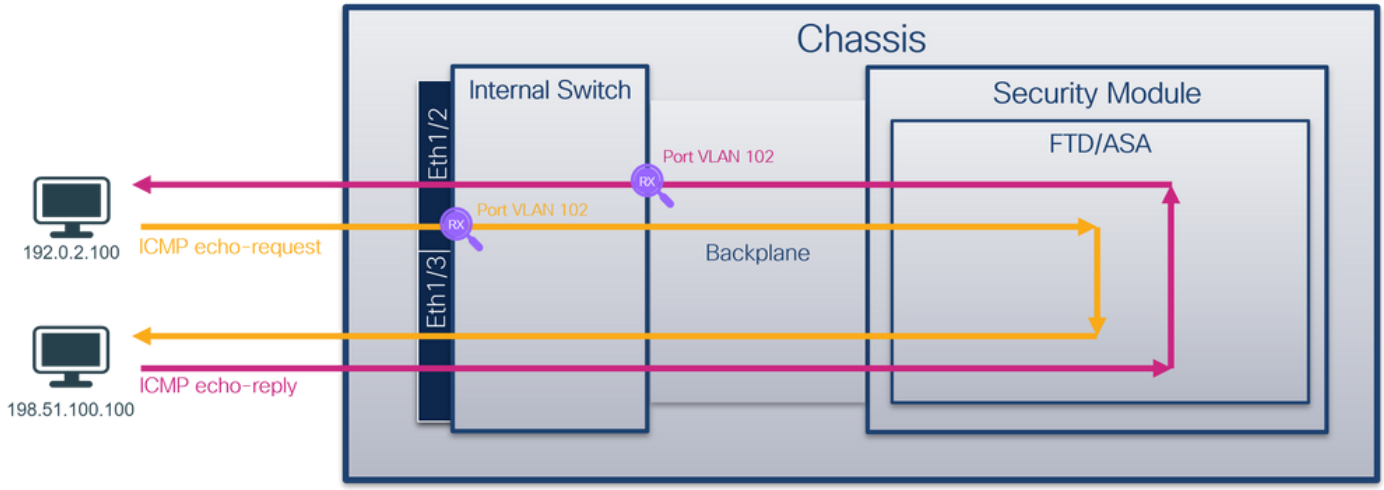
任务2

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

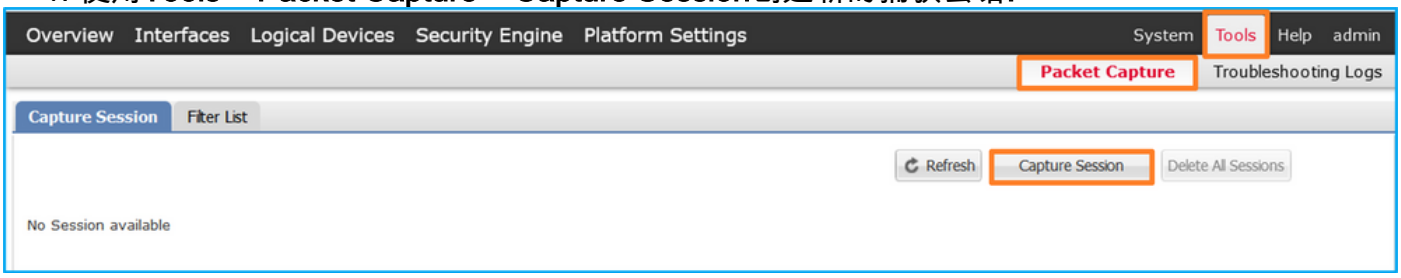


配置

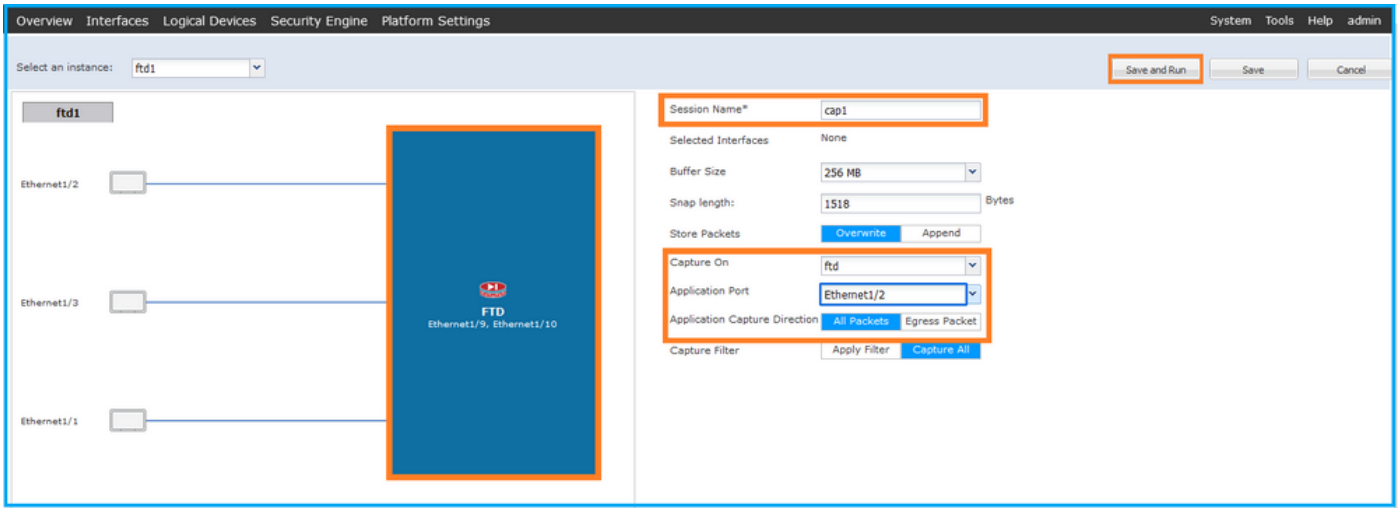
FCM

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
```

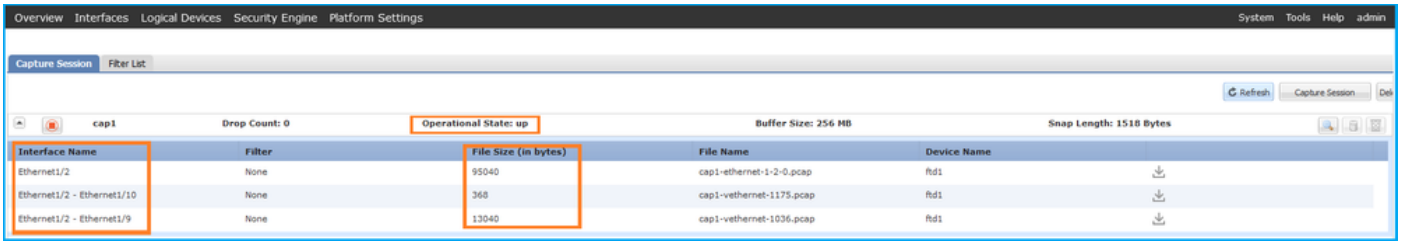
2. 创建捕获会话：

```
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：



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

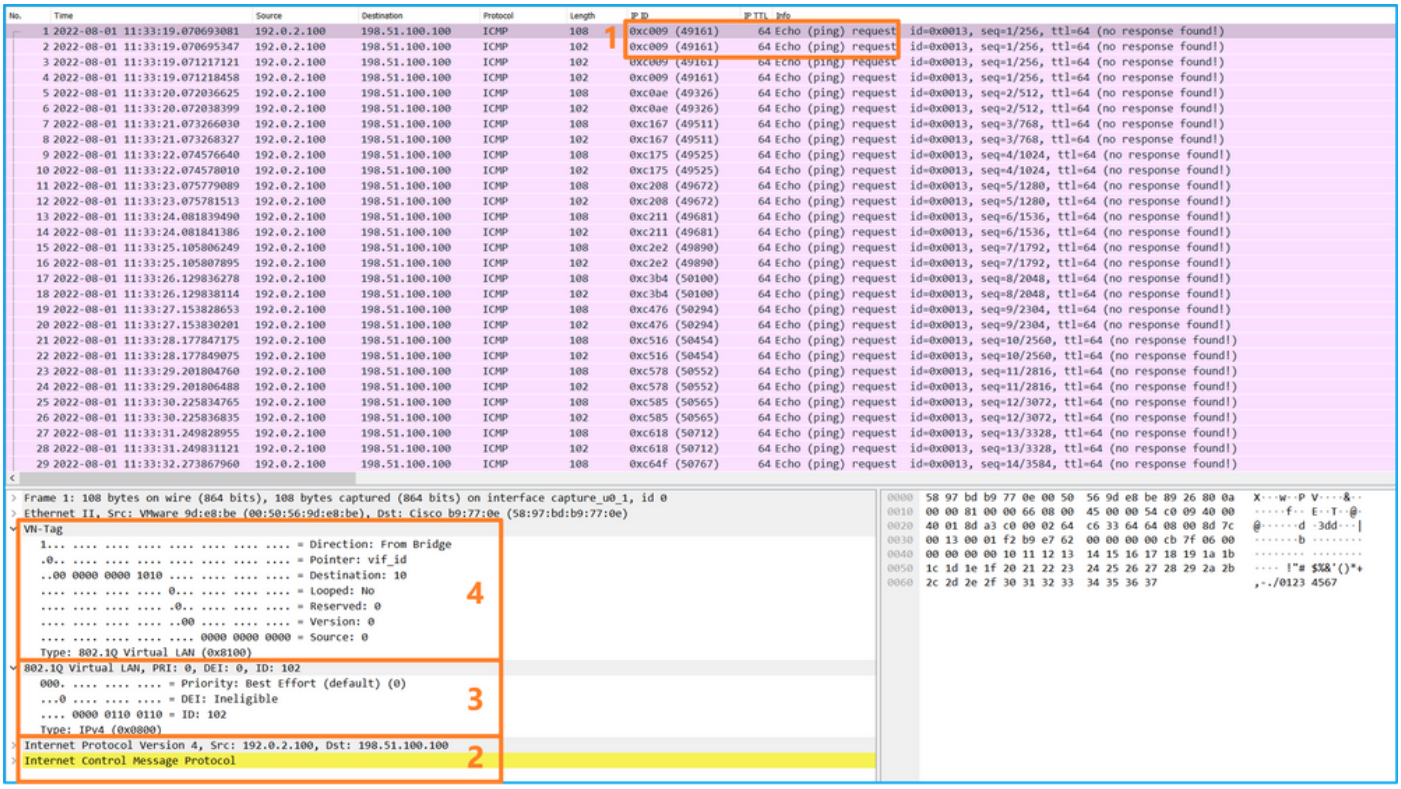
按照**收集Firepower 4100/9300内部交换机捕获文件**部分中的步骤进行操作。

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。

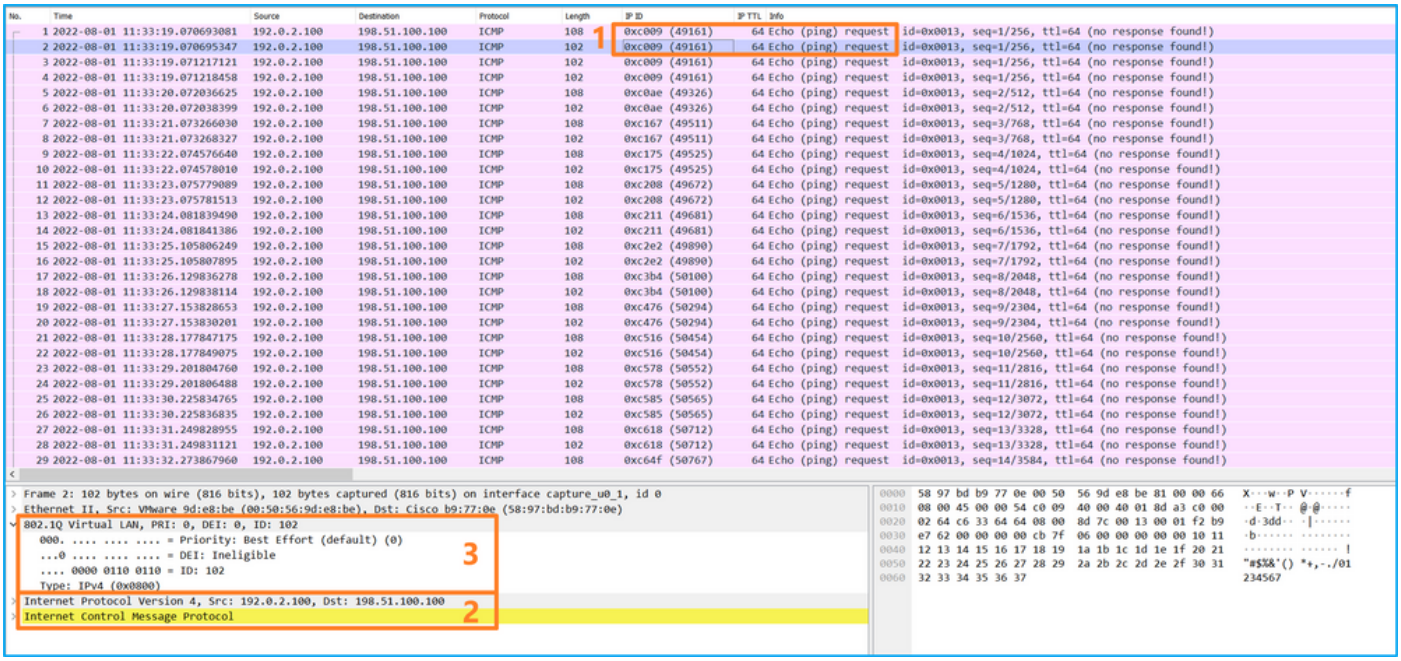
打开接口Ethernet1/2的捕获文件，选择第一个数据包，然后检查要点：

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。



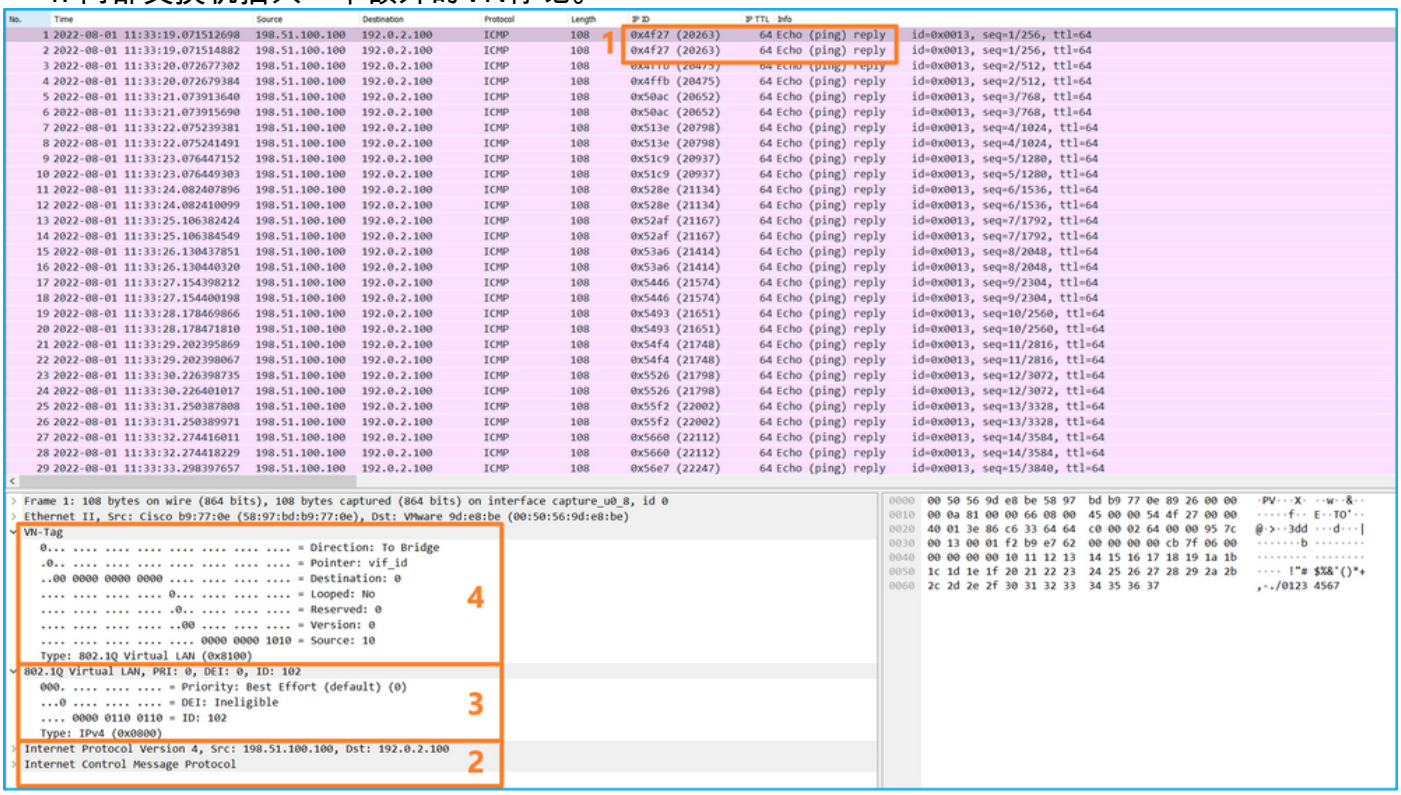
选择第二个数据包并检查要点：

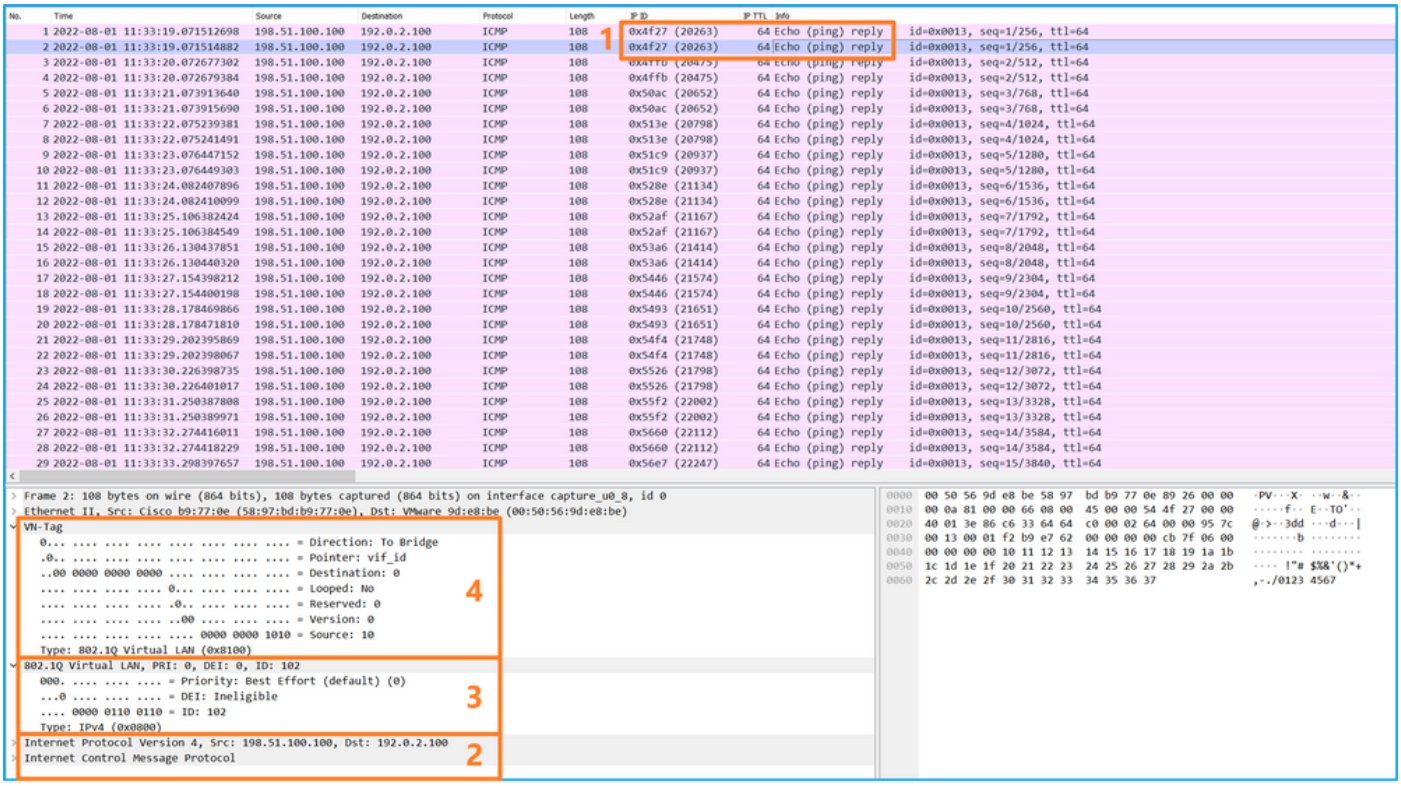
1. 仅捕获ICMP回应请求数据包。捕获每个数据包并显示2次。
2. 原始数据包报头没有VLAN标记。
3. 内部交换机插入标识入口接口Ethernet1/2的额外端口VLAN标记**102**。



打开接口Ethernet1/9的捕获文件，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。





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。

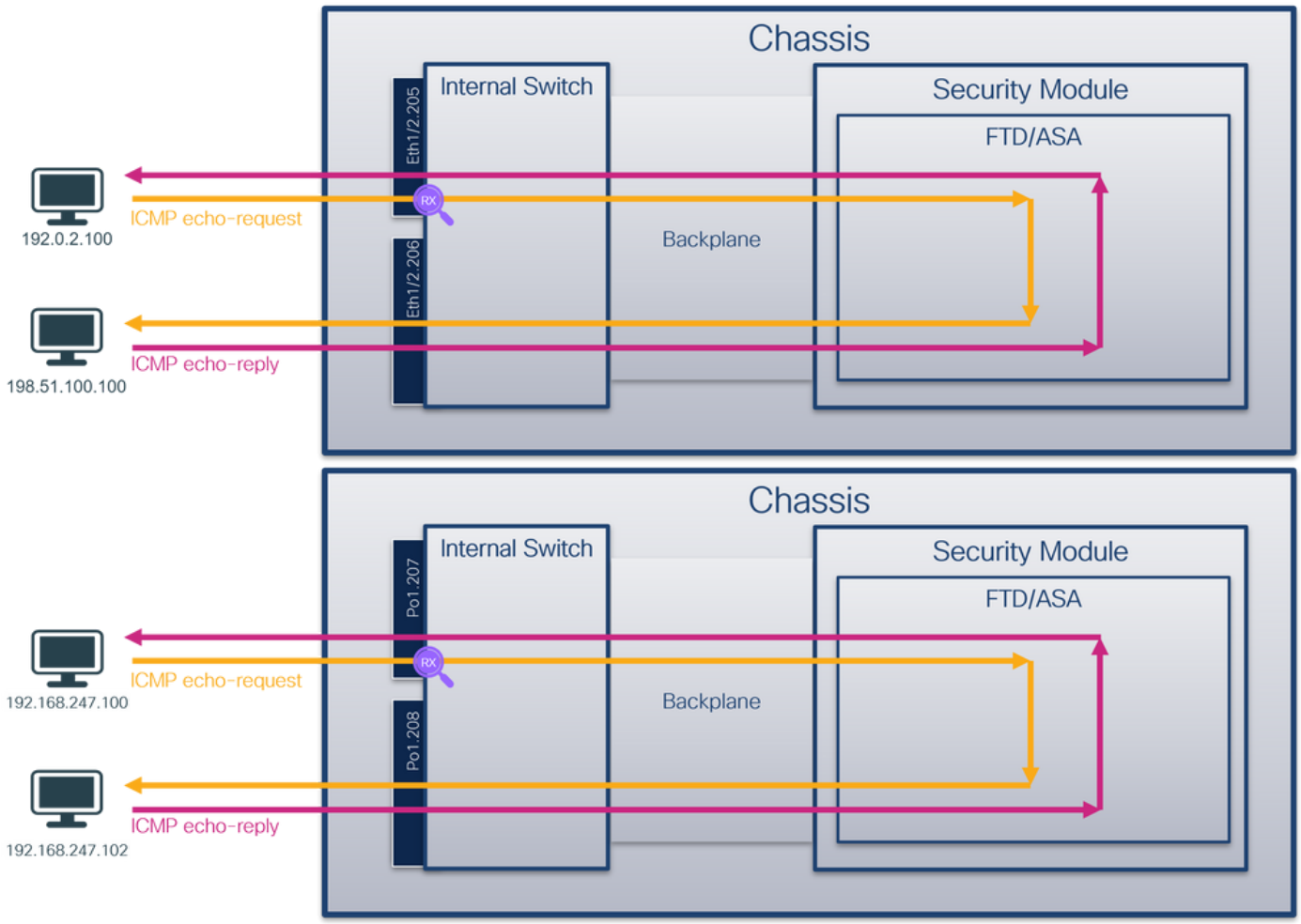
此表概述了任务：

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

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

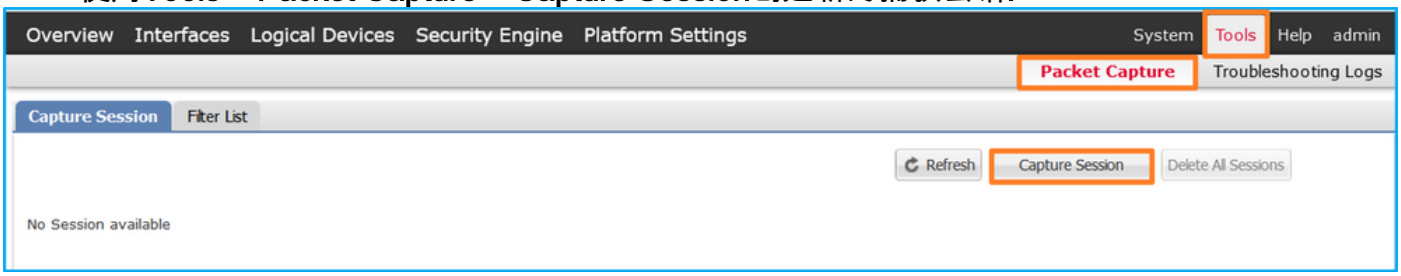


配置

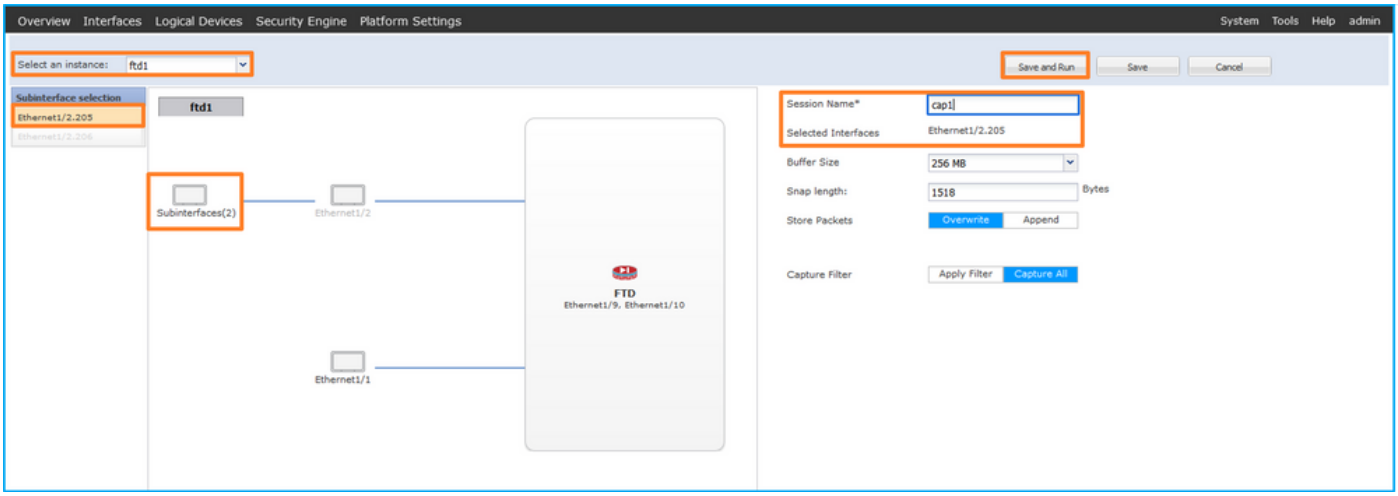
FCM

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：

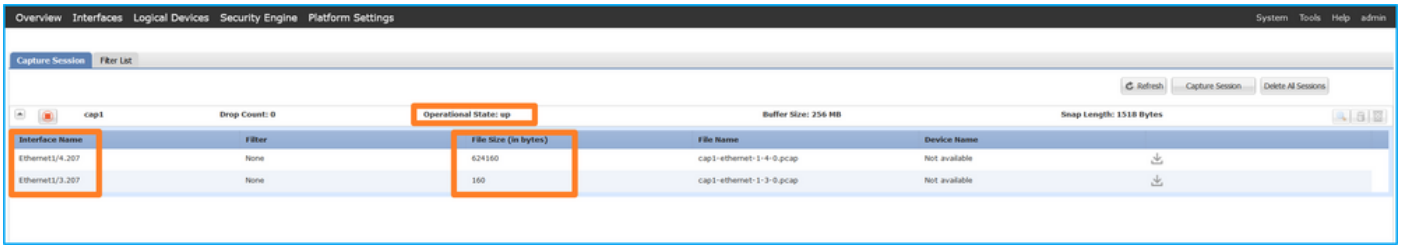
```
firepower#  scope packet-capture
firepower /packet-capture # create filter vlan207
firepower /packet-capture/filter* # set ovlan 207
firepower /packet-capture/filter* # up
firepower /packet-capture* # create session cap1
firepower /packet-capture/session*  create phy-port Eth1/3
firepower /packet-capture/session/phy-port* # 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：

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：



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
```

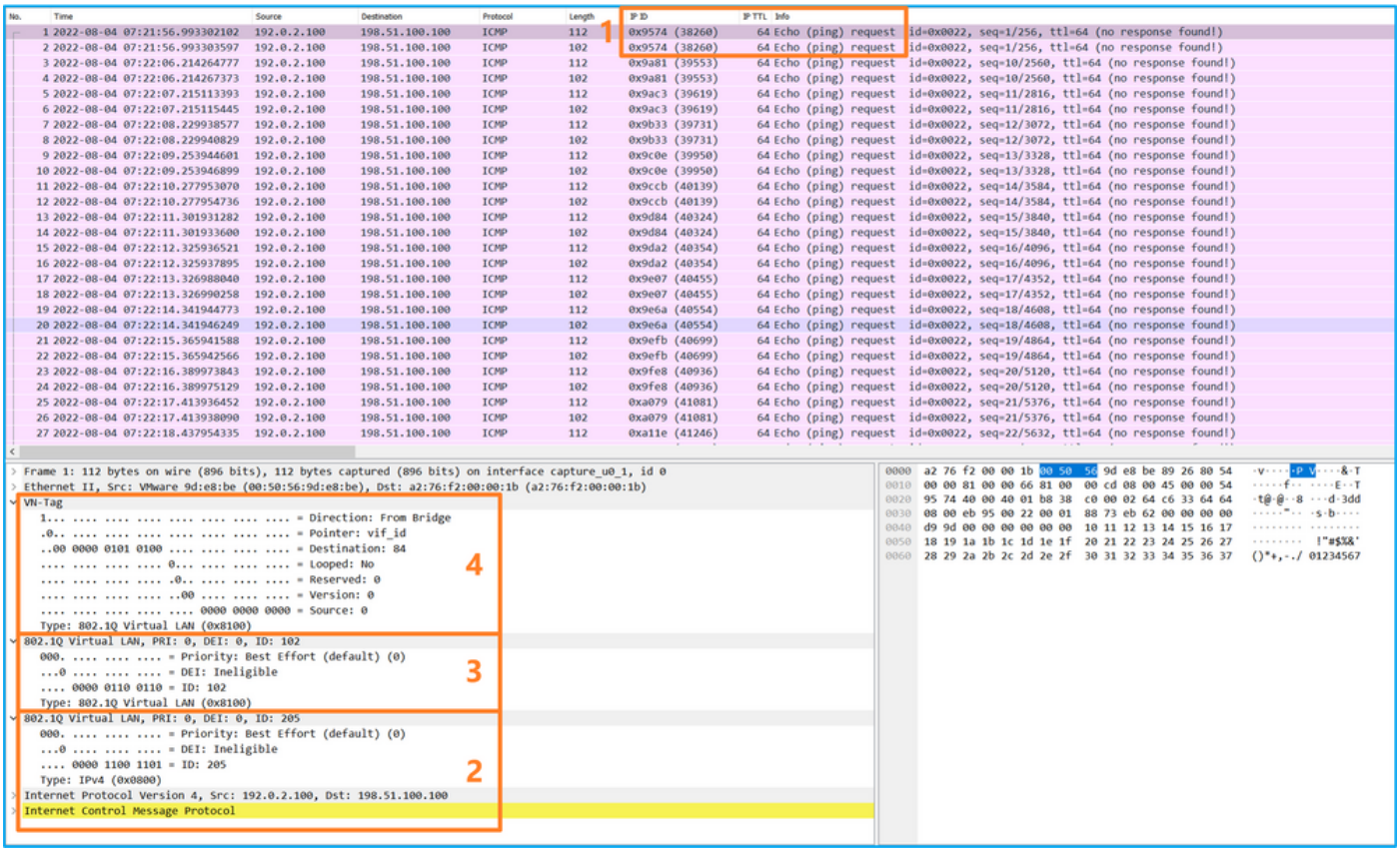
收集捕获文件

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

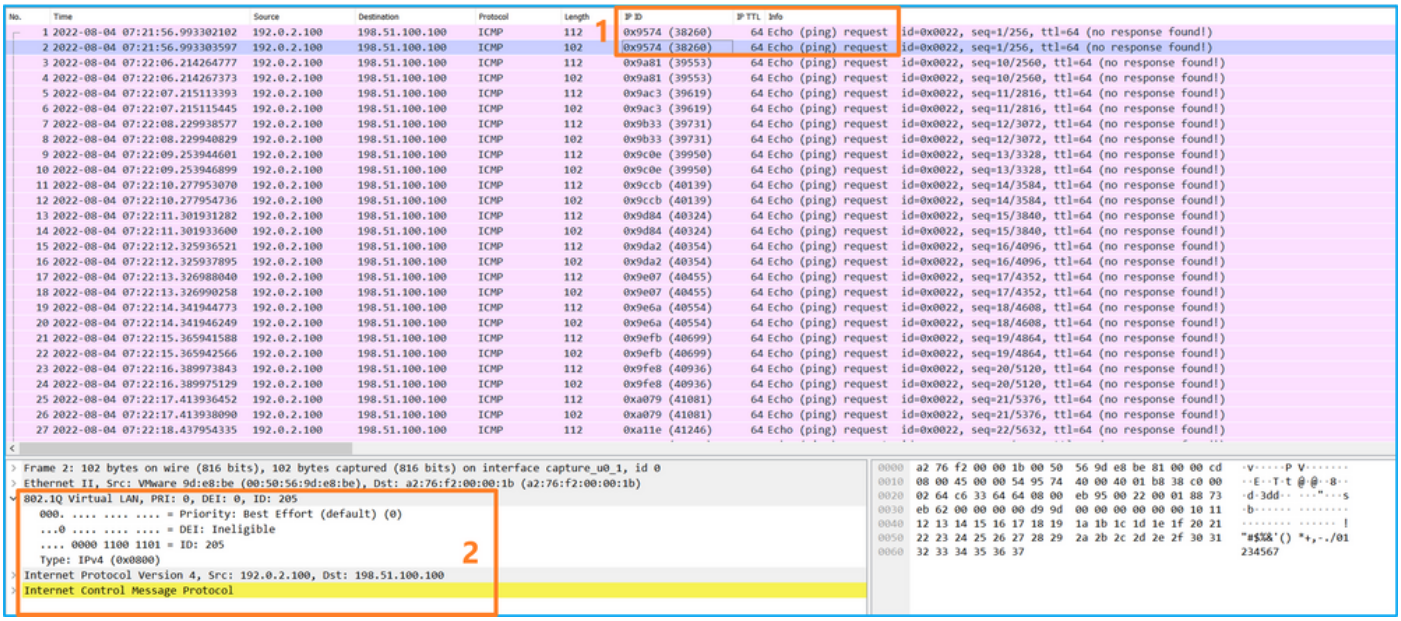
使用数据包捕获文件读取器应用程序打开捕获文件。选择第一个数据包并检查要点：

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。



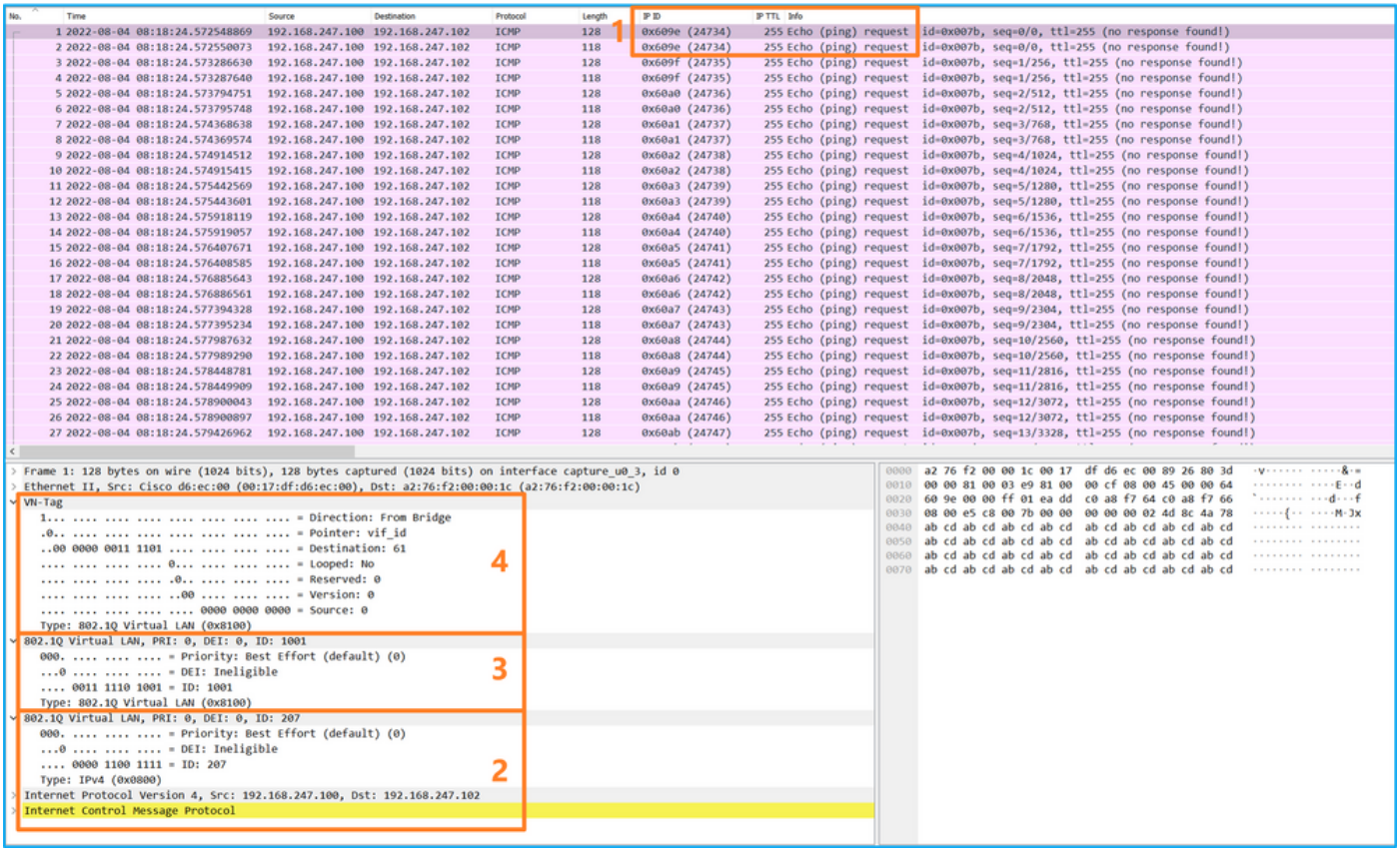
选择第二个数据包并检查要点：

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**。



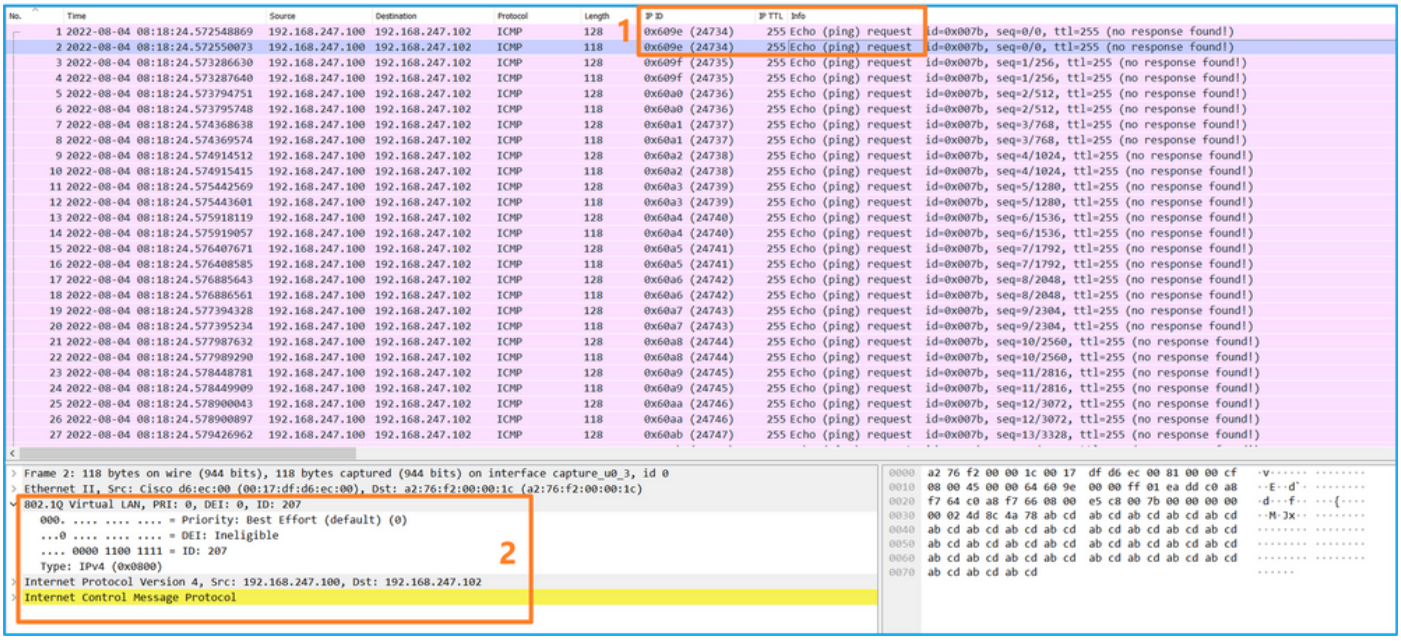
现在打开Portchannel1.207的捕获文件。选择第一个数据包并检查要点

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。

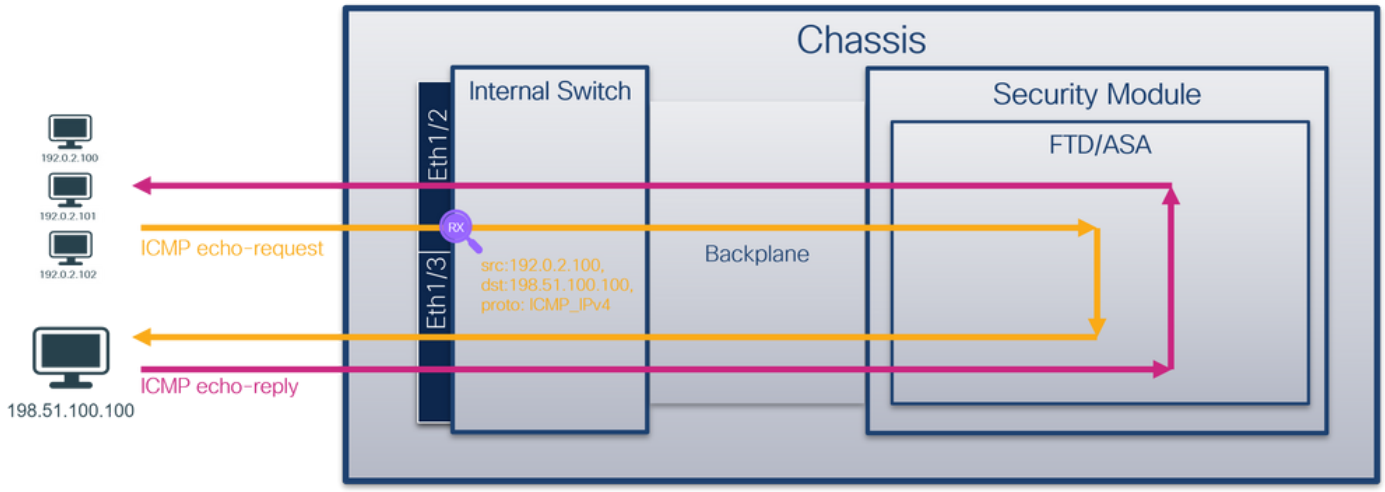
此表概述了任务：

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

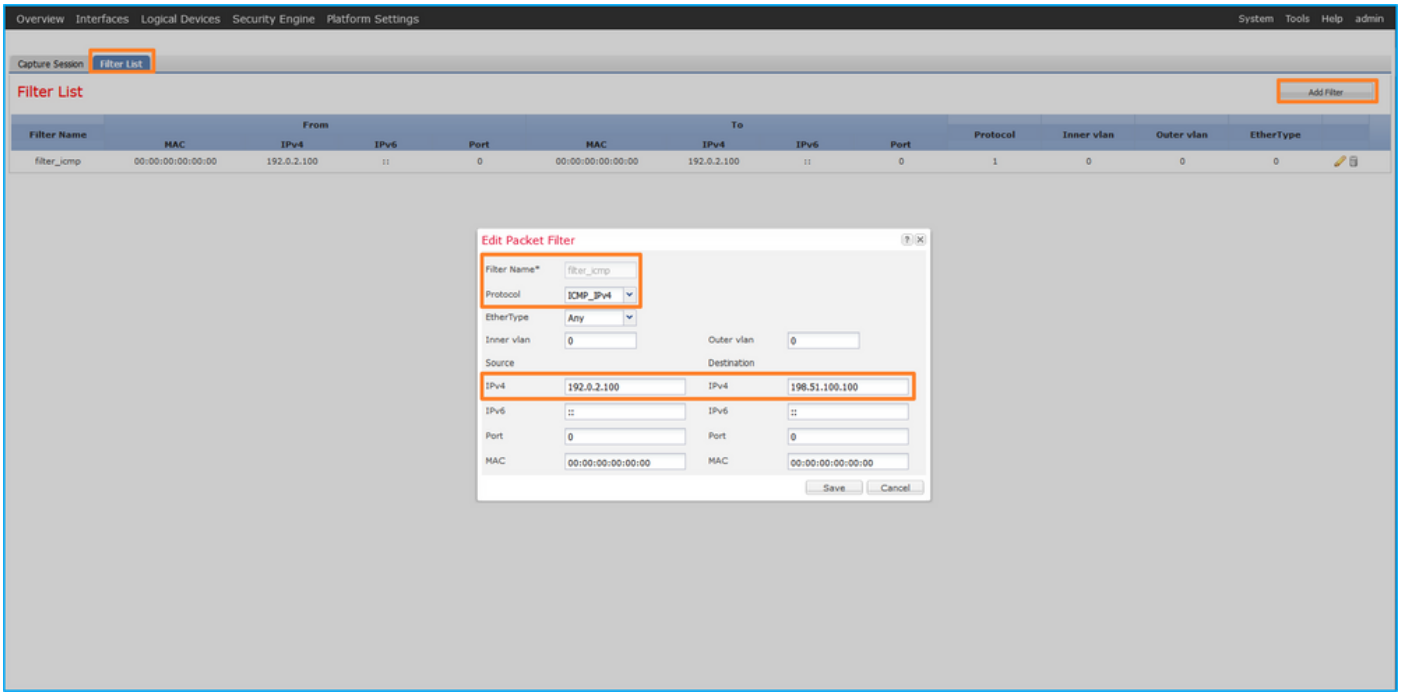


配置

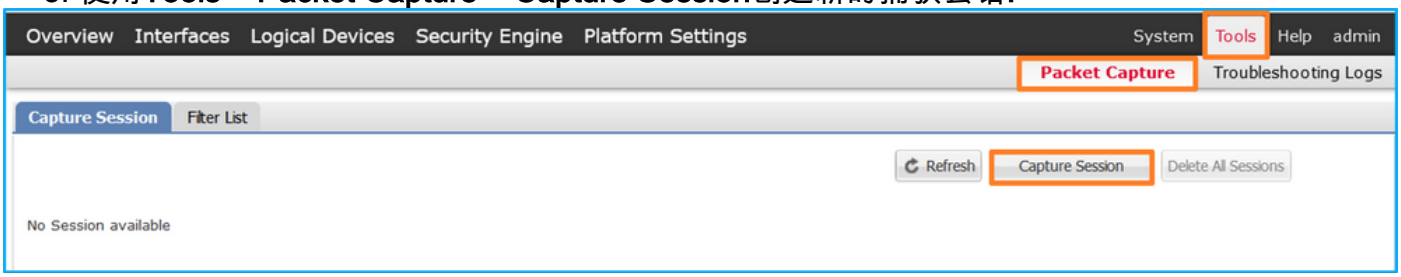
FCM

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：

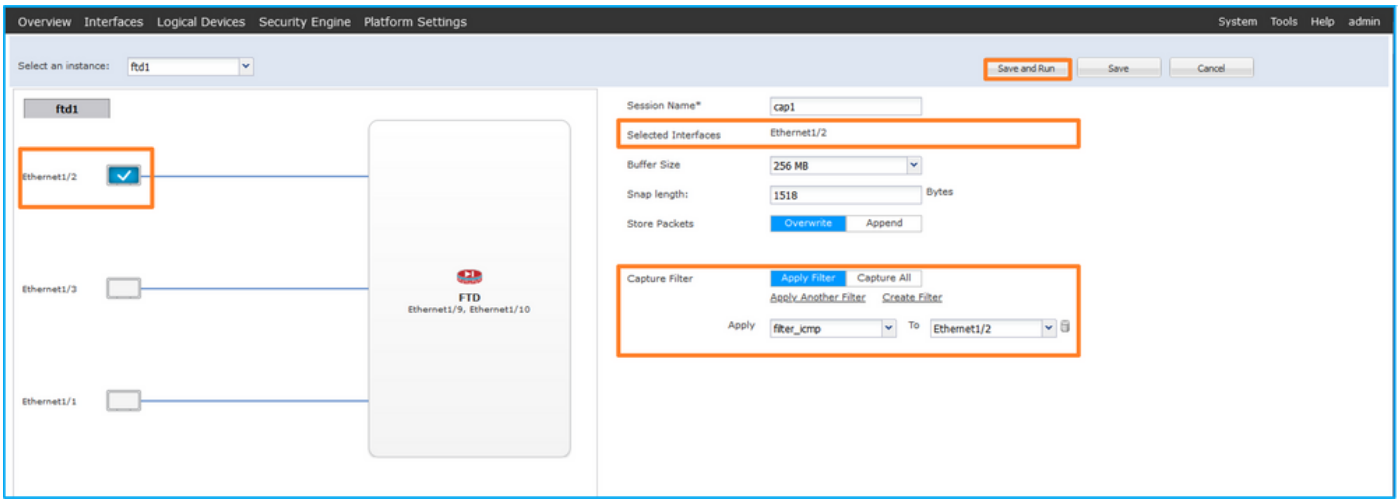
1. 使用**Tools > Packet Capture > Filter List > Add Filter**创建捕获过滤器。
2. 指定**Filter Name、Protocol、Source IPv4、Destination IPv4**，然后单击**Save:**



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：

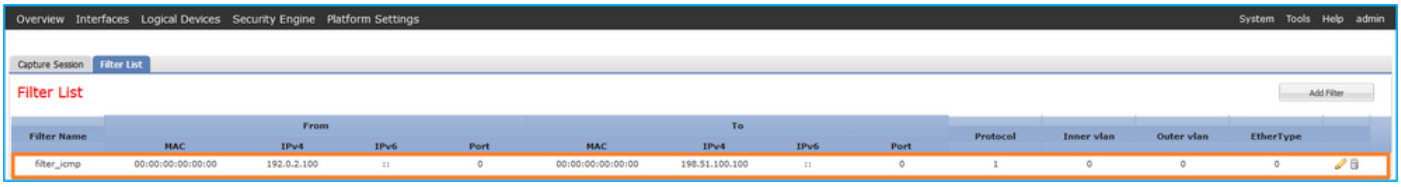
2.

```
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 #
```

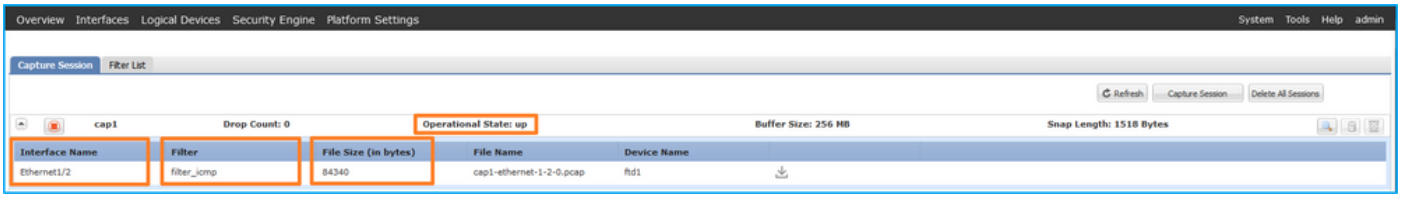
确认

FCM

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



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：



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
```

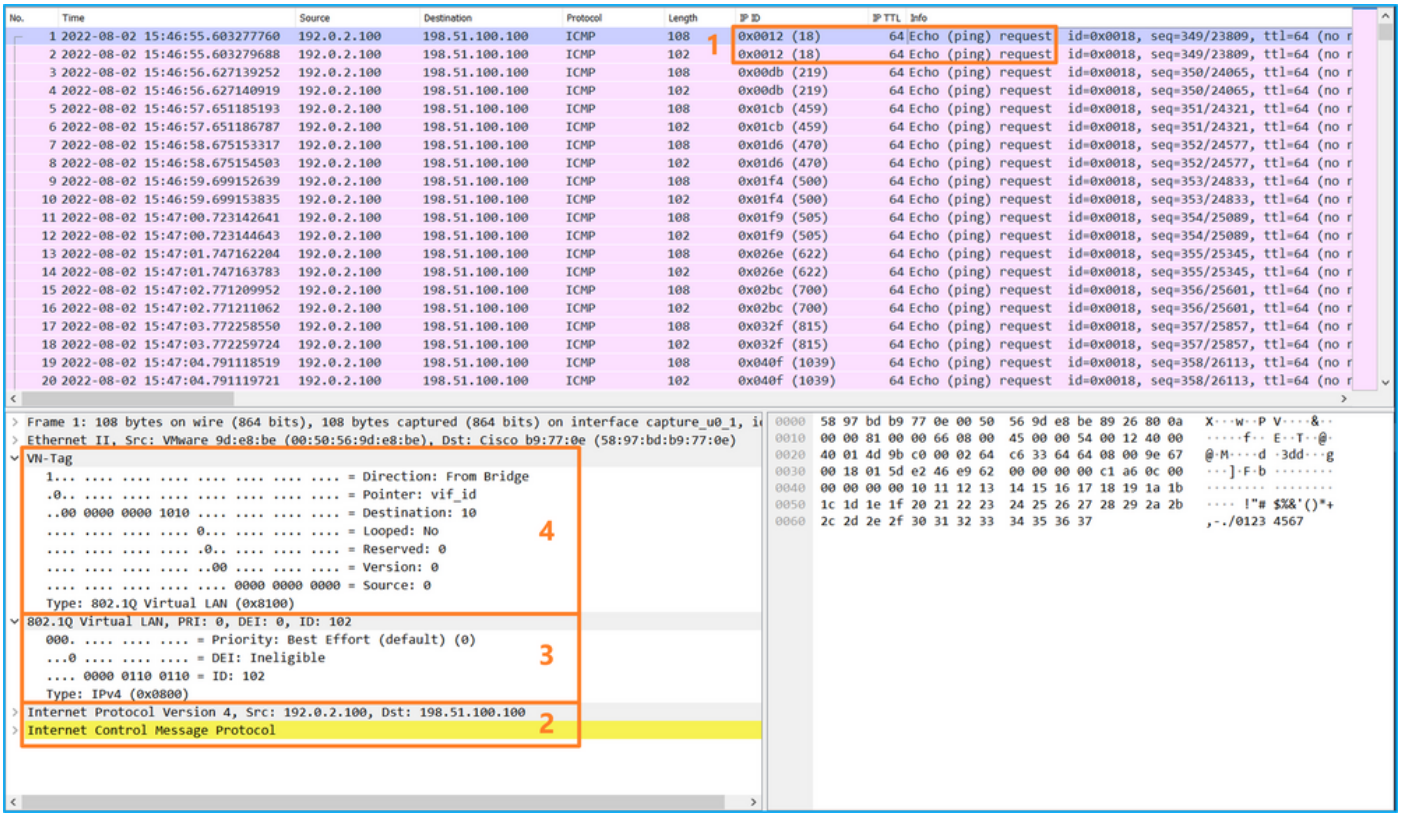
收集捕获文件

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

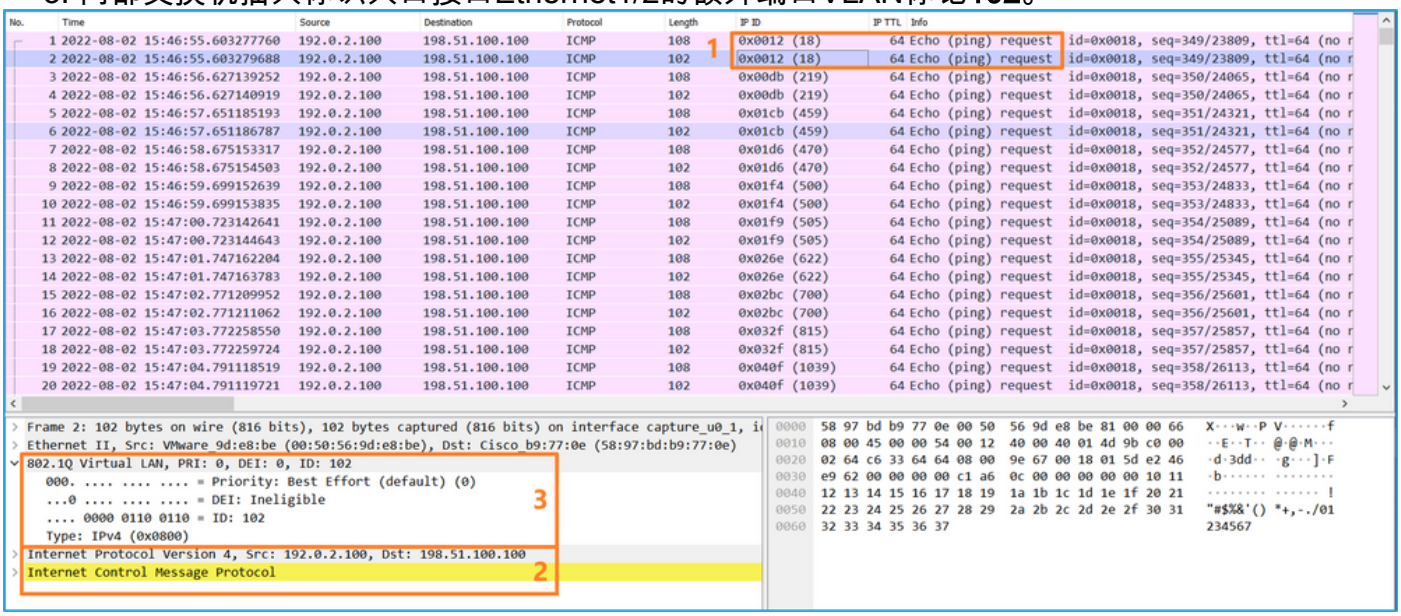
使用数据包捕获文件读取器应用程序打开捕获文件。选择第一个数据包并检查要点

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。



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**。



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：

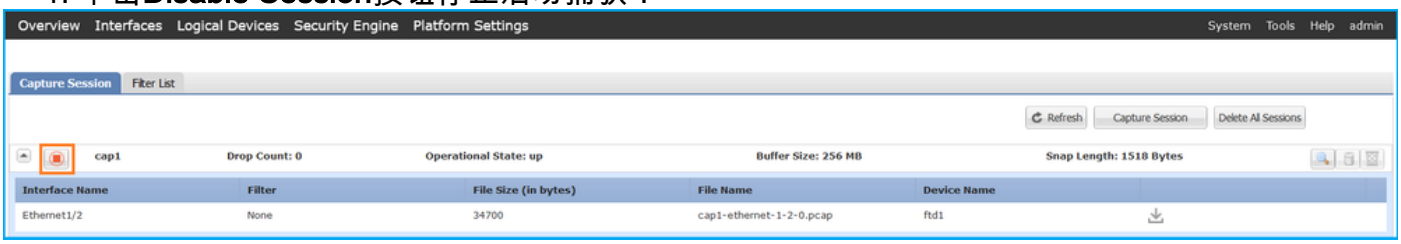
任务	捕获点	捕获数据包中的内部端口VLAN	方向	用户过滤器	捕获的流量
使用前接口Ethernet1/2上的过滤器配置并检验数据包捕获	以太网1/2	102	仅限入口	协议：ICMP 源：192.0.2.100 目的地：198.51.100.100	从主机192.0.2.100到主机198.51.100.100的ICMP回应

收集Firepower 4100/9300内部交换机捕获文件

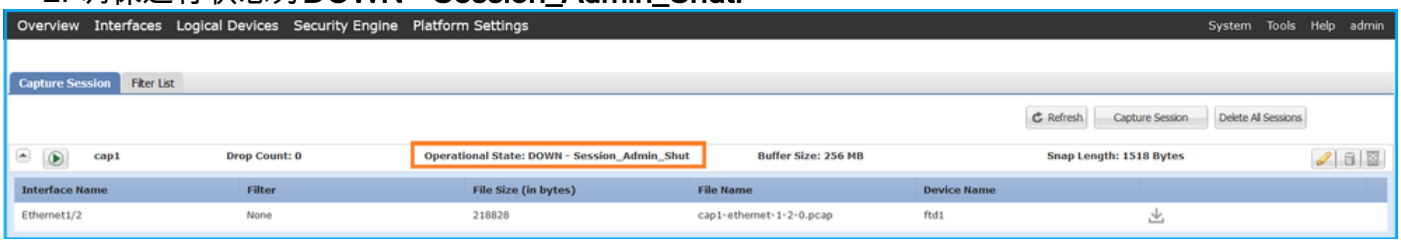
FCM

按照FCM上的以下步骤收集内部交换机捕获文件：

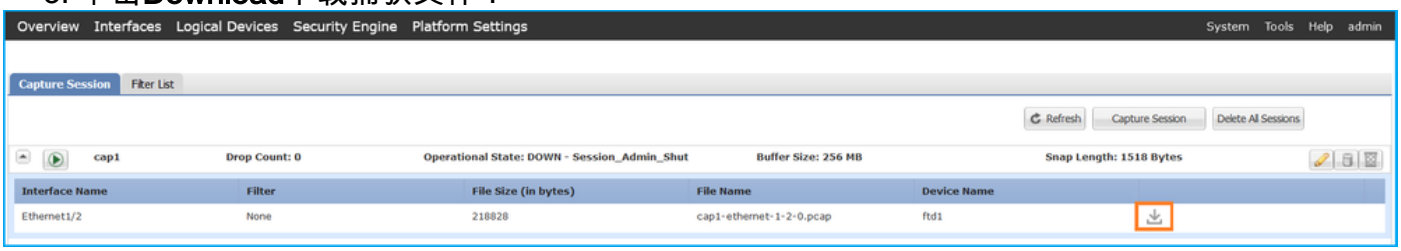
1. 单击**Disable Session**按钮停止活动捕获：



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

4. 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 capsw switch interface inside match ip
>no capture capsw 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。

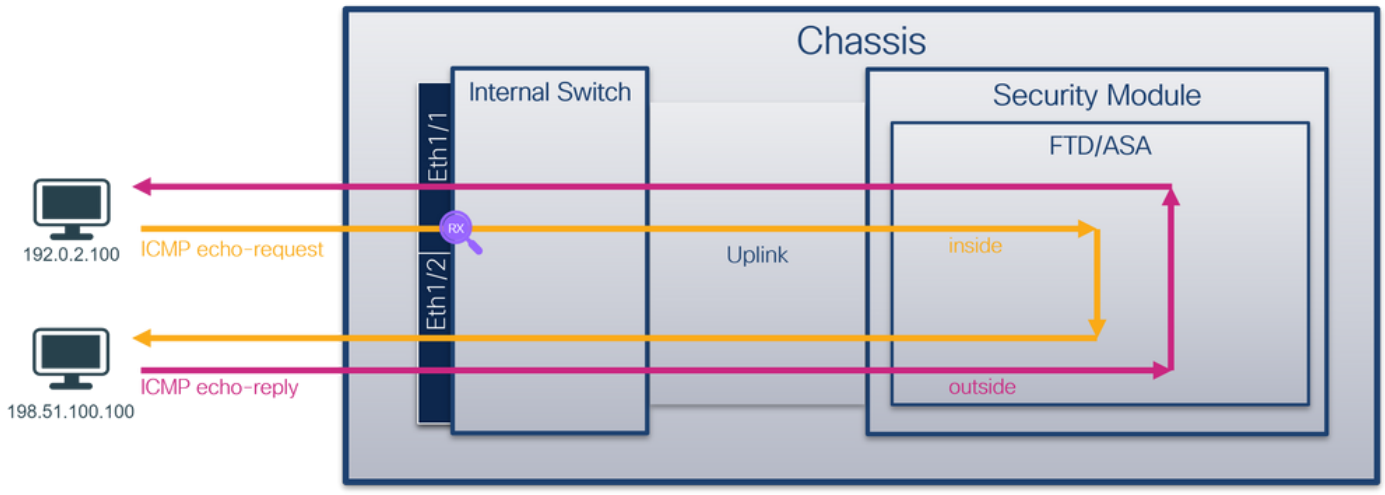
在版本7.2中，FMC或FDM不支持内部交换机捕获配置。对于ASA软件版本9.18(1)及更高版本，可以在ASDM版本7.18.1.x及更高版本中配置内部交换机捕获。

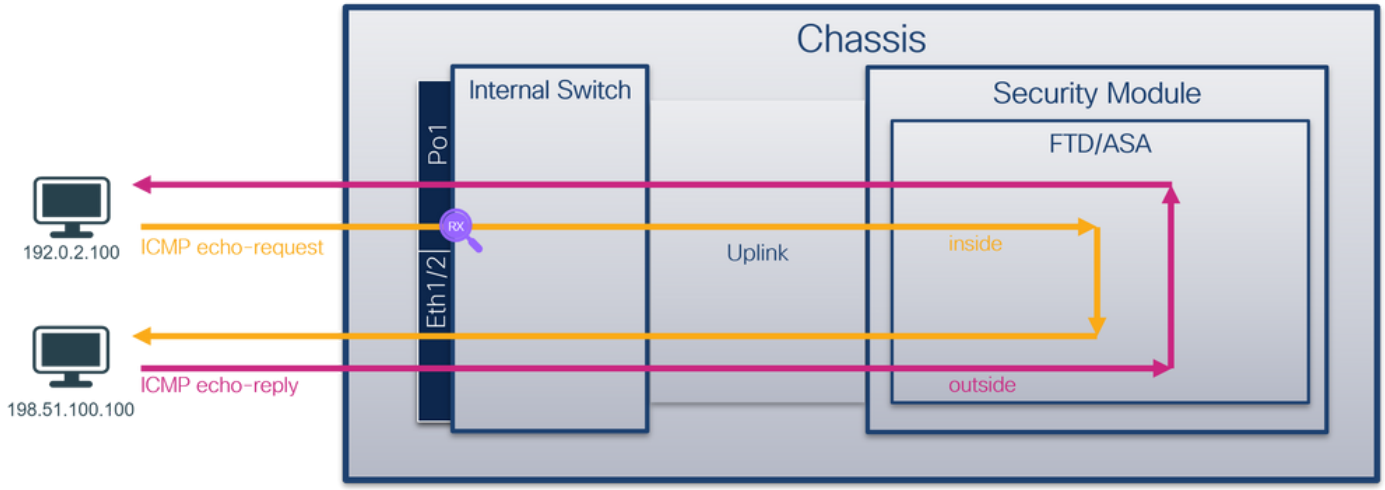
这些场景包括安全防火墙3100内部交换机捕获的常见使用案例。

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。

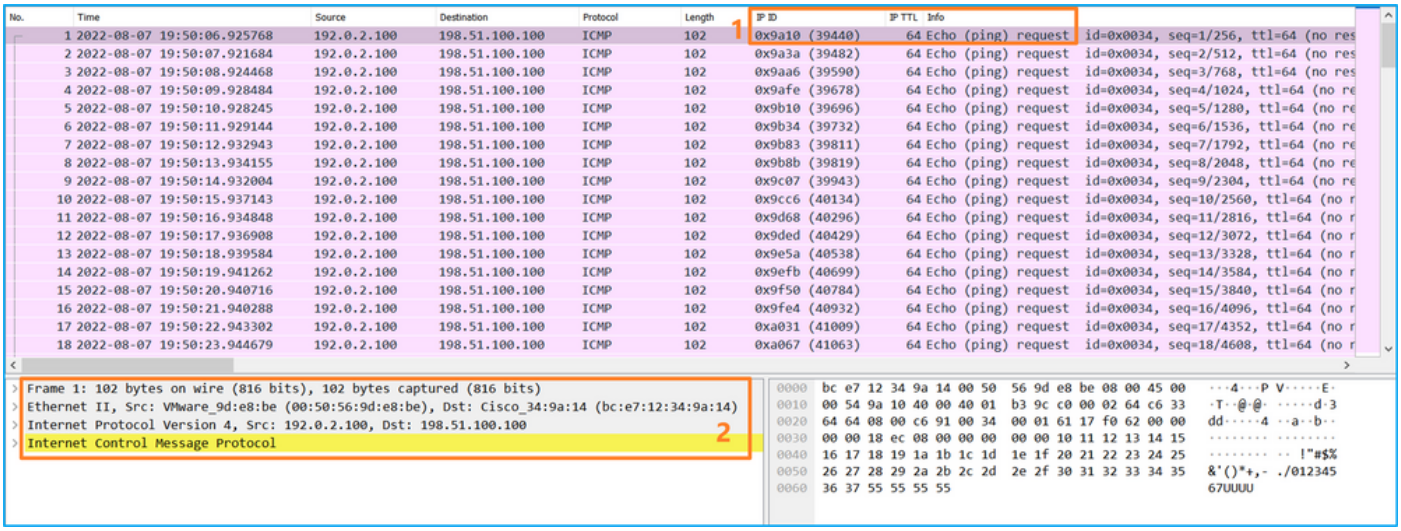
收集捕获文件

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

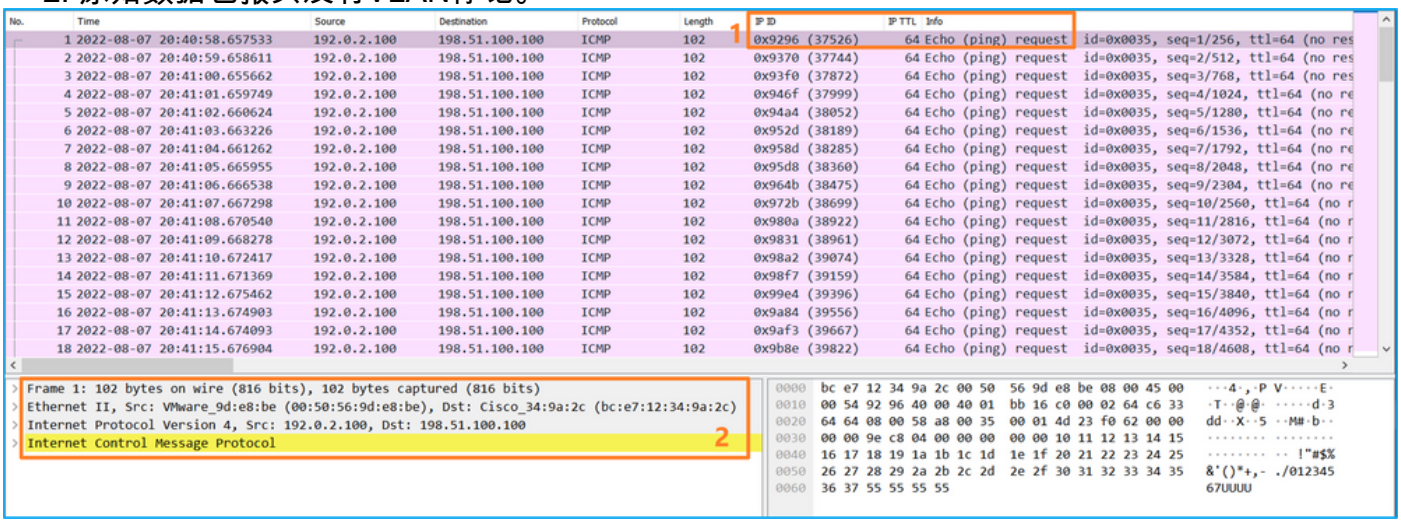
使用数据包捕获文件读取器应用程序打开Ethernet1/1的捕获文件。选择第一个数据包并检查要点：

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。



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。



说明

交换机捕获配置在接口Ethernet1/1或Portchannel1上。

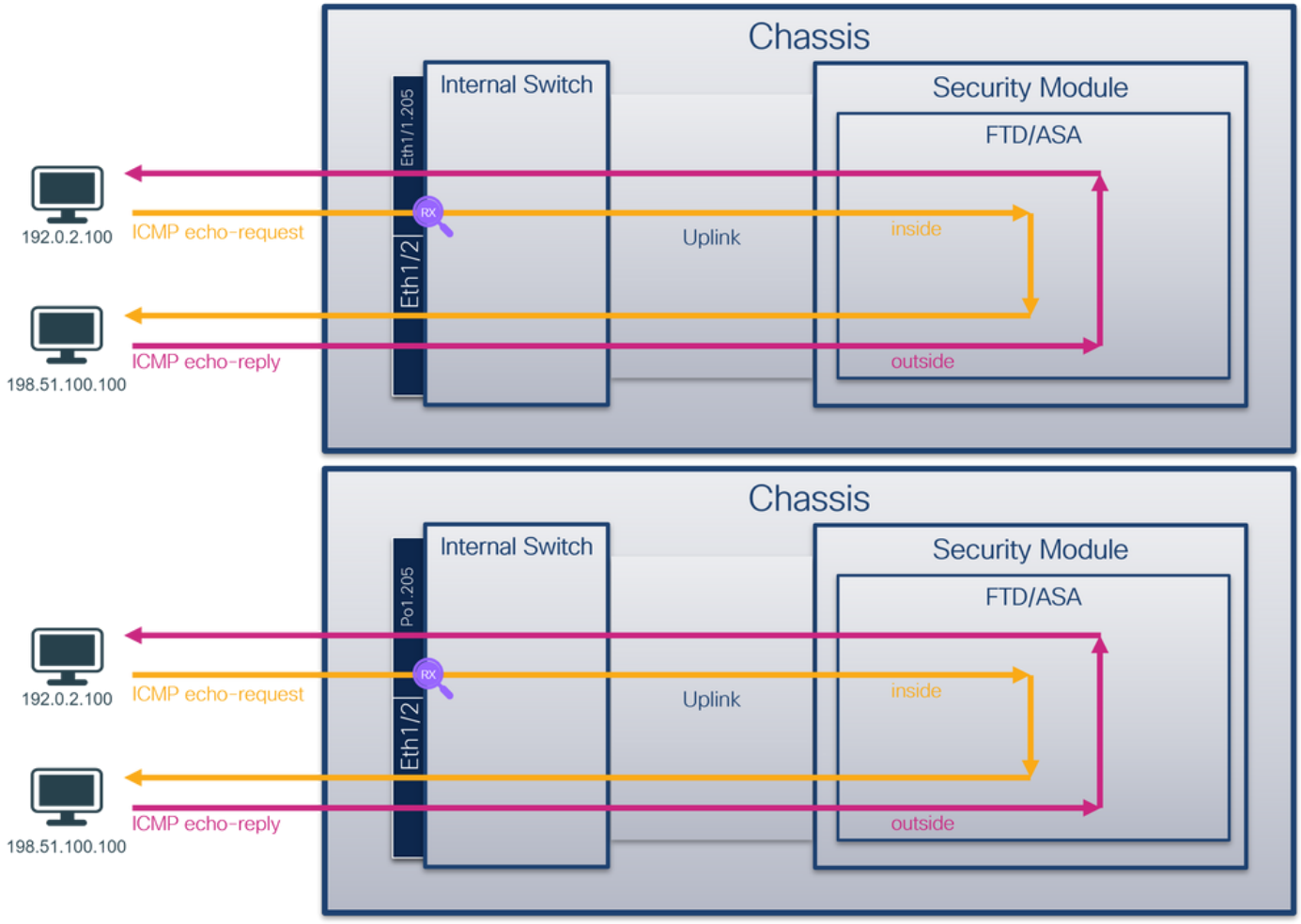
此表概述了任务：

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

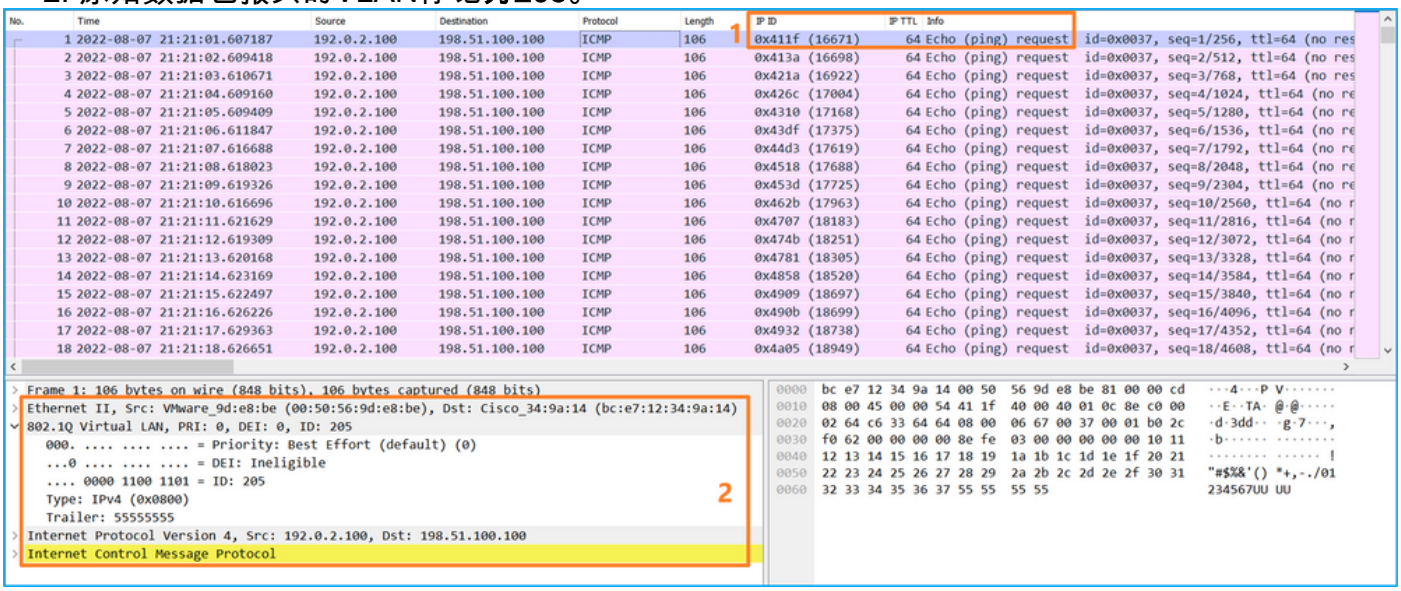
按照**收集安全防火墙3100内部交换机捕获文件**部分中的步骤进行操作。

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：

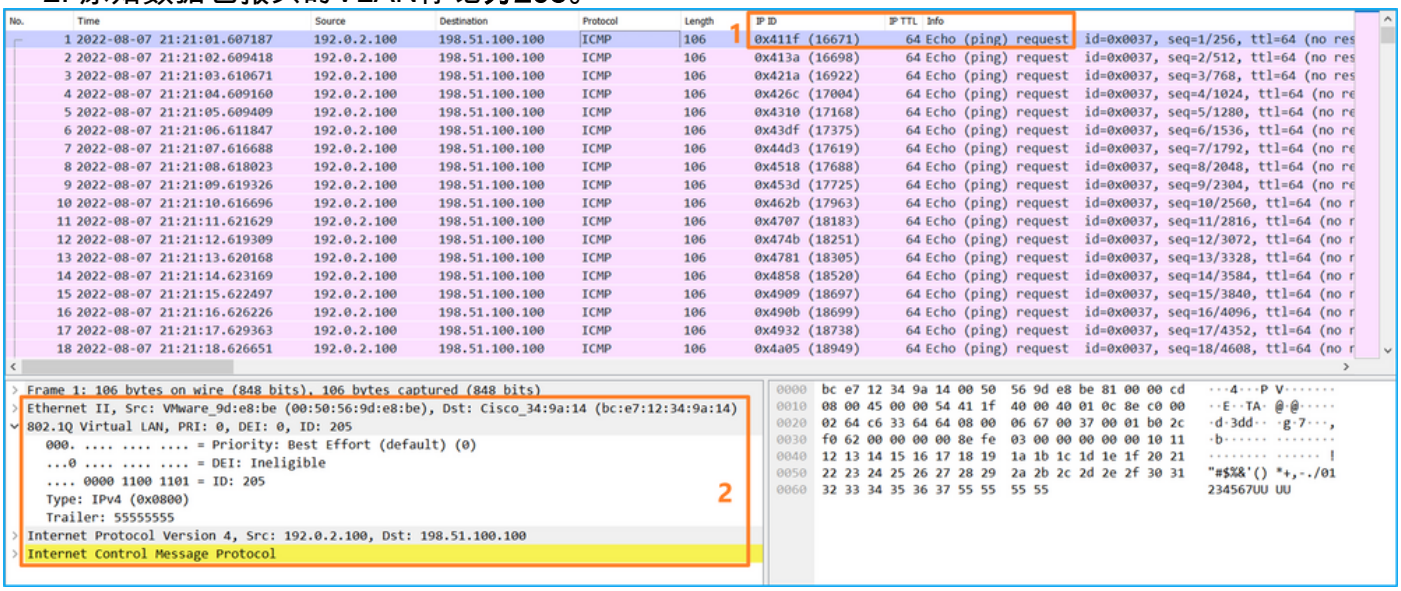
1. 仅捕获ICMP回应请求数据包。

2. 原始数据包报头的VLAN标记为205。



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。



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VLAN 205	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VLAN 205	仅限入口	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

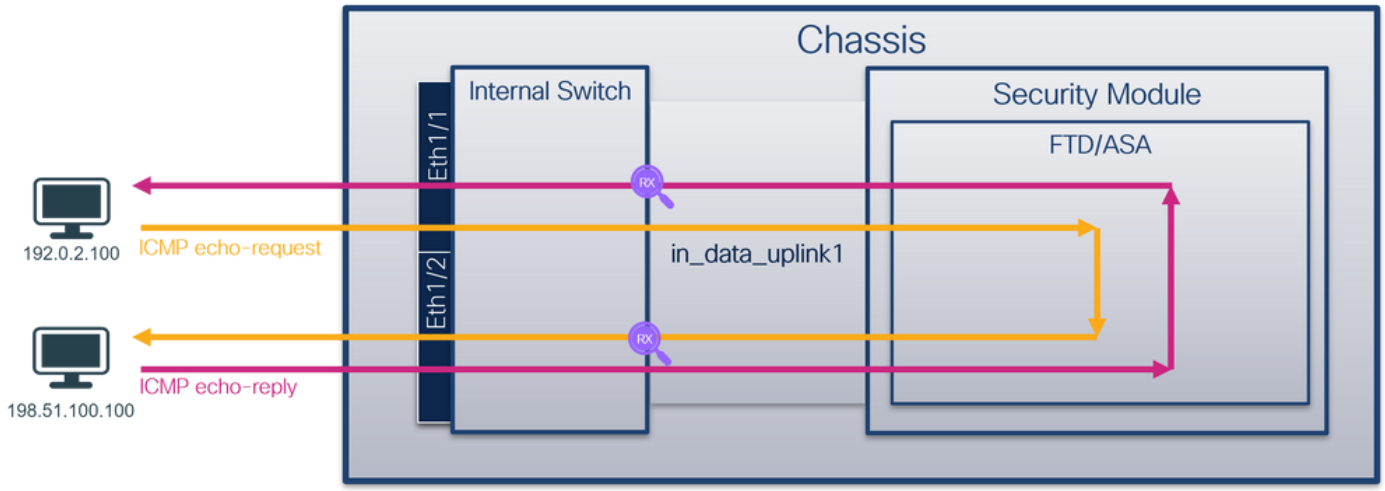
安全防火墙具有2个内部接口：

- **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
```

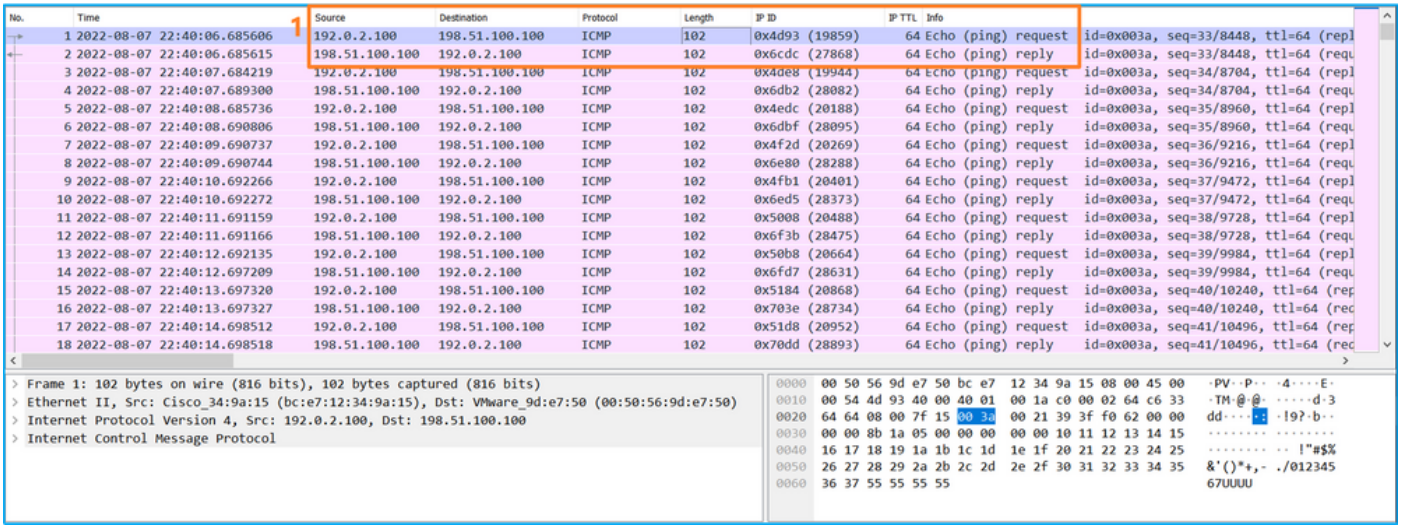
要访问ASA上的FXOS，请运行**connect fxos admin**命令。如果是多情景，请在管理情景中运行此命令。

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。



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：

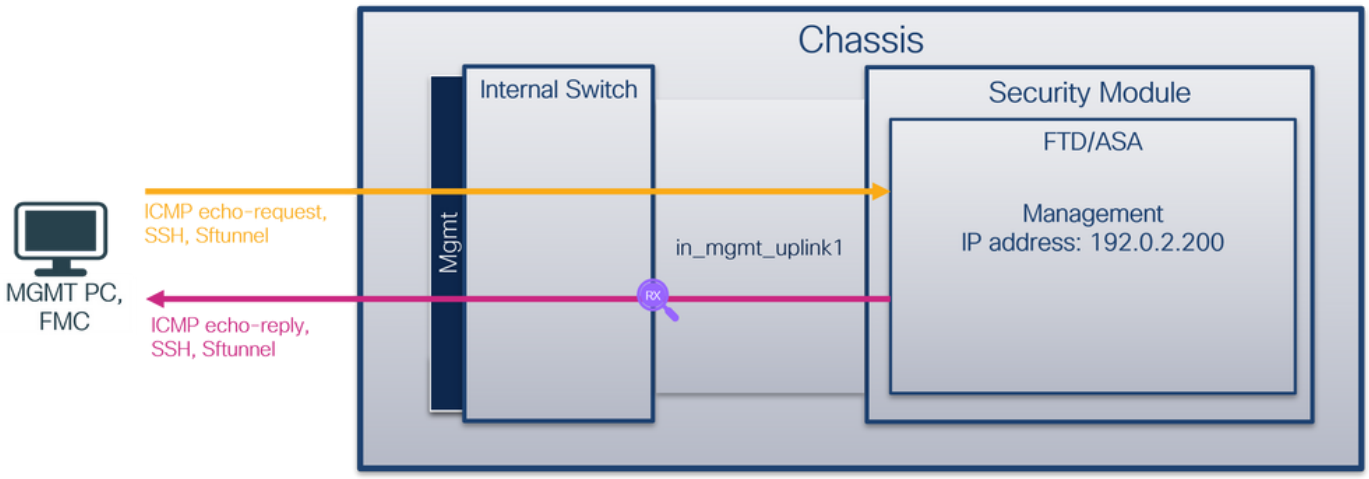
任务	捕获点	内部过滤器	方向	捕获的流量
在in_data_uplink1的上行链路接口上配置并检验数据包捕获	in_data_uplink1	无	仅限入口	从主机192.0.2.100到主机198.51.100.100的ICMP回应请求 从主机198.51.100.100到主机

192.0.2.100的ICMP回应应答

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
```

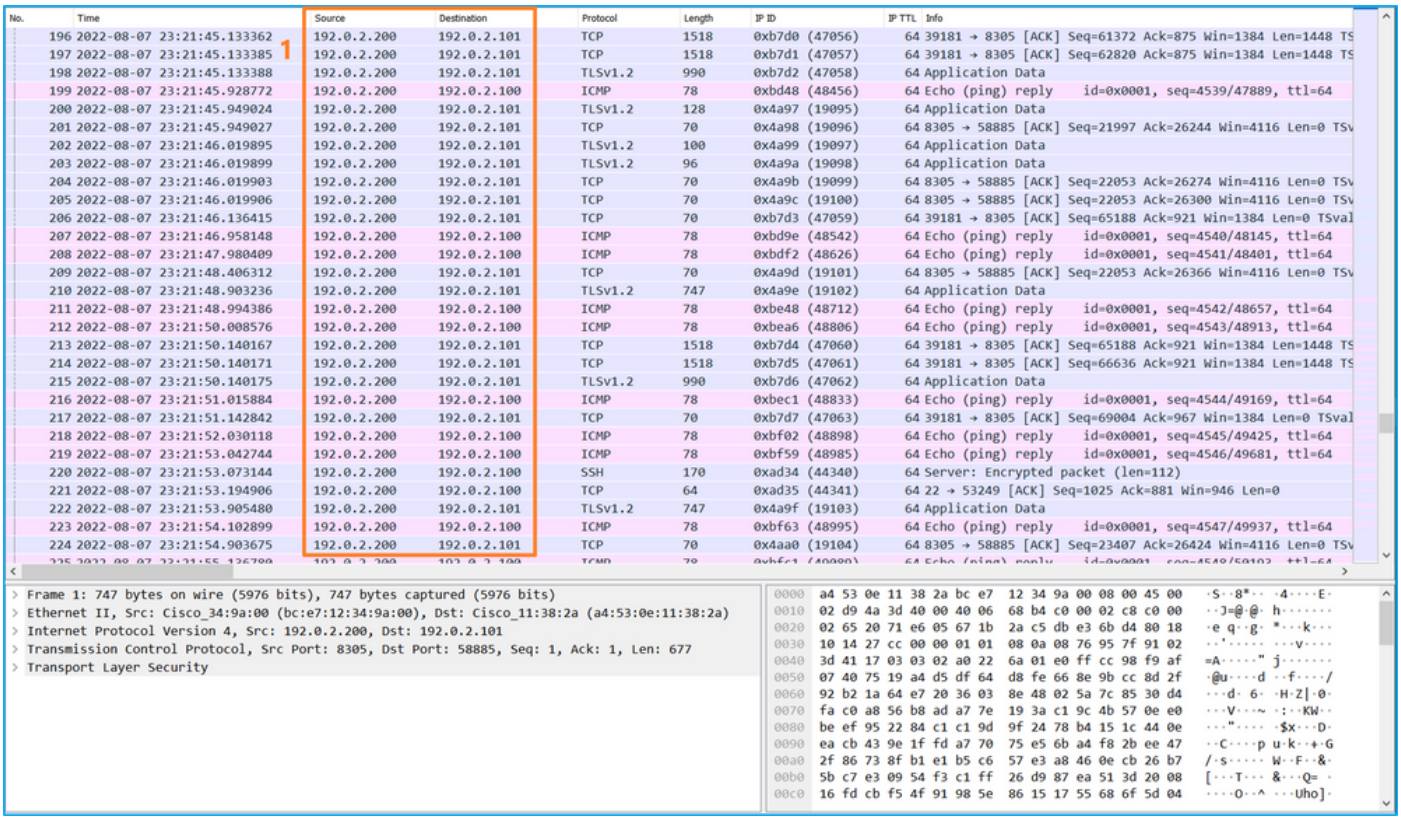
要访问ASA上的FXOS，请运行**connect fxos admin**命令。如果是多情景，请在管理情景中运行此命令。

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。



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

		滤器		
配置并验证管理上行链路接口上的数据包捕获	in_mgmt_uplink1	无	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:            capsw-1-1

Packet Capture Filter Info
  Name:              capsw-1-1
 Protocol:          0
 Ivlan:             0
 Ovlan:             0
 Src Ip:            0.0.0.0
 Dest Ip:           0.0.0.0
 Src Ipv6:          ::
 Dest Ipv6:         ::
 Src MAC:           00:00:00:00:00:00
 Dest MAC:          00:00:00:00:00:00
 Src Port:          0
 Dest Port:         0
 Ethertype:         2054

Total Physical breakout ports involved in Packet Capture: 0

0 packet captured on disk using switch capture

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

这是ICMP过滤器的验证。IP协议1是ICMP:

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

Total Physical ports involved in Packet Capture: 1

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

Packet Capture Filter Info
  Name:              capsw-1-1
 Protocol:          1
 Ivlan:             0
 Ovlan:             0
 Src Ip:            198.51.100.100
 Dest Ip:           0.0.0.0
 Src Ipv6:          ::
 Dest Ipv6:         ::
 Src MAC:           00:00:00:00:00:00
 Dest MAC:          00:00:00:00:00:00
 Src Port:          0
```

```
 Dest Port:         0
 Ethertype:         0

Total Physical breakout ports involved in Packet Capture: 0

0 packets captured on disk using switch capture

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

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：

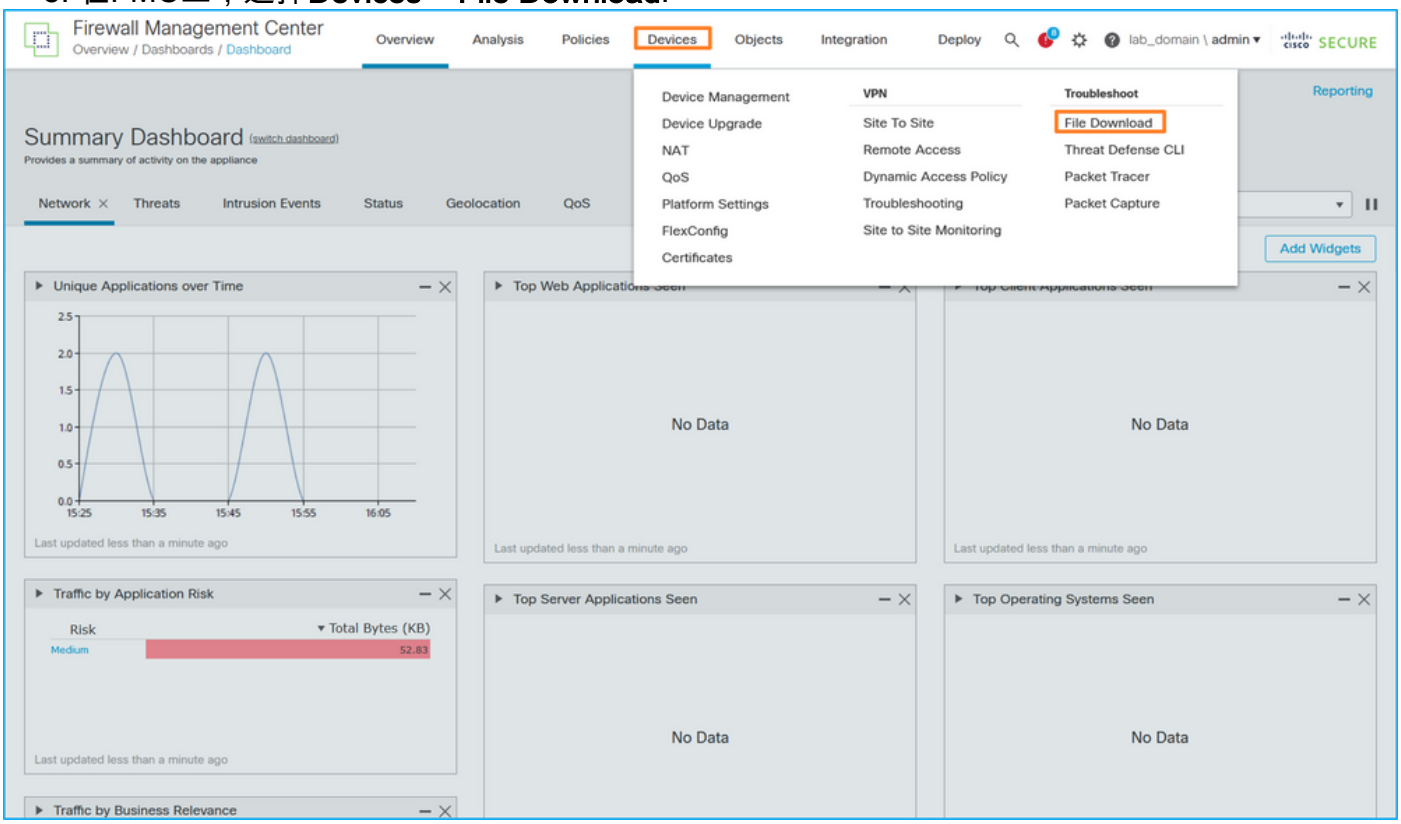
```
> expert
admin@firepower:~$ sudo su
root@firepower:/home/admin
```

4. 将捕获文件复制到/ngfw/var/common/:

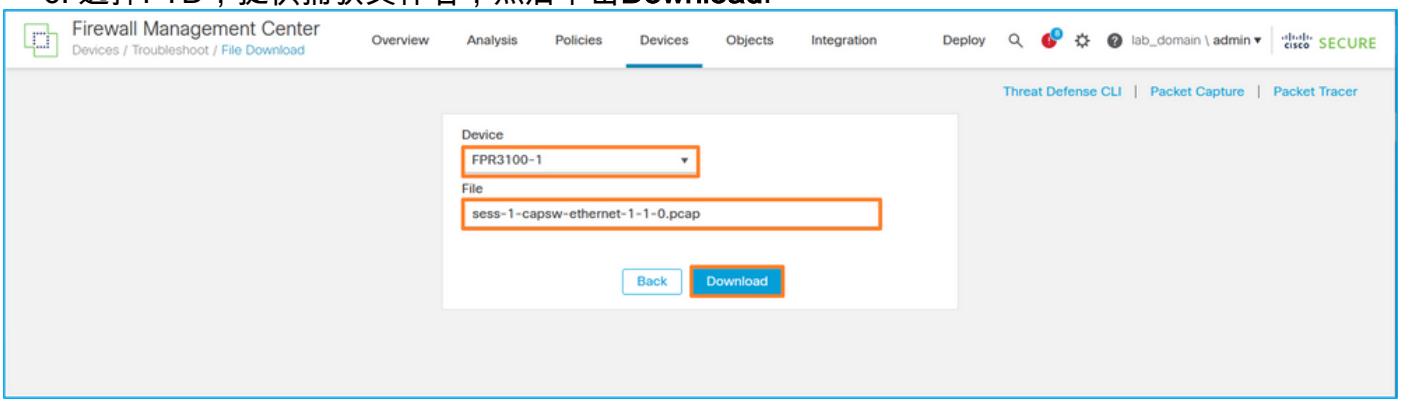
```
root@KSEC-FPR3100-1:/home/admin cp /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
/ngfw/var/common/
```

```
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**:



6. 选择FTD，提供捕获文件名，然后单击**Download**:



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）。