配置并验证安全防火墙和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1200/3100/4200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
- 第2层交换机端口接口上的数据包捕获
- 多实例机箱上的数据包捕获
- 收集Secure Firewall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。

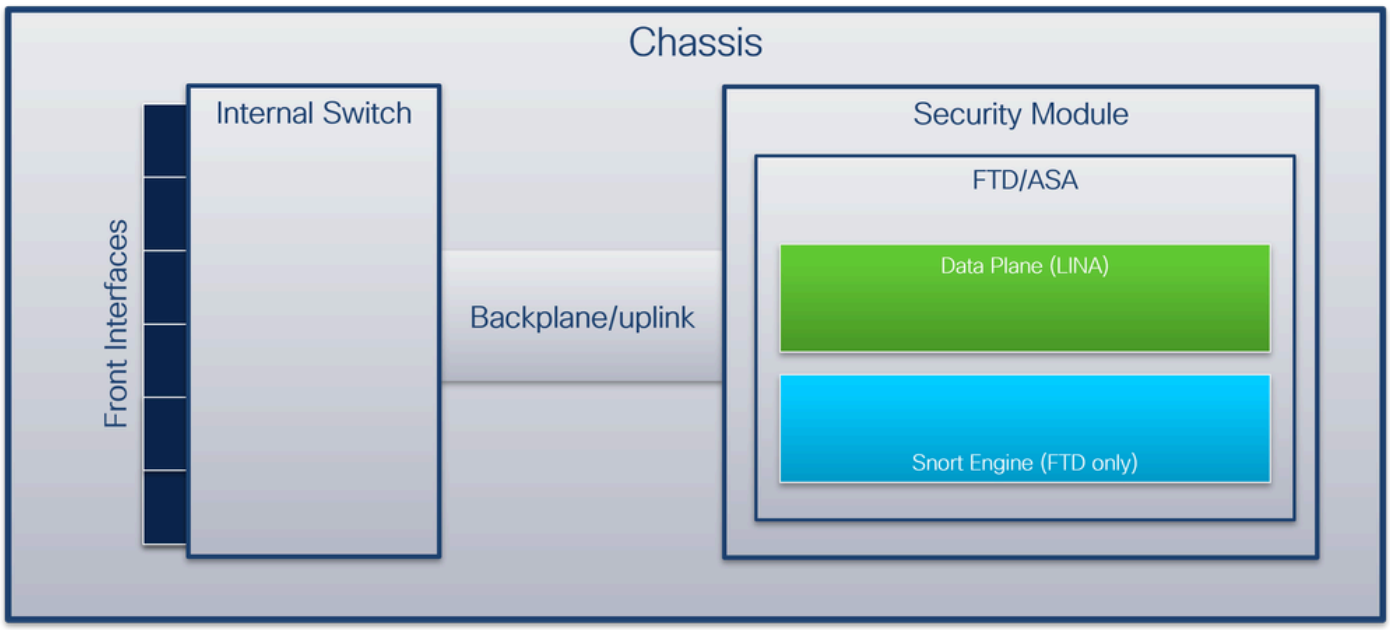
本文档中的信息基于以下软件和硬件版本：

- 安全防火墙1200、3100、4200
- Firepower 4100/9300
- 思科安全可扩展操作系统(FXOS)2.12.0.x、2.17(0.x)
- 思科安全防火墙威胁防御(FTD)7.2.0.x、7.4.1-172、7.7.0.89
- 思科安全防火墙管理中心(FMC)7.2.0.x、7.4.1-172、7.7.0.89
- 自适应安全设备(ASA)9.18(1)x、9.20(x)
- Wireshark 3.6.7(https://www.wireshark.org/download.html)

背景信息

系统架构高级概述

从数据包流的角度而言，Firepower 4100/9300和安全防火墙1200/3100/4200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。
- 管理上行链路 — 专用于Secure Firewall 3100/4200的内部接口，提供内部交换机和应用之间的管理流量路径。
- 管理接口 — 机箱上的物理接口。
- 数据接口 — 分配给用于转发流量的应用的接口。

对于安全防火墙3100/4200，数据、管理和上行链路接口映射到特定的内部交换机端口。

注意：对于安全防火墙1200，数据和上行链路接口映射到特定的内部交换机端口。但是，管理端口是带外接口，不是内部交换机的一部分。

可以在FXOS local-mgmt命令shell show portmanager switch status命令输出的输出中验证映射。

在本示例中，端口0/17是机箱管理接口，端口0/18是背板/上行链路接口，端口0/19是管理上行链路接口。

<#root>

```
firepower-3140#

connect local-mgmt


Warning: network service is not available when entering 'connect local-mgmt'
firepower-3140(local-mgmt)#

show portmanager switch status


Dev/Port     Mode     Link   Speed  Duplex    Loopback      Autoneg      FEC         Link Scan   Port Mana
---------  --------  -----  -----  ------  -------------  ---------  ----------   -----------  ---------
0/1          SGMII    Up     1G     Full        None        No         None          None       Link-Up
0/2          SGMII    Up     1G     Full        None        No         None          None       Link-Up
0/3          SGMII   Down    1G     Full         n/a        No         None          None      Force-Li
0/4          SGMII   Down    1G     Full         n/a        No         None          None      Force-Li
0/5          SGMII   Down    1G     Full         n/a        No         None          None      Force-Li
0/6          SGMII   Down    1G     Full         n/a        No         None          None      Force-Li
0/7          SGMII   Down    1G     Full         n/a        No         None          None      Force-Li
0/8          SGMII   Down    1G     Full         n/a        No         None          None      Force-Li
0/9          SR_LR   Down    25G    Full         n/a        No         None          None      Force-Li
0/10         SR_LR   Down    25G    Full         n/a        No         None          None      Force-Li
0/11       1000_BaseXDown    1G     Full         n/a        No         None          None      Force-Li
0/12       1000_BaseXDown    1G     Full         n/a        No         None          None      Force-Li
0/13       1000_BaseXDown    1G     Full         n/a        No         None          None      Force-Li
0/14       1000_BaseXDown    1G     Full         n/a        No         None          None      Force-Li
0/15       1000_BaseXDown    1G     Full         n/a        No         None          None      Force-Li
0/16       1000_BaseXDown    1G     Full         n/a        No         None          None      Force-Li
0/17       1000_BaseX Up     1G     Full        None        No         None          None       Link-Up

0/18          KR2     Up     50G

Full        None         No          None          None       Link-Up

0/19          KR      Up     25G
```

```
 Full         None         No          None          None       Link-Up
0/20          KR       Up      25G    Full         None         No          None          None       Link-Up
```

下表显示了Firepower 4100/9300上的背板接口和安全防火墙1200/3100/4200上的数据上行链路接口：

Platform	支持的安全模块数量	背板/上行链路接口	用于背板/上行链路的映射内部交换机端口	映射的应用接口
Firepower 4100（Firepower 4110/4112除外）	1	SM1: Ethernet1/9 以太网 1/10	不适用	Internal-Data0/0 Internal-Data0/1
Firepower 4110/4112	1	Ethernet1/9	不适用	Internal-Data0/0 Internal-Data0/1
Firepower 9300	3	SM1: Ethernet1/9 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	不适用	Internal-Data0/0 Internal-Data0/1 Internal-Data0/0 Internal-Data0/1 Internal-Data0/0 Internal-Data0/1
安全防火墙1210	1	in_data_uplink1	端口 9	Internal-Data0/1
安全防火墙1220	1	in_data_uplink1 in_data_uplink2 in_data_uplink3	端口 11 端口 12 端口 13	Internal-Data0/1 Internal-Data0/2 Internal-Data0/3

安全防火墙1230 安全防火墙1240	1	in_data_uplink1 in_data_uplink2 in_data_uplink3	端口 13 端口 14 端口 15	Internal-Data0/1 Internal-Data0/2 Internal-Data0/3
安全防火墙1250	1	in_data_uplink1	端口 13	Internal-Data0/1
安全防火墙3100	1	in_data_uplink1	端口 18	Internal-Data0/1
安全防火墙4200	1	in_data_uplink1 in_data_uplink2（仅4245）	端口 11 端口12（仅4245）	Internal-Data0/1 Internal-Data0/2（仅4245）

下表显示了安全防火墙1200/3100/4200上的管理接口和管理上行链路接口：

Platform	机箱管理接口	机箱管理接口的映射内部交换机端口	用于管理上行链路接口的映射内部交换机端口	映射的应用接口
安全防火墙1210	管理1	未映射到任何内部交换机端口	不适用	不适用
安全防火墙1200 （1210除外）	管理1	未映射到任何内部交换机端口	不适用	不适用
安全防火墙3100	管理1	端口 0/17	端口 0/19	in_mgmt_uplink1
安全防火墙4200	管理1 管理2	端口 0/9 端口 0/10	端口 0/13 端口 0/14	in_mgmt_uplink1 in_mgmt_uplink2

如果每个模块具有2个背板接口的Firepower 4100/9300或具有2个数据上行链路接口的Secure Firewall 4245，则内部交换机和模块上的应用会在这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 — 应用中的背板或上行链路接口的名称，例如FTD或ASA。

此外，Secure Firewall 1200采用具有三个数据上行链路接口的新架构。内部交换机和应用程序在这些接口之间执行负载均衡。

使用show interface detail命令验证内部接口：

```
<#root>

>

show interface detail | grep Interface


Interface Internal-Control0/0 "ha_ctl_nlp_int_tap", is up, line protocol is up
  Control Point Interface States:
        Interface number is 6
        Interface config status is active
        Interface state is active

Interface Internal-Data0/0 "", is up, line protocol is up


  Control Point Interface States:
        Interface number is 2
        Interface config status is active
        Interface state is active

Interface Internal-Data0/1 "", is up, line protocol is up


  Control Point Interface States:
        Interface number is 3
        Interface config status is active
        Interface state is active
Interface Internal-Data0/2 "nlp_int_tap", is up, line protocol is up
  Control Point Interface States:
        Interface number is 4
        Interface config status is active
        Interface state is active
Interface Internal-Data0/3 "ccl_ha_nlp_int_tap", is up, line protocol is up
  Control Point Interface States:
        Interface number is 5
        Interface config status is active
        Interface state is active
Interface Internal-Data0/4 "cmi_mgmt_int_tap", is up, line protocol is up
  Control Point Interface States:
        Interface number is 7
        Interface config status is active
        Interface state is active
Interface Port-channel6.666 "", is up, line protocol is up
Interface Ethernet1/1 "diagnostic", is up, line protocol is up
  Control Point Interface States:
        Interface number is 8
        Interface config status is active
        Interface state is active
```

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标记插入到前接口上的每个入口数据包中。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：

<#root>

```
firepower#
```

connect fxos

```
…
firepower(fxos)#
```

show run int e1/2

```
!Command: show running-config interface Ethernet1/2
!Time: Tue Jul 12 22:32:11 2022

version 5.0(3)N2(4.120)

interface Ethernet1/2
  description U: Uplink
  no lldp transmit
  no lldp receive
  no cdp enable
  switchport mode dot1q-tunnel
```

switchport trunk native vlan 102

```
  speed 1000
  duplex full
  udld disable
  no shutdown
```

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1200/3100/4200

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

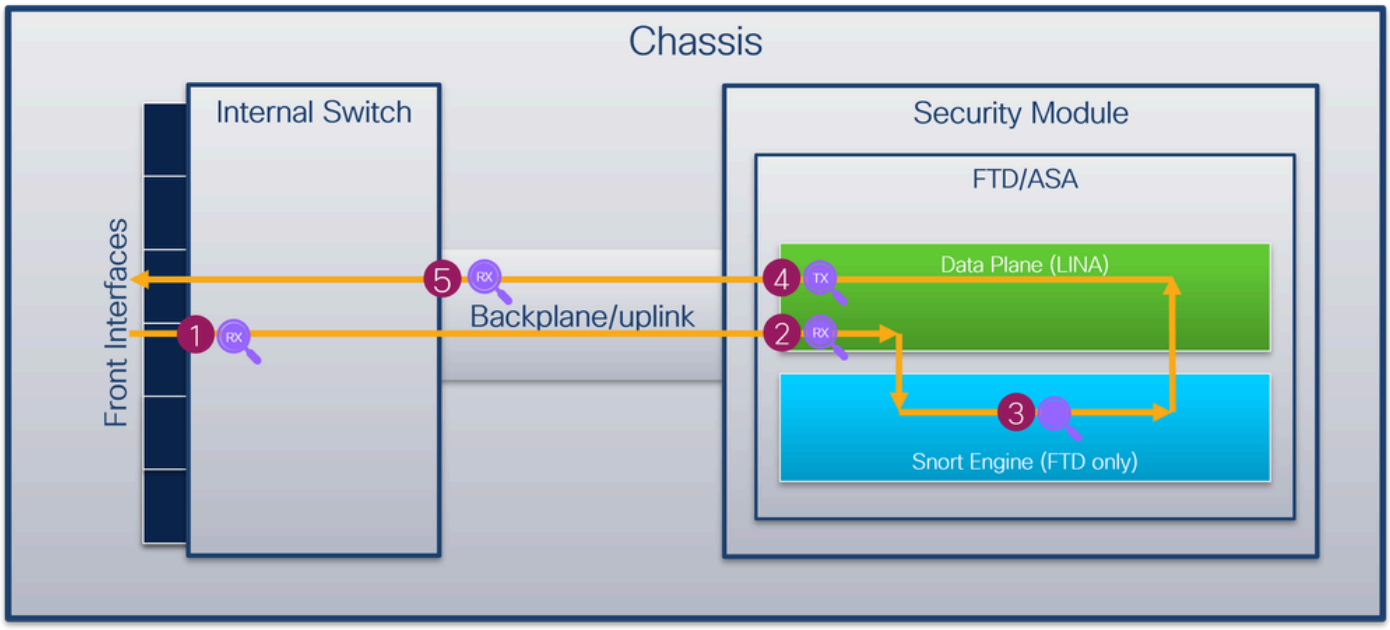
端口VLAN标记与应用共享。应用程序将各个出口接口VLAN标记插入到每个数据包中。当上行链路接口上的内部交换机收到来自应用的数据包时，交换机读取出口接口VLAN标记，识别出口接口，剥离端口VLAN标记，并将数据包转发到网络。

数据包流和捕获点

Firepower 4100/9300和安全防火墙3100

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：



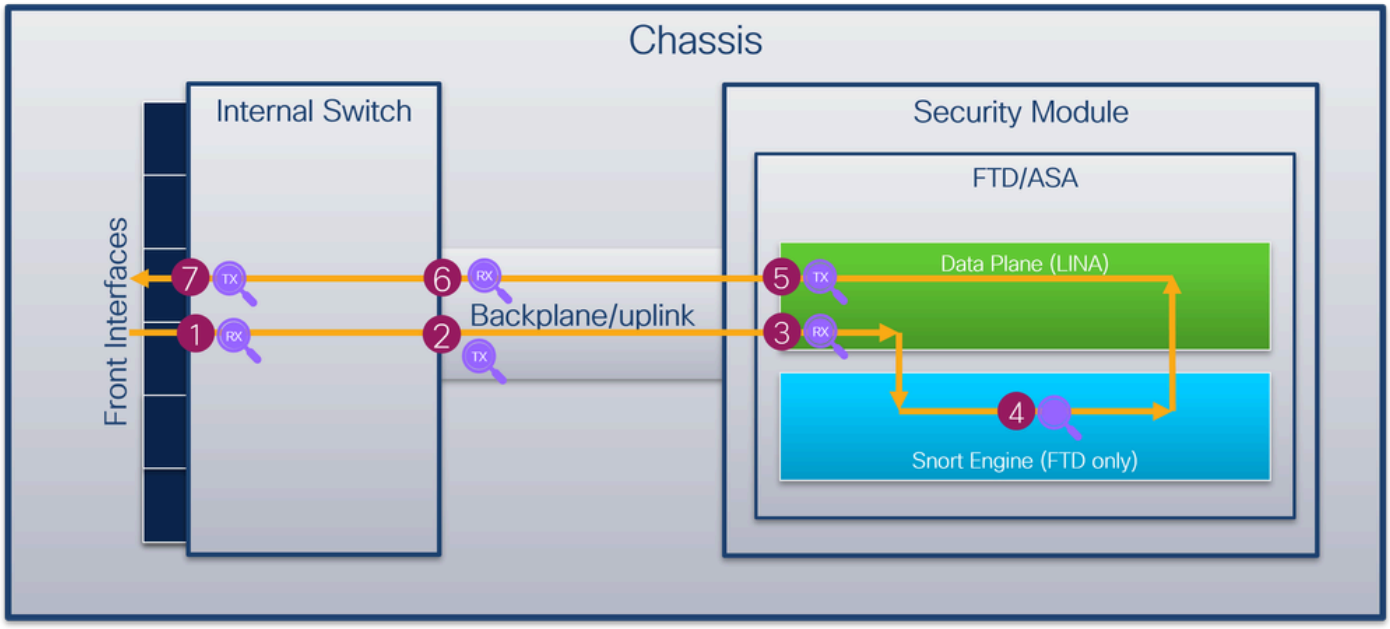
捕获点包括：

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。

安全防火墙1200/4200

安全防火墙1200/4200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. 内部交换机背板接口出口捕获点。
3. 数据平面接口入口捕获点
4. Snort捕获点
5. 数据平面接口出口捕获点
6. 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。
7. 内部交换机前接口出口捕获点。

内部交换机可选择支持双向（入口和出口）捕获。默认情况下，内部交换机捕获入口方向的数据包。

> 注意：安全防火墙1200上的管理接口是带外接口，不属于内部交换机。因此，安全防火墙1200不支持在交换机级别捕获管理接口流量。

Firepower 4100/9300上的配置和验证

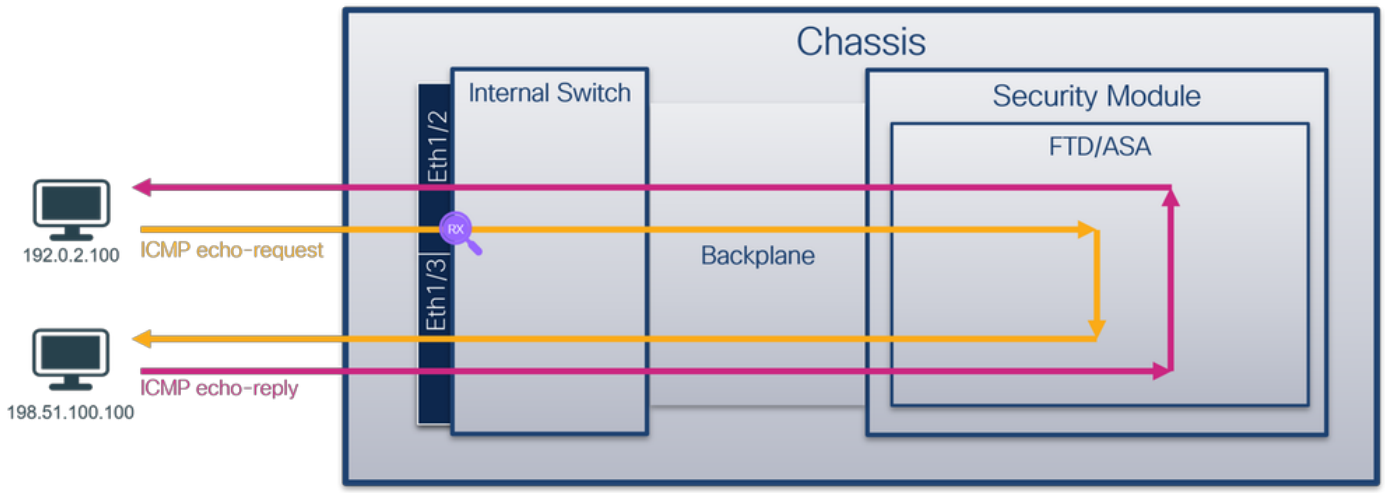
Firepower 4100/9300内部交换机捕获可以在FCM上的Tools > Packet Capture中配置，或在FXOS CLI中的scope packet-capture中配置。有关数据包捕获选项的说明，请参阅Cisco Firepower 4100/9300 FXOS机箱管理器配置指南或Cisco Firepower 4100/9300 FXOS CLI配置指南一章故障排除,数据包捕获一节。

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接口上配置并检验数据包捕获。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

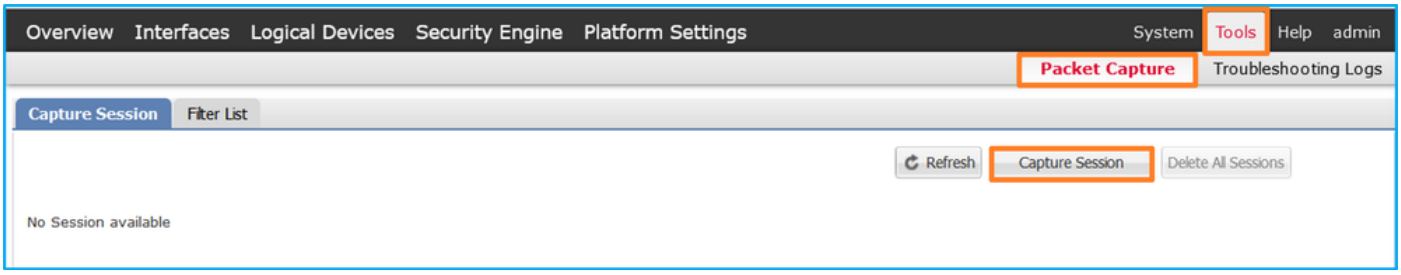


配置

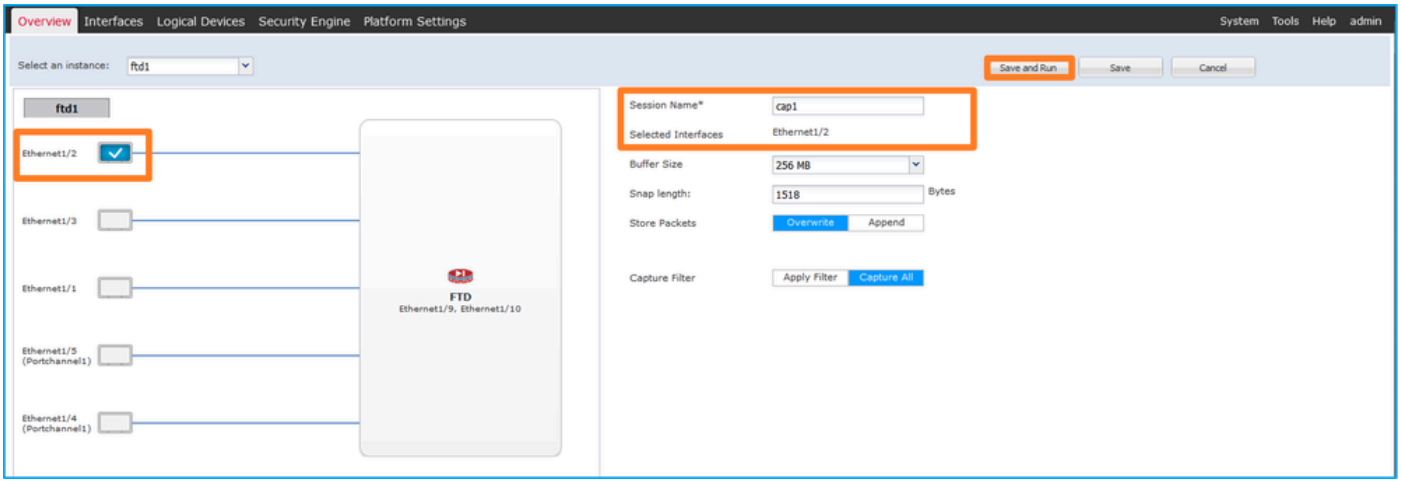
FCM

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

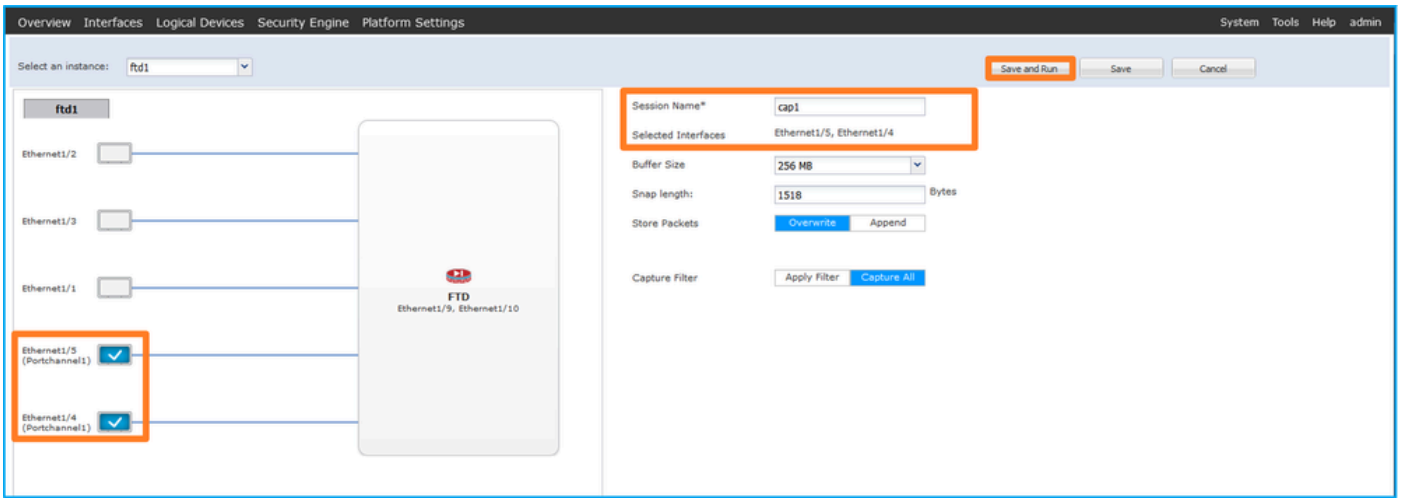
1. 使用Tools > Packet Capture > Capture Session创建新的捕获会话:



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：

```
<#root>

firepower#

scope ssa

firepower /ssa #

show app-instance

App Name    Identifier Slot ID     Admin State Oper State       Running Version Startup Version Deploy Ty
----------- ---------- ---------- ----------- --------------- --------------- --------------- ---------

ftd         ftd1

        1           Enabled      Online           7.2.0.82        7.2.0.82        Native      No
```

2. 对于端口通道接口，请标识其成员接口：

```
<#root>

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：

```
<#root>

firepower#

scope packet-capture

firepower /packet-capture #

create session cap1

firepower /packet-capture/session* #

create phy-port Eth1/2

firepower /packet-capture/session/phy-port* #

set app ftd

firepower /packet-capture/session/phy-port* #

set app-identifier ftd1

firepower /packet-capture/session/phy-port* #

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：

<#root>

```
firepower#
scope packet-capture

firepower /packet-capture #
create session cap1

firepower /packet-capture/session* #
create phy-port Eth1/4

firepower /packet-capture/session/phy-port* #
set app ftd

firepower /packet-capture/session/phy-port* #
set app-identifier ftd1

firepower /packet-capture/session/phy-port* #
up

firepower /packet-capture/session* #
create phy-port Eth1/5

firepower /packet-capture/session/phy-port* #
set app ftd

firepower /packet-capture/session/phy-port* #
set app-identifier ftd1

firepower /packet-capture/session/phy-port* #
up

firepower /packet-capture/session* #
enable

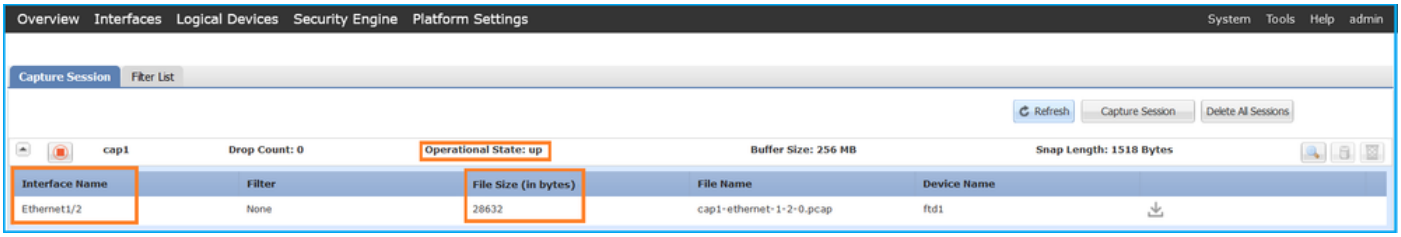
firepower /packet-capture/session* #
commit

firepower /packet-capture/session #
```

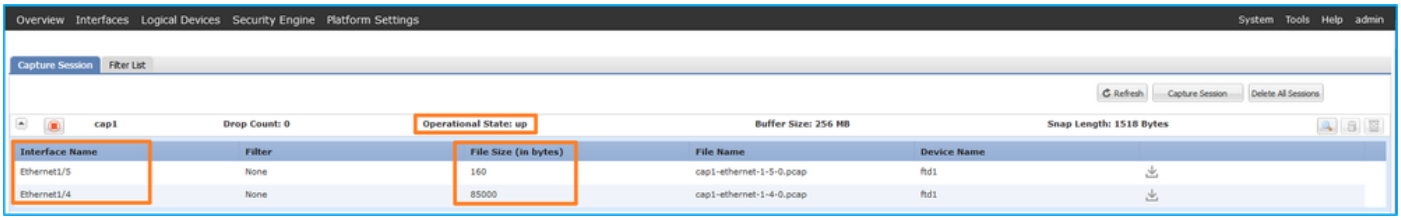
确认

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:

```
<#root>
firepower#
scope packet-capture

firepower /packet-capture #
show session cap1


Traffic Monitoring Session:
    Packet Capture Session Name: cap1

    Session: 1
    Admin State: Enabled


    Oper State: Up


    Oper State Reason: Active


    Config Success: Yes
    Config Fail Reason:
    Append Flag: Overwrite
    Session Mem Usage: 256  MB
    Session Pcap Snap Len: 1518  Bytes
```

```
    Error Code: 0
    Drop Count: 0

Physical ports involved in Packet Capture:

    Slot Id: 1


    Port Id: 2


    Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap


    Pcapsize: 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:

```
<#root>

firepower#

scope packet-capture


firepower /packet-capture #

show session cap1


Traffic Monitoring Session:

    Packet Capture Session Name: cap1


    Session: 1

    Admin State: Enabled


    Oper State: Up


    Oper State Reason: Active


    Config Success: Yes
    Config Fail Reason:
```

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

Physical ports involved in Packet Capture:


Slot Id: 1


    Port Id: 4


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


    Pcapsize: 310276  bytes


    Filter:
    Sub Interface: 0

    Application Instance Identifier: ftd1


    Application Name: ftd




Slot Id: 1


    Port Id: 5


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


    Pcapsize: 160  bytes


    Filter:
    Sub Interface: 0

    Application Instance Identifier: ftd1


    Application Name: ftd
```

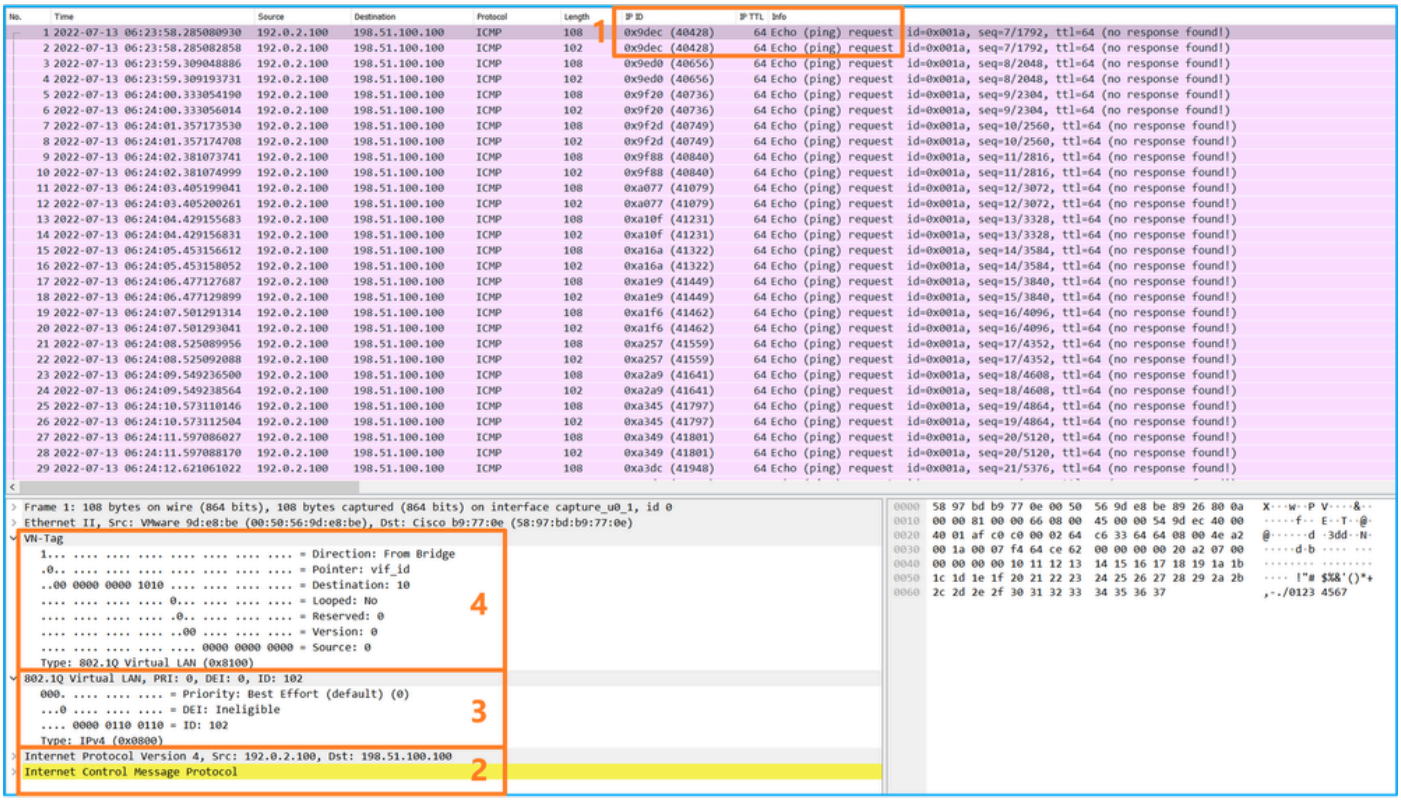
收集捕获文件

执行收集Firepower 4100/9300内部交换机捕获文件部分中的步骤。

捕获文件分析

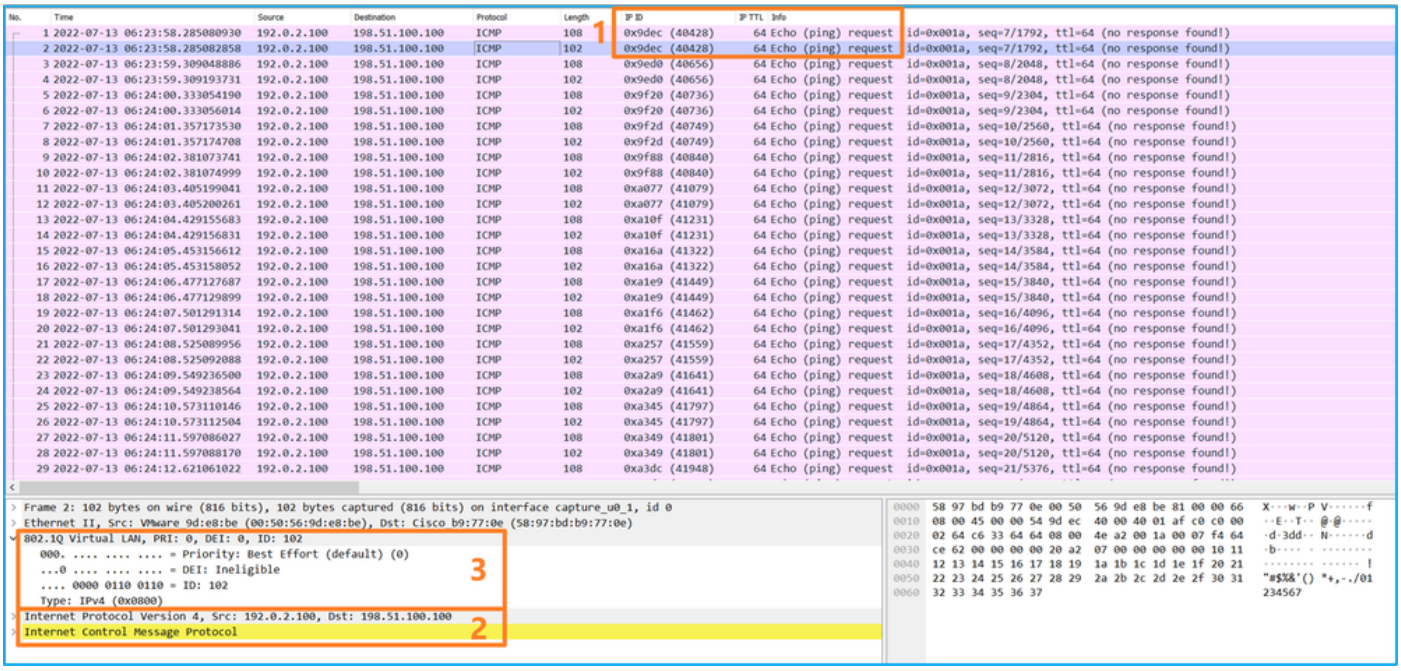
使用数据包捕获文件读取器应用程序打开Ethernet1/2的捕获文件。选择第一个数据包并检查要点：

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。



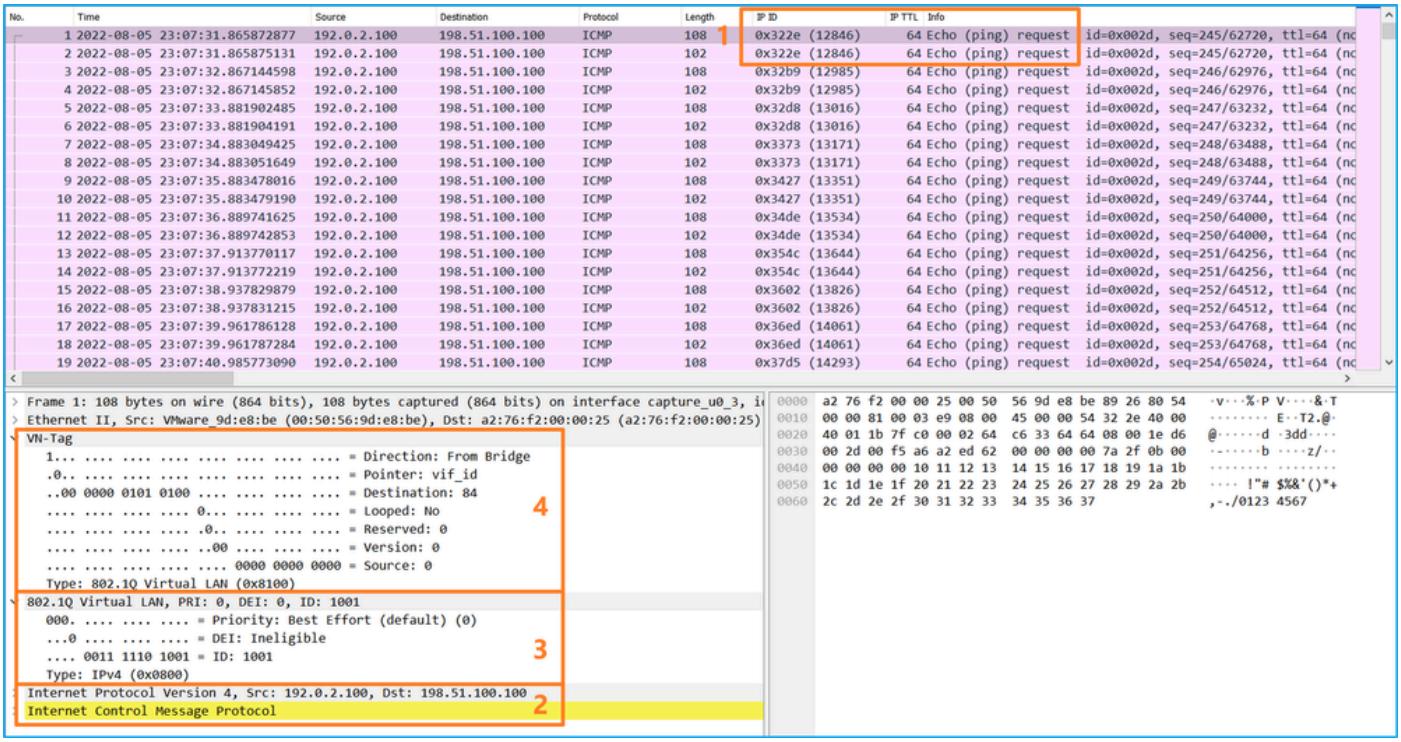
选择第二个数据包并检查要点：

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。



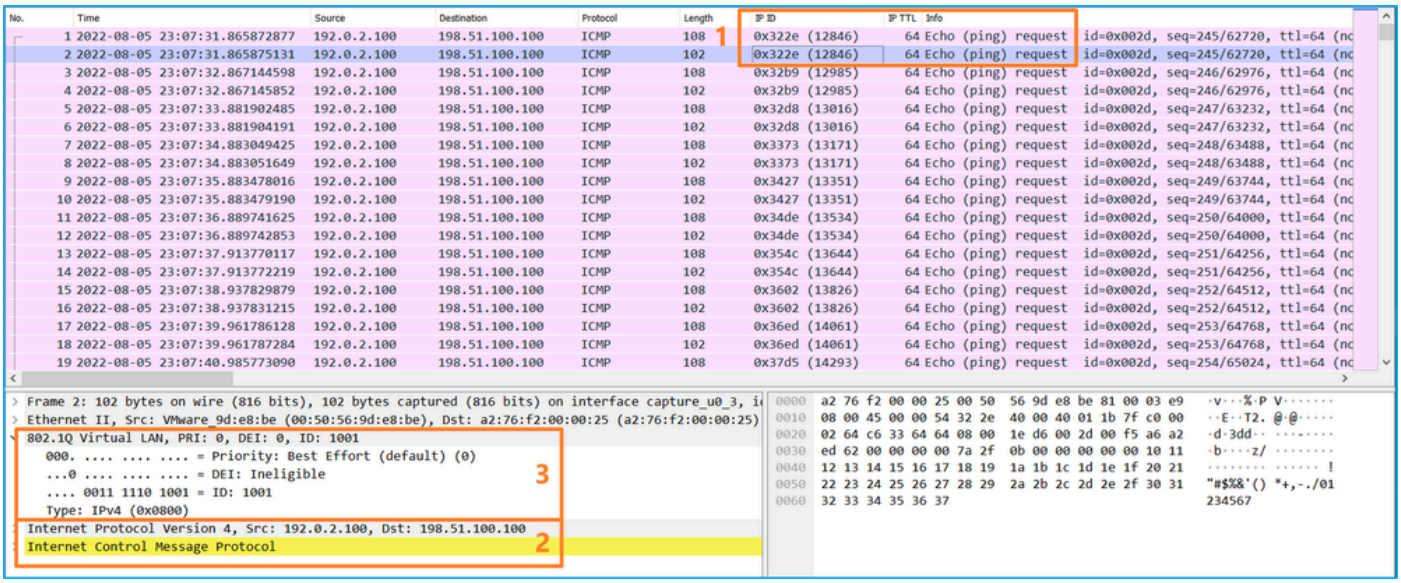
打开Portchannel1成员接口的捕获文件。选择第一个数据包并检查要点：

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

当在前接口上配置数据包捕获时，交换机将同时捕获每个数据包两次：

- 在插入端口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。

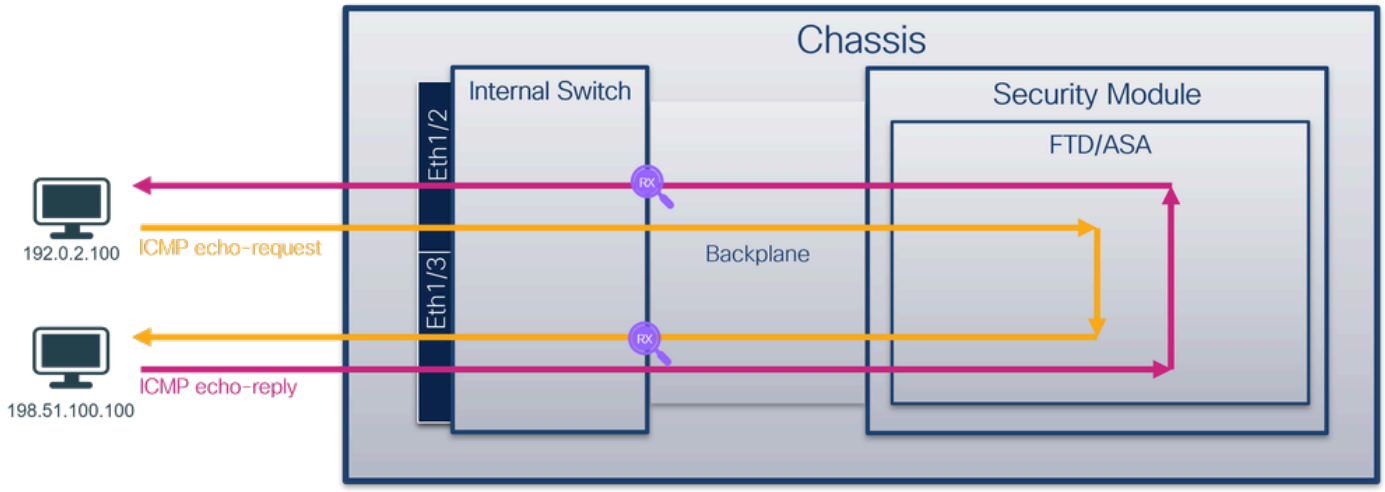
此表概述了任务：

任务	捕获点	捕获数据包中的内部端口VLAN	方向	捕获的流量
在接口Ethernet1/2上配置并检验数据包捕获	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

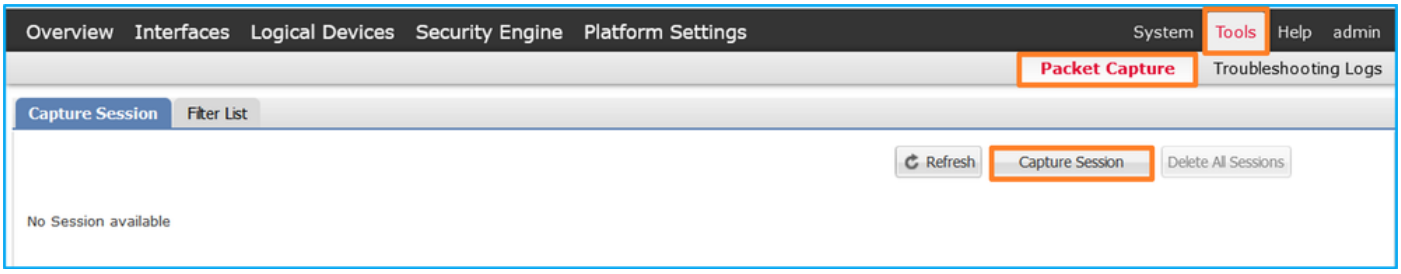


配置

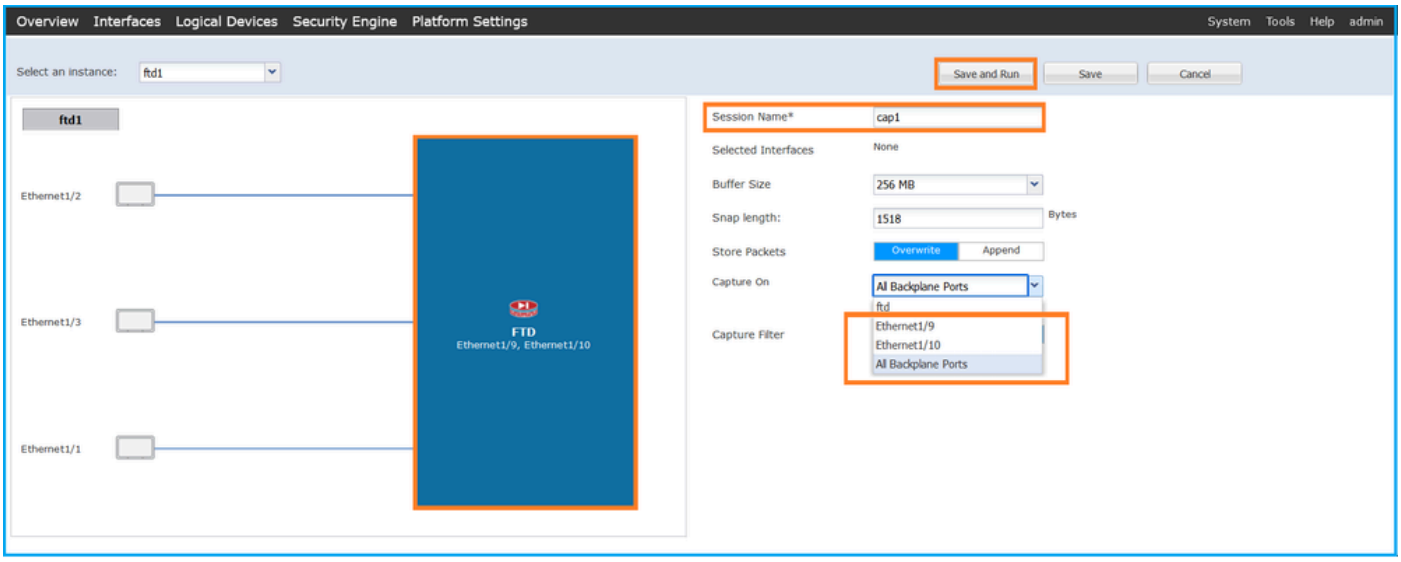
FCM

在FCM上执行以下步骤以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

在FXOS CLI上执行以下步骤以配置背板接口上的数据包捕获：

1. 标识应用类型和标识符：

```
<#root>
firepower#
scope ssa

firepower /ssa#
show app-instance

App Name   Identifier Slot ID    Admin State Oper State       Running Version Startup Version Deploy Ty
---------- ---------- ---------- ----------- ---------------- --------------- --------------- ---------
ftd        ftd1
       1          Enabled     Online          7.2.0.82        7.2.0.82        Native      No
```

2. 创建捕获会话：

```
<#root>
firepower#
scope packet-capture

firepower /packet-capture #
create session cap1

firepower /packet-capture/session* #
create phy-port Eth1/9

firepower /packet-capture/session/phy-port* #
set app ftd

firepower /packet-capture/session/phy-port* #
set app-identifier ftd1

firepower /packet-capture/session/phy-port* #
up

firepower /packet-capture/session* #
create phy-port Eth1/10
```

```
firepower /packet-capture/session/phy-port* #
set app ftd

firepower /packet-capture/session/phy-port* #
set app-identifier ftd1

firepower /packet-capture/session/phy-port* #
up

firepower /packet-capture/session* #
enable

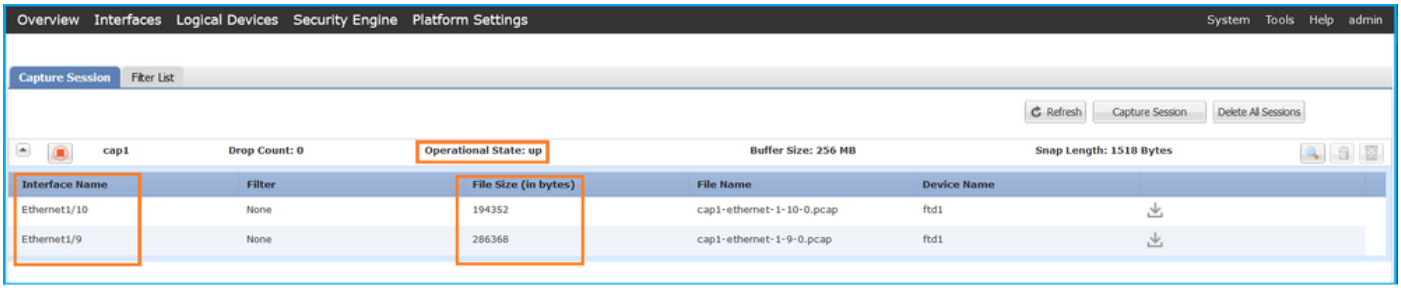
firepower /packet-capture/session* #
commit

firepower /packet-capture/session #
```

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:

```
<#root>
firepower#
scope packet-capture

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

Traffic Monitoring Session:

Packet Capture Session Name: cap1

Session: 1

Admin State: Enabled

Oper State: Up

Oper State Reason: Active

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

Physical ports involved in Packet Capture:

Slot Id: 1

Port Id: 10

Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-10-0.pcap

Pcapsize: 1017424 bytes

Filter:
Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

Slot Id: 1

Port Id: 9

Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-9-0.pcap

```
Pcapsize: 1557432  bytes


Filter:
Sub Interface: 0
Application Instance Identifier: ftd1


Application Name: ftd
```

收集捕获文件

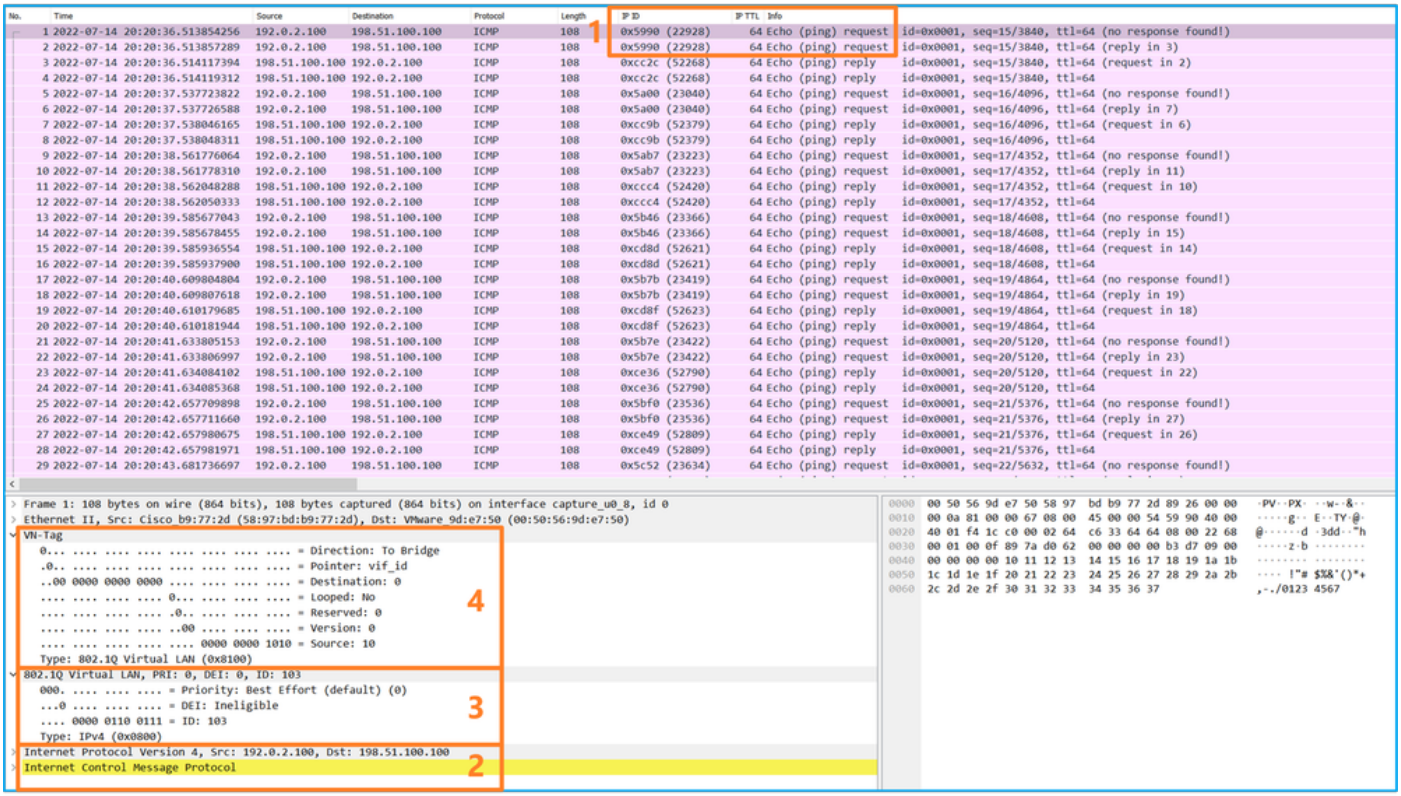
执行收集Firepower 4100/9300内部交换机捕获文件部分中的步骤。

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：

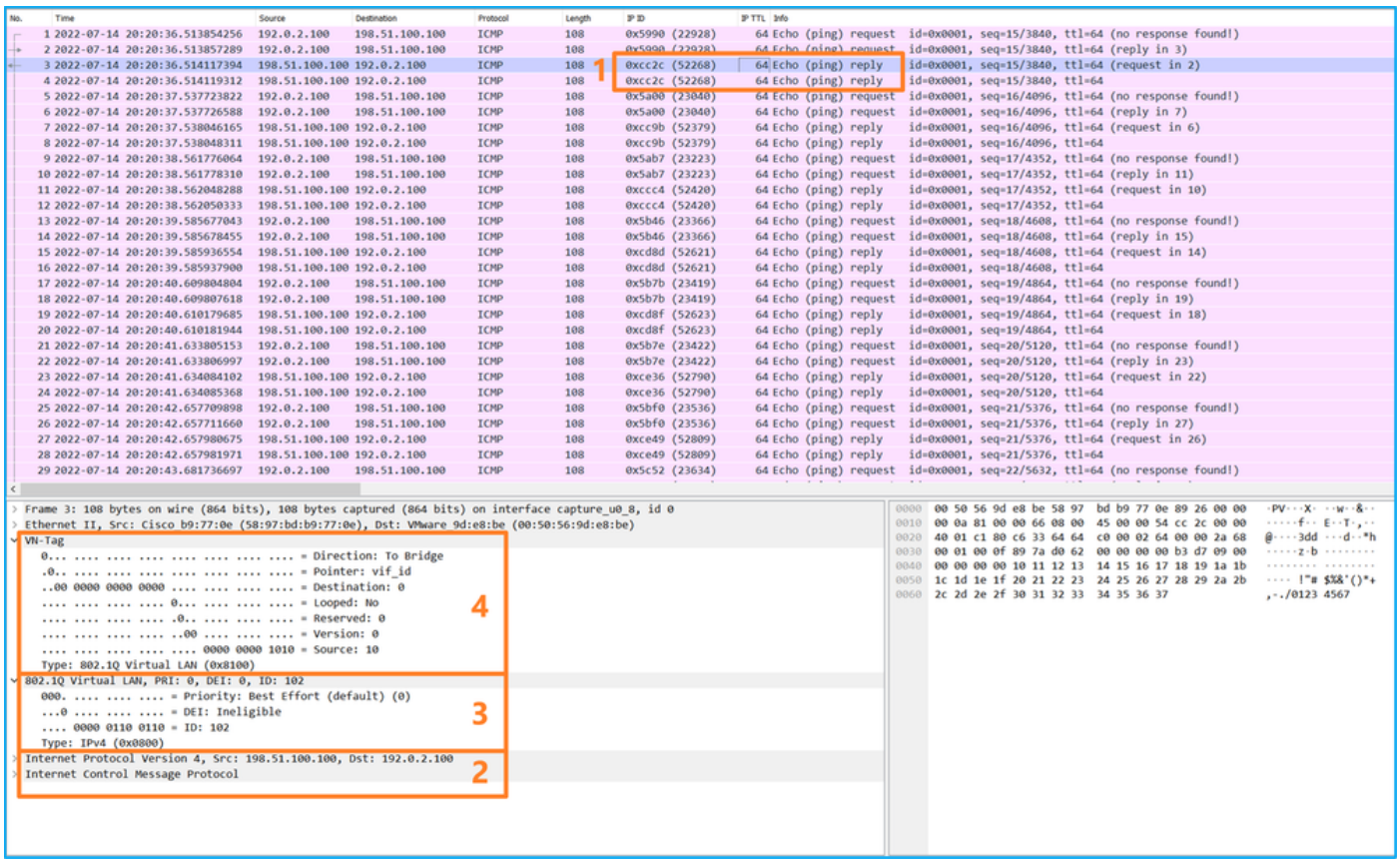
1. 捕获每个ICMP回应请求数据包，并显示2次。
2. 原始数据包报头没有VLAN标记。
3. 内部交换机插入标识出口接口Ethernet1/3的额外端口VLAN标记103。
4. 内部交换机插入一个额外的VN标记。



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
配置并检验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：

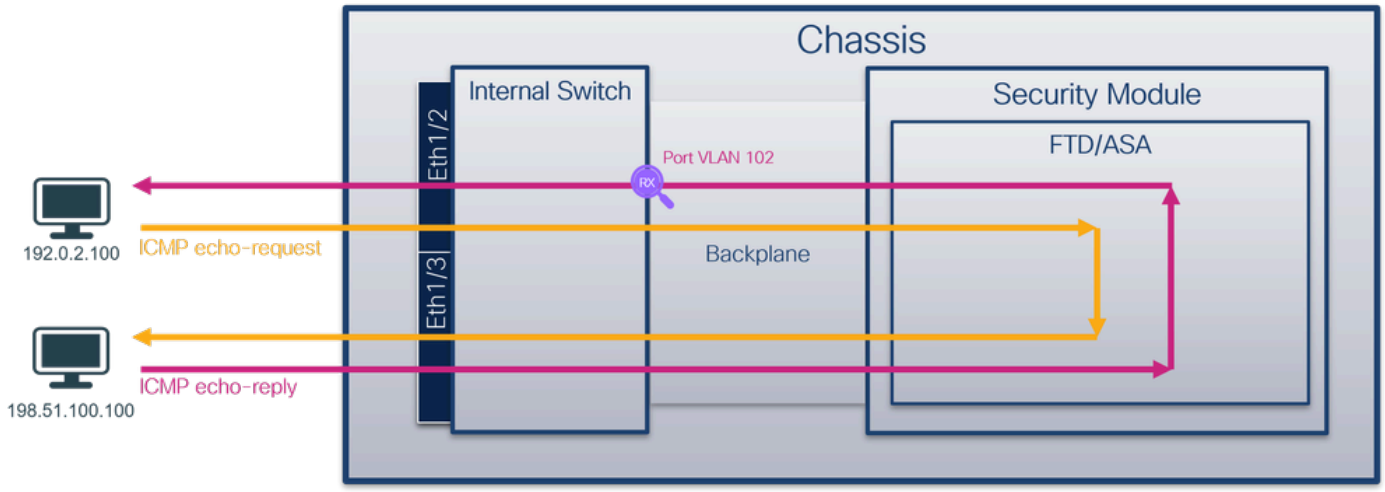
- 为离开特定前接口的数据包配置背板接口上的数据包捕获。例如，在背板接口Ethernet1/9上为离开接口Ethernet1/2的数据包配置数据包捕获。
- 在特定前接口和背板接口上配置同步数据包捕获。例如，在接口Ethernet1/2和背板接口Ethernet1/9上为离开接口Ethernet1/2的数据包配置同步数据包捕获。

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

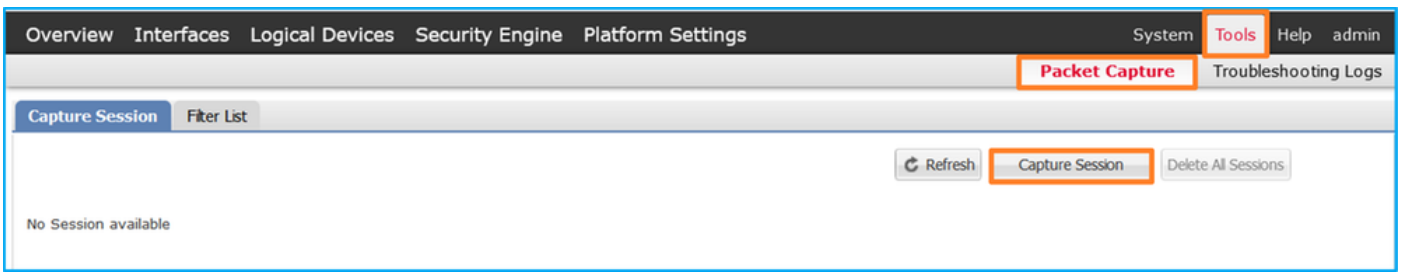


配置

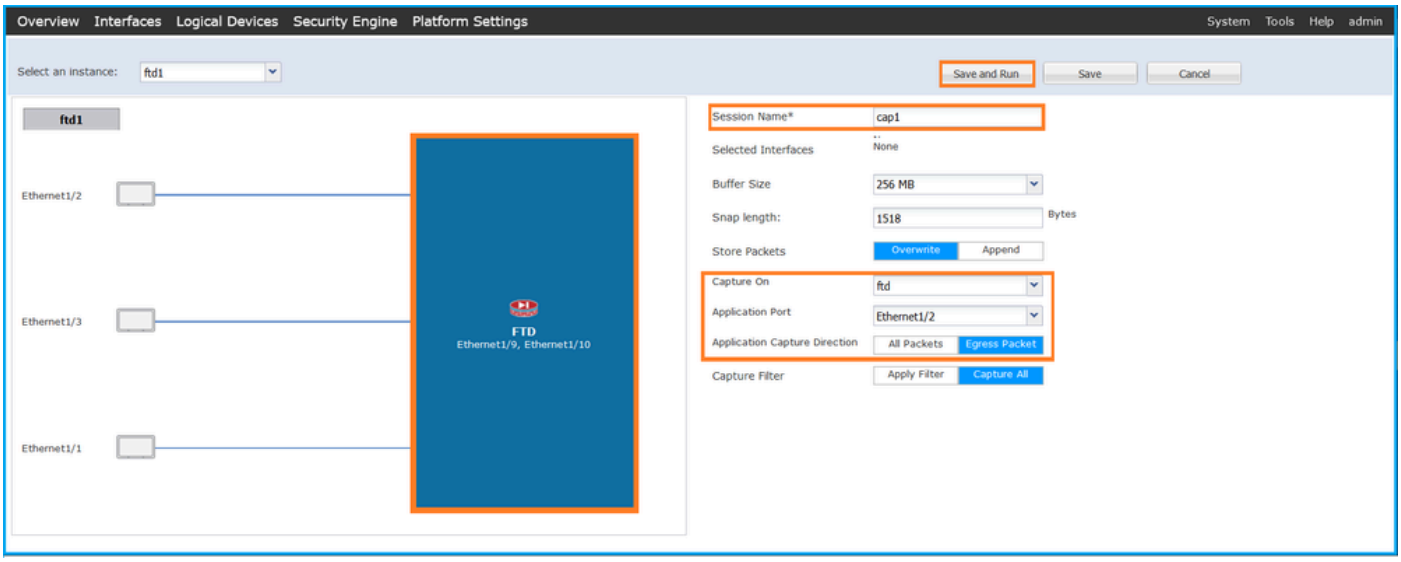
FCM

在FCM上执行以下步骤，以在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

在FXOS CLI上执行以下步骤以配置背板接口上的数据包捕获：

1. 标识应用类型和标识符：

```
<#root>

firepower#

scope ssa

firepower /ssa#

show app-instance

App Name    Identifier Slot ID     Admin State Oper State       Running Version Startup Version Deploy Ty
---------- ---------- ---------- ----------- --------------- --------------- --------------- ---------

ftd         ftd1

       1          Enabled      Online           7.2.0.82        7.2.0.82        Native      No
```

2. 创建捕获会话：

```
<#root>

firepower#

scope packet-capture

firepower /packet-capture #
```

```
create session cap1

firepower /packet-capture/session* #
create app-port 1 l12 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

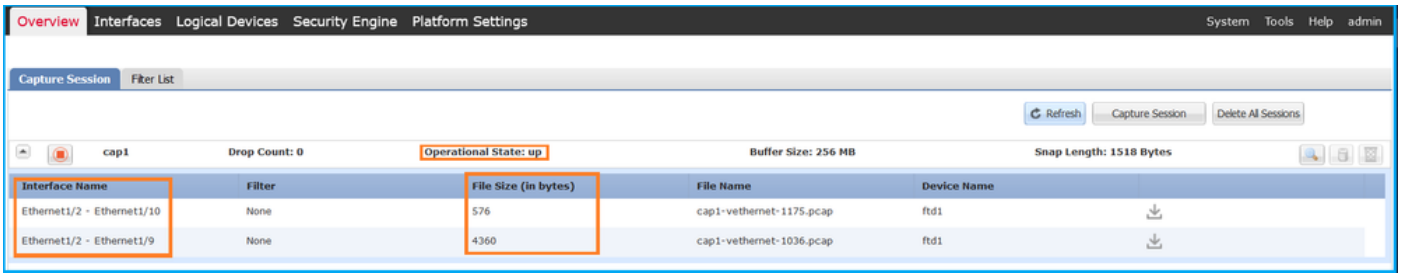
firepower /packet-capture/session/app-port* #
up

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:

```
<#root>
firepower#
scope packet-capture
```

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


Traffic Monitoring Session:
    Packet Capture Session Name: cap1

    Session: 1
    Admin State: Enabled

    Oper State: Up

    Oper State Reason: Active

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

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

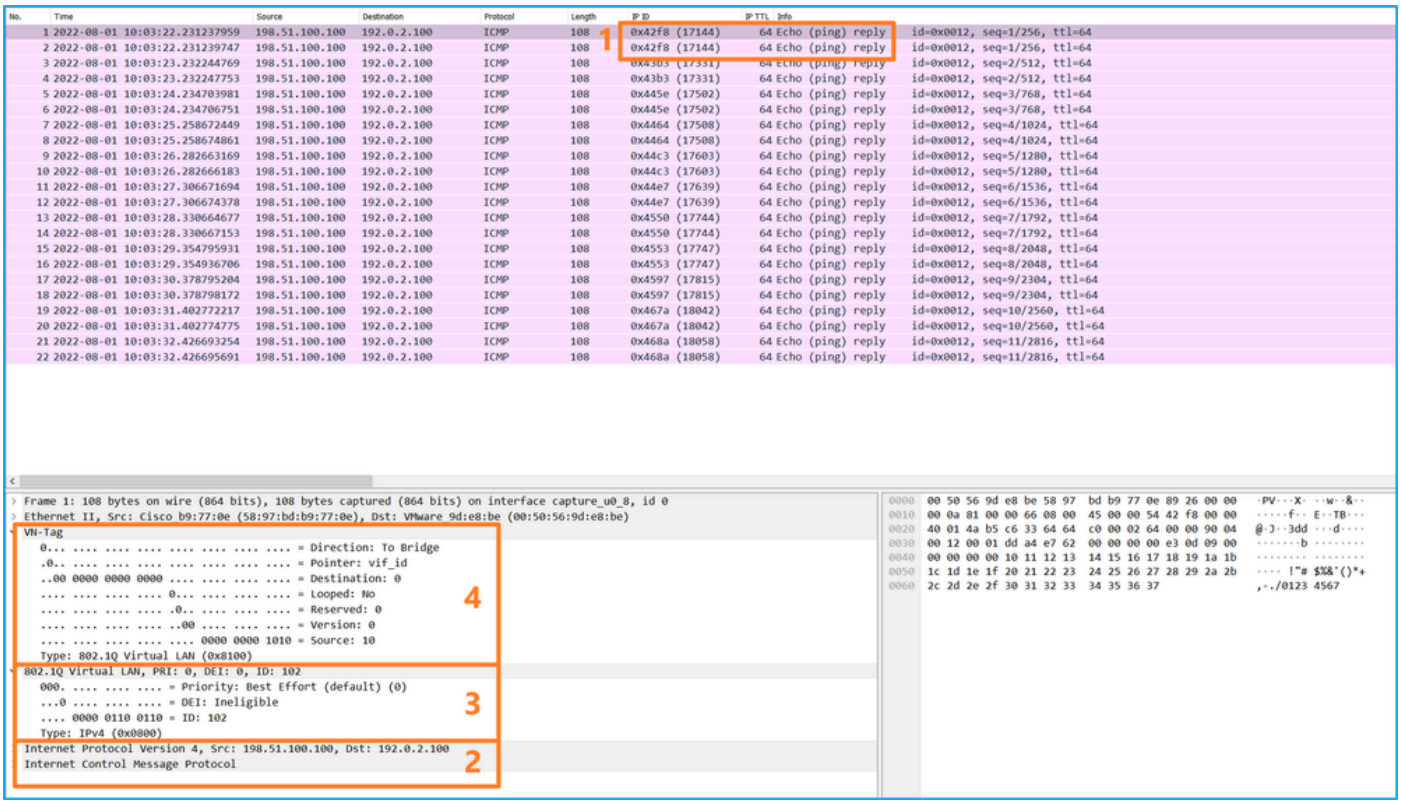
执行收集Firepower 4100/9300内部交换机捕获文件部分中的步骤。

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

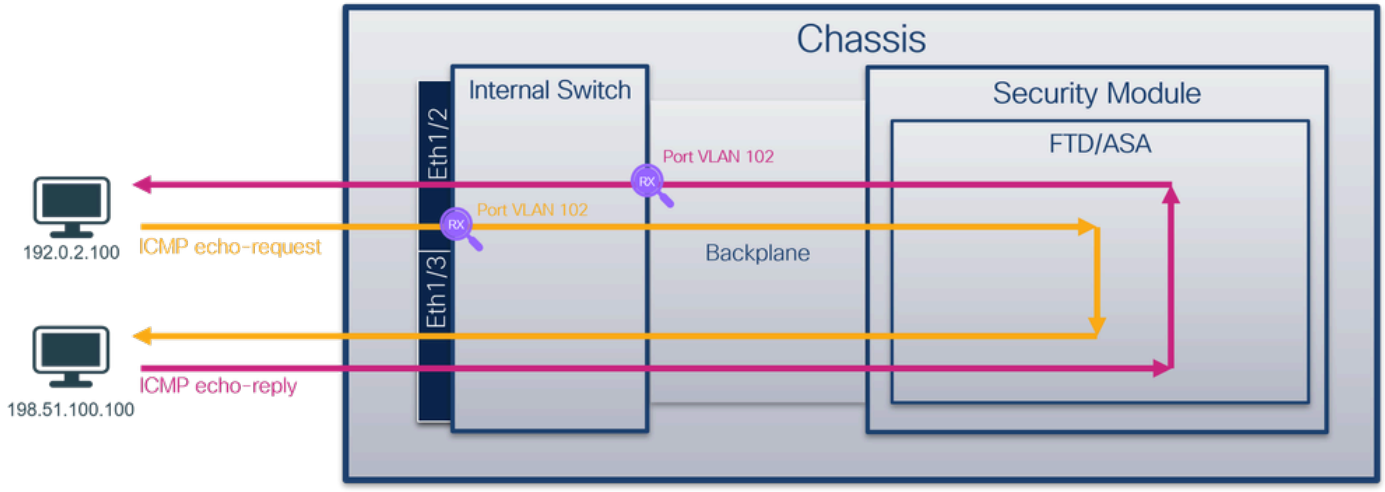
任务2

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

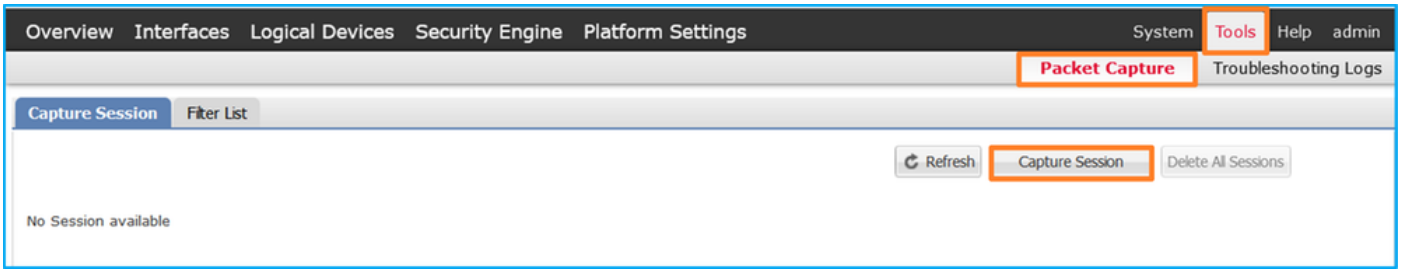


配置

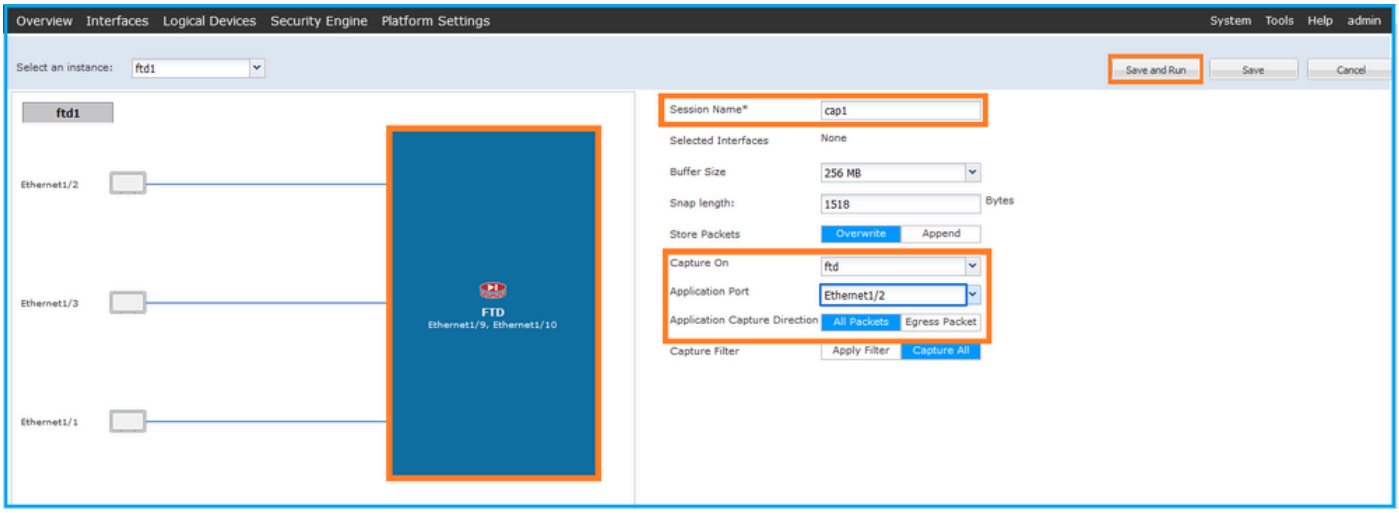
FCM

在FCM上执行以下步骤，以在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

在FXOS CLI上执行以下步骤以配置背板接口上的数据包捕获：

1. 标识应用类型和标识符：

```
<#root>
firepower#
scope ssa

firepower /ssa#
show app-instance

App Name   Identifier Slot ID    Admin State Oper State       Running Version Startup Version Deploy Ty
---------- ---------- ---------- ----------- ---------------- --------------- --------------- ---------
ftd        ftd1
       1          Enabled     Online           7.2.0.82        7.2.0.82        Native      No
```

2. 创建捕获会话：

```
<#root>
firepower#
scope packet-capture

firepower /packet-capture #
create session cap1

firepower /packet-capture/session* #
create phy-port eth1/2

firepower /packet-capture/session/phy-port* #
set app-identifier ftd1

firepower /packet-capture/session/phy-port* #
exit

firepower /packet-capture/session* #
create app-port 1 link12 Ethernet1/2 ftd

firepower /packet-capture/session/app-port* #
set app-identifier ftd1

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

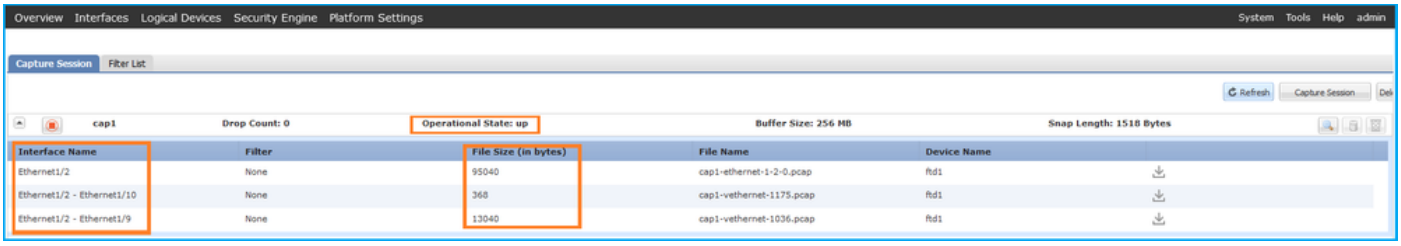
```
enable

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

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:

<#root>

```
firepower#
scope packet-capture

firepower /packet-capture #
show session cap1


Traffic Monitoring Session:
    Packet Capture Session Name: cap1

    Session: 1
    Admin State: Enabled


    Oper State: Up


    Oper State Reason: Active
```

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

Physical ports involved in Packet Capture:

    Slot Id: 1


    Port Id: 2


    Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap


    Pcapsize: 410444  bytes


    Filter:
    Sub Interface: 0

    Application Instance Identifier: ftd1


    Application Name: ftd


Application ports involved in Packet Capture:


Slot Id: 1


    Link Name: link12


    Port Name: Ethernet1/2


    App Name: ftd


    Sub Interface: 0

    Application Instance Identifier: ftd1


Application ports resolved to:
    Name: vnic1


Eq Slot Id: 1


    Eq Port Id: 9
```

```
    Pcapfile: /workspace/packet-capture/session-1/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

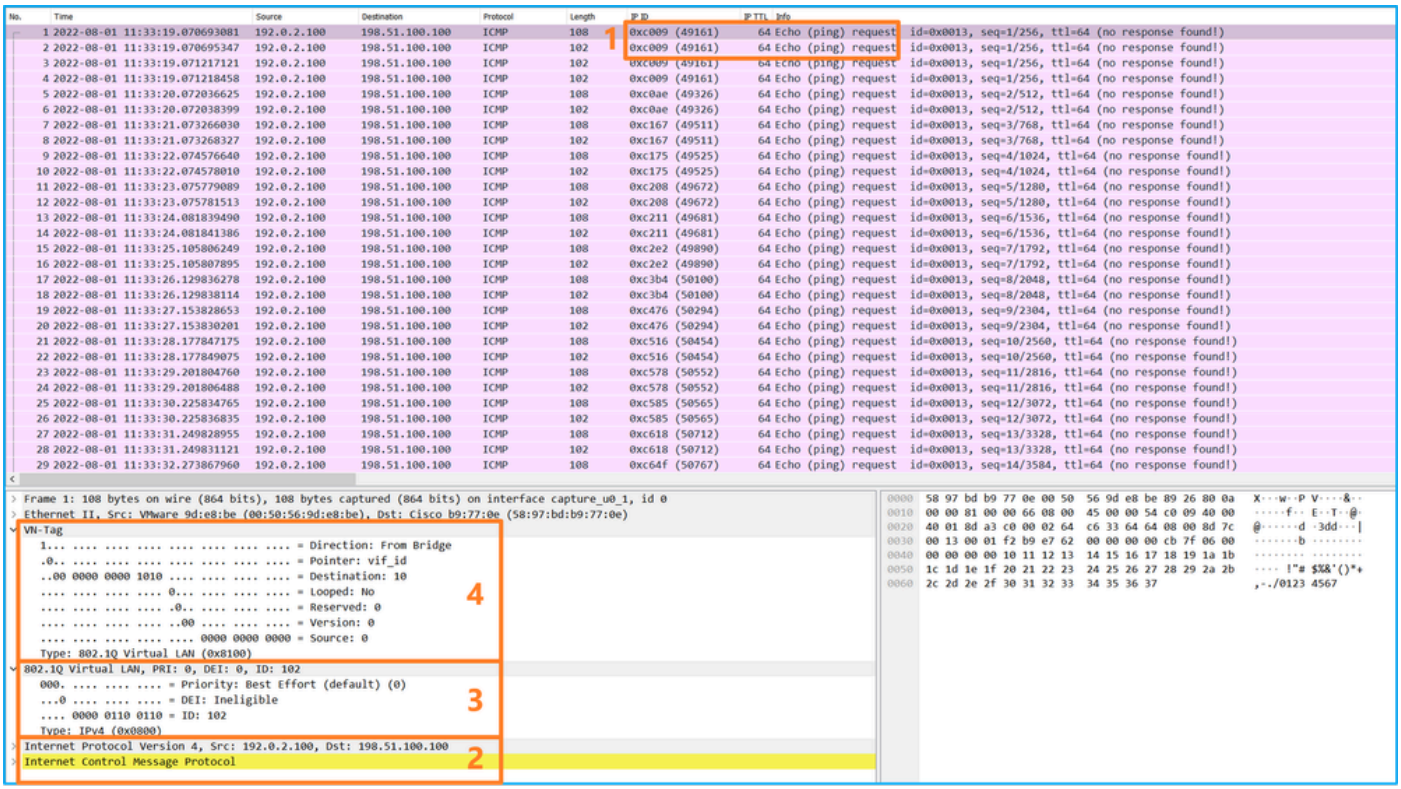
执行收集Firepower 4100/9300内部交换机捕获文件部分中的步骤。

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。

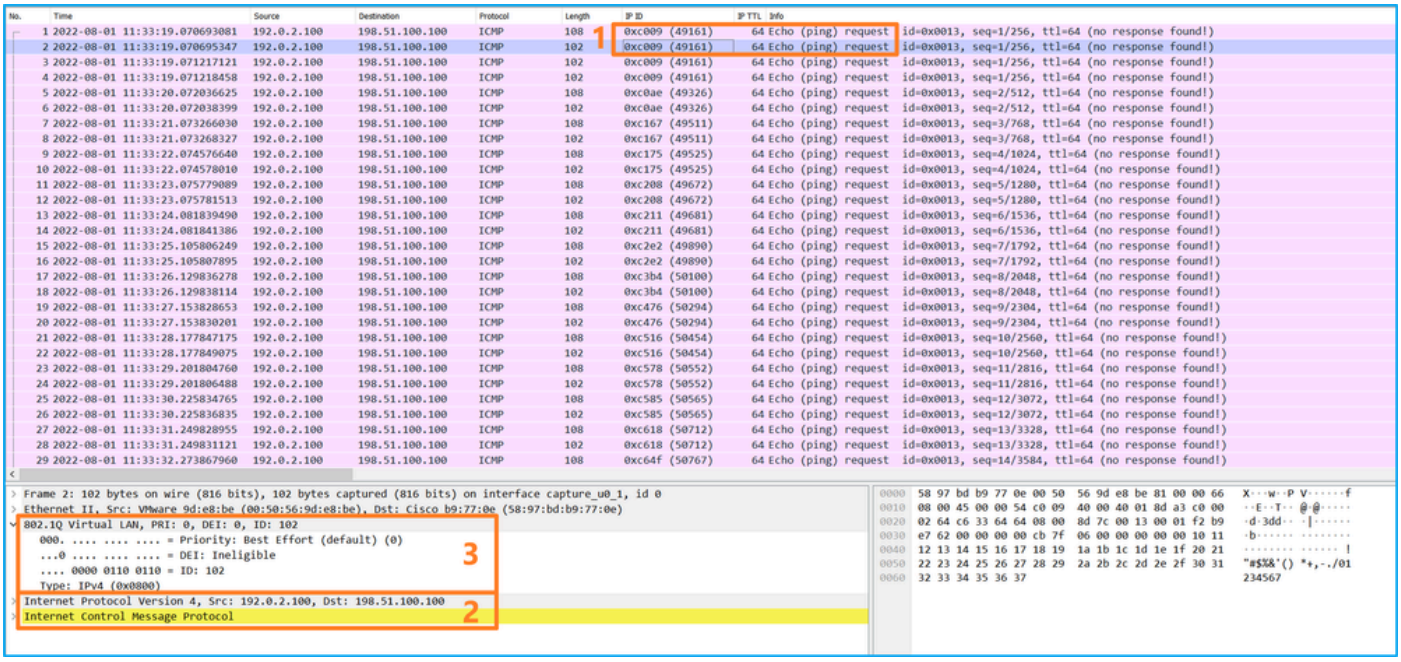
打开接口Ethernet1/2的捕获文件，选择第一个数据包，然后检查要点：

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：

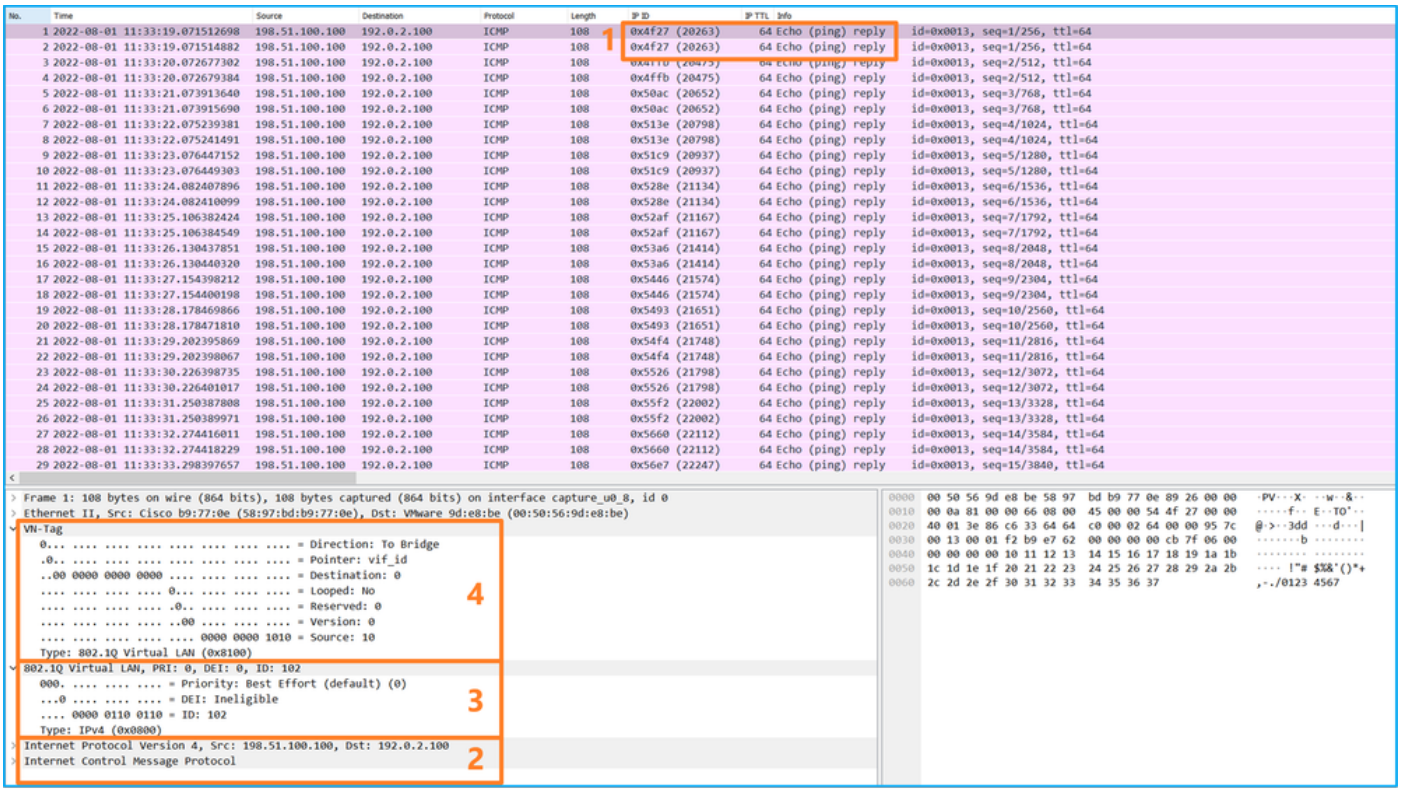
1. 仅捕获ICMP回应请求数据包。捕获每个数据包，并显示2次。
2. 原始数据包报头没有VLAN标记。
3. 内部交换机插入标识入口接口Ethernet1/2的额外端口VLAN标记102。



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。

当在前接口上配置数据包捕获时，交换机将同时捕获每个数据包两次：

- 在插入端口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：

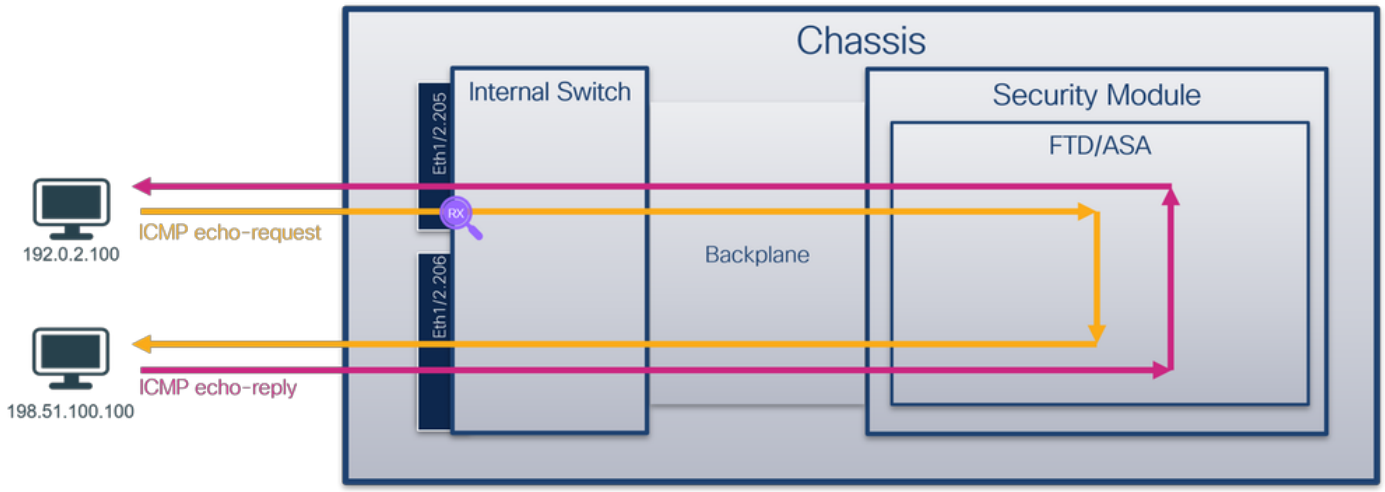
任务	捕获点	捕获数据包中的内部端口VLAN	方向	捕获的流量

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上的捕获。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

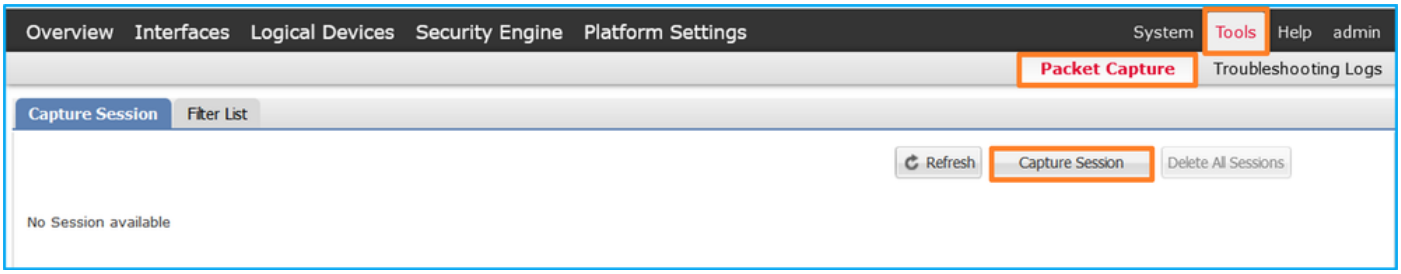


配置

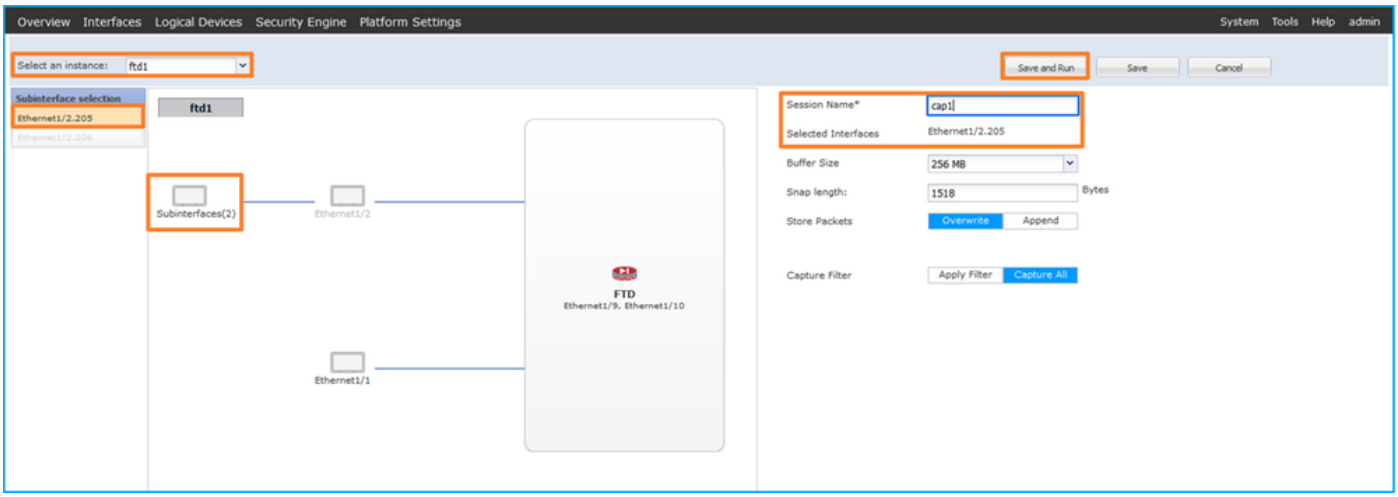
FCM

在FCM上执行以下步骤，以在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：

```
<#root>

firepower#

scope ssa

firepower /ssa #

show app-instance

App Name   Identifier Slot ID    Admin State Oper State       Running Version Startup Version Deploy Ty
---------- ---------- ---------- ----------- ---------------- --------------- --------------- ---------

ftd        ftd1

       1          Enabled     Online           7.2.0.82        7.2.0.82        Container   No          R
ftd        ftd2       1           Enabled     Online           7.2.0.82        7.2.0.82        Container
```

2. 对于端口通道接口，请标识其成员接口：

```
<#root>

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：

<#root>

firepower#

scope packet-capture

firepower /packet-capture #

create session cap1

firepower /packet-capture/session* #

create phy-port Eth1/2

firepower /packet-capture/session/phy-port* #

set app ftd

firepower /packet-capture/session/phy-port* #

set app-identifier ftd1

firepower /packet-capture/session/phy-port* #

set subinterface 205

firepower /packet-capture/session/phy-port* #

up

firepower /packet-capture/session* #

enable

firepower /packet-capture/session* #

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：

```
<#root>
firepower#
scope packet-capture

firepower /packet-capture #
create filter vlan207

firepower /packet-capture/filter* #
set ovlan 207

firepower /packet-capture/filter* #
up

firepower /packet-capture* #
create session cap1

firepower /packet-capture/session*
create phy-port Eth1/3

firepower /packet-capture/session/phy-port* #
set app ftd

firepower /packet-capture/session/phy-port* #
set app-identifier ftd1

firepower /packet-capture/session/phy-port* #
set subinterface 207

firepower /packet-capture/session/phy-port* #
up

firepower /packet-capture/session* #
create phy-port Eth1/4

firepower /packet-capture/session/phy-port* #
```

```
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 #
```

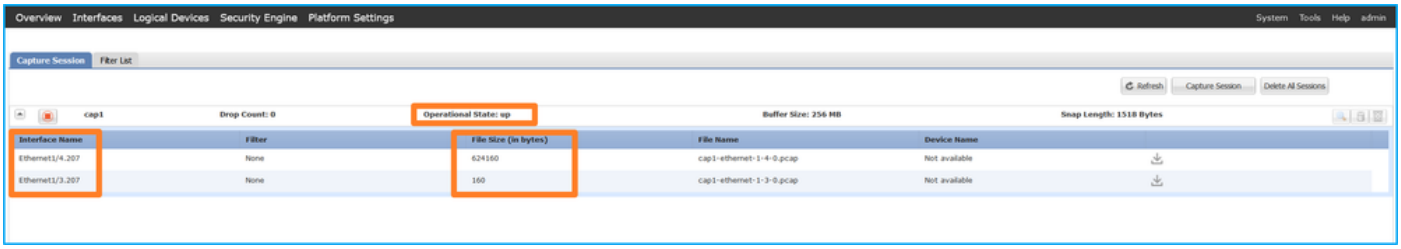
确认

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:

<#root>

```
firepower#
scope packet-capture

firepower /packet-capture #
show session cap1


Traffic Monitoring Session:
    Packet Capture Session Name: cap1

    Session: 1
    Admin State: Enabled

    Oper State: Up

    Oper State Reason: Active

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

Physical ports involved in Packet Capture:
    Slot Id: 1

    Port Id: 2

    Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap

    Pcapsize: 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:

<#root>

firepower#

scope packet-capture

firepower /packet-capture # show session cap1

Traffic Monitoring Session:

Packet Capture Session Name: cap1

Session: 1

Admin State: Enabled

Oper State: Up

Oper State Reason: Active

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

Physical ports involved in Packet Capture:

Slot Id: 1

Port Id: 3

Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-3-0.pcap

Pcapsize: 160 bytes

Filter:

Sub Interface: 207

Application Instance Identifier: ftd1

```
    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
```

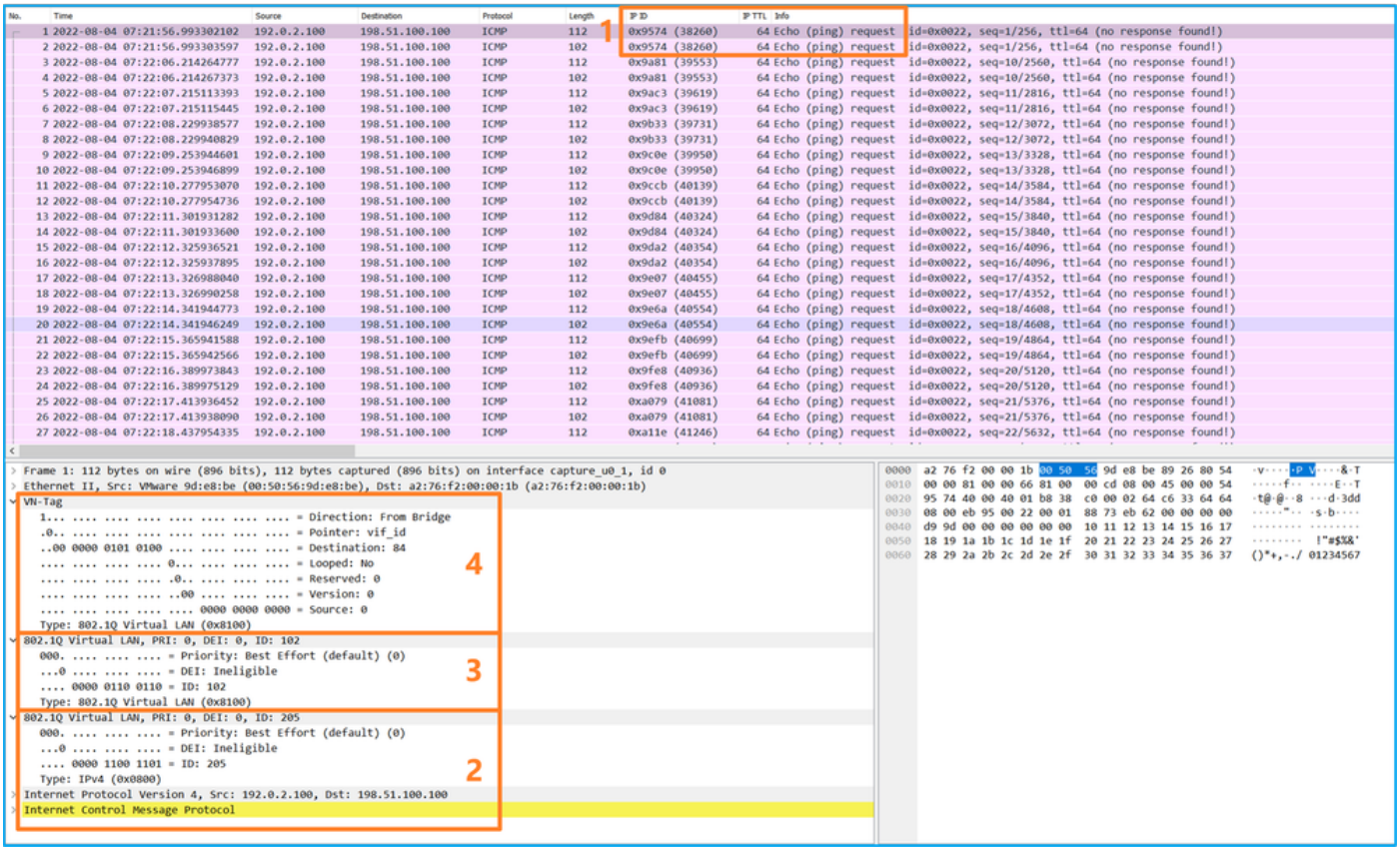
收集捕获文件

执行收集Firepower 4100/9300内部交换机捕获文件部分中的步骤。

捕获文件分析

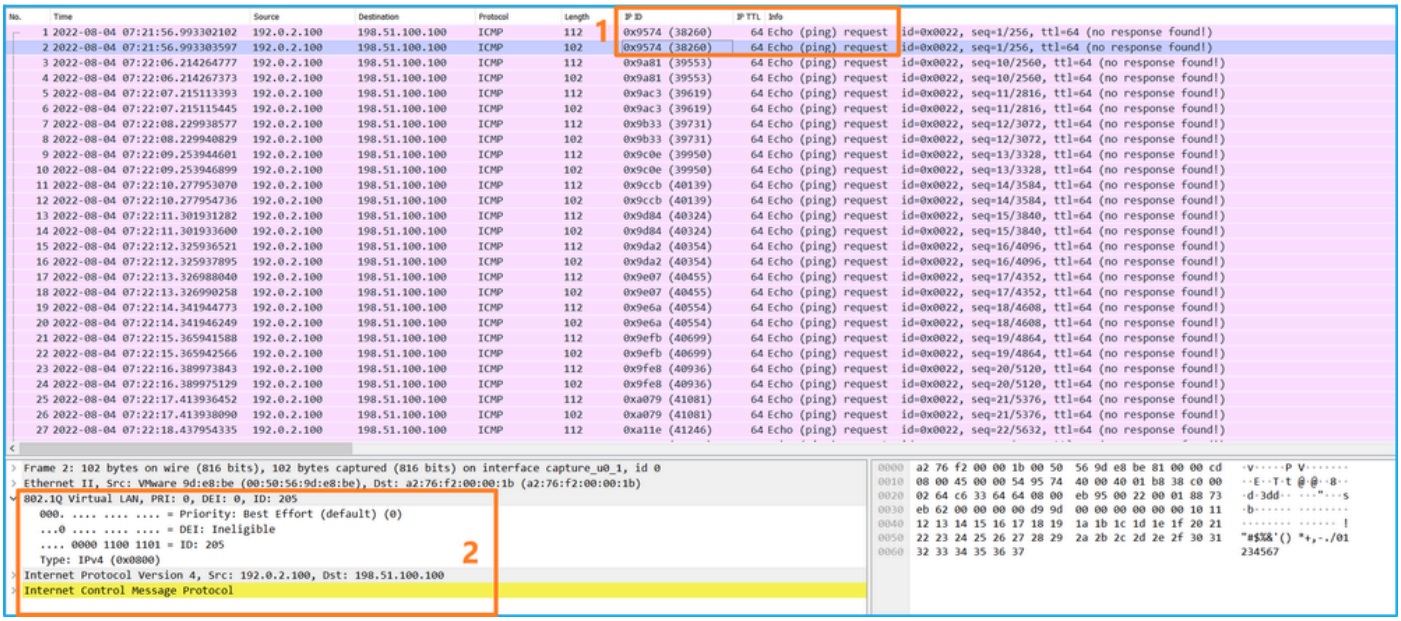
使用数据包捕获文件读取器应用程序打开捕获文件。选择第一个数据包并检查要点：

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。



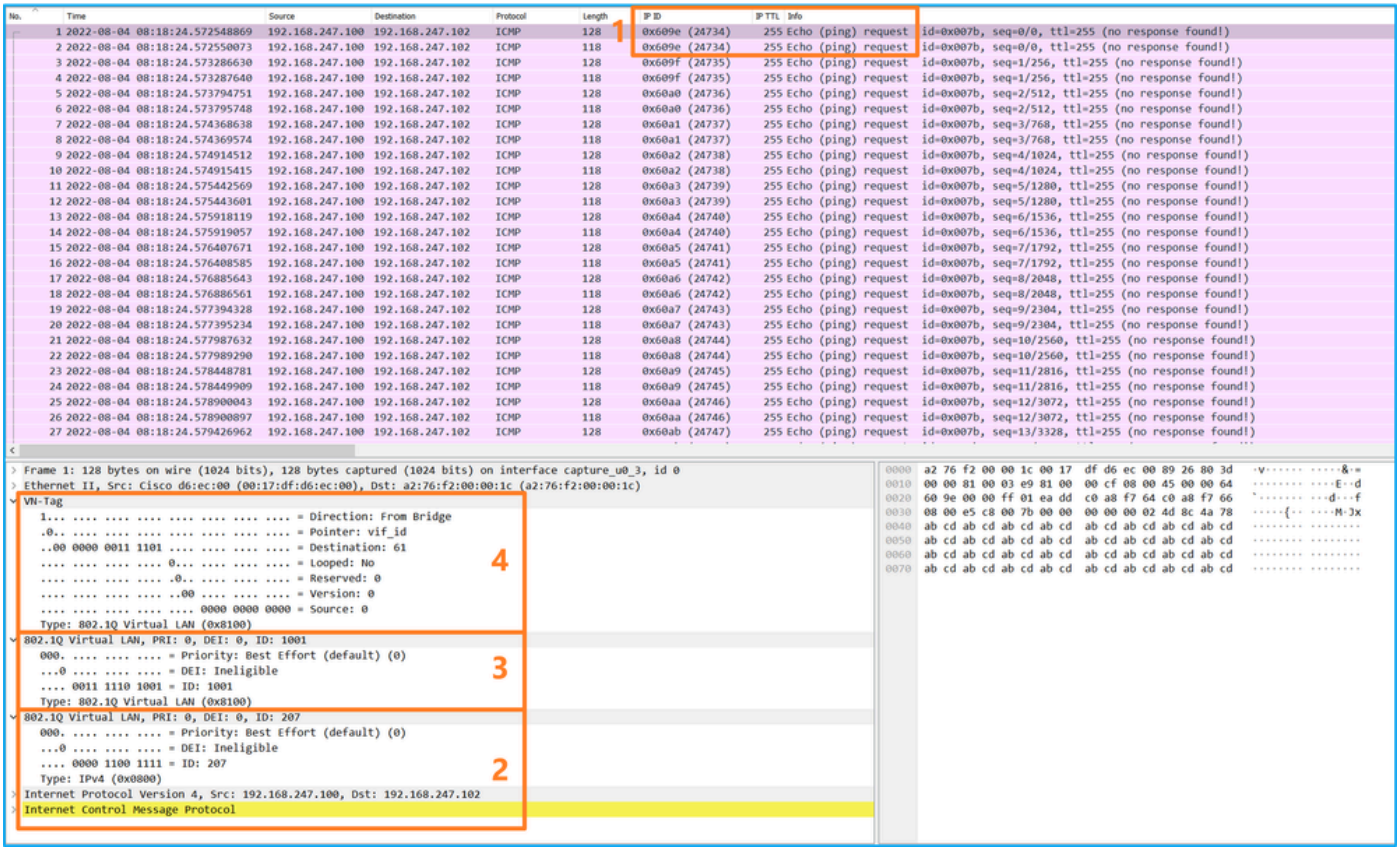
选择第二个数据包并检查要点：

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。



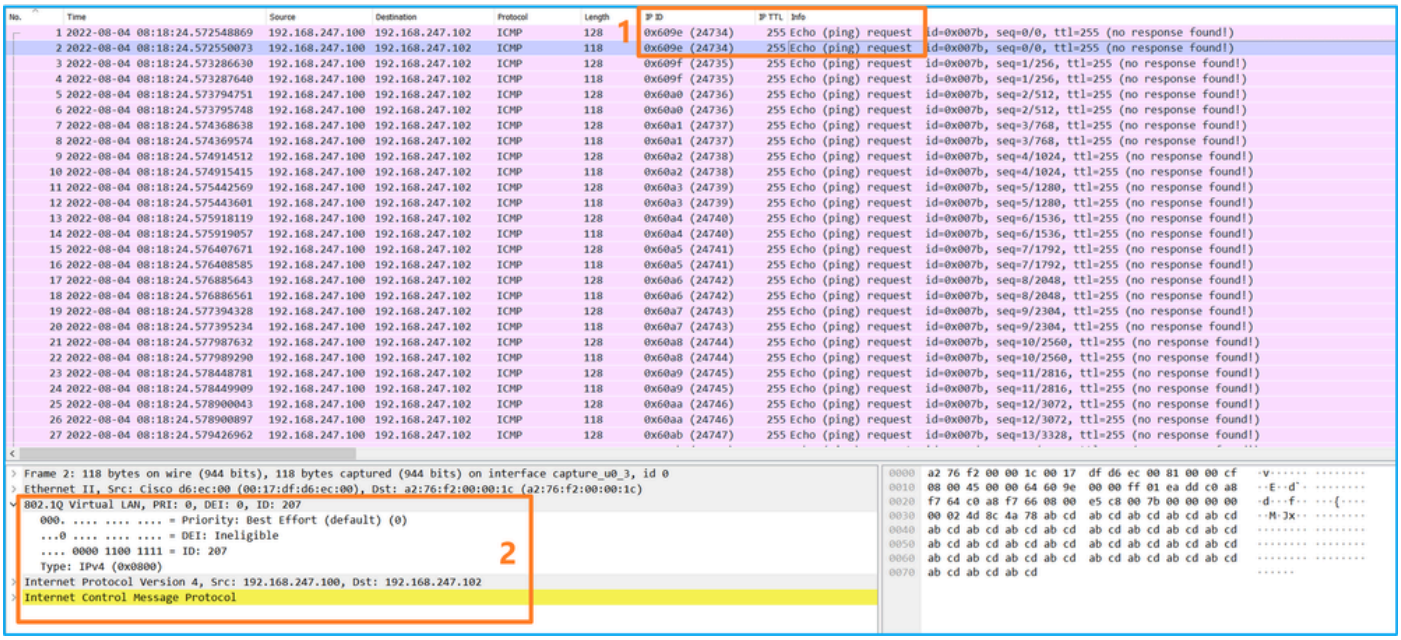
现在打开Portchannel1.207的捕获文件。选择第一个数据包并检查要点

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

当在前接口上配置数据包捕获时，交换机将同时捕获每个数据包两次：

- 在插入端口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。

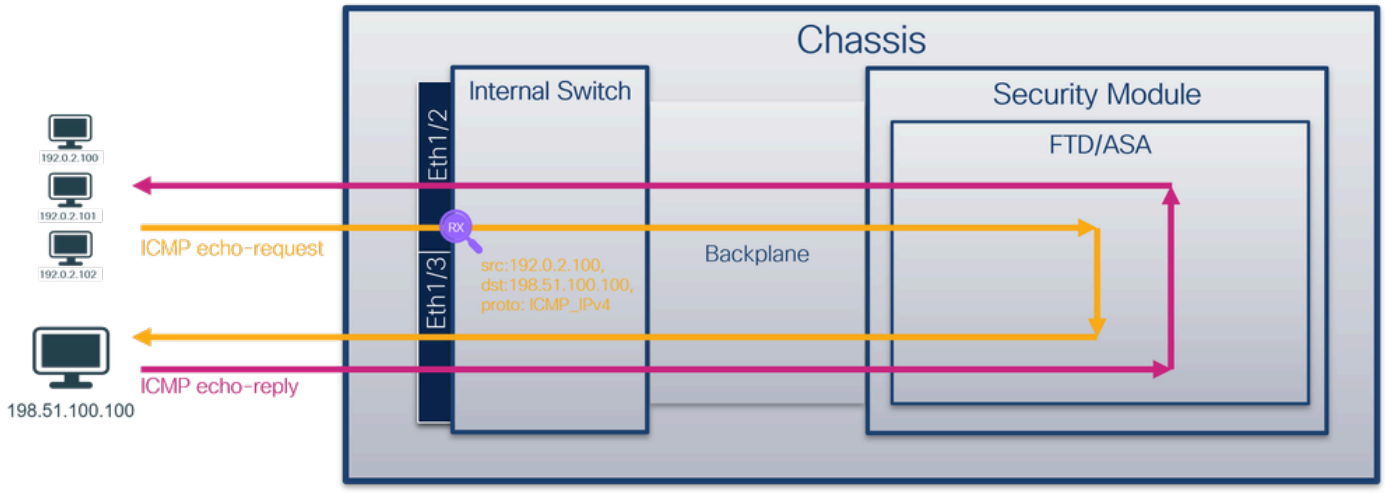
此表概述了任务：

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	Ethernet1/3 Ethernet1/4	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



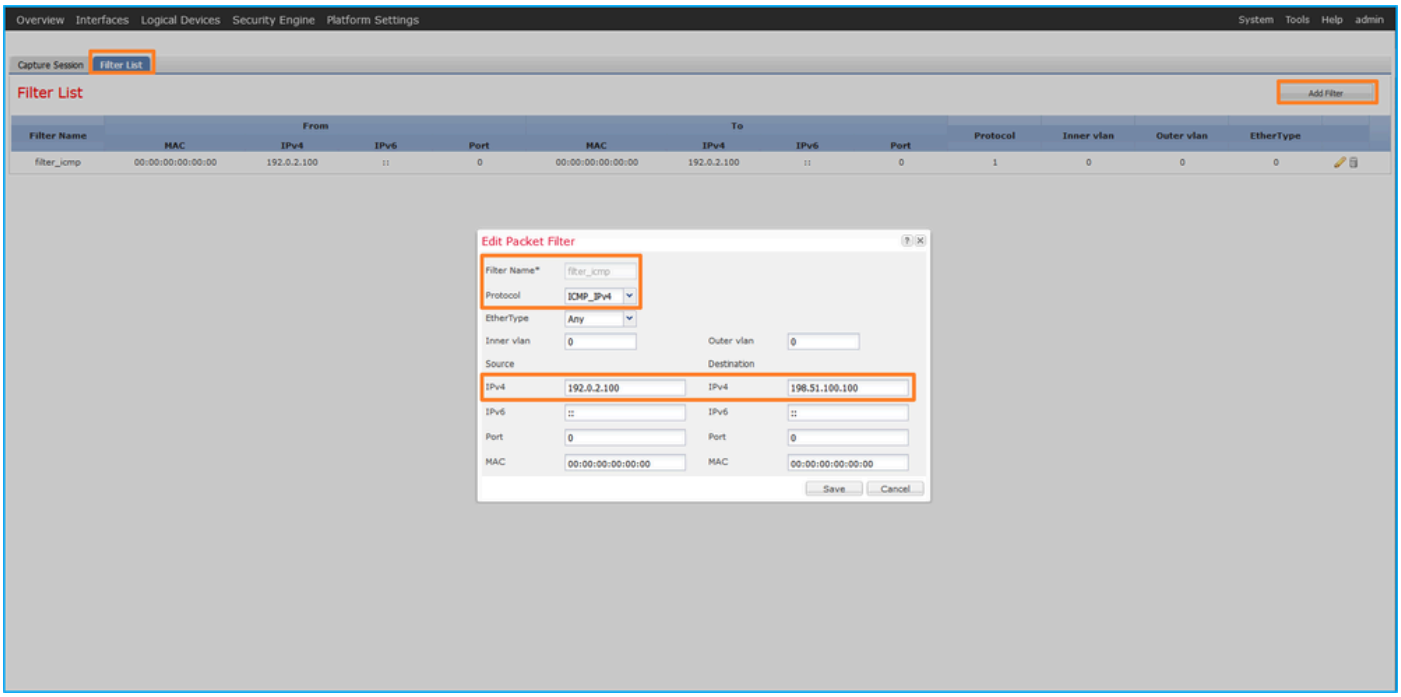
配置

FCM

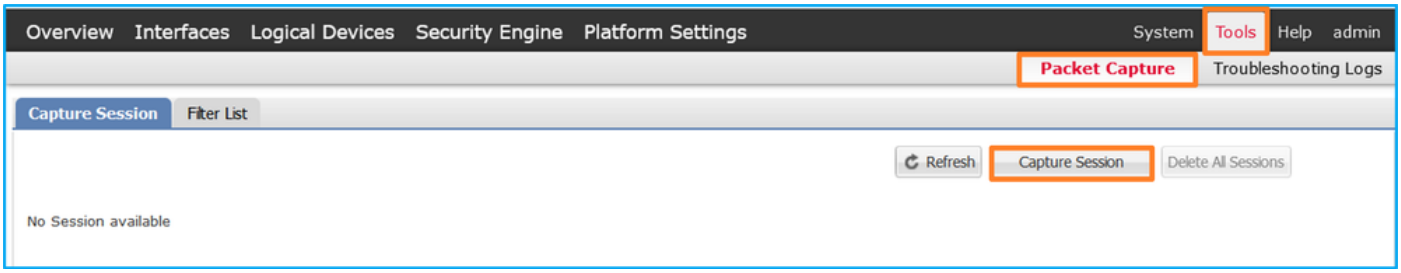
在FCM上执行以下步骤，为从主机192.0.2.100到主机198.51.100.100的ICMP回应请求数据包配置捕获过滤器，并将其应用于接口Ethernet1/2上的数据包捕获：

1. 使用Tools > Packet Capture > Filter List > Add Filter 创建捕获过滤器。

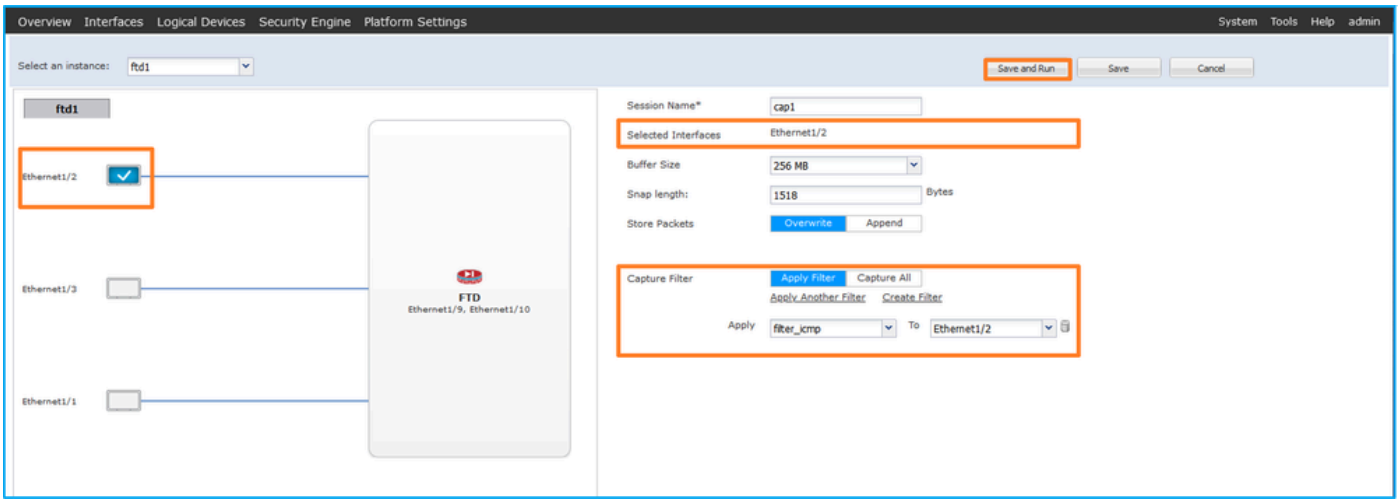
2. 指定Filter Name、Protocol、Source IPv4、Destination IPv4，然后单击Save:



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

在FXOS CLI上执行以下步骤以配置背板接口上的数据包捕获：

1. 标识应用类型和标识符：

```
<#root>

firepower#

scope ssa


firepower /ssa#

show app-instance


App Name   Identifier Slot ID    Admin State Oper State       Running Version Startup Version Deploy Ty
---------- ---------- ---------- ----------- ---------------- --------------- --------------- ---------

ftd        ftd1

       1          Enabled     Online           7.2.0.82        7.2.0.82        Native      No
```

2.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：

```
<#root>

firepower#

scope packet-capture


firepower /packet-capture #

create filter filter_icmp


firepower /packet-capture/filter* #

set destip 198.51.100.100


firepower /packet-capture/filter* #

set protocol 1


firepower /packet-capture/filter* #

set srcip 192.0.2.100


firepower /packet-capture/filter* #

exit


firepower /packet-capture* #
```

```
create session cap1

firepower /packet-capture/session* #
create phy-port Ethernet1/2

firepower /packet-capture/session/phy-port* #
set app ftd

firepower /packet-capture/session/phy-port* #
set 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

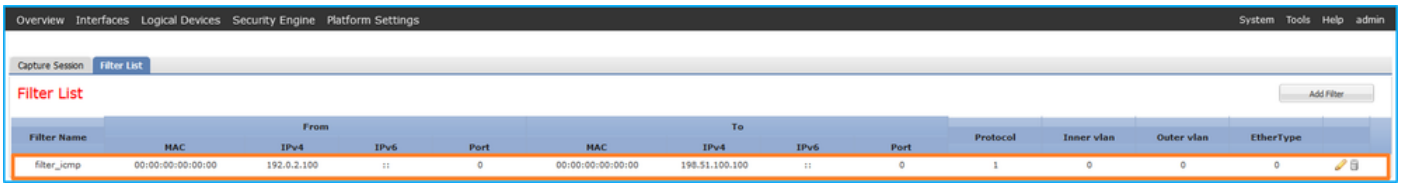
firepower /packet-capture/session* #
commit

firepower /packet-capture/session #
```

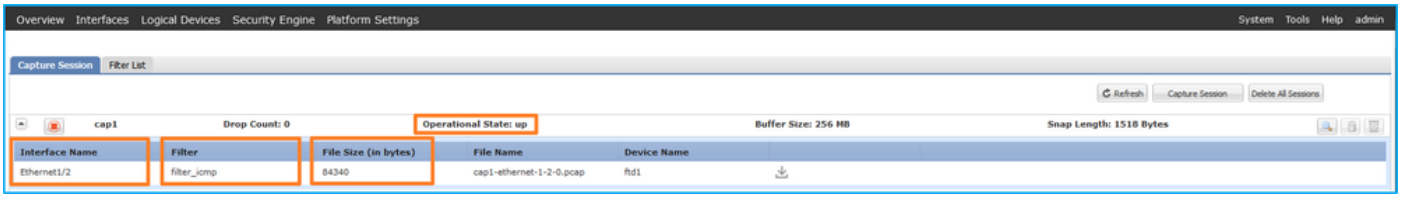
确认

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:

<#root>

firepower#

scope packet-capture

firepower /packet-capture #

show filter detail

Configure a filter for packet capture:

Name: filter_icmp

    Protocol: 1

    Ivlan: 0
    Ovlan: 0

Src Ip: 192.0.2.100

    Dest Ip: 198.51.100.100

    Src MAC: 00:00:00:00:00:00
    Dest MAC: 00:00:00:00:00:00
    Src Port: 0
    Dest Port: 0
    Ethertype: 0
    Src Ipv6: ::
    Dest Ipv6: ::
firepower /packet-capture #

show session cap1

Traffic Monitoring Session:

    Packet Capture Session Name: cap1

    Session: 1

    Admin State: Enabled

    Oper State: Up

```
    Oper State Reason: Active


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

Physical ports involved in Packet Capture:

Slot Id: 1


    Port Id: 2


    Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap


    Pcapsize: 213784  bytes



Filter: filter_icmp


    Sub Interface: 0
    Application Instance Identifier: ftd1


    Application Name: ftd
```

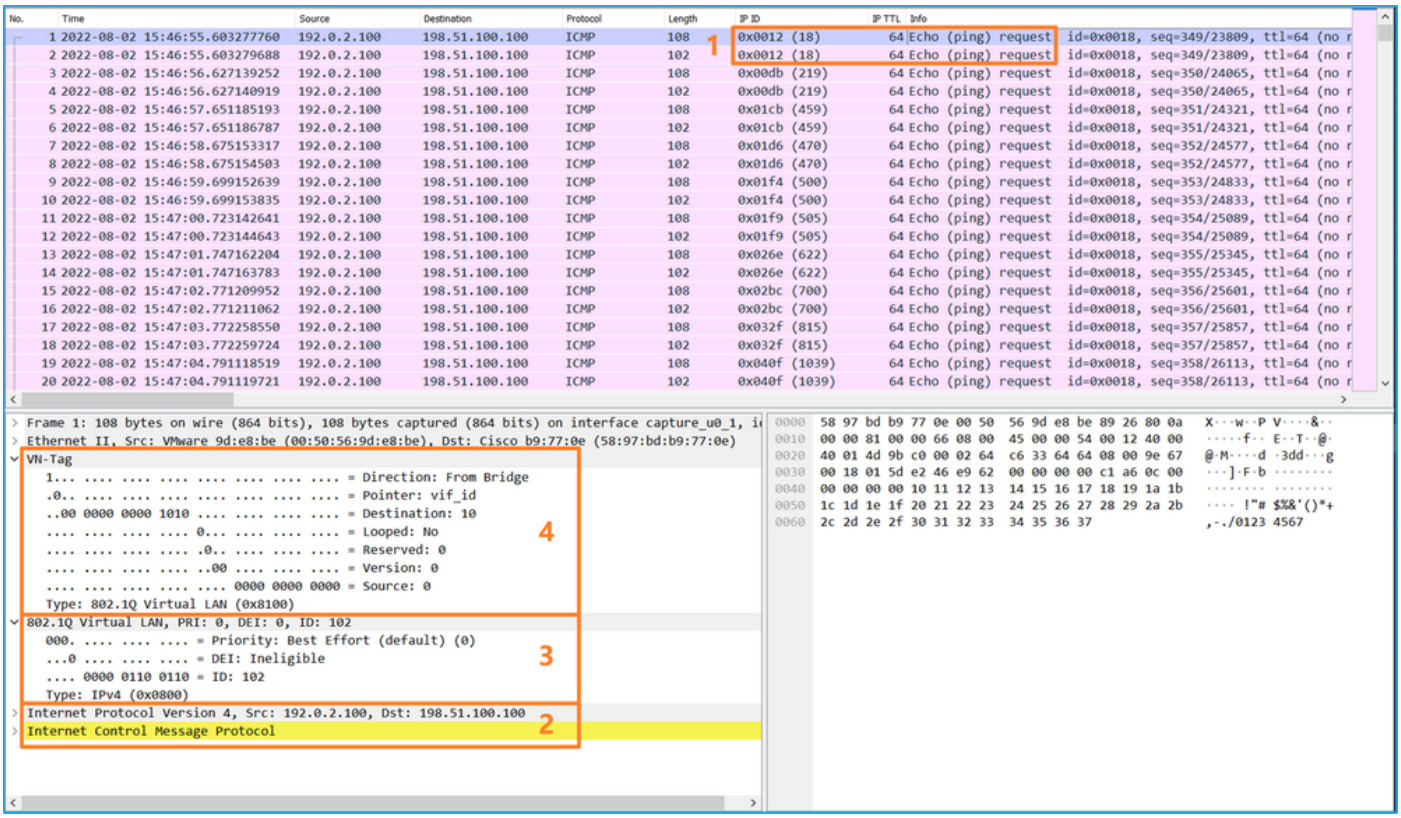
收集捕获文件

执行收集Firepower 4100/9300内部交换机捕获文件部分中的步骤。

捕获文件分析

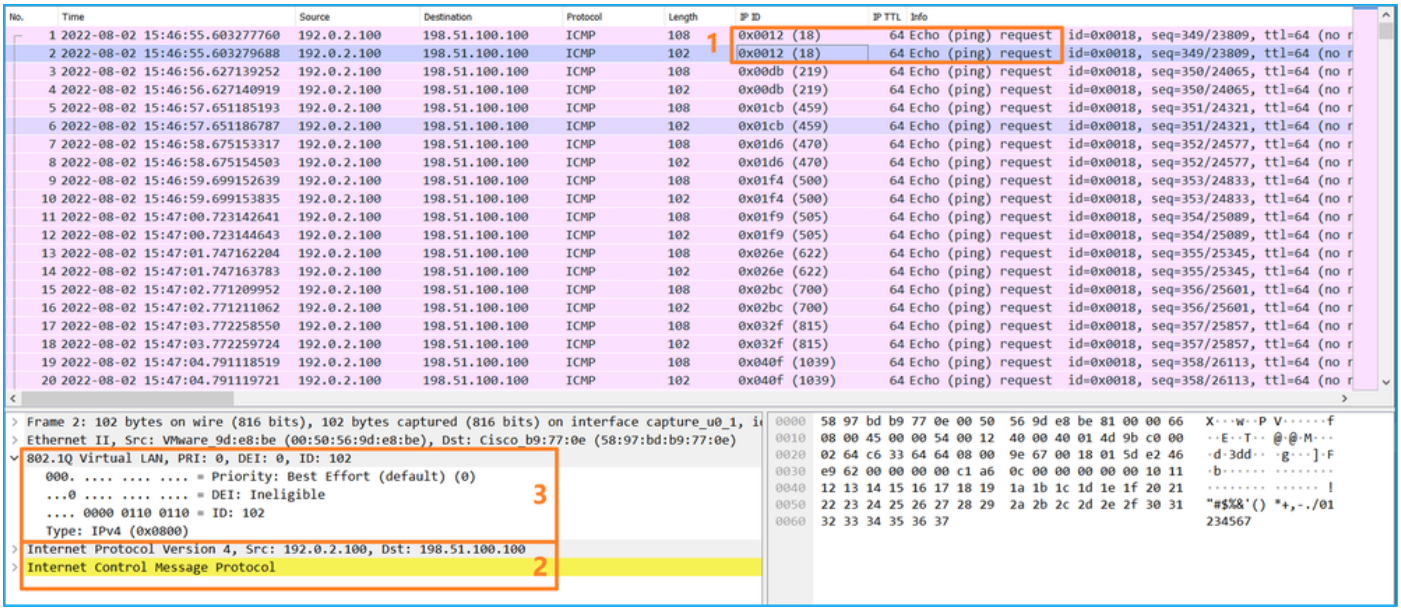
使用数据包捕获文件读取器应用程序打开捕获文件。选择第一个数据包并检查要点

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

当在前接口上配置数据包捕获时，交换机将同时捕获每个数据包两次：

- 在插入端口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：

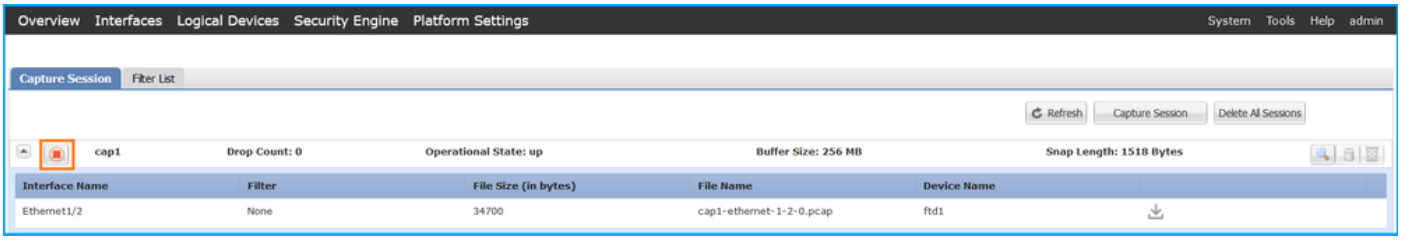
任务	捕获点	捕获数据包中的内部端口VLAN	方向	用户过滤器	捕获的流量
使用前接口Ethernet1/2上的过滤器配置并检验数据包捕获	以太网1/2	102	仅限入口	协议：ICMP 源：192.0.2.100 目的地：198.51.100.100	从主机192.0.2.100到主机198.51.100.100的ICMP回应请求

收集Firepower 4100/9300内部交换机捕获文件

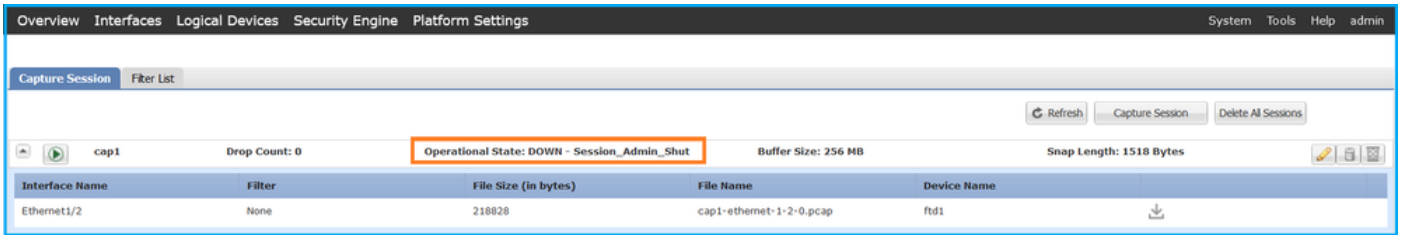
FCM

在FCM上执行以下步骤以收集内部交换机捕获文件：

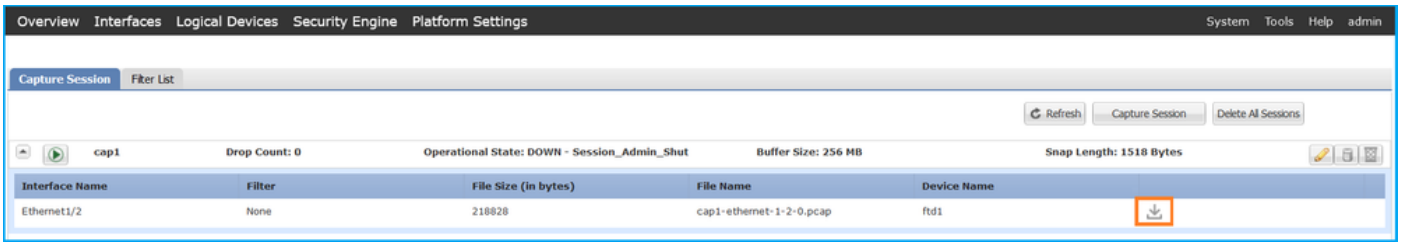
1. 单击Disable Session按钮停止活动捕获：



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，请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：

```
<#root>
firepower#
scope packet-capture

firepower /packet-capture #
scope session cap1

firepower /packet-capture/session #
disable

firepower /packet-capture/session* #
commit

firepower /packet-capture/session #
up

firepower /packet-capture #
show session cap1 detail


Traffic Monitoring Session:
    Packet Capture Session Name:
cap1

    Session: 1
    Admin State: Disabled


    Oper State: Down
```

```
    Oper State Reason: Admin Disable


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

Physical ports involved in Packet Capture:
    Slot Id: 1
    Port Id: 2
    Pcapfile:
/workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap


    Pcapsize: 115744  bytes
    Filter:
    Sub Interface: 0
    Application Instance Identifier: ftd1
    Application Name: ftd
```

2. 从local-mgmt命令范围上传捕获文件：

```
<#root>

firepower#

connect local-mgmt


firepower(local-mgmt)#

copy /packet-capture/session-1/cap1-ethernet-1-2-0.pcap ?


  ftp:        Dest File URI
  http:       Dest File URI
  https:      Dest File URI
  scp:        Dest File URI
  sftp:       Dest File URI
  tftp:       Dest File URI
  usbdrive:   Dest File URI
  volatile:   Dest File URI
  workspace:  Dest File URI

firepower(local-mgmt)#

copy /packet-capture/session-1/cap1-ethernet-1-2-0.pcap ftp://ftpuser@10.10.10.1/cap1-ethernet-1-2-0.pca


Password:
```

对于端口通道接口，请为每个成员接口复制捕获文件。

内部交换机数据包捕获指南、限制和最佳实践

有关Firepower 4100/9300内部交换机捕获的准则和限制，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一章数据包捕获部分。

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上的丢弃计数。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，然后打开新文件。

安全防火墙1200/3100/4200的配置与验证

与Firepower 4100/9300不同，安全防火墙1200/3100/4200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：

```
<#root>

> capture cap_sw switch

 ?
  buffer         Configure size of capture buffer, default is 256MB
  ethernet-type  Capture Ethernet packets of a particular type, default is IP
  interface      Capture packets on a specific interface
  ivlan          Inner Vlan
  match          Capture packets based on match criteria
  ovlan          Outer Vlan
  packet-length  Configure maximum length to save from each packet, default is
                 64 bytes
  real-time      Display captured packets in real-time. Warning: using this
                 option with a slow console connection may result in an
```

```
                excessive amount of non-displayed packets due to performance
                limitations.
  stop          Stop packet capture
  trace         Trace the captured packets
  type          Capture packets based on a particular type
  <cr>
```

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：

<#root>

>

capture capsw switch interface ?

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

  management       Name of interface Management1/1
```

安全防火墙1200/4200支持双向捕获。除非另有指定，否则默认值为ingress:

<#root>

>

capture capi switch interface inside direction

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

此外，Secure Firewall 4245具有2个内部数据和2个管理上行链路接口：

<#root>

>

capture capsw switch interface

```
  eventing         Name of interface Management1/2
```

```
  in_data_uplink1  Capture packets on internal data uplink1 interface
  in_data_uplink2  Capture packets on internal data uplink2 interface
  in_mgmt_uplink1  Capture packets on internal mgmt uplink1 interface
  in_mgmt_uplink2  Capture packets on internal mgmt uplink2 interface
  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:

```
<#root>

>

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：

```
<#root>

>

capture capsw switch interface inside match ?


  <0-255>  Enter protocol number (0 - 255)
  ah
  eigrp
  esp
  gre
  icmp
  icmp6
  igmp
  igrp
  ip
  ipinip
  ipsec
  mac      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。命令no capture <name> switch stop将激活捕获:

```
<#root>

>

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在/mnt/disk0/packet-capture/文件夹中。
- 捕获条件。软件根据捕获条件自动创建捕获过滤器。

```
<#root>

>

show capture capsw


27 packet captured on disk using switch capture

Reading of capture file from disk is not supported

>

show capture capsw  detail

Packet Capture info
  Name:              capsw

  Session:           1
  Admin State:       enabled

  Oper State:        up
```

```
Oper State Reason: Active


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

Total Physical ports involved in Packet Capture: 1
Physical port:
  Slot Id:           1
  Port Id:           1


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


  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：

<#root>

>

capture capsw switch stop

>

show capture capsw detail

Packet Capture info

  Name: **capsw**

  Session: 1

  Admin State: **disabled**

  Oper State: **down**

  Oper State Reason: **Session_Admin_Shut**

  Config Success: yes
  Config Fail Reason:
  Append Flag: overwrite
  Session Mem Usage: 256
  Session Pcap Snap Len: 1518
  Error Code: 0
  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。执行收集安全防火墙内部交换机捕获文件部分中的步骤。

在安全防火墙软件版本7.7中，FMC或FDM不支持内部交换机捕获配置。在ASA软件版本9.18(1)及更高版本中，可以在ASDM版本7.18.1.x及更高版本中配置内部交换机捕获。

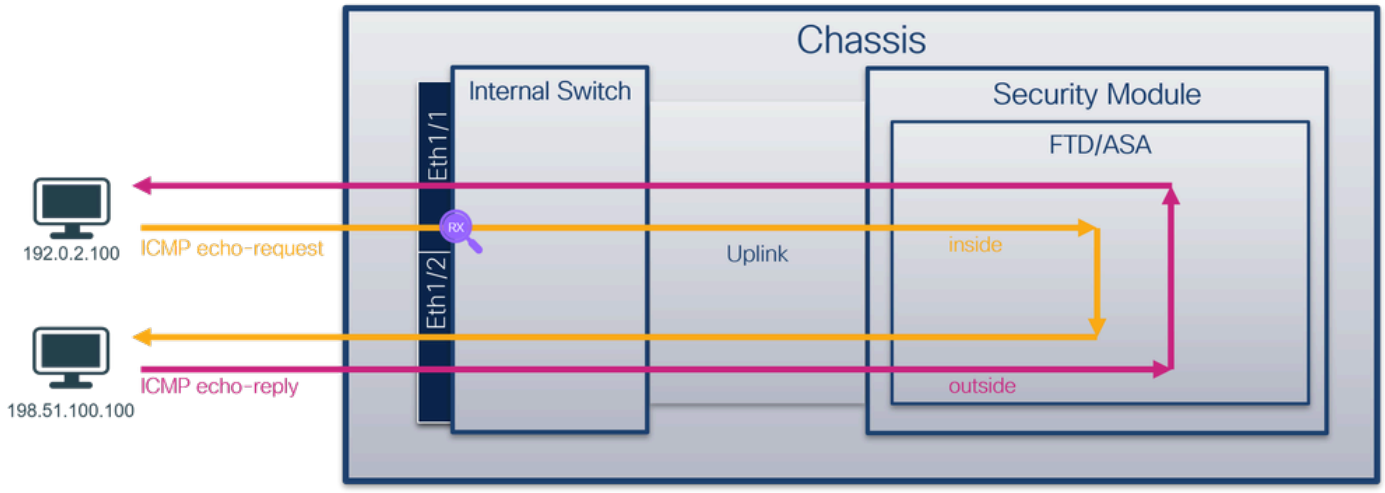
这些场景包括安全防火墙1200/3100/4200内部交换机捕获的常见使用案例。

物理或端口通道接口上的数据包捕获

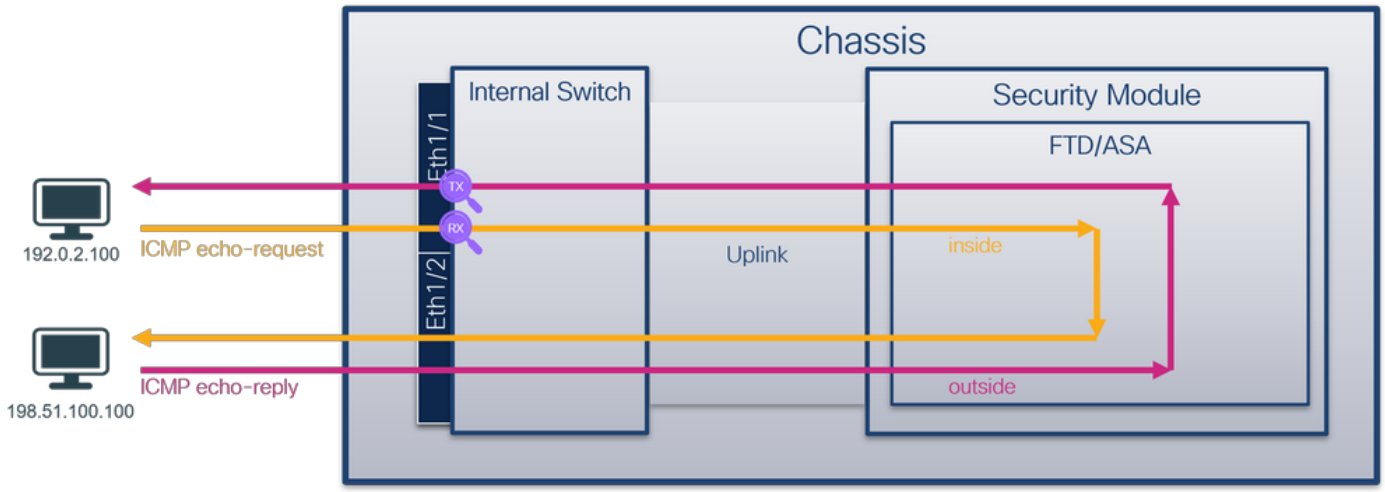
使用FTD或ASA CLI在接口Ethernet1/1或Portchannel1接口上配置和验证数据包捕获。两个接口都有nameif inside。

拓扑、数据包流和捕获点

安全防火墙3100:



安全防火墙1200/4200:



配置

在ASA或FTD CLI上执行以下步骤以配置接口Ethernet1/1或Port-channel1上的数据包捕获：

1. 验证名称if:

<#root>

>

show nameif

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

<#root>

>

show nameif

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

2. 创建捕获会话

<#root>

>

capture capsw switch interface inside

安全防火墙1200/4200支持捕获方向性：

<#root>

> capture capsw switch interface inside direction ?

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

> capture capsw switch interface inside direction both

3. 启用捕获会话：

<#root>

> 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：

<#root>

>

show capture capsw detail

Packet Capture info

Name: capsw

Session: 1

Admin State: enabled

Oper State: up

Oper State Reason: Active

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

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1

Port Id: 1

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

Pcapsize: 12653

```
  Filter:            capsw-1-1

Packet Capture Filter Info
  Name:              capsw-1-1
  Protocol:          0
  Ivlan:             0
  Ovlan:             0
  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
```

安全防火墙1200/4200:

<#root>

>

show cap capsw detail

Packet Capture info

Name: **capsw**

Session: 1

Admin State: **enabled**

Oper State: **up**

Oper State Reason: Active

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

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

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


Direction:         both


  Drop:              disable
  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

33 packet 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：

```
<#root>

>

show capture capsw detail


Packet Capture info

  Name:              capsw


  Session:           1

  Admin State:       enabled


  Oper State:        up
```

```
  Oper State Reason: Active


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

Total Physical ports involved in Packet Capture: 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：

```
<#root>

>

connect fxos


…
firewall#

connect local-mgmt


firewall(local-mgmt)#

show portchannel summary


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

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。

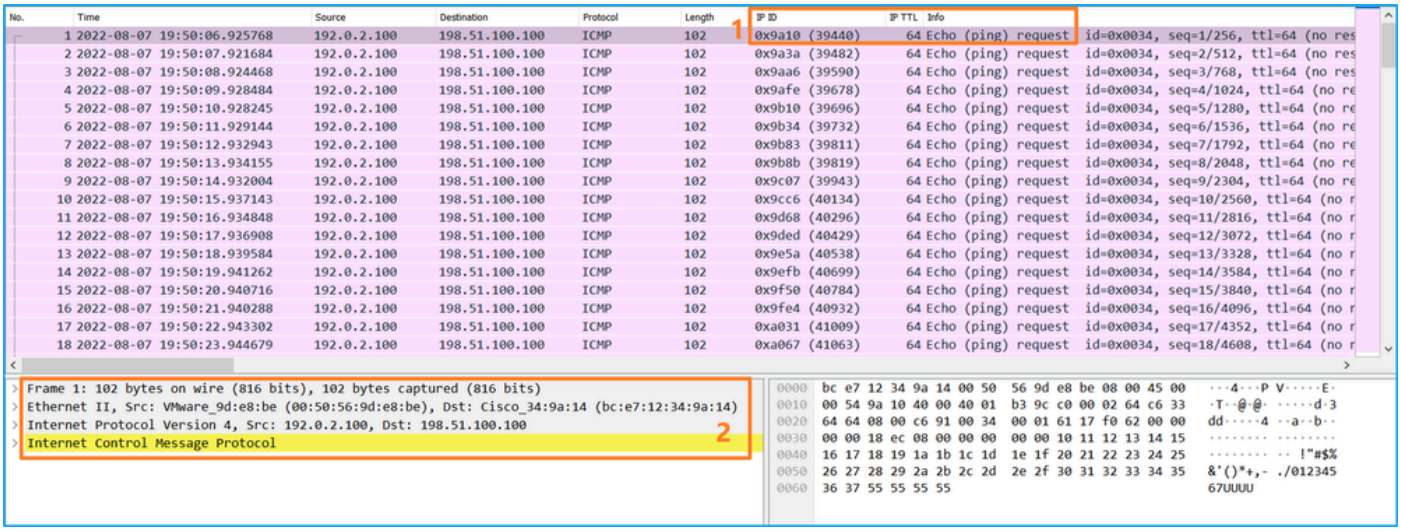
收集捕获文件

执行收集安全防火墙内部交换机捕获文件部分中的步骤。

捕获文件分析

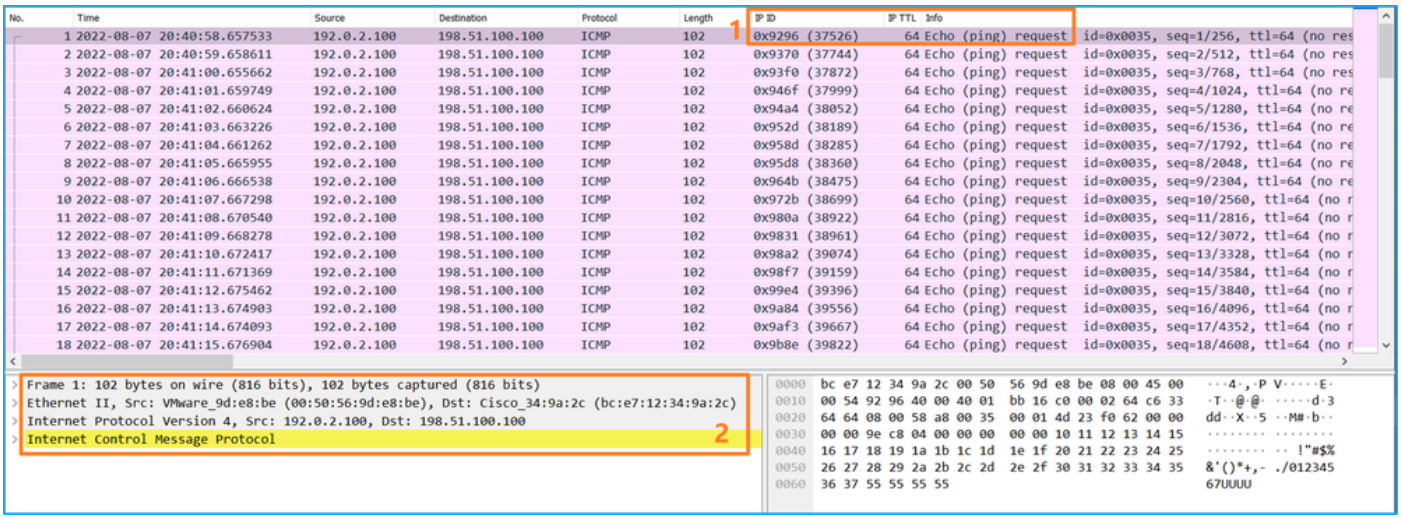
使用数据包捕获文件读取器应用程序打开Ethernet1/1的捕获文件。在本示例中，分析在安全防火墙3100上捕获的数据包。选择第一个数据包并检查要点：

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
在接口Ethernet1/1上配置并检验数据包捕获	Ethernet1/1	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	Ethernet1/3 Ethernet1/4	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

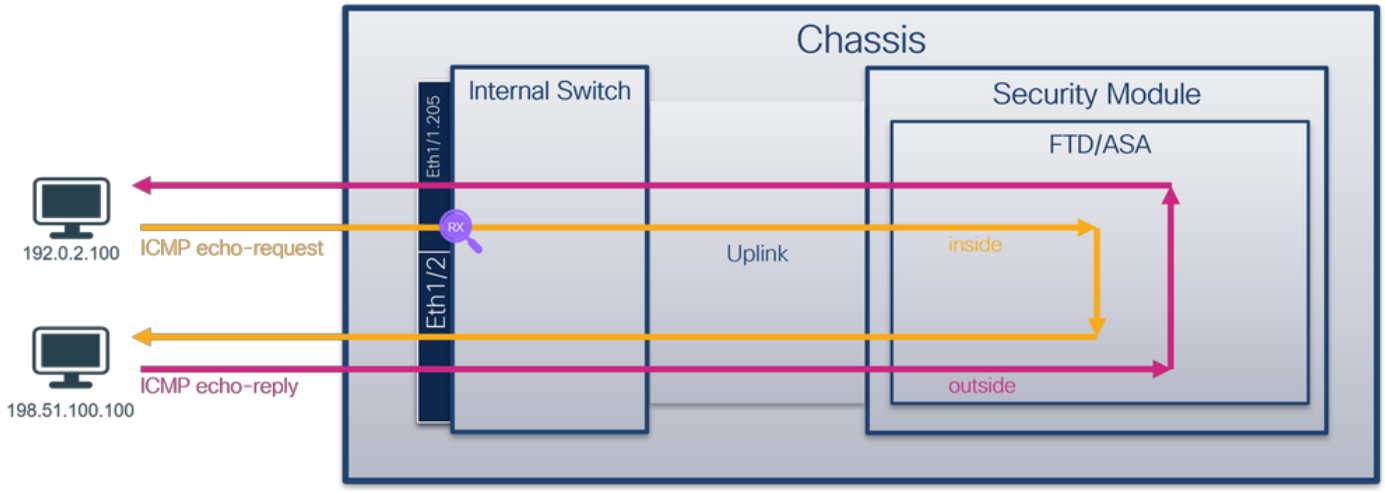
*与3100不同，安全防火墙1200/4200支持双向（入口和出口）捕获。

物理或端口通道接口的子接口上的数据包捕获

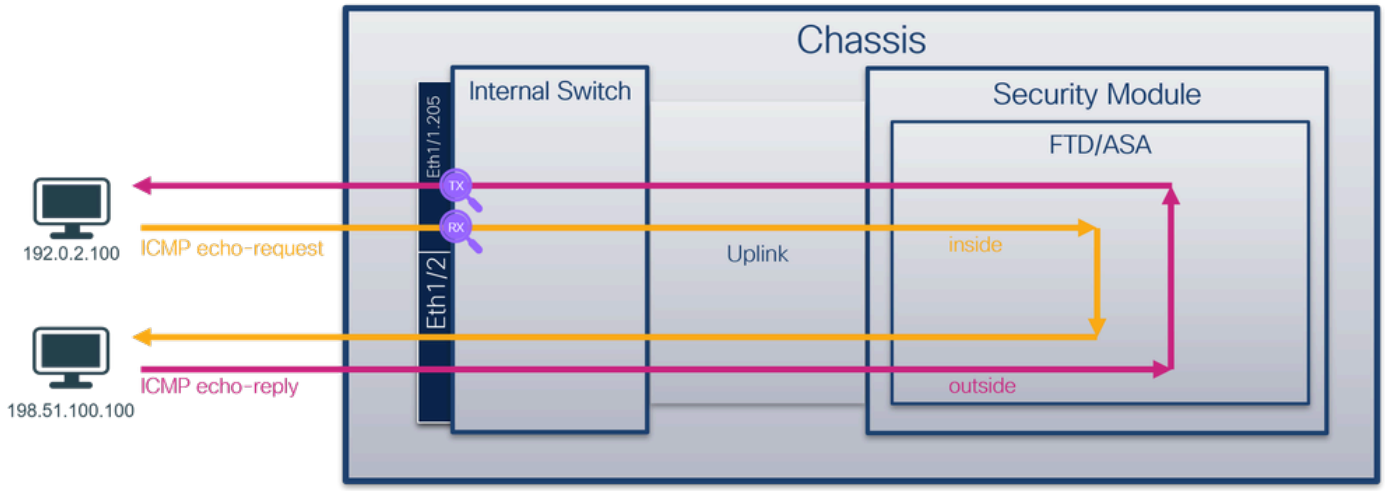
使用FTD或ASA CLI在子接口Ethernet1/1.205或Portchannel1.205上配置和验证数据包捕获。两个子接口都具有inside名称。

拓扑、数据包流和捕获点

安全防火墙3100:



安全防火墙1200/4200:



配置

在ASA或FTD CLI上执行以下步骤以配置接口Ethernet1/1或Port-channel1上的数据包捕获：

1. 验证名称if:

```
<#root>

>

show nameif

Interface                  Name                       Security
Ethernet1/1.205            inside                     0

Ethernet1/2                outside                    0
Management1/1              diagnostic                 0

<#root>
```

```
>
show nameif

Interface                Name                    Security
Port-channel1.205        inside                  0

Ethernet1/2              outside                 0
Management1/1            diagnostic              0
```

2. 创建捕获会话：

<#root>

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

安全防火墙1200/4200支持捕获方向性：

<#root>

```
> capture capsw switch interface inside direction ?

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

> capture capsw switch interface inside direction both
```

3.启用捕获会话：

<#root>

```
> 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：

<#root>

>

show capture capsw detail

```
Packet Capture info
  Name:              capsw
  Session:           1
  Admin State:       enabled
  Oper State:        up
  Oper State Reason: Active
  Config Success:    yes
  Config Fail Reason:
  Append Flag:       overwrite
  Session Mem Usage: 256
  Session Pcap Snap Len: 1518
  Error Code:        0
  Drop Count:        0
Total Physical ports involved in Packet Capture: 1
Physical port:
  Slot Id:           1
  Port Id:           1
  Pcapfile:          /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
  Pcapsize:          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：

```
<#root>

>

show capture capsw detail


Packet Capture info

  Name:              capsw

  Session:           1

  Admin State:       enabled


  Oper State:        up


  Oper State Reason: Active


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

Total Physical ports involved in Packet Capture: 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：

```
<#root>

>

connect fxos


…
firewall#

connect local-mgmt


firewall(local-mgmt)#

show portchannel summary


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

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。

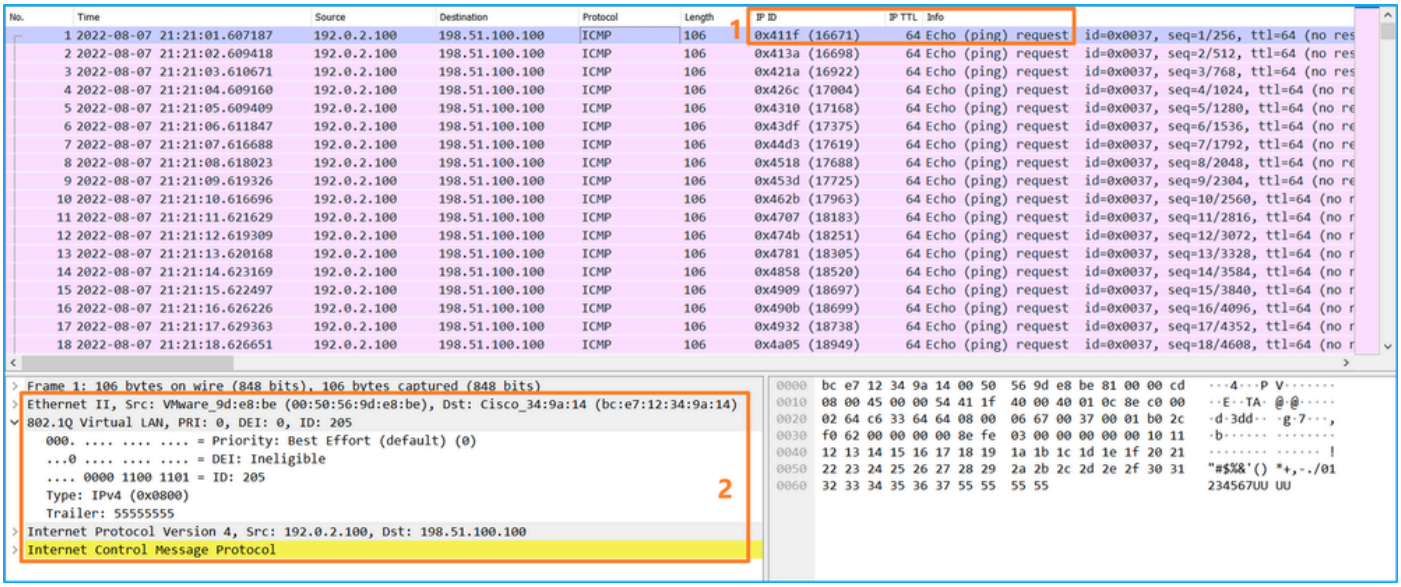
收集捕获文件

执行收集安全防火墙内部交换机捕获文件部分中的步骤。

捕获文件分析

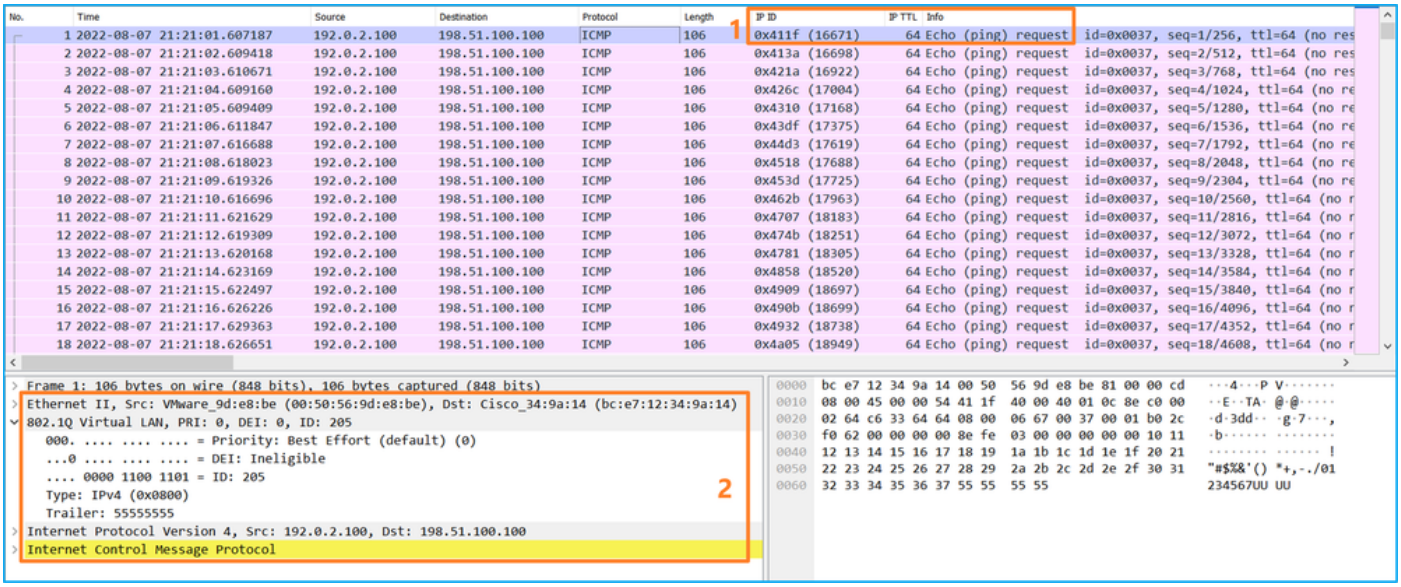
使用数据包捕获文件读取器应用程序打开Ethernet1/1.205的捕获文件。在本示例中，分析在安全防火墙3100上捕获的数据包。选择第一个数据包并检查要点：

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，其过滤器与外部VLAN 205匹配。

此表概述了任务：

任务	捕获点	内部过滤	方向	捕获的流量

		器		
在子接口Ethernet1/1.205上配置并检验数据包捕获	Ethernet1/1	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	Ethernet1/3 Ethernet1/4	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

*与3100不同，安全防火墙1200/4200支持双向（入口和出口）捕获。

内部接口上的数据包捕获

安全防火墙3100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。

Secure Firewall 1200最多具有3个内部接口：

- in_data_uplink1 — 特定于1210和1250，这些接口将应用程序连接到内部交换机。
- in_data_uplink1、in_data_uplink2、in_data_uplink3和in_mgmt_uplink2 — 特定于1220、1230和1240，这些接口将应用程序连接到内部交换机。

注意：由于安全防火墙1200上的管理接口是带外接口，因此此型号上没有in_mgmt_uplink接口。

Secure Firewall 4200最多具有4个内部接口：

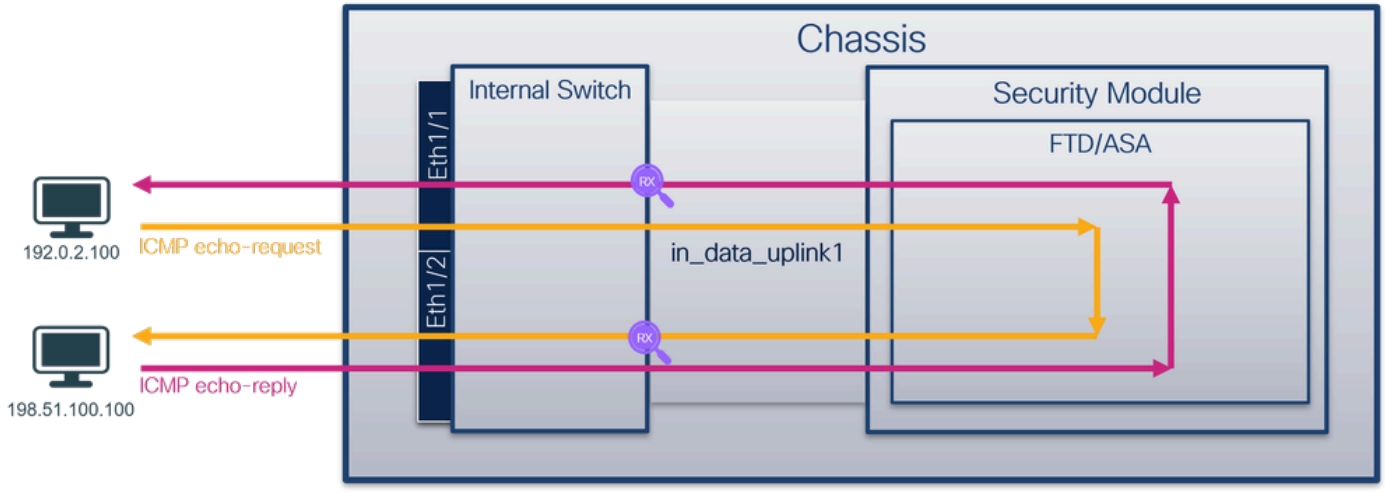
- in_data_uplink1 和in_data_uplink2（仅限4245） — 这些接口将应用程序连接到内部交换机。对于4245，数据包在2个上行链路接口之间实现负载均衡。
- in_mgmt_uplink1和in_mgmt_uplink2 — 这些接口为管理连接（例如到管理接口的SSH）或管理连接（也称为sftunnel）提供专用数据包路径，在FMC和FTD之间。安全防火墙4200支持2个管理接口。

任务1

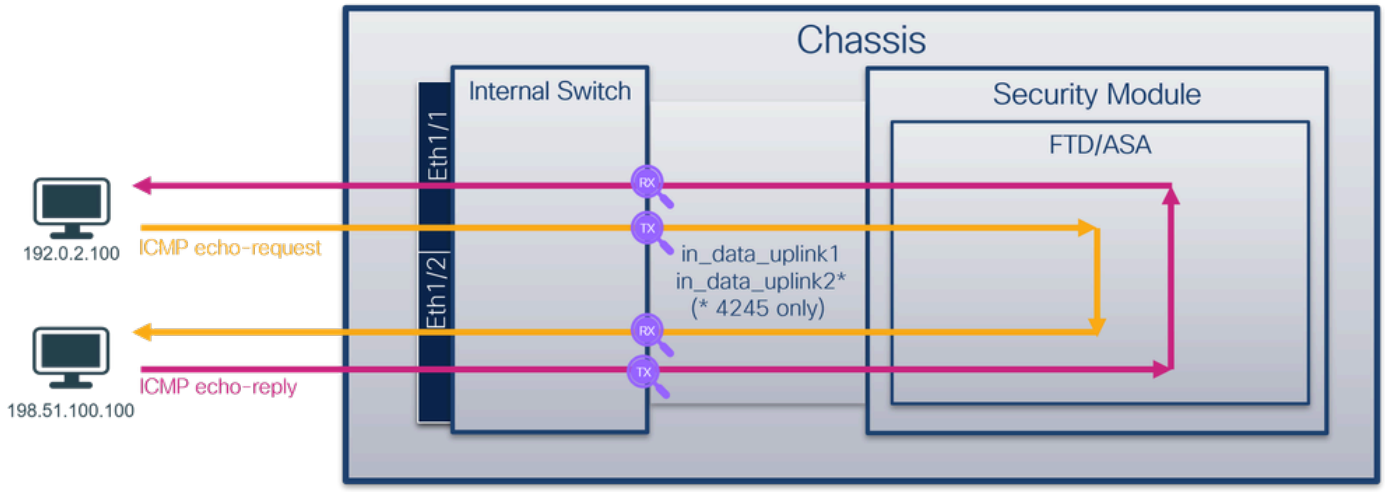
使用FTD或ASA CLI配置并验证数据上行链路接口上的数据包捕获。

拓扑、数据包流和捕获点

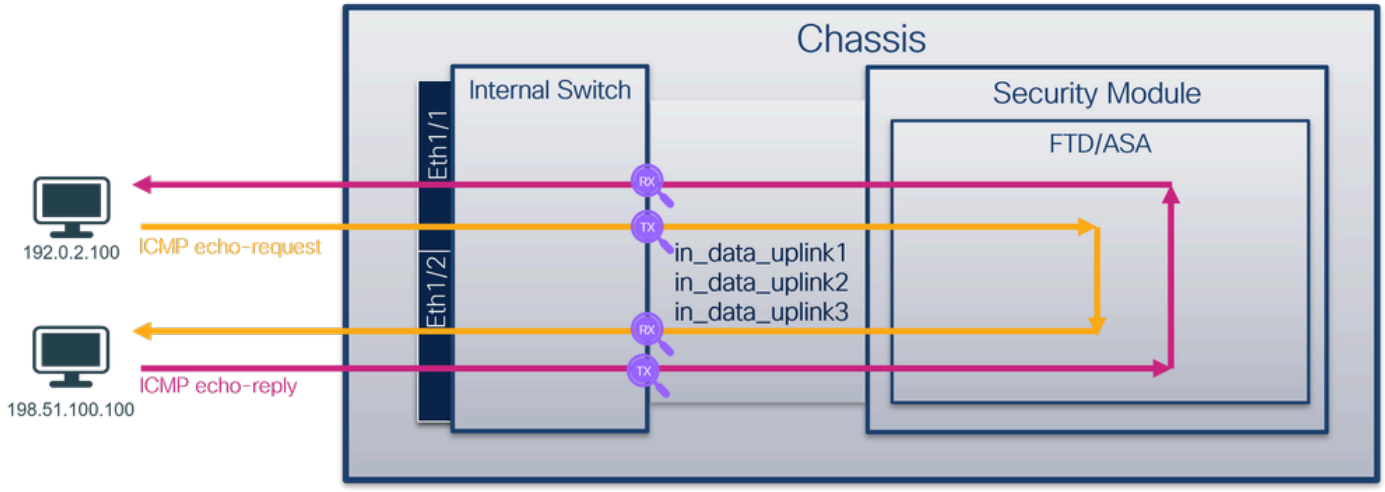
安全防火墙3100:



安全防火墙4200:



安全防火墙1200:



配置

在ASA或FTD CLI上执行这些步骤，以配置数据上行链路接口上的数据包捕获。

请注意，安全防火墙1210、1250、3100和4200（4245除外）只有1个活动上行链路接口in_data_uplink1。

安全防火墙1200（1210和1250除外）和4245有多个上行链路接口in_data_uplink1、in_data_uplink2等。务必确保包括所有数据上行链路接口。

以下是Secure Firewall 1220的输出：

```
<#root>

>

cap capsw switch interface ?


Available interfaces to listen:

in_data_uplink1

 Capture packets on internal data uplink1 interface

in_data_uplink2

 Capture packets on internal data uplink2 interface

in_data_uplink3

 Capture packets on internal data uplink3 interface
...
```

1. 创建捕获会话：

```
<#root>

>

capture capsw switch interface in_data_uplink1
```

安全防火墙1200/4200支持捕获方向性：

```
<#root>

> capture capsw switch interface in_data_uplink1 direction ?


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


> capture capsw switch interface in_data_uplink1 direction both
```

2.启用捕获会话：

<#root>

> 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：

<#root>

>

show capture capsw detail

Packet Capture info

Name: **capsw**

Session: 1

Admin State: **enabled**

Oper State: **up**

Oper State Reason: **Active**

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

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: **1**

Port Id: **18**

Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-data-uplink1.pcap

Pcapsize: **7704**

```
  Filter:            capsw-1-18

Packet Capture Filter Info
  Name:              capsw-1-18
  Protocol:          0
  Ivlan:             0
  Ovlan:             0
  Src Ip:            0.0.0.0
  Dest Ip:           0.0.0.0
  Src Ipv6:          ::
  Dest Ipv6:         ::
  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:

```
<#root>

>

connect fxos


…
firewall#

connect local-mgmt


firewall(local-mgmt)#

show portmanager switch status


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

0/12	1000_BaseX	Down	1G	Full	None	Link-Down
0/13	1000_BaseX	Down	1G	Full	None	Link-Down
0/14	1000_BaseX	Down	1G	Full	None	Link-Down
0/15	1000_BaseX	Down	1G	Full	None	Link-Down
0/16	1000_BaseX	Down	1G	Full	None	Link-Down
0/17	1000_BaseX	Up	1G	Full	None	Link-Up
0/18	**KR2**	**Up**	**50G**	**Full**	**None**	**Link-Up**
0/19	KR	Up	25G	Full	None	Link-Up
0/20	KR	Up	25G	Full	None	Link-Up
0/21	KR4	Down	40G	Full	None	Link-Down
0/22	n/a	Down	n/a	Full	N/A	Reset
0/23	n/a	Down	n/a	Full	N/A	Reset
0/24	n/a	Down	n/a	Full	N/A	Reset
0/25	1000_BaseX	Down	1G	Full	None	Link-Down
0/26	n/a	Down	n/a	Full	N/A	Reset
0/27	n/a	Down	n/a	Full	N/A	Reset
0/28	n/a	Down	n/a	Full	N/A	Reset
0/29	1000_BaseX	Down	1G	Full	None	Link-Down
0/30	n/a	Down	n/a	Full	N/A	Reset
0/31	n/a	Down	n/a	Full	N/A	Reset
0/32	n/a	Down	n/a	Full	N/A	Reset
0/33	1000_BaseX	Down	1G	Full	None	Link-Down
0/34	n/a	Down	n/a	Full	N/A	Reset
0/35	n/a	Down	n/a	Full	N/A	Reset
0/36	n/a	Down	n/a	Full	N/A	Reset

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。

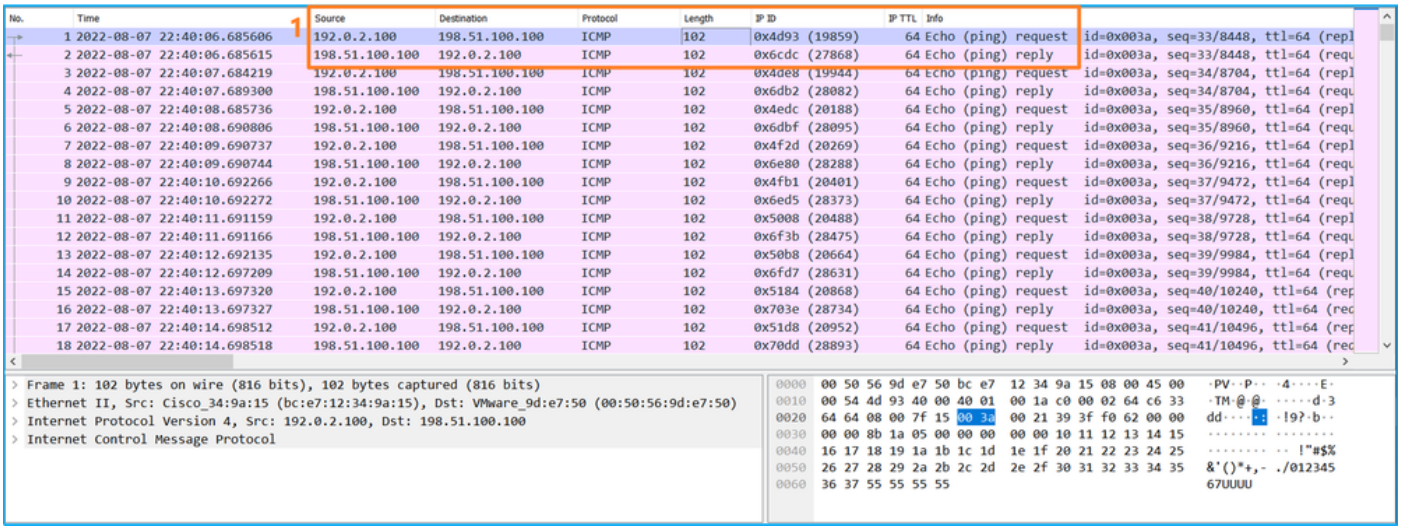
收集捕获文件

执行收集安全防火墙内部交换机捕获文件部分中的步骤。

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。在此示例中，分析在安全防火墙3100上捕获的数据包。

检查关键点 — 在本例中，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

当在上行链路接口上配置交换机捕获时，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

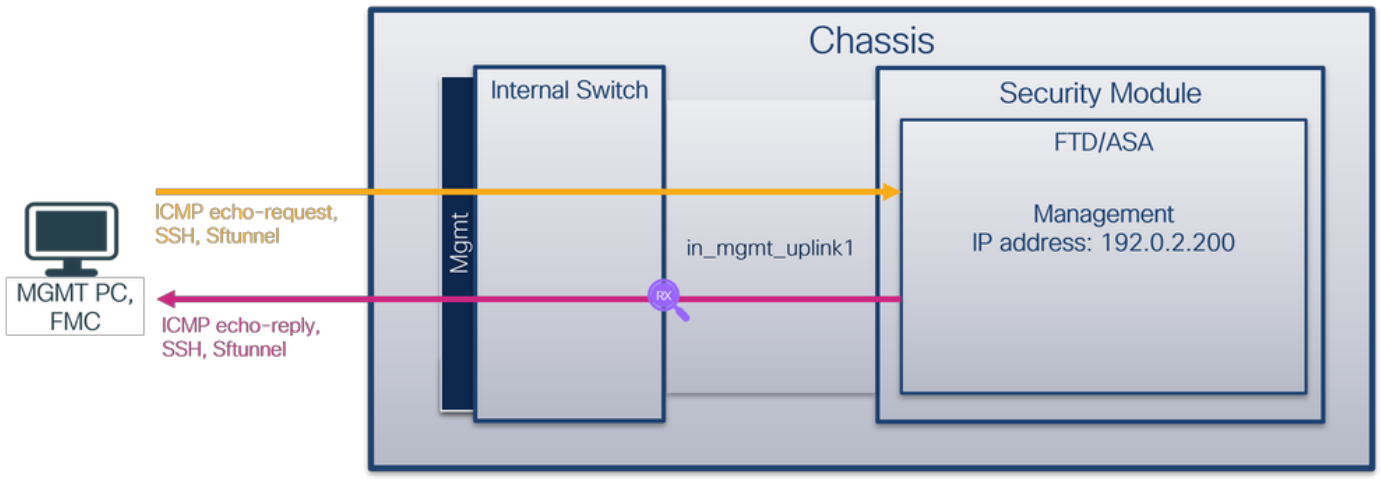
*与3100不同，安全防火墙1200/4200支持双向（入口和出口）捕获。

任务2

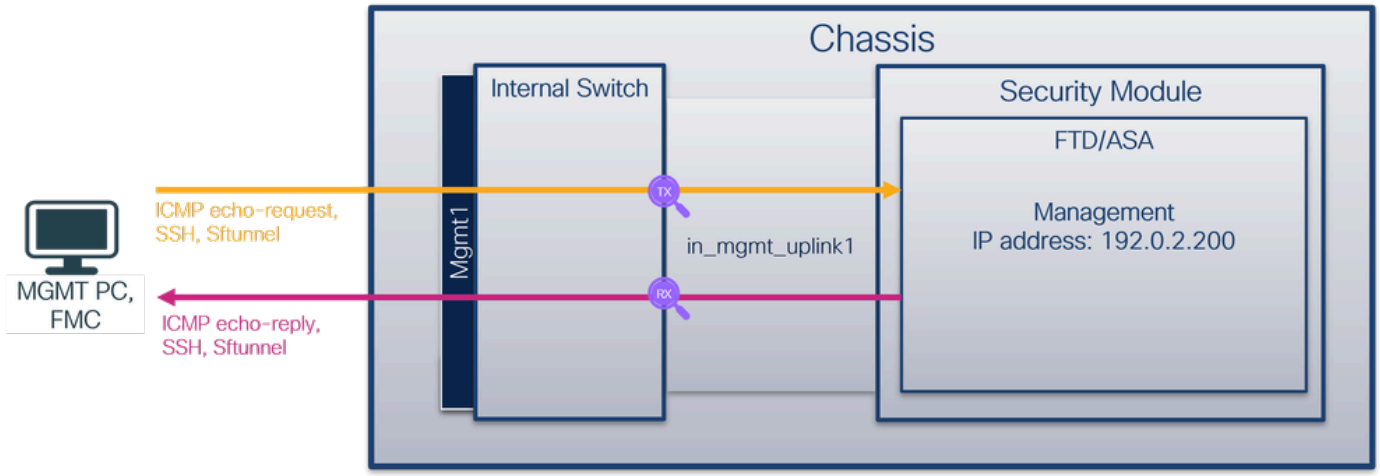
使用FTD或ASA CLI配置并验证上行链路接口in_mgmt_uplink1上的数据包捕获。仅捕获管理平面连接的数据包。

拓扑、数据包流和捕获点

安全防火墙3100:



安全防火墙4200:



配置

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

1. 创建捕获会话：

<#root>

>

capture capsw switch interface in_mgmt_uplink1

安全防火墙4200支持捕获方向性：

<#root>

> capture capsw switch interface in_mgmt_uplink1 direction ?

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

```
> capture capsw switch interface in_mgmt_uplink1 direction both
```

2.启用捕获会话：

<#root>

```
> 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：

<#root>

```
> show capture capsw detail

Packet Capture info

Name:              capsw

  Session:           1

Admin State:       enabled


  Oper State:        up


  Oper State Reason: Active


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

Total Physical ports involved in Packet Capture: 1

Physical port:

  Slot Id:           1


  Port Id:           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:

```
<#root>

>

connect fxos


…
firewall#

connect local-mgmt


firewall(local-mgmt)#

show portmanager switch status


Dev/Port         Mode        Link   Speed  Duplex  Loopback Mode  Port Manager
---------  ----------------  -----  -----  ------  -------------  ------------
0/1             SGMII         Up     1G     Full    None           Link-Up
0/2             SGMII         Up     1G     Full    None           Link-Up
0/3             SGMII         Up     1G     Full    None           Link-Up
```

0/4	SGMII	Up	1G	Full	None	Link-Up
0/5	SGMII	Down	1G	Half	None	Mac-Link-Down
0/6	SGMII	Down	1G	Half	None	Mac-Link-Down
0/7	SGMII	Down	1G	Half	None	Mac-Link-Down
0/8	SGMII	Down	1G	Half	None	Mac-Link-Down
0/9	1000_BaseX	Down	1G	Full	None	Link-Down
0/10	1000_BaseX	Down	1G	Full	None	Link-Down
0/11	1000_BaseX	Down	1G	Full	None	Link-Down
0/12	1000_BaseX	Down	1G	Full	None	Link-Down
0/13	1000_BaseX	Down	1G	Full	None	Link-Down
0/14	1000_BaseX	Down	1G	Full	None	Link-Down
0/15	1000_BaseX	Down	1G	Full	None	Link-Down
0/16	1000_BaseX	Down	1G	Full	None	Link-Down
0/17	1000_BaseX	Up	1G	Full	None	Link-Up
0/18	KR2	Up	50G	Full	None	Link-Up
0/19	**KR**	**Up**	**25G**	**Full**	**None**	**Link-Up**
0/20	KR	Up	25G	Full	None	Link-Up
0/21	KR4	Down	40G	Full	None	Link-Down
0/22	n/a	Down	n/a	Full	N/A	Reset
0/23	n/a	Down	n/a	Full	N/A	Reset
0/24	n/a	Down	n/a	Full	N/A	Reset
0/25	1000_BaseX	Down	1G	Full	None	Link-Down
0/26	n/a	Down	n/a	Full	N/A	Reset
0/27	n/a	Down	n/a	Full	N/A	Reset
0/28	n/a	Down	n/a	Full	N/A	Reset
0/29	1000_BaseX	Down	1G	Full	None	Link-Down
0/30	n/a	Down	n/a	Full	N/A	Reset
0/31	n/a	Down	n/a	Full	N/A	Reset
0/32	n/a	Down	n/a	Full	N/A	Reset
0/33	1000_BaseX	Down	1G	Full	None	Link-Down
0/34	n/a	Down	n/a	Full	N/A	Reset
0/35	n/a	Down	n/a	Full	N/A	Reset
0/36	n/a	Down	n/a	Full	N/A	Reset

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。

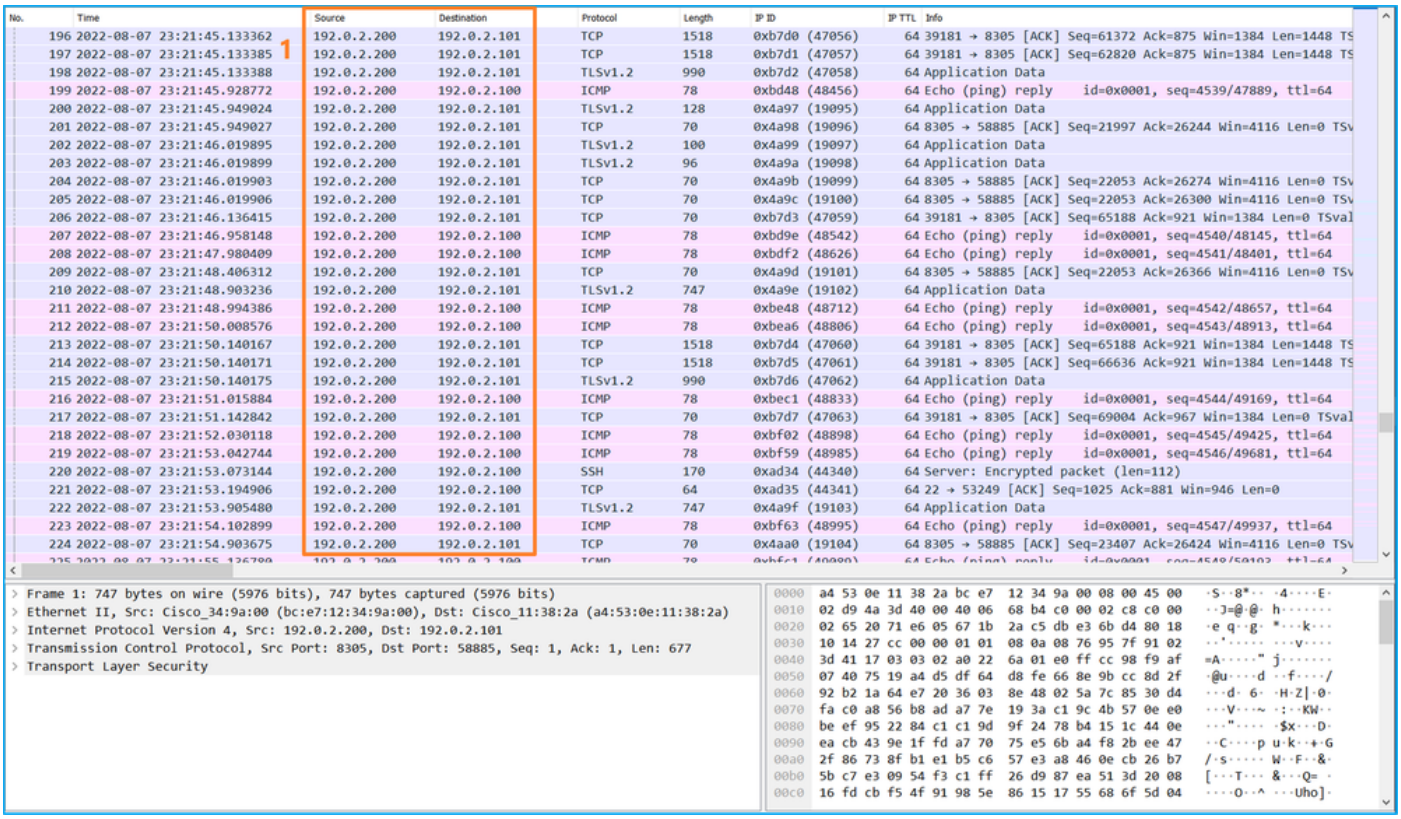
收集捕获文件

执行收集安全防火墙内部交换机捕获文件部分中的步骤。

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。在此示例中，分析在安全防火墙3100上捕获的数据包。

检查关键点 — 在本例中，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	内部过滤器	方向	捕获的流量
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

*与3100不同，安全防火墙1200/4200支持双向（入口和出口）捕获。

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，以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if:

```
<#root>

>

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：

```
<#root>

>

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

```
<#root>

> 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:

```
<#root>

>

show capture capsw detail

Packet Capture info

 Name:              capsw

  Session:           1
```

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

Total Physical ports involved in Packet Capture: 1

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

Filter:            capsw-1-1



Packet Capture Filter Info


  Name:              capsw-1-1


  Protocol:          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:

```
<#root>

>
```

show capture capsw detail

```
Packet Capture info

Name:              capsw

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

Total Physical ports involved in Packet Capture: 1

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

Filter:            capsw-1-1



Packet Capture Filter Info

  Name:              capsw-1-1



Protocol:          1

  Ivlan:             0
  Ovlan:             0

Src Ip:            198.51.100.100

  Dest Ip:           0.0.0.0
  Src Ipv6:          ::
  Dest Ipv6:         ::
  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
```

第2层交换机端口接口上的数据包捕获

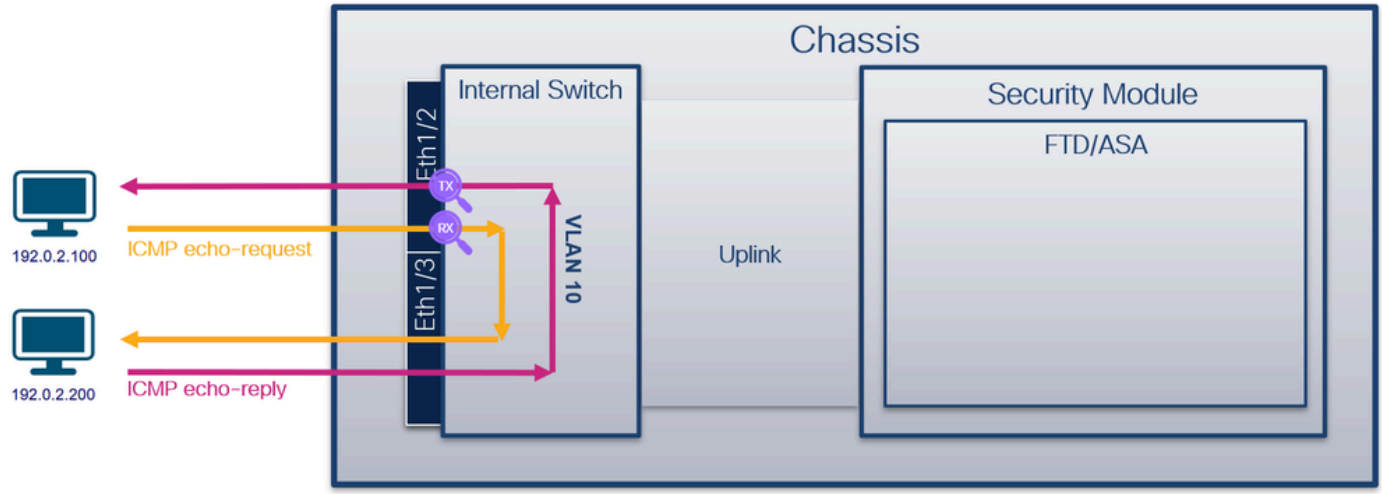
交换机端口使用硬件中的交换功能在第2层转发流量。同一个VLAN中的交换机端口可以使用硬件交换相互通信，并且流量不受威胁防御安全策略的约束。接入端口仅接受无标记流量，您可以将其分配给单个VLAN。中继端口接受无标记和标记流量，并且可以属于多个VLAN。默认情况下，Ethernet 1/2到1/8(1210)或Ethernet 1/2到1/10(1220)配置为VLAN 1上的接入交换机端口。不能将管理接口配置为交换机端口。

任务1

使用FTD或ASA CLI在子接口Ethernet1/1或Ethernet1/2上配置和验证数据包捕获。这两个接口都是分配给VLAN 10的交换机接口。

拓扑、数据包流和捕获点

安全防火墙1200:



配置

在ASA或FTD CLI上执行以下步骤以配置接口Ethernet1/2或Ethernet1/3上的数据包捕获：

1. 检验L2交换机端口：

<#root>

>

show switch vlan

```
VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    -                                   down      E1/4, E1/5, E1/6, E1/7
                                                   E1/8
```

```
10   VLAN-10                          up         E1/2, E1/3
```

2.创建捕获会话，1200支持捕获方向性：

```
<#root>

>

capture capsw switch interface switchport 2 direction ?


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

>

capture capsw switch interface switchport 2 direction both
```



注意：虽然端口标记为Ethernet1/2，但是在执行第2层交换机捕获时，不能以Ethernet1/2格式指定该端口。而应使用switchport 2。

3.启用捕获会话

```
<#root>

>

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：

```
<#root>

>

show capture capsw detail


Packet Capture info
  Name:

capsw


  Session:           2
  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

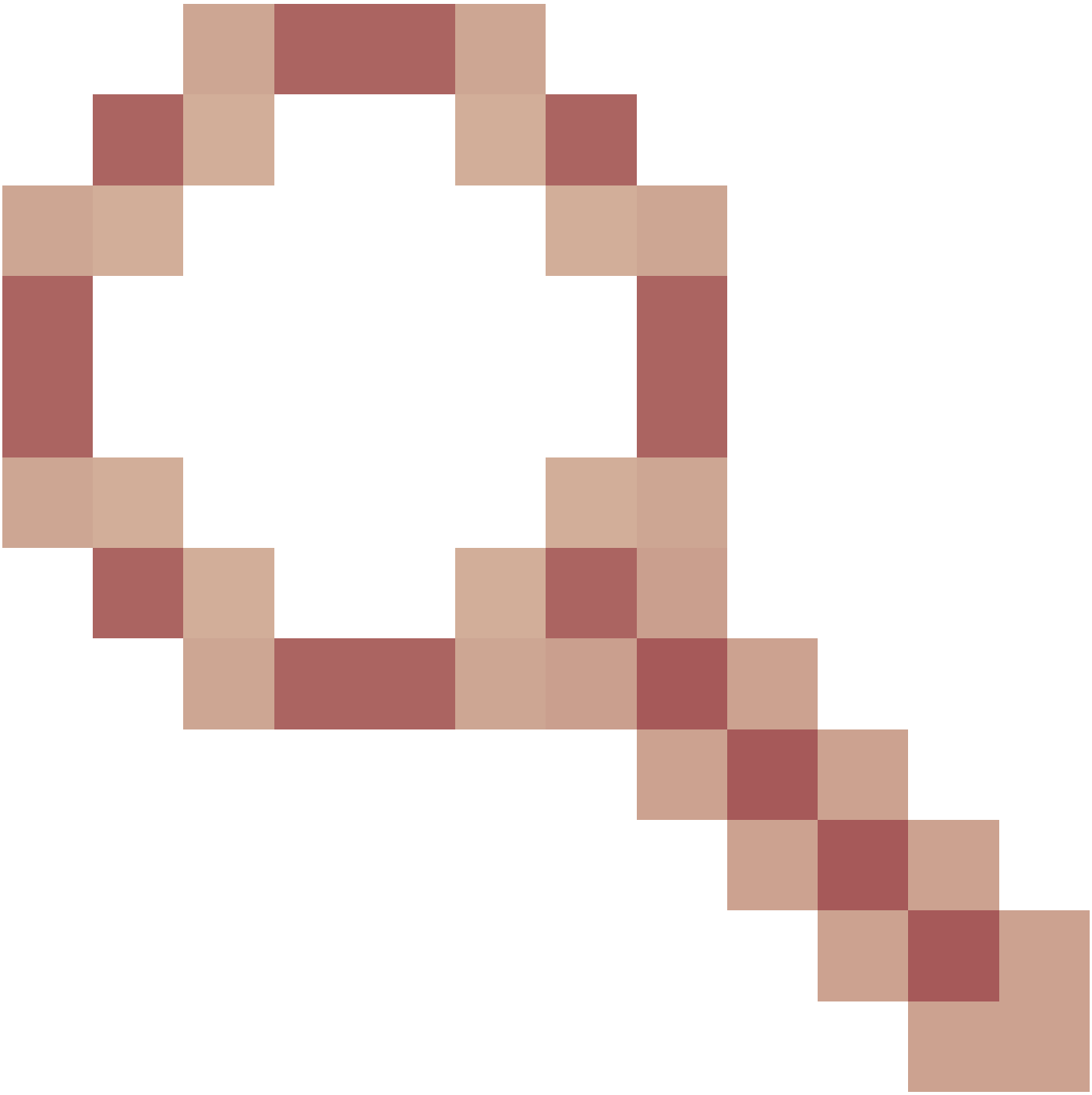
Physical port:
  Slot Id:           1
  Port Id:           2
  Pcapfile:          /mnt/disk0/packet-capture/sess-2-capsw-ethernet-1-2-0.pcap
  Pcapsize:          24
  Direction:         both
  Filter:            capsw-1-2

Packet Capture Filter Info
  Name:              capsw-1-2
  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
```

0 packet captured on disk using switch capture

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

由于CSCwq55508缺陷



因此，对于安全防火墙1200上的交换机捕获，show capture命令的输出中不会更新数据包大小和数据包计数。作为解决方法，可以在FXOS local-mgmt命令shell中通过show portmanager switch pktcap-rules hardware命令进行验证：

<#root>

```
Firewall-1200(local-mgmt)#
show portmanager switch pktcap-rules hardware

Hardware DB rule: 1 /
Direction: egress

 HwIndex= 8196
```

```
 RuleId= 6144
 CounterIndex= 10
```

PacketCount= 38

```
 Slot= 1
 Interface= 2
 Protocol= 0
 EthertypeAtL2Offset= 0x0000
 EtherTypeAtL3Offset= 0x0000
 Ivlan= 0
 Ovlan= 0
 FlowId= 0
 SrcEport= 0
 TrgEport= 0
 SrcId= 0
 TcpUdpSrcPort= 0
 TcpUdpDstPort= 0
 SrcIpAddr= 0.0.0.0
 DstIpAddr= 0.0.0.0
 SrcIpv6Addr= ::
 DestIpv6Addr= ::
 SrcMacAddr= 00:00:00:00:00:00
 DestMacAddr= 00:00:00:00:00:00

Hardware DB rule: 2 /
```

Direction: ingress

```
 HwIndex= 4104
 RuleId= 5120
 CounterIndex= 0
```

PacketCount= 37

```
 Slot= 1
 Interface= 2
 Protocol= 0
 EthertypeAtL2Offset= 0x0000
 EtherTypeAtL3Offset= 0x0000
 Ivlan= 0
 Ovlan= 0
 FlowId= 0
 SrcEport= 0
 TrgEport= 0
 SrcId= 0
 TcpUdpSrcPort= 0
 TcpUdpDstPort= 0
 SrcIpAddr= 0.0.0.0
 DstIpAddr= 0.0.0.0
 SrcIpv6Addr= ::
 DestIpv6Addr= ::
 SrcMacAddr= 00:00:00:00:00:00
 DestMacAddr= 00:00:00:00:00:00
```

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。

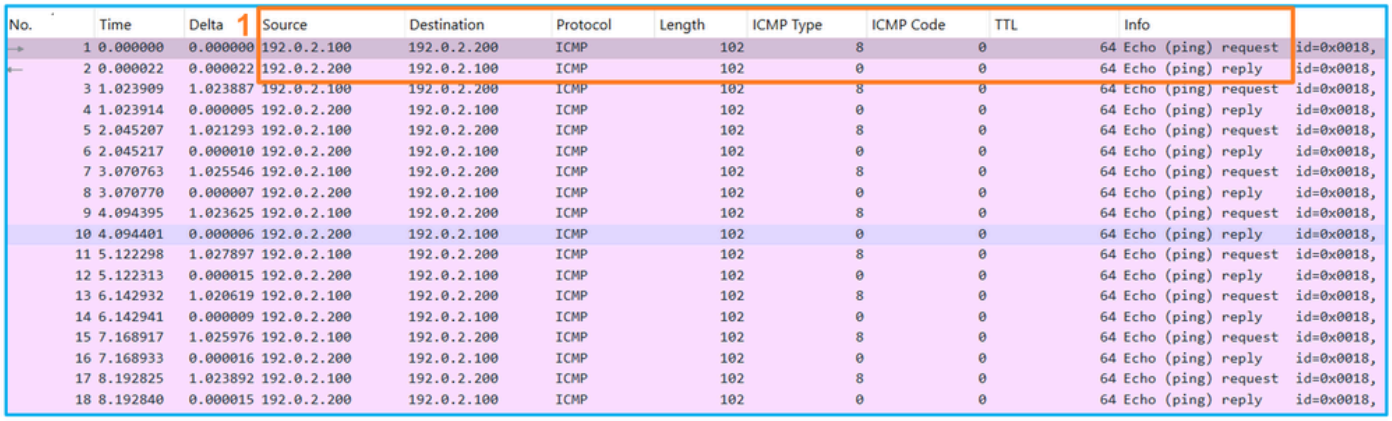
收集捕获文件

执行收集安全防火墙内部交换机捕获文件部分中的步骤。

捕获文件分析

使用数据包捕获文件读取器应用程序打开交换机L2接口Ethernet 1/2的捕获文件。在本示例中，分析在安全防火墙1210上捕获的数据包。

检查关键点 — 在本例中，捕获的是ICMP回应请求和应答数据包。



No.	Time	Delta	Source	Destination	Protocol	Length	ICMP Type	ICMP Code	TTL	Info
1	0.000000	0.000000	192.0.2.100	192.0.2.200	ICMP	102	8	0	64	Echo (ping) request id=0x0018,
2	0.000022	0.000022	192.0.2.200	192.0.2.100	ICMP	102	0	0	64	Echo (ping) reply id=0x0018,
3	1.023909	1.023887	192.0.2.100	192.0.2.200	ICMP	102	8	0	64	Echo (ping) request id=0x0018,
4	1.023914	0.000005	192.0.2.200	192.0.2.100	ICMP	102	0	0	64	Echo (ping) reply id=0x0018,
5	2.045207	1.021293	192.0.2.100	192.0.2.200	ICMP	102	8	0	64	Echo (ping) request id=0x0018,
6	2.045217	0.000010	192.0.2.200	192.0.2.100	ICMP	102	0	0	64	Echo (ping) reply id=0x0018,
7	3.070763	1.025546	192.0.2.100	192.0.2.200	ICMP	102	8	0	64	Echo (ping) request id=0x0018,
8	3.070770	0.000007	192.0.2.200	192.0.2.100	ICMP	102	0	0	64	Echo (ping) reply id=0x0018,
9	4.094395	1.023625	192.0.2.100	192.0.2.200	ICMP	102	8	0	64	Echo (ping) request id=0x0018,
10	4.094401	0.000006	192.0.2.200	192.0.2.100	ICMP	102	0	0	64	Echo (ping) reply id=0x0018,
11	5.122298	1.027897	192.0.2.100	192.0.2.200	ICMP	102	8	0	64	Echo (ping) request id=0x0018,
12	5.122313	0.000015	192.0.2.200	192.0.2.100	ICMP	102	0	0	64	Echo (ping) reply id=0x0018,
13	6.142932	1.020619	192.0.2.100	192.0.2.200	ICMP	102	8	0	64	Echo (ping) request id=0x0018,
14	6.142941	0.000009	192.0.2.200	192.0.2.100	ICMP	102	0	0	64	Echo (ping) reply id=0x0018,
15	7.168917	1.025976	192.0.2.100	192.0.2.200	ICMP	102	8	0	64	Echo (ping) request id=0x0018,
16	7.168933	0.000016	192.0.2.200	192.0.2.100	ICMP	102	0	0	64	Echo (ping) reply id=0x0018,
17	8.192825	1.023892	192.0.2.100	192.0.2.200	ICMP	102	8	0	64	Echo (ping) request id=0x0018,
18	8.192840	0.000015	192.0.2.200	192.0.2.100	ICMP	102	0	0	64	Echo (ping) reply id=0x0018,

说明

这些数据包不会转发到应用(FTD/ASA)，因为两台主机都连接到同一VLAN中的第2层交换机端口。

此表概述了任务：

任务	捕获点	内部过滤器	方向	捕获的流量
在交换机端口L2接口Ethernet1/2上配置并检验数据包捕获	以太网1/2	无	两者	从主机192.0.2.200到主机192.0.2.100的ICMP回应请求 从主机192.0.2.100到主机192.0.2.200的ICMP回应应答

多实例机箱上的数据包捕获

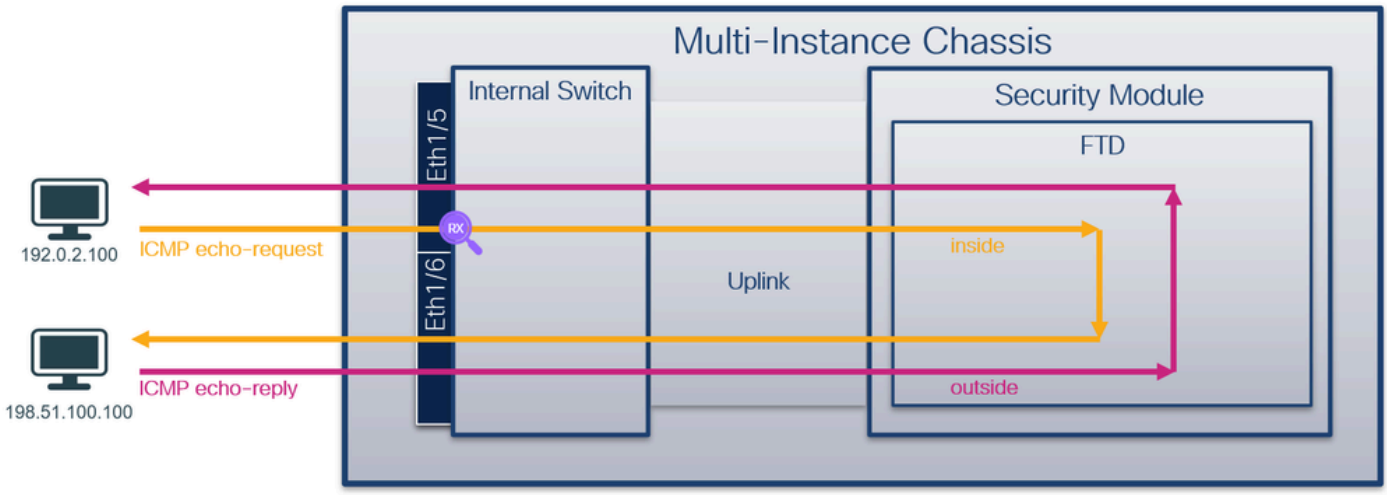
多实例部署模式中3100/4200平台上的交换机数据包捕获与本地模式中的交换机捕获不同。在多实例模式下，capture <name> switch命令在FTD实例上不可用。相反，需要使用机箱上的FXOS CLI配置数据包捕获，这与4100/9300平台的过程类似 — 通过使用scope packet-capture命令。

任务1

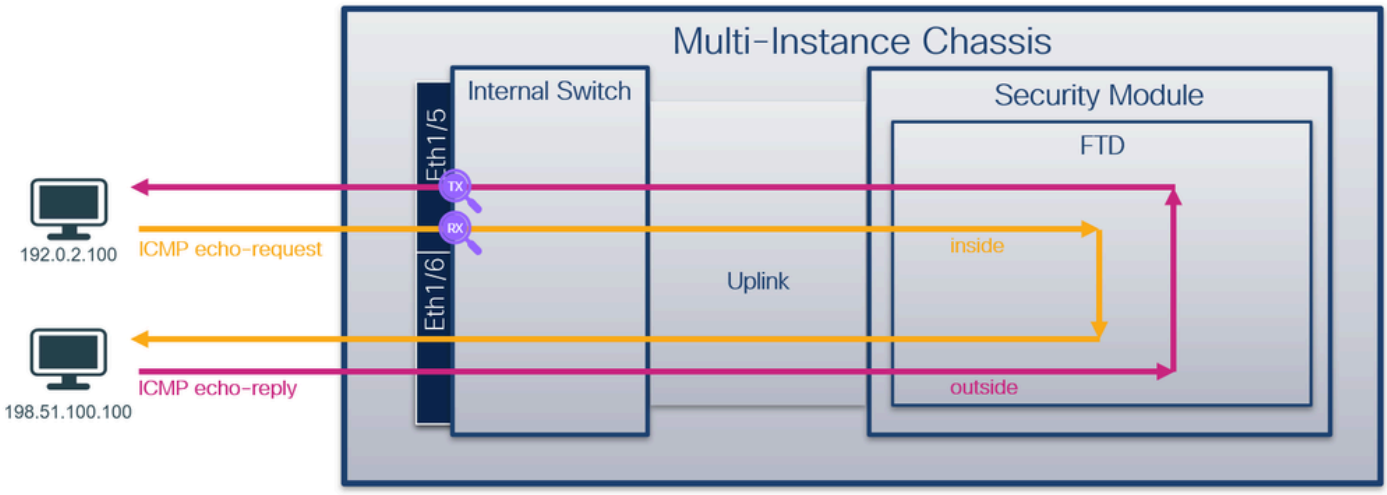
使用多实例机箱上的FXOS CLI配置和验证接口Ethernet1/5上的交换机数据包捕获。

拓扑、数据包流和捕获点

安全防火墙3100:



具有双向捕获功能的安全防火墙4200:



配置

FXOS CLI

在机箱FXOS CLI上执行以下步骤，在接口Ethernet1/5上配置数据包捕获：

1.标识申请类型和标识：

<#root>

```
firepower-3120 #
scope ssa

firepower-3120 /ssa #
show app-instance
```

```
Application Name     Identifier           Slot ID    Admin State     Operational State    Running Versi
-------------------- -------------------- ---------- --------------- -------------------- -------------
ftd

ftd1
                  1          Enabled         Online               7.7.0.89        7.7.0.89        Contai
```

2.创建捕获会话：

```
<#root>
firepower-3120#
scope packet-capture

firepower-3120 /packet-capture #
create session cap1

firepower-3120 /packet-capture/session* #
create phy-port Eth1/5

firepower-3120 /packet-capture/session/phy-port* #
set app ftd

firepower-3120 /packet-capture/session/phy-port* #
set app-instance ftd1

firepower-3120 /packet-capture/session/phy-port* #
up

firepower-3120 /packet-capture/session* #
enable

firepower-3120 /packet-capture/session* #
commit-buffer

firepower-3120 /packet-capture/session #
```

安全防火墙4200:

<#root>

```
firepower-4245#
scope packet-capture

firepower-4245 /packet-capture #
create session cap1

firepower-4245 /packet-capture/session* #
create phy-port Eth1/5

firepower-4245 /packet-capture/session/phy-port* #
set app ftd

firepower-4245 /packet-capture/session/phy-port* #
set app-instance ftd1

firepower-4245 /packet-capture/session/phy-port* #
set direction both

firepower-4245 /packet-capture/session/phy-port* #
up

firepower-4245 /packet-capture/session* #
enable

firepower-4245 /packet-capture/session* #
commit-buffer

firepower-4245 /packet-capture/session #
```

确认

FXOS CLI

在范围数据包捕获中验证捕获详细信息。具体而言，验证捕获会话名称、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：

<#root>

```
firepower-3120#
scope packet-capture
```

```
firepower-3120 /packet-capture #
show session cap1



SSP Traffic Monitoring 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
    Error Code: 0
    Drop Count: 0


 Packet Count: 420



Physical ports involved in Packet Capture:
    Slot Id: 1
    Port Id: 5
    Pcapfile: /workspace/packet-capture/sess-1-cap1-ethernet-1-5-0.pcap


Pcapsize: 49128  bytes


    Filter:
    Sub Interface: 0
    Application Instance:
ftd1


    Application Name:
ftd


    Direction: Ingress
    Drop: Disable
```

安全防火墙4200:

<#root>

```
firepower-4245#
```

scope packet-capture

firepower-4245 /packet-capture #

show session cap1

SSP Traffic Monitoring 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
    Error Code: 0
    Drop Count: 0

Packet Count: 95

Physical ports involved in Packet Capture:
    Slot Id: 1
    Port Id: 5
    Pcapfile: /workspace/packet-capture/sess-1-cap1-ethernet-1-5-0.pcap

Pcapsize: 11050 bytes

    Filter:
    Sub Interface: 0
    Application Instance:

ftd1

    Application Name:

ftd

Direction: Both

    Drop: Disable

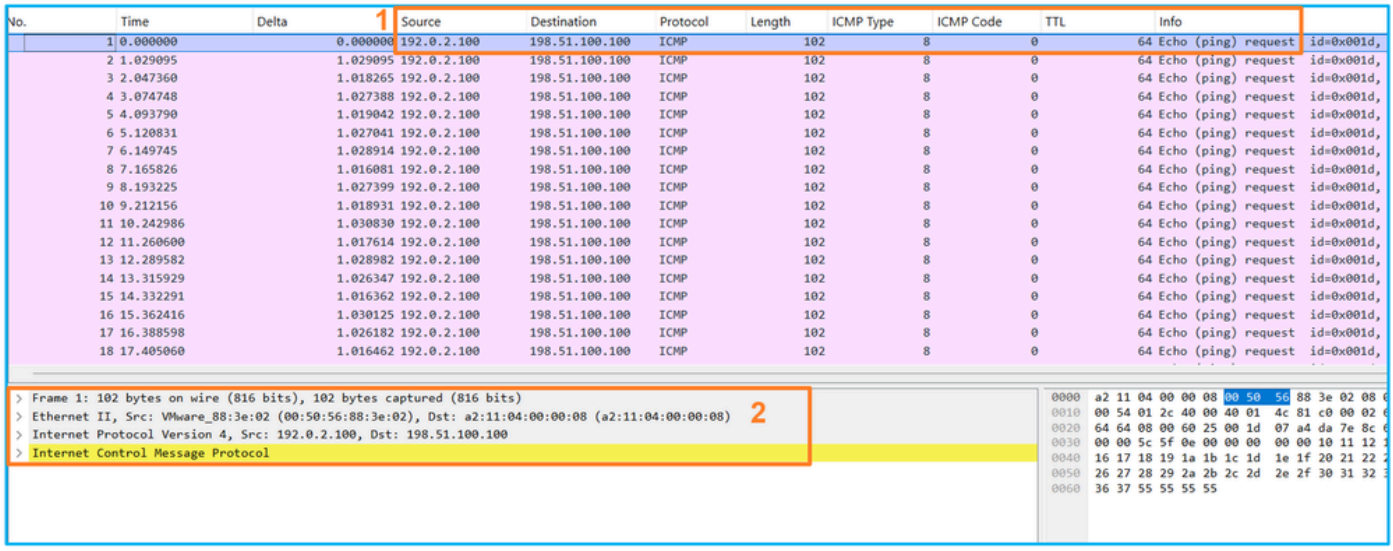
收集捕获文件

执行收集Firepower 4100/9300内部交换机捕获文件部分中的FXOS CLI步骤。

捕获文件分析

使用数据包捕获文件读取器应用程序打开Ethernet1/5的捕获文件。在本示例中，分析在安全防火墙3100上捕获的数据包。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

交换机捕获在接口Ethernet1/5上配置。

此表概述了任务：

任务	捕获点	内部过滤器	方向	捕获的流量
在接口Ethernet1/5上配置并检验数据包捕获	Ethernet1/5	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

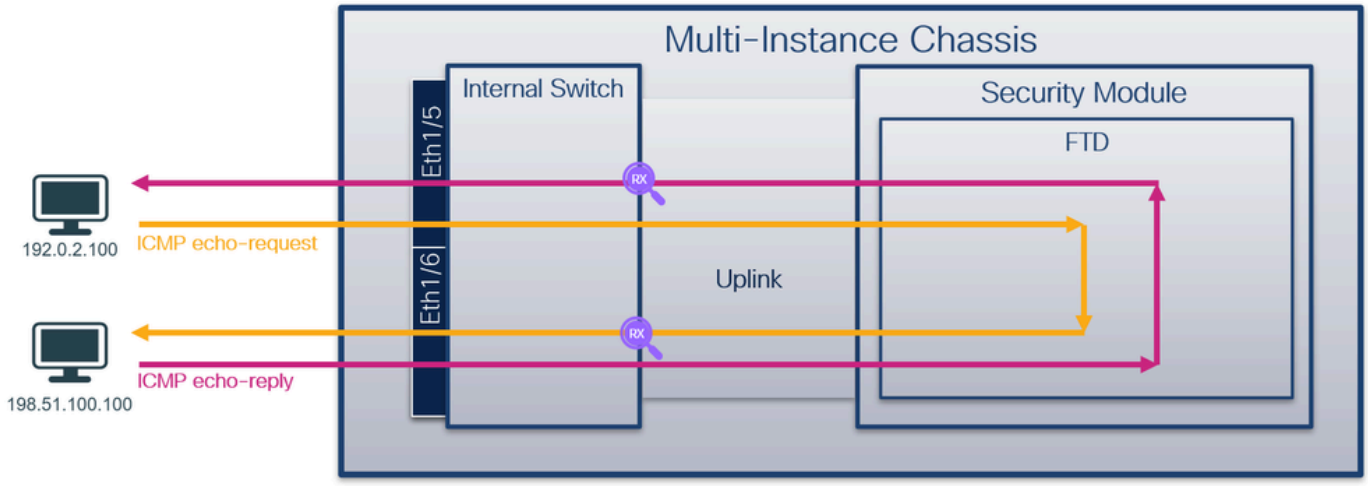
*与3100不同，安全防火墙4200支持双向（入口和出口）捕获。

任务2

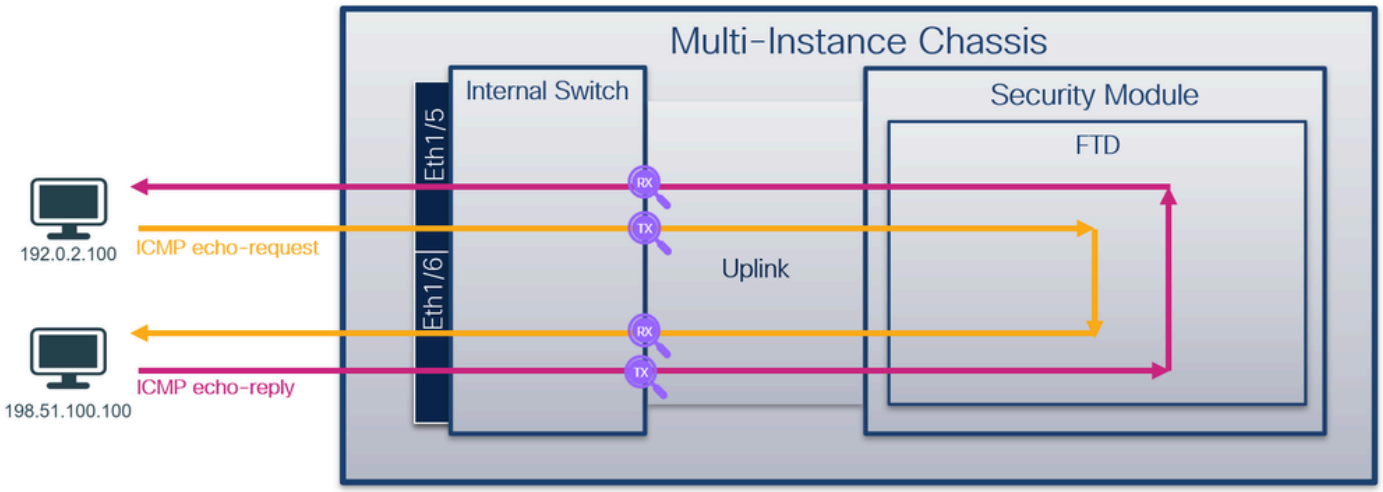
在多实例机箱上使用FXOS CLI配置并验证数据上行链路接口上的交换机数据包捕获。

拓扑、数据包流和捕获点

安全防火墙3100:



安全防火墙4200:



配置

FXOS CLI

在机箱FXOS CLI上执行以下步骤，在数据上行链路接口上配置数据包捕获：

1. 标识应用类型和标识符：

```
<#root>

firepower-3120 /ssa #

show app-instance

Application Name      Identifier           Slot ID     Admin State      Operational State     Running Versi
-------------------- -------------------- ---------- --------------- -------------------- -------------

ftd

ftd1

                  1          Enabled          Online               7.7.0.89         7.7.0.89         Contai
```

2.创建捕获会话：

```
<#root>
firepower-3120#
scope packet-capture

firepower-3120 /packet-capture #
create session cap1

firepower-3120 /packet-capture/session* #
create phy-port Eth1/18

firepower-3120 /packet-capture/session/phy-port* #
set app ftd

firepower-3120 /packet-capture/session/phy-port* #
set app-instance ftd1

firepower-3120 /packet-capture/session/phy-port* #
up

firepower-3120 /packet-capture/session* #
enable

firepower-3120 /packet-capture/session* #
commit-buffer

firepower-3120 /packet-capture/session #
```

注意：与本地部署不同，在多实例模式下使用端口号而不是接口名称。请参阅系统架构高级概述部分中的表，检查内部交换机端口映射。

安全防火墙4200:

```
<#root>
firepower-4245#
scope packet-capture
```

```
firepower-4245 /packet-capture #
create session cap1

firepower-4245 /packet-capture/session* #
create phy-port Eth1/11

firepower-4245 /packet-capture/session/phy-port* #
set app ftd

firepower-4245 /packet-capture/session/phy-port* #
set app-instance ftd1

firepower-4245 /packet-capture/session/phy-port* #
set direction both

firepower-4245 /packet-capture/session/phy-port* #
up

firepower-4245 /packet-capture/session* #
create phy-port Eth1/12

firepower-4245 /packet-capture/session/phy-port* #
set app ftd

firepower-4245 /packet-capture/session/phy-port* #
set app-instance ftd1

firepower-4245 /packet-capture/session/phy-port* #
set direction both

firepower-4245 /packet-capture/session/phy-port* #
up

firepower-4245 /packet-capture/session* #
enable

firepower-4245 /packet-capture/session* #
commit-buffer

firepower-4245 /packet-capture/session #
```

确认

FXOS CLI

在范围数据包捕获中验证捕获详细信息。具体而言，验证捕获会话名称、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：

```
<#root>

firepower-3120#

scope packet-capture


firepower-3120 /packet-capture #

show session cap1



SSP Traffic Monitoring 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
    Error Code: 0
    Drop Count: 0


Packet Count: 171



Physical ports involved in Packet Capture:
    Slot Id: 1
    Port Id: 18
    Pcapfile: /workspace/packet-capture/sess-1-cap1-data-uplink1.pcap


 Pcapsize: 19932  bytes


    Filter:
    Sub Interface: 0
    Application Instance:

ftd1
```

```
    Application Name:
ftd

    Direction:
Ingress

    Drop: Disable
```

安全防火墙4200:

<#root>

```
firepower-4245#
scope packet-capture

firepower-4245 /packet-capture #
show session cap1


SSP Traffic Monitoring 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
    Error Code: 0
    Drop Count: 0

Packet Count: 70


Physical ports involved in Packet Capture:
    Slot Id:
 1

    Port Id:
11
```

```
    Pcapfile: /workspace/packet-capture/sess-1-cap1-data-uplink1.pcap

Pcapsize: 8320  bytes

    Filter:
    Sub Interface: 0
    Application Instance: ftd1
    Application Name: ftd
    D
irection: Both

    Drop: Disable

    Slot Id:
1

    Port Id:
12

    Pcapfile: /workspace/packet-capture/sess-1-cap1-data-uplink2.pcap

 Pcapsize: 172  bytes

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

 Direction: Both

    Drop: Disable
```

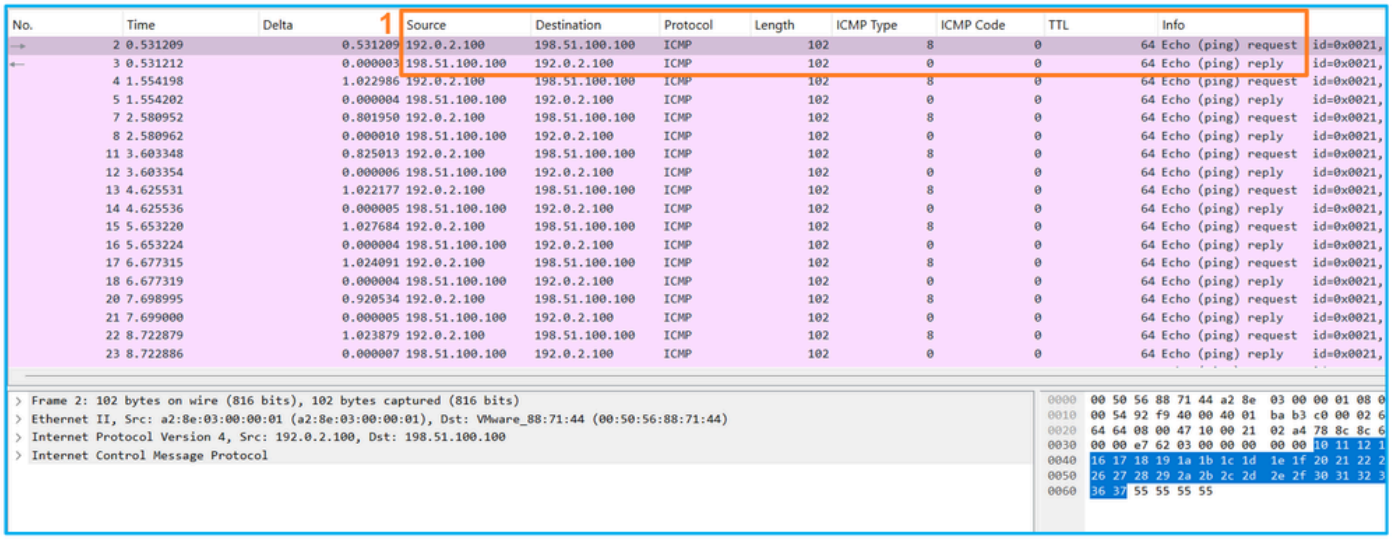
收集捕获文件

执行收集Firepower 4100/9300内部交换机捕获文件部分中的FXOS CLI步骤。

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。在此示例中，分析在安全防火墙3100上捕获的数据包。

检查关键点 — 在本例中，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

当在上行链路接口上配置交换机捕获时，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

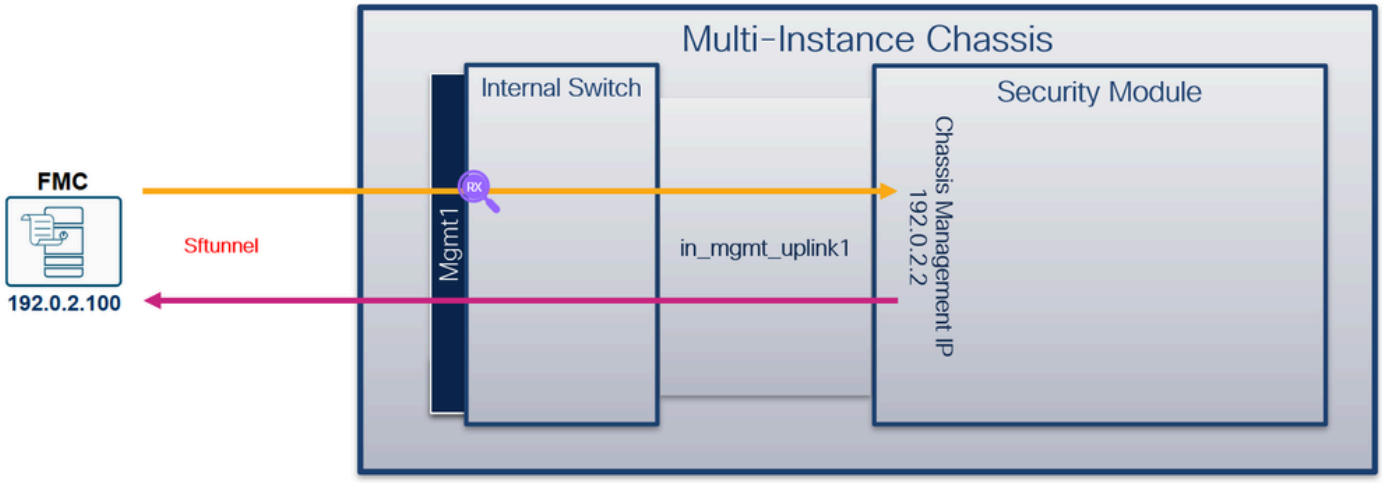
*与3100不同，安全防火墙4200支持双向（入口和出口）捕获。

任务3

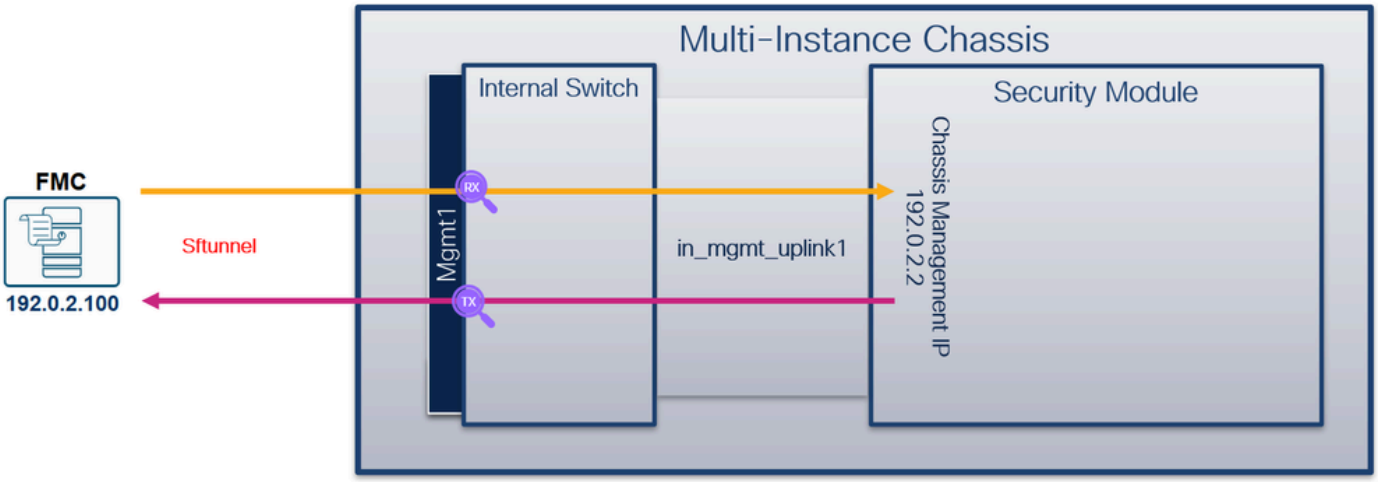
使用多实例机箱上的FXOS CLI在管理接口上配置和验证交换机数据包捕获，捕获机箱和FMC之间的sftunnel流量。

拓扑、数据包流和捕获点

安全防火墙3100:



具有双向捕获功能的安全防火墙4200:



配置

FXOS CLI

在机箱FXOS CLI上执行以下步骤，为管理接口上的sftunnel流量配置数据包捕获。

1.创建数据包捕获过滤器以仅捕获TCP流量（协议号6）。

```
<#root>
firepower-4245#
scope packet-capture

firepower-4245 /packet-capture #
create filter filter1

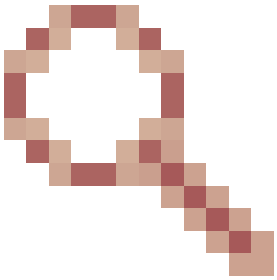
firepower-4245 /packet-capture/filter* #
set protocol 6
```

```
firepower-4245 /packet-capture/filter* #
commit-buffer

firepower-4245 /packet-capture/filter #
up

firepower-4245 /packet-capture #
```





注意：由于CSCwq64141漏洞，尽管安全防火墙4200支持双向交换机捕获但是，使用捕获双向流量的匹配条件创建特定交换机捕获过滤器是行不通的。因此，此任务中的过滤器配置为匹配所有TCP流量，从而能够在安全防火墙4200上捕获双向的sftunnel流量。

2.为管理接口创建捕获会话。根据系统体系结构高级概述部分中的表，安全防火墙3100上的管理端口映射到内部交换机端口Eth1/17:

<#root>

```
firepower-3120#
scope packet-capture

firepower-3120 /packet-capture #
create session cap1

firepower-3120 /packet-capture/session* #
create phy-port Eth1/17

firepower-3120 /packet-capture/session/phy-port* #
set filter filter1

firepower-3120 /packet-capture/session/phy-port* #
up

firepower-3120 /packet-capture/session* #
enable

firepower-3120 /packet-capture/session* #
```

```
up

firepower-3120 /packet-capture* #
commit-buffer

firepower-3120 /packet-capture #
```

安全防火墙4200上的管理端口1映射到内部交换机端口Eth1/9:

```
<#root>
firepower-4245#
scope packet-capture

firepower-4245 /packet-capture #
create session cap1

firepower-4245 /packet-capture/session* #
create phy-port Eth1/9

firepower-4245 /packet-capture/session/phy-port* #
set direction both

firepower-4245 /packet-capture/session/phy-port* #
set filter filter1

firepower-4245 /packet-capture/session/phy-port* #
up

firepower-4245 /packet-capture/session* #
enable

firepower-4245 /packet-capture/session* #
commit-buffer
```

确认

FXOS CLI

在范围数据包捕获中验证捕获详细信息。具体而言，验证捕获会话名称、管理和操作状态、接口插槽、过滤器和标识符。确保Pcapsize值（以字节为单位）增加，且捕获的数据包数量非零：

```
<#root>

firepower-3120#

scope packet-capture


firepower-3120 /packet-capture #

show session cap1



SSP Traffic Monitoring 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
    Error Code: 0
    Drop Count: 0
    Packet Count:

694



Physical ports involved in Packet Capture:
    Slot Id:

 1


    Port Id:

17


    Pcapfile:

/workspace/packet-capture/sess-1-cap1-management-1-1.pcap


    Pcapsize:

81093  bytes


    Filter:

filter1


    Sub Interface: 0
    Application Instance:
```

```
    Application Name:
    Direction:
```

Ingress

```
    Drop: Disable
```

安全防火墙4200:

<#root>

```
firepower-4245#
```

scope packet-capture

```
firepower-4245 /packet-capture #
```

show session cap1

```
SSP Traffic Monitoring 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
    Error Code: 0
    Drop Count: 0
    Packet Count:
```

222

```
Physical ports involved in Packet Capture:
    Slot Id:
```

1

```
    Port Id:
```

9

```
    Pcapfile:
```

/workspace/packet-capture/sess-1-cap1-management-1-1.pcap

```
    Pcapsize:
40180  bytes


    Filter: filter1
    Sub Interface: 0
    Application Instance:
    Application Name:
    Direction:
Both


    Drop: Disable
```

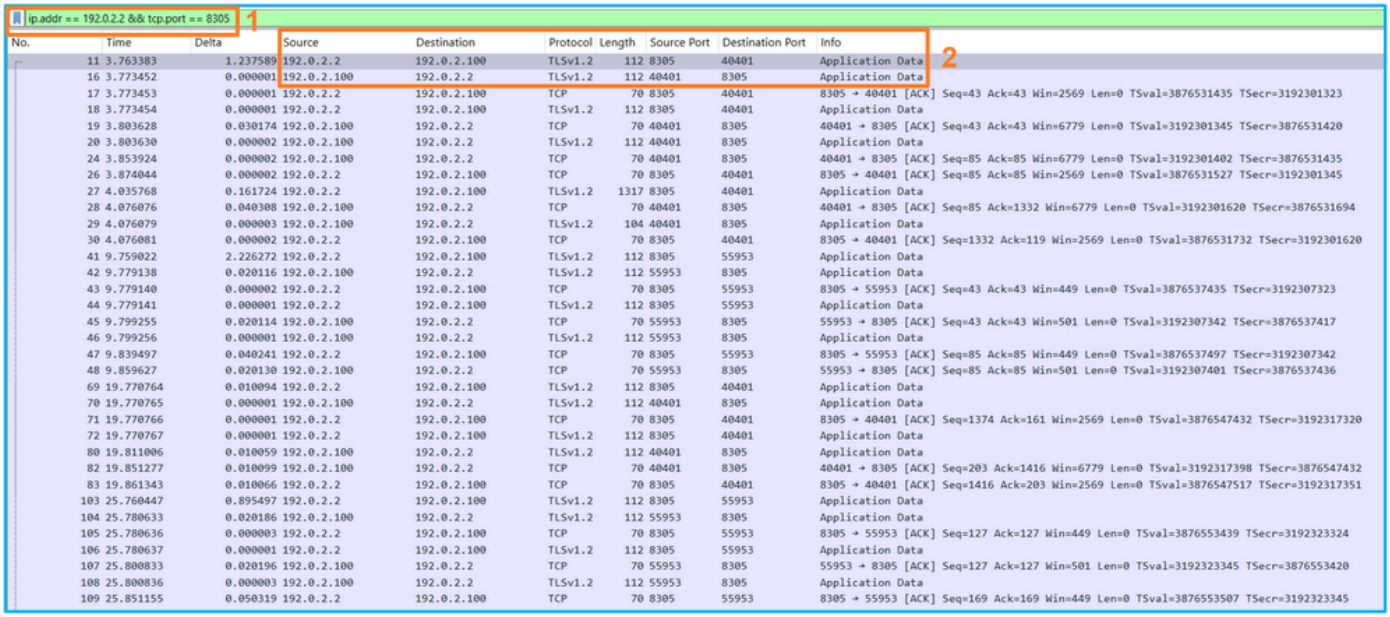
收集捕获文件

执行收集Firepower 4100/9300内部交换机捕获文件部分中的FXOS CLI步骤。

捕获文件分析

使用数据包捕获文件读取器应用程序打开管理接口的捕获文件。在本示例中，分析在安全防火墙4200上捕获的数据包。检查要点：

1. 需要过滤器来清理捕获并仅显示sftunnel流量。
2. sftunnel流量在两个方向被捕获。



说明

交换机捕获是在管理接口上配置的。

此表概述了任务：

任务	捕获点	内部过滤器	方向	捕获的流量
配置并验证管理接口上sftunnel流量的数据包捕获	*Ethernet1/9	TCP流量	**两个	主机192.0.2.100与主机192.0.2.2之间的Sftunnel流量（TCP端口8305）

*请参阅“系统架构高级概述”部分中的表以检查内部交换机端口映射。

**与3100不同，安全防火墙4200支持双向（入口和出口）捕获。

收集Secure Firewall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

在上执行以下步骤以收集ASA CLI上的内部交换机捕获文件：

1. 停止捕获：

```
<#root>
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。

```
<#root>
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：

```
<#root>

asa#

copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap ?
```

```
  cluster:        Copy to cluster: file system
  disk0:          Copy to disk0: file system
  disk1:          Copy to disk1: file system
  flash:          Copy to flash: file system
  ftp:            Copy to ftp: file system
  running-config  Update (merge with) current system configuration
  scp:            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

执行以下步骤收集FTD CLI上的内部交换机捕获文件，并将这些文件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:

<#root>

```
>
```

system support diagnostic-cli

```
Attaching to Diagnostic CLI ... Click 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower>
```

enable

```
Password:
```

<-- Enter

```
firepower#
```

2. 停止捕获：

<#root>

```
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：

```
<#root>
firepower#
show capture capsw detail

Packet Capture info

Name:              capsw

  Session:           1

Admin State:       disabled


  Oper State:        down


  Oper State Reason: Session_Admin_Shut


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

Total Physical ports involved in Packet Capture: 1
Physical port:
  Slot Id:           1
  Port Id:           1

  Pcapfile:

/mnt/disk0/packet-capture/

sess-1-capsw-ethernet-1-1-0.pcap


  Pcapsize:          139826
  Filter:            capsw-1-1

Packet Capture Filter Info
  Name:              capsw-1-1
  Protocol:          0
  Ivlan:             0
  Ovlan:             0
  Src Ip:            0.0.0.0
```

```
  Dest Ip:           0.0.0.0
  Src Ipv6:          ::
  Dest Ipv6:         ::
  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。

<#root>

```
firepower#

copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap ?


  cluster:        Copy to cluster: file system
  disk0:          Copy to disk0: file system
  disk1:          Copy to disk1: file system
  flash:          Copy to flash: file system
  ftp:            Copy to ftp: file system
  running-config  Update (merge with) current system configuration
  scp:            Copy to scp: file system
  smb:            Copy to smb: file system
  startup-config  Copy to startup configuration
  system:         Copy to system: file system
  tftp:           Copy to tftp: file system

firepower#

copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap tftp://198.51.100.10/


Source filename [/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap]?
Destination filename [sess-1-capsw-ethernet-1-1-0.pcap]?
Copy in progress...C

139826 bytes copied in 0.532 secs
```

执行以下步骤，通过File Download选项从FMC收集捕获文件：

1. 停止捕获：

<#root>

```
>

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：

```
<#root>

>

show capture capsw detail


Packet Capture info


Name:              capsw


  Session:           1


Admin State:       disabled


  Oper State:        down


  Oper State Reason: Session_Admin_Shut


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

Total Physical ports involved in Packet Capture: 1

Physical port:
  Slot Id:           1
  Port Id:           1

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


  Pcapsize:          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：

```
<#root>

>

expert


admin@firepower:~$

sudo su


root@firepower:/home/admin
```

4. 将捕获文件复制到/ngfw/var/common/:

```
<#root>

root@KSEC-FPR3100-1:/home/admin

cp /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap /ngfw/var/common/


root@KSEC-FPR3100-1:/home/admin

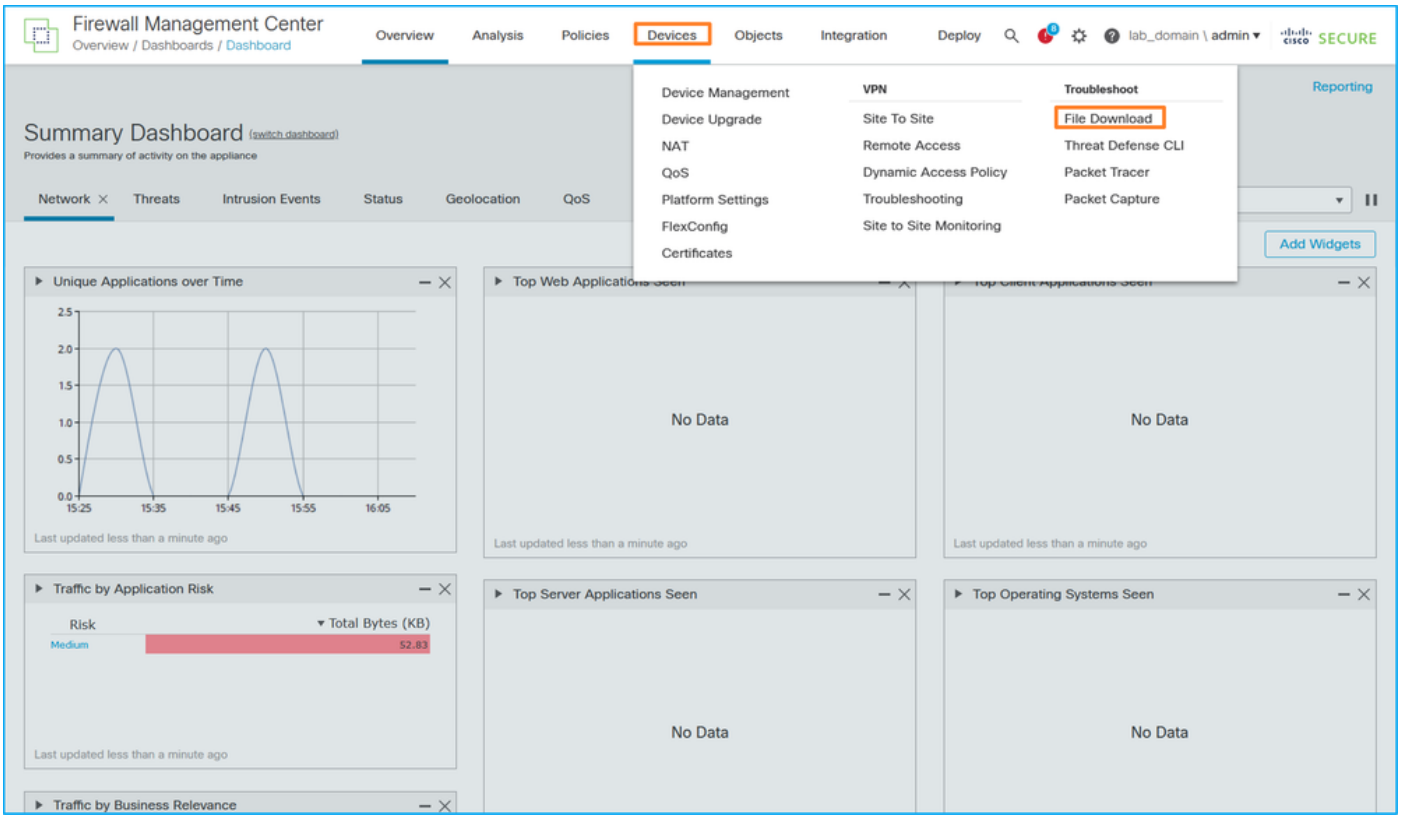
ls -l /ngfw/var/common/sess*


-rwxr-xr-x 1 root admin 139826 Aug  7 20:14

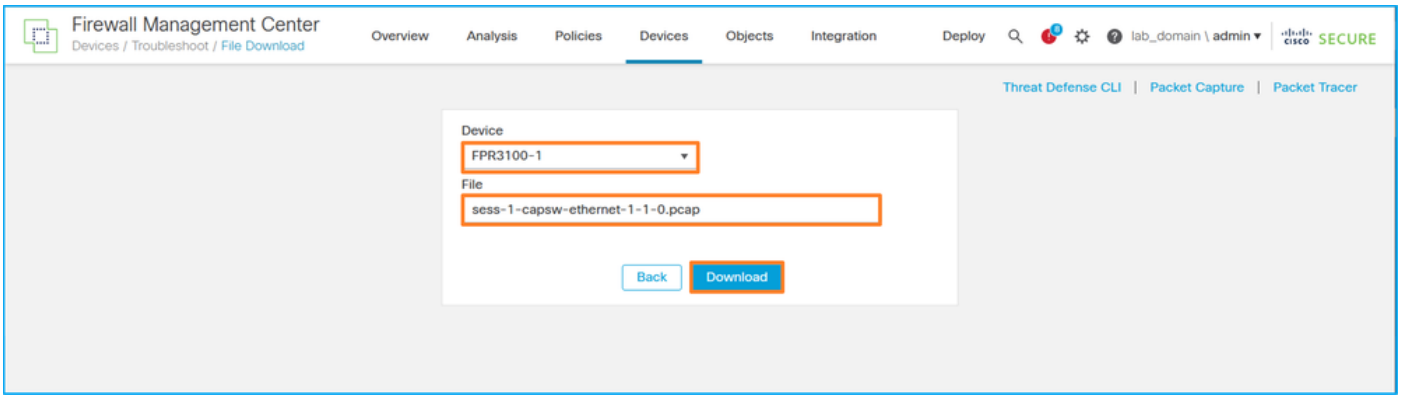
/ngfw/var/common/sess-1-capsw-ethernet-1-1-0.pcap


-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。
- 在多情景ASA中，数据接口上的交换机捕获是在用户情景中配置的。只有管理情景中才支持交换机在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）。