Configurar e verificar as capturas de firewall seguro e do switch interno Firepower

Contents

Introduction
Prerequisites
Requirements
Componentes Utilizados
Informações de Apoio
Visão geral de alto nível da arquitetura do sistema
Visão geral de alto nível das operações internas do switch
Fluxo de pacotes e pontos de captura
Configuração e verificação no Firepower 4100/9300
Captura de pacotes em uma interface física ou de canal de porta
Capturas de pacotes nas interfaces do backplane
Capturas de pacotes nas portas do aplicativo e do aplicativo
Captura de pacotes em uma subinterface de uma interface física ou de canal de porta
Filtros de captura de pacotes
Coletar Arquivos De Captura Do Switch Interno Firepower 4100/9300
Diretrizes, limitações e práticas recomendadas para captura de pacotes de switch interno
Configuração e verificação no Secure Firewall 3100
Captura de pacotes em uma interface física ou de canal de porta
Captura de pacotes em uma subinterface de uma interface física ou de canal de porta
Captura de pacotes em interfaces internas
Filtros de captura de pacotes
Coletar arquivos de captura do switch interno do Secure Firewall 3100
Diretrizes, limitações e práticas recomendadas para captura de pacotes de switch interno
Informações Relacionadas

Introduction

Este documento descreve a configuração e a verificação do Firepower e as capturas de switches internos do Secure Firewall.

Prerequisites

Requirements

Conhecimento básico do produto, análise de captura.

Componentes Utilizados

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

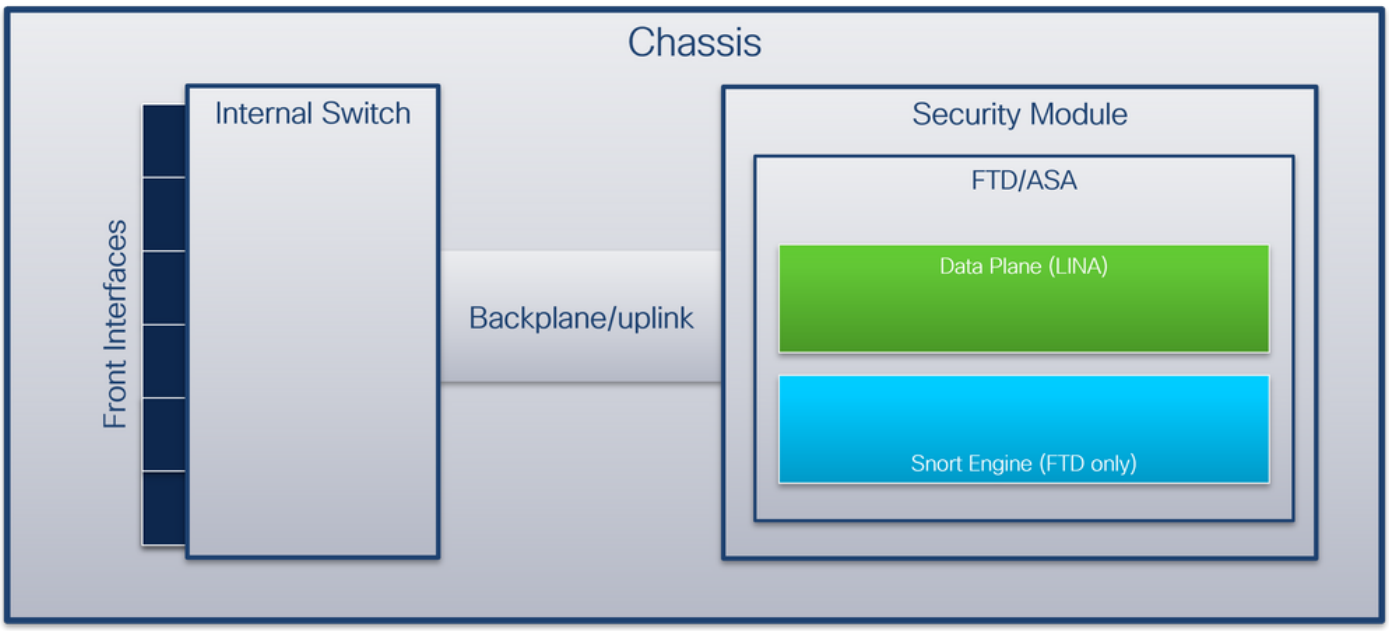
As informações neste documento são baseadas nestas versões de software e hardware:

- Firewall seguro 31xx
- Firepower 41xx
- Firepower 93xx
- Cisco Secure eXtensible Operating System (FXOS) 2.12.0.x
- Cisco Secure Firewall Threat Defense (FTD) 7.2.0.x
- Cisco Secure Firewall Management Center (FMC) 7.2.0.x
- Cisco Secure Firewall Device Manager (FDM) 7.2.0.x
- Adaptive Security Appliance (ASA) 9.18(1)x
- Adaptive Security Appliance Device Manager (ASDM) 7.18.1.x
- Wireshark 3.6.7 (https://www.wireshark.org/download.html)

Informações de Apoio

Visão geral de alto nível da arquitetura do sistema

Da perspectiva do fluxo de pacotes, a arquitetura do Firepower 4100/9300 e do Secure Firewall 3100 pode ser visualizada como mostrado na figura:



O chassi inclui estes componentes:

- **Switch interno** - encaminha o pacote da rede para o aplicativo e vice-versa. O switch interno é conectado às **interfaces frontais** que residem no módulo de interface interno ou módulos de rede externos e se conecta a dispositivos externos, como switches. Exemplos de interfaces frontais são Ethernet 1/1, Ethernet 2/4 e assim por diante. A "frente" não é uma definição técnica forte. Neste documento, ele é usado para distinguir interfaces conectadas a dispositivos externos das interfaces de backplane ou uplink.

- **Backplane ou uplink** - uma interface interna que conecta o módulo de segurança (SM) ao switch interno. Esta tabela mostra as interfaces de backplane no Firepower 4100/9300 e a interface de uplink no Secure Firewall 3100:

Platform	Número de módulos de segurança suportados	Interfaces de backplane/uplink	Interfaces de aplic mapeadas
Firepower 4100 (exceto Firepower 4110/4112)	1	SM1: Ethernet1/9 Ethernet1/10	Internal-Data0/0 Internal-Data0/1
Firepower 4110/4112	1	Ethernet1/9	Internal-Data0/0
Firepower 9300	3	SM1: Ethernet1/9 Ethernet1/10 SM2: Ethernet1/11 Ethernet1/12 SM3: Ethernet1/13 Ethernet1/14	Internal-Data0/0 Internal-Data0/1 Internal-Data0/0 Internal-Data0/1 Internal-Data0/0 Internal-Data0/1
Firewall seguro 3100	1	SM1: in_data_uplink1	Internal-Data0/1

No caso de 2 interfaces de painel traseiro por módulo, o switch interno e os aplicativos nos módulos executam o balanceamento de carga de tráfego nas 2 interfaces.

- **Módulo de segurança, mecanismo de segurança** ou **blade** - o módulo onde aplicativos como FTD ou ASA estão instalados. O Firepower 9300 suporta até 3 módulos de segurança.
- **Interface de aplicativo mapeada** - aplicativos, como FTD ou ASA, mapeiam as interfaces de backplane ou uplink para interfaces internas. Em outras palavras, as interfaces de backplane ou uplink são visíveis como interfaces internas em aplicativos.

Use o comando **show interface detail** para verificar interfaces internas:

```
> 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
```

Visão geral de alto nível das operações internas do switch

Firepower 4100/9300

Para tomar uma decisão de encaminhamento, o switch interno usa uma **marca de VLAN de interface**, ou **marca de VLAN de porta**, e uma **marca de rede virtual (marca de VLAN)**.

A marca de VLAN de porta é usada pelo switch interno para identificar uma interface. O switch insere a tag de VLAN da porta em cada pacote de entrada que veio nas interfaces frontais. A marca da VLAN é configurada automaticamente pelo sistema e não pode ser alterada manualmente. O valor da marca pode ser verificado no shell de comando **fxos**:

```
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
```

A marca VN também é inserida pelo switch interno e usada para encaminhar os pacotes ao aplicativo. Ele é configurado automaticamente pelo sistema e não pode ser alterado manualmente.

A marca da VLAN da porta e a marca da VLAN são compartilhadas com o aplicativo. O aplicativo insere as respectivas marcas VLAN de interface de saída e as marcas VLAN em cada pacote. Quando um pacote do aplicativo é recebido pelo switch interno nas interfaces do painel traseiro, o switch lê a marca VLAN da interface de saída e a marca VN, identifica o aplicativo e a interface de saída, retira a marca VLAN da porta e a marca VN e encaminha o pacote para a rede.

Firewall seguro 3100

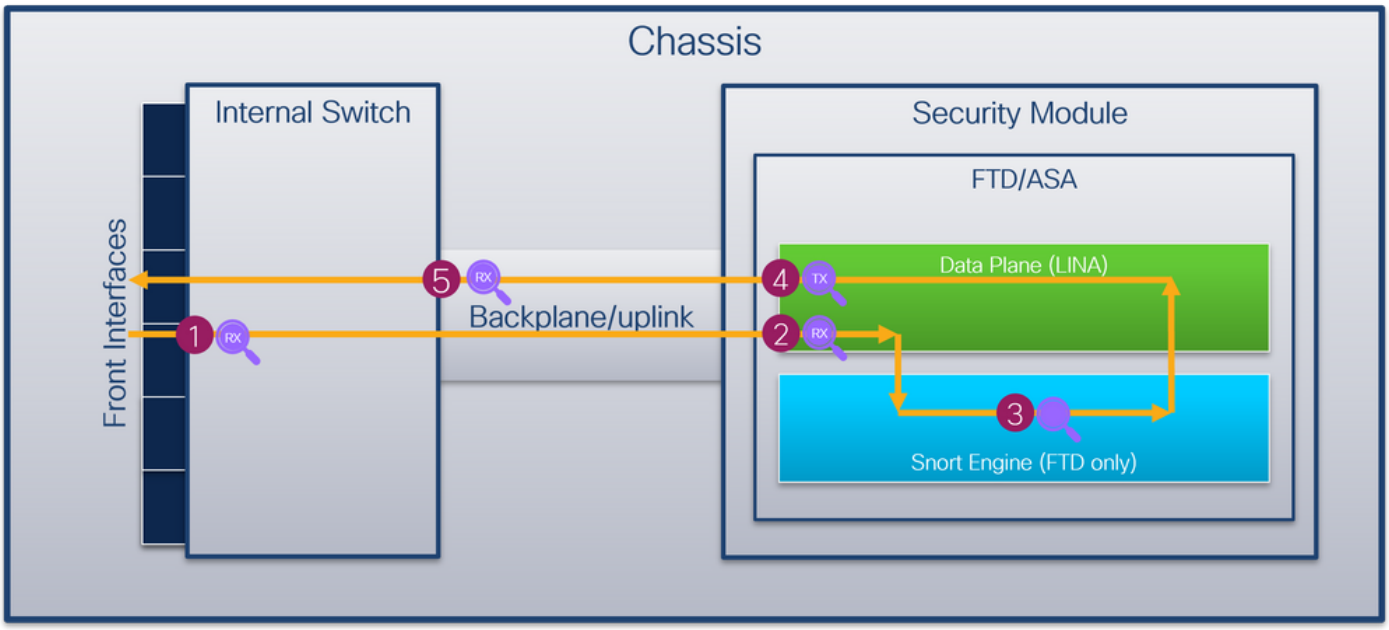
Como no Firepower 4100/9300, a marca de VLAN de porta é usada pelo switch interno para identificar uma interface.

A marca da porta VLAN é compartilhada com o aplicativo. O aplicativo insere as respectivas marcas VLAN de interface de saída em cada pacote. Quando um pacote do aplicativo é recebido pelo switch interno na interface de uplink, o switch lê a marca VLAN da interface de saída, identifica a interface de saída, retira a marca VLAN da porta e encaminha o pacote para a rede.

Fluxo de pacotes e pontos de captura

Os firewalls Firepower 4100/9300 e Secure Firewall 3100 suportam capturas de pacotes nas interfaces do switch interno.

Esta figura mostra os pontos de captura de pacotes ao longo do caminho do pacote dentro do chassi e do aplicativo:



Os pontos de captura são:

1. Ponto de captura de ingresso da interface frontal do switch interno. Uma interface frontal é qualquer interface conectada aos dispositivos pares, como switches.
2. Ponto de captura de ingresso da interface do plano de dados
3. Ponto de captura Snort
4. Ponto de captura de saída da interface do plano de dados
5. Painel traseiro interno do switch ou ponto de captura de entrada de uplink. Uma interface de backplane ou uplink conecta o switch interno ao aplicativo.

O switch interno suporta apenas capturas de interface de entrada. Isso significa que somente os pacotes recebidos da rede ou do aplicativo ASA/FTD podem ser capturados. **Não há suporte para capturas de pacotes de saída.**

Configuração e verificação em Firepower 4100/9300

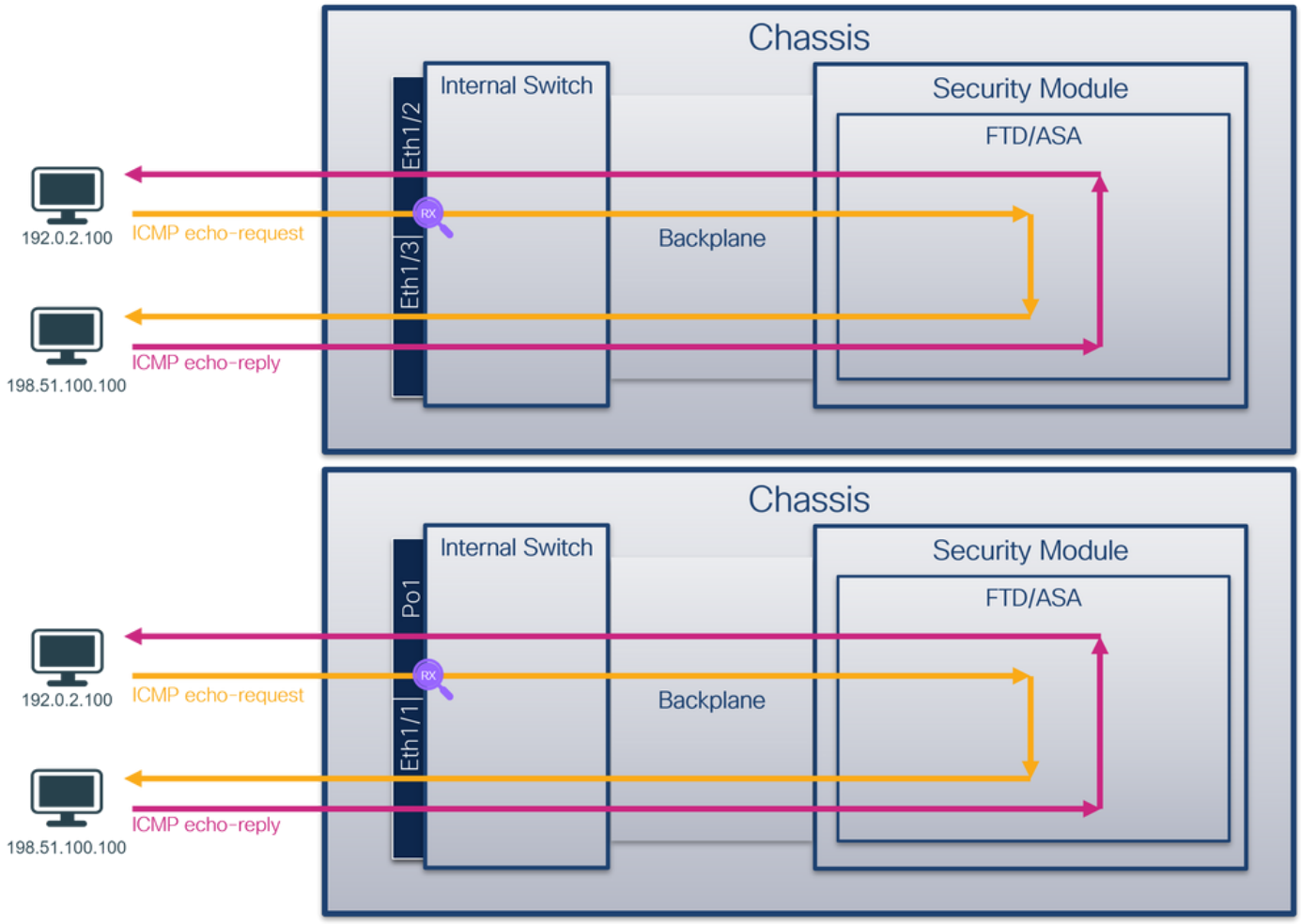
As capturas internas do switch Firepower 4100/9300 podem ser configuradas em **Ferramentas > Captura de pacotes** no FCM ou em **captura de pacote de escopo** no FXOS CLI. **Para obter a descrição das opções de captura de pacote, consulte o** *Guia de configuração do gerenciador de chassi FXOS do Cisco Firepower 4100/9300* ou o *Guia de configuração da CLI FXOS do Cisco Firepower 4100/9300*, capítulo **Solução de problemas**, seção *Captura de pacote*.

Esses cenários abordam casos de uso comuns de capturas de switch interno Firepower 4100/9300.

Captura de pacotes em uma interface física ou de canal de porta

Use o FCM e a CLI para configurar e verificar uma captura de pacote na interface Ethernet1/2 ou Portchannel1. No caso de uma interface port-channel, certifique-se de selecionar todas as interfaces físicas membro.

Topologia, fluxo de pacotes e pontos de captura

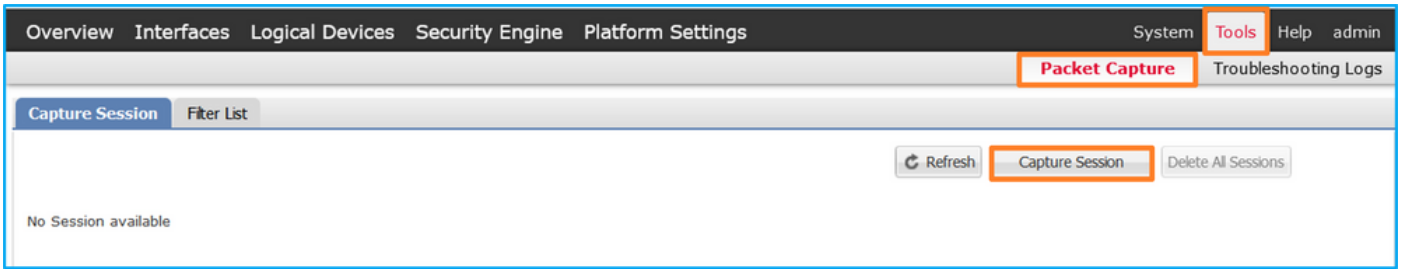


Configuração

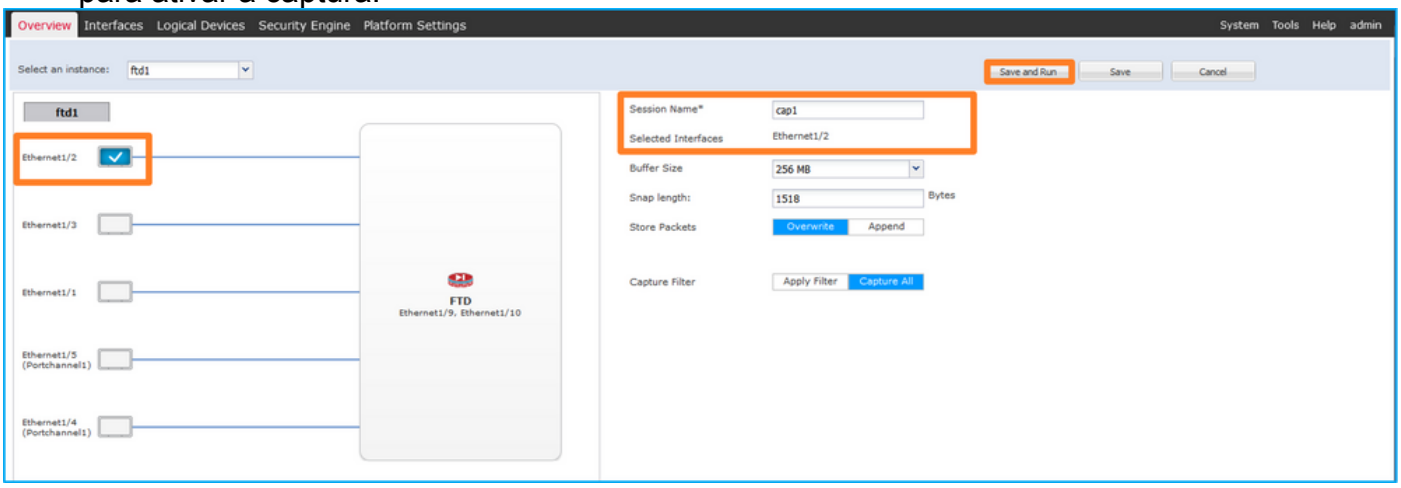
FCM

Siga estas etapas no FCM para configurar uma captura de pacote nas interfaces Ethernet1/2 ou Portchannel1:

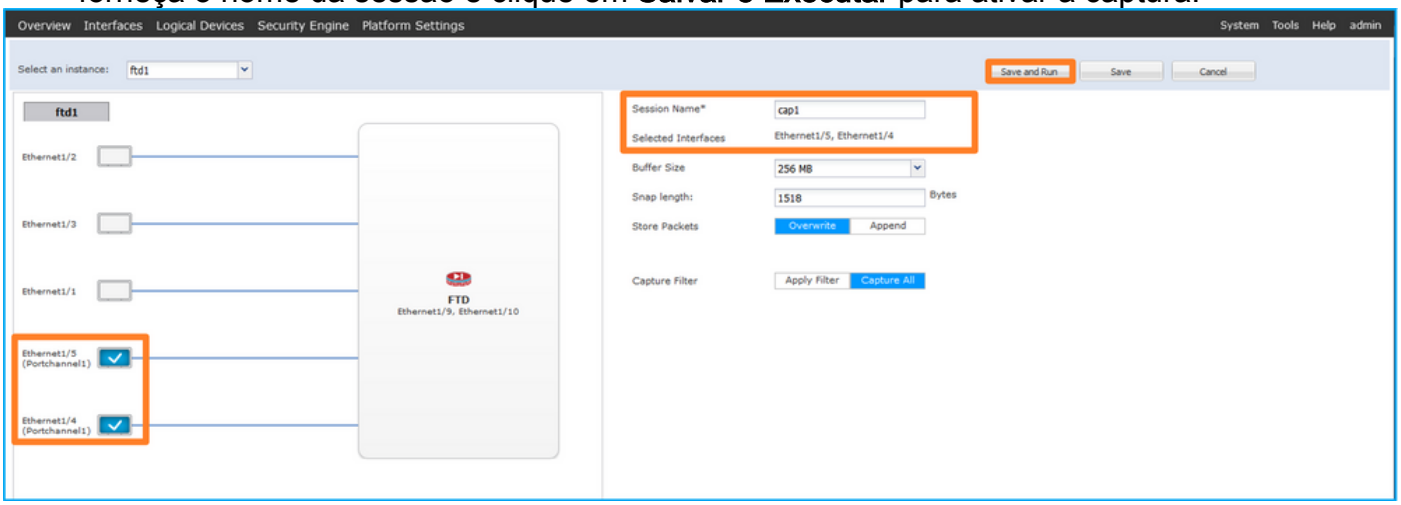
1. Use **Tools > Packet Capture > Capture Session** para criar uma nova sessão de captura:



2. Selecione a interface **Ethernet1/2**, forneça o nome da sessão e clique em **Save and Run** para ativar a captura:



3. No caso de uma interface port-channel, selecione todas as interfaces físicas do membro, forneça o nome da sessão e clique em **Salvar e Executar** para ativar a captura:



CLI FXOS

Siga estas etapas na CLI FXOS para configurar uma captura de pacote nas interfaces Ethernet1/2 ou Portchannel1:

1. Identificar o tipo de aplicativo e o identificador:

```
firepower# scope ssa
firepower /ssa # show app-instance
App Name    Identifier Slot ID     Admin State Oper State       Running Version Startup Version
Deploy Type Turbo Mode Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- --------------- --------------- --
--------- ---------- ------------ --------------- ------------
ftd         ftd1        1           Enabled     Online           7.2.0.82        7.2.0.82
```

```
Native      No                      Not Applicable  None
```

2. No caso de uma interface port-channel, identifique suas interfaces membro:

```
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. Criar uma sessão de captura:

```
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 #
```

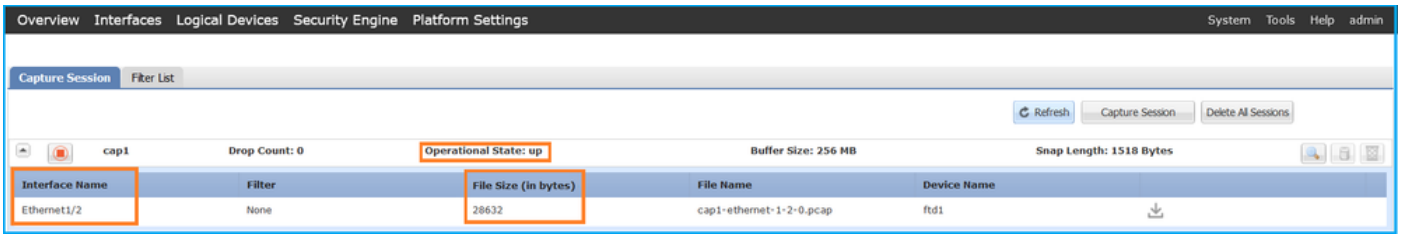
Para interfaces port-channel, uma captura separada para cada interface membro é configurada:

```
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 #
```

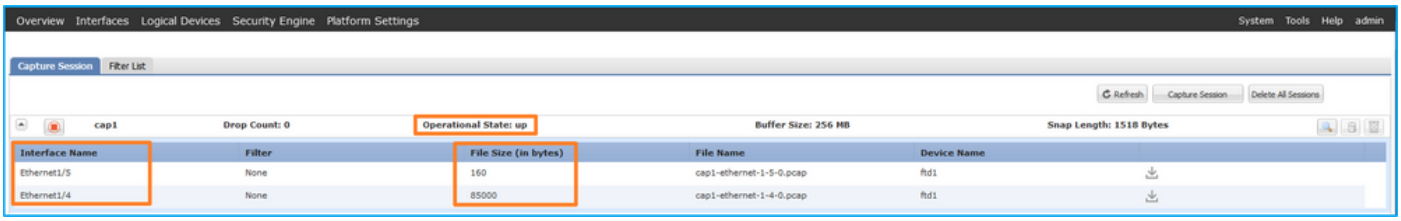
Verificação

FCM

Verifique o **nome da interface**, certifique-se de que o **status operacional** esteja ativo e que o **tamanho do arquivo (em bytes)** aumente:



Portchannel1 com interfaces membro Ethernet1/4 e Ethernet1/5:



CLI FXOS

Verifique os detalhes da captura em **scope packet-capture**:

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

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

Canal de porta 1 com interfaces membro Ethernet1/4 e Ethernet1/5:

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

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

Physical ports involved in Packet Capture:
```

```
Slot Id: 1
 Port Id: 4
 Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-4-0.pcap
 Pcapsize: 310276  bytes
Filter:
Sub Interface: 0
 Application Instance Identifier: ftd1
 Application Name: ftd

Slot Id: 1
 Port Id: 5
 Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-5-0.pcap
 Pcapsize: 160  bytes
Filter:
Sub Interface: 0
 Application Instance Identifier: ftd1
 Application Name: ftd
```

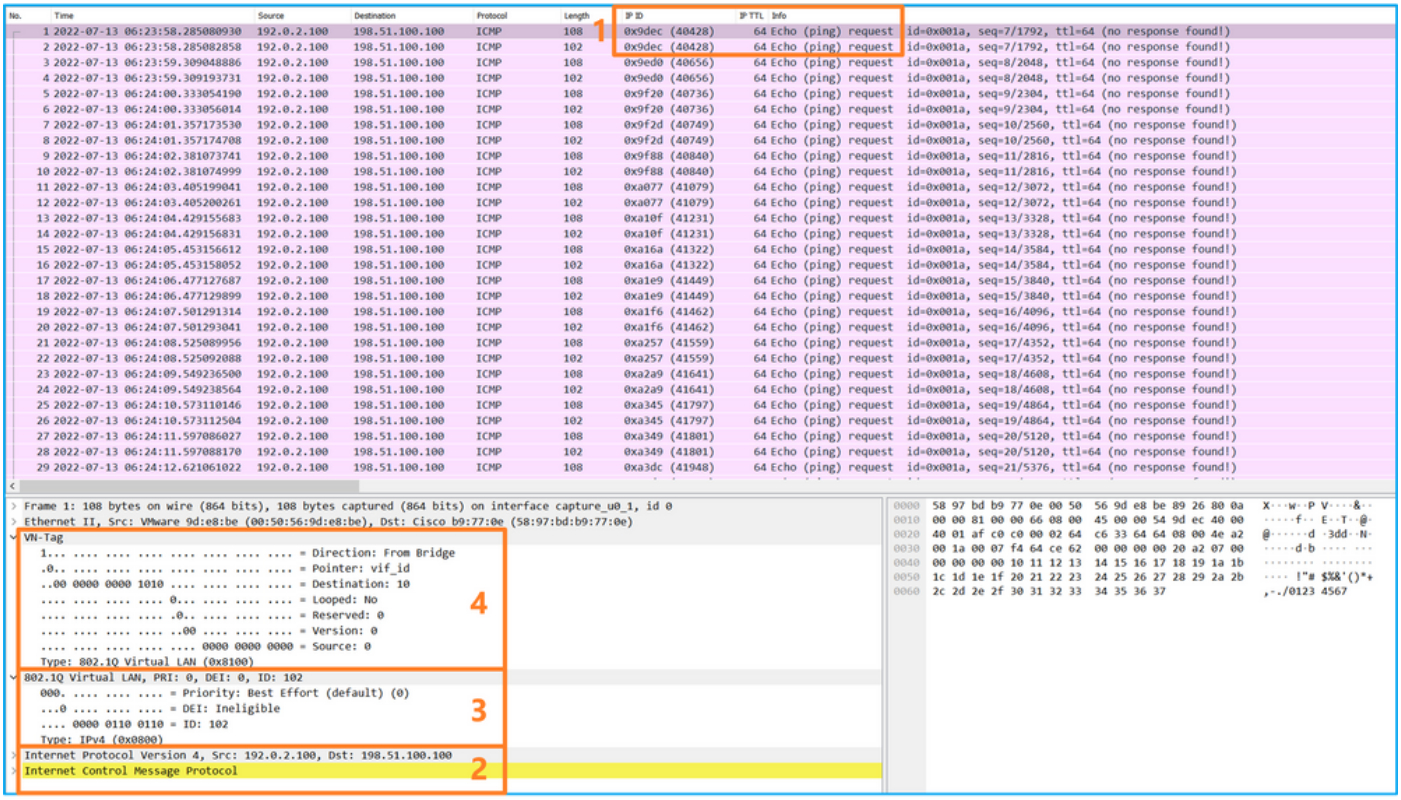
Coletar arquivos de captura

Siga as etapas na seção **Coletar arquivos de captura do switch interno Firepower 4100/9300**.

Capturar análise de arquivo

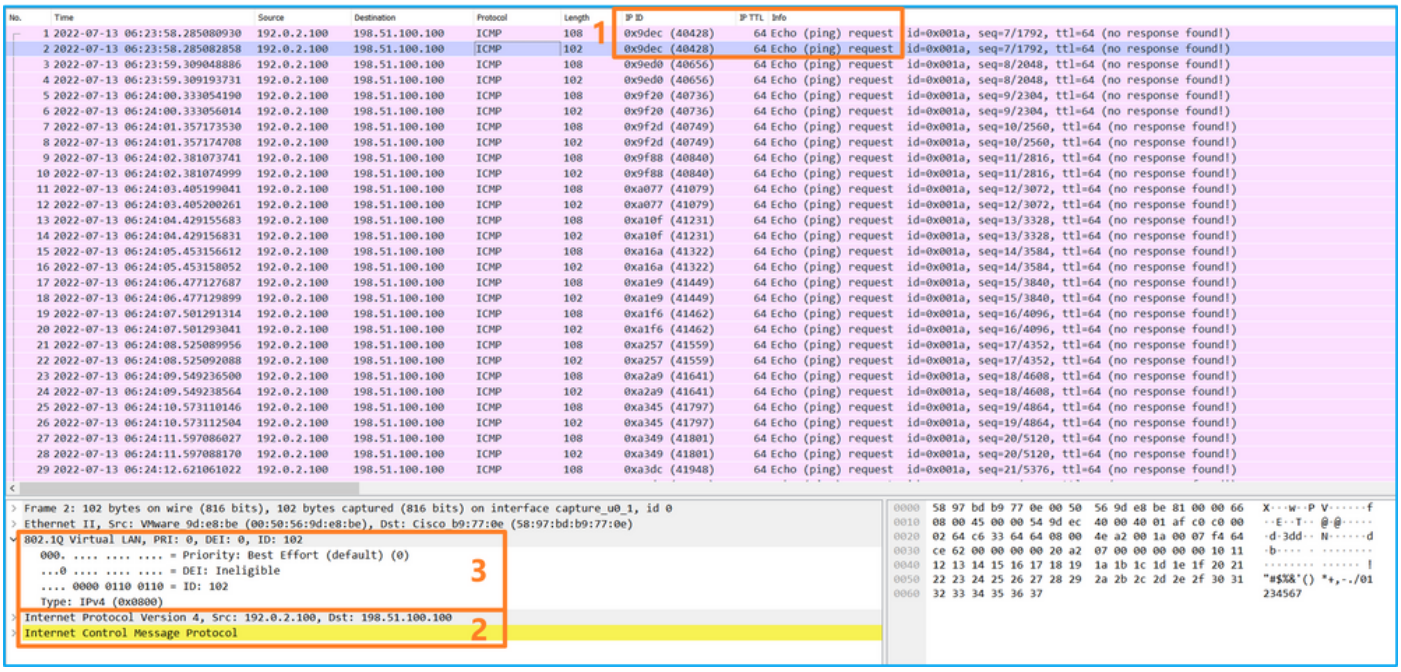
Use um aplicativo leitor de arquivo de captura de pacote para abrir o arquivo de captura para Ethernet1/2. Selecione o primeiro pacote e verifique os pontos principais:

1. Somente os pacotes ICMP de solicitação de eco são capturados. Cada pacote é capturado e mostrado 2 vezes.
2. O cabeçalho do pacote original está sem a marca VLAN.
3. O switch interno insere a tag de VLAN de porta adicional **102** que identifica a interface de entrada Ethernet1/2.
4. O switch interno insere uma marca VN adicional.



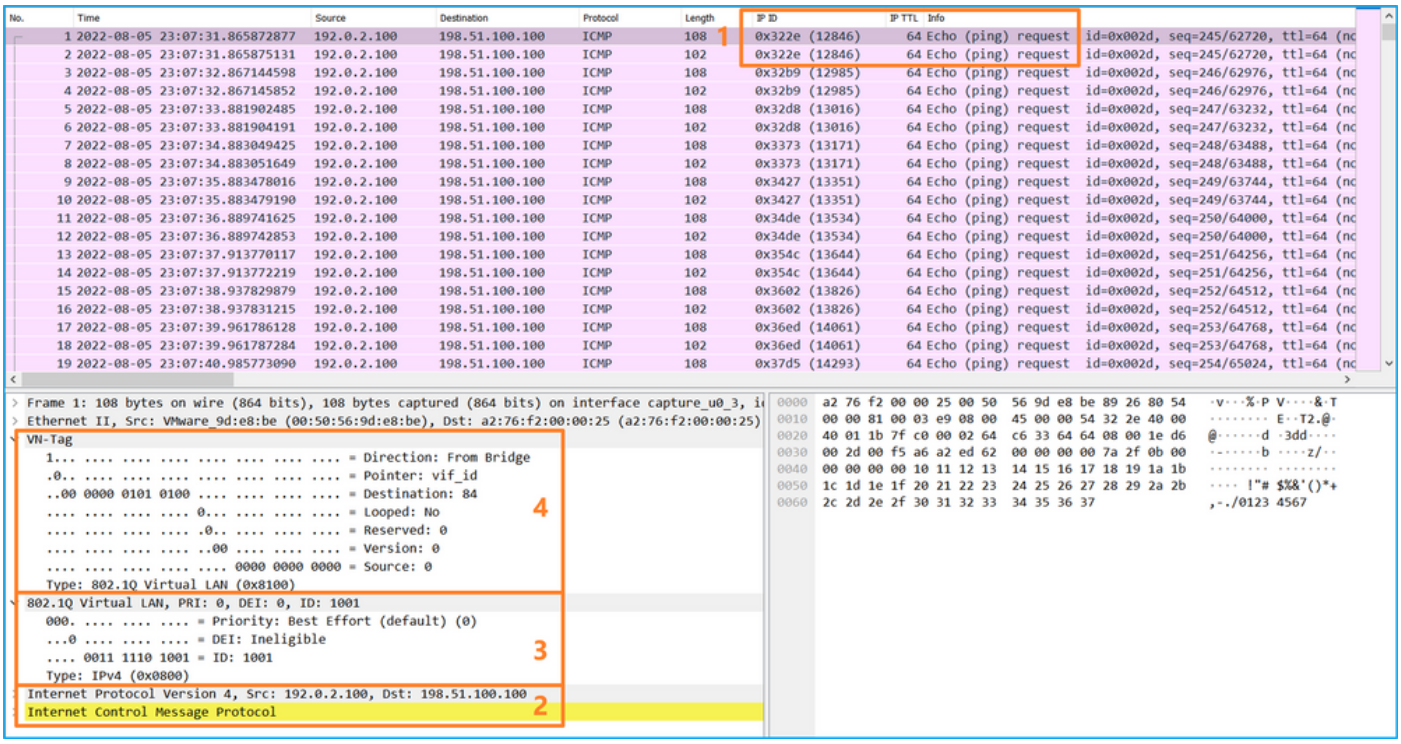
Selecione o segundo pacote e verifique os pontos principais:

1. Somente os pacotes ICMP de solicitação de eco são capturados. Cada pacote é capturado e mostrado 2 vezes.
2. O cabeçalho do pacote original está sem a marca VLAN.
3. O switch interno insere a tag de VLAN de porta adicional **102** que identifica a interface de entrada Ethernet1/2.



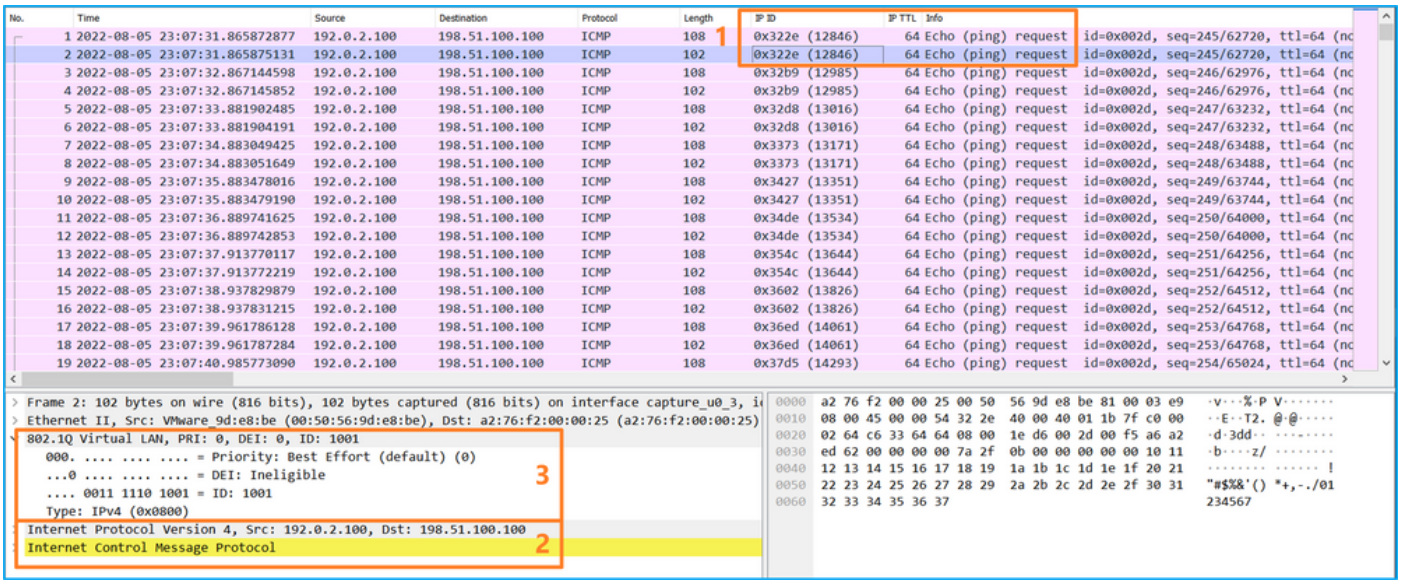
Abra os arquivos de captura para as interfaces membro Portchannel1. Selecione o primeiro pacote e verifique os pontos principais:

1. Somente os pacotes ICMP de solicitação de eco são capturados. Cada pacote é capturado e mostrado 2 vezes.
2. O cabeçalho do pacote original está sem a marca VLAN.
3. O switch interno insere uma tag de VLAN de porta adicional **1001** que identifica a interface de entrada Portchannel1.
4. O switch interno insere uma marca VN adicional.



Selecione o segundo pacote e verifique os pontos principais:

1. Somente os pacotes ICMP de solicitação de eco são capturados. Cada pacote é capturado e mostrado 2 vezes.
2. O cabeçalho do pacote original está sem a marca VLAN.
3. O switch interno insere uma tag de VLAN de porta adicional **1001** que identifica a interface de entrada Portchannel1.



Explicação

Quando uma captura de pacote em uma interface frontal é configurada, o switch captura simultaneamente cada pacote duas vezes:

- Após a inserção da marca da porta VLAN.
- Após a inserção da tag VN.

Na ordem de operações, a tag VN é inserida em um estágio posterior à inserção da tag VLAN da porta. No entanto, no arquivo de captura, o pacote com a marca VN é mostrado antes do pacote com a marca VLAN da porta.

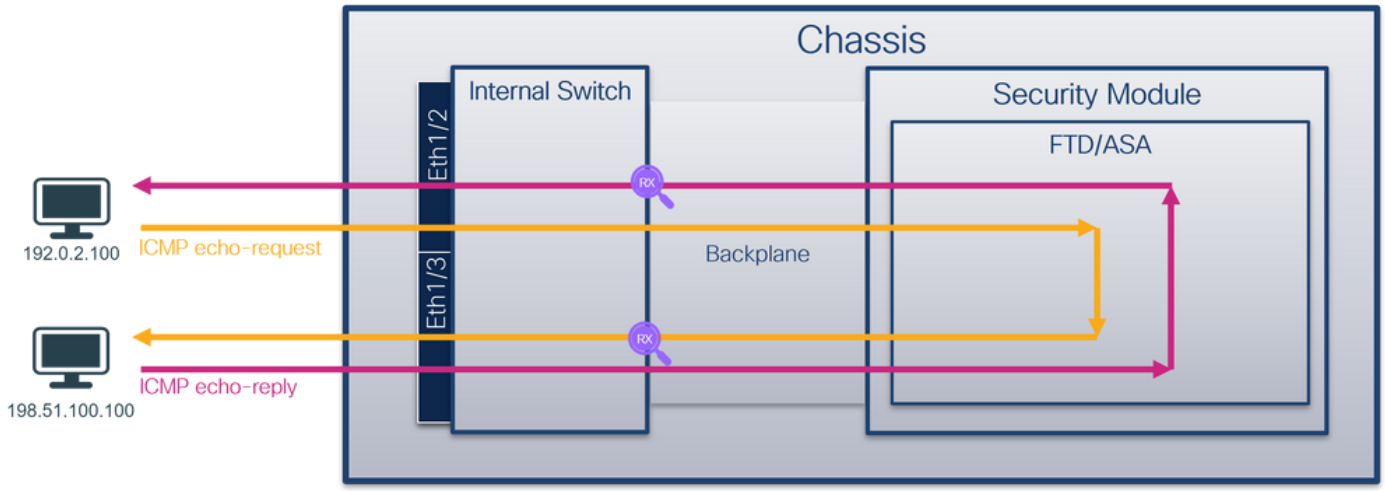
Esta tabela resume a tarefa:

Tarefa	Ponto de captura	VLAN de porta interna em pacotes capturados	Direção	Tráfego capturado
Configurar e verificar uma captura de pacote na interface Ethernet1/2	Ethernet1/2	102	Somente entrada	Solicitações de eco ICMP do hos 192.0.2.100 para o host 198.51.100.100
Configurar e verificar uma captura de pacote na interface Portchannel1 com as interfaces membro Ethernet1/4 e Ethernet1/5	Ethernet1/4 Ethernet1/5	1001	Somente entrada	Solicitações de eco ICMP do hos 192.0.2.100 para o host 198.51.100.100

Capturas de pacotes nas interfaces do backplane

Use o FCM e a CLI para configurar e verificar uma captura de pacotes nas interfaces do painel traseiro.

Topologia, fluxo de pacotes e pontos de captura

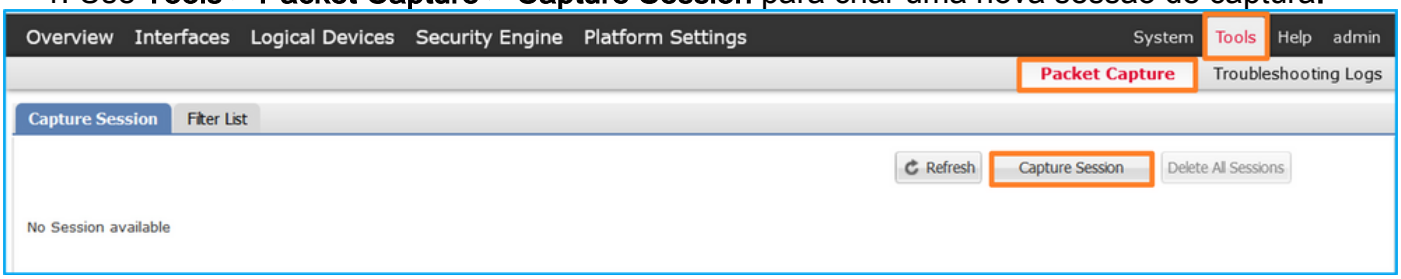


Configuração

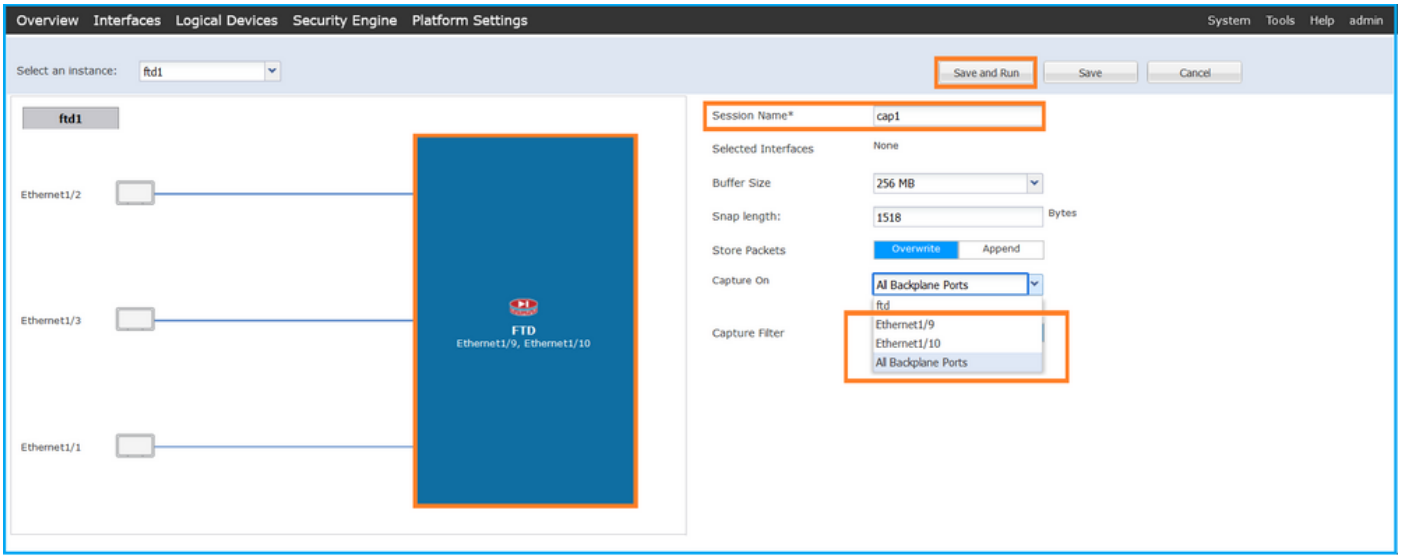
FCM

Siga estas etapas no FCM para configurar capturas de pacotes em interfaces de backplane:

1. Use **Tools > Packet Capture > Capture Session** para criar uma nova sessão de captura:



2. Para capturar pacotes em todas as interfaces de backplane, selecione o aplicativo e, em seguida, **All Backplane Ports** na lista suspensa **Capture On**. Como alternativa, escolha a interface específica do painel traseiro. Nesse caso, as interfaces de backplane Ethernet1/9 e Ethernet1/10 estão disponíveis. Forneça o **Nome da Sessão** e clique em **Salvar e Executar** para ativar a captura:



CLI FXOS

Siga estas etapas na CLI FXOS para configurar capturas de pacotes em interfaces de backplane:

1. Identificar o tipo de aplicativo e o identificador:

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

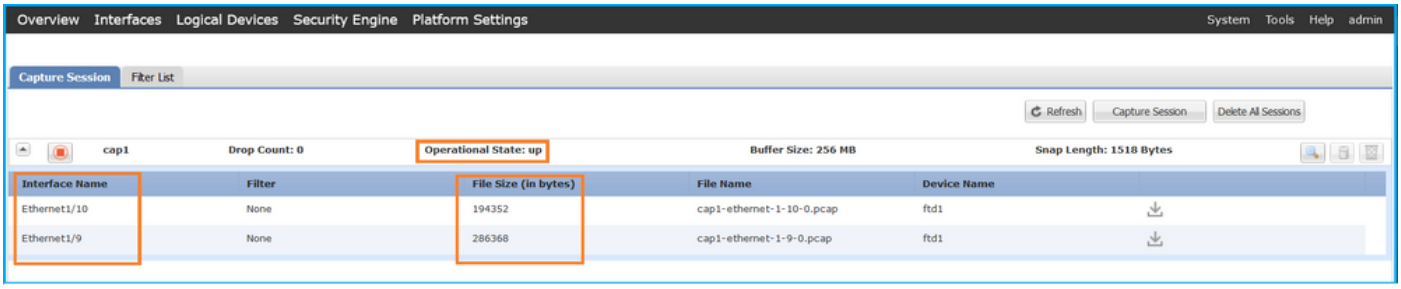
2. Criar uma sessão de captura:

```
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 #
```

Verificação

FCM

Verifique o **nome da interface**, certifique-se de que o **status operacional** esteja ativo e que o **tamanho do arquivo (em bytes)** aumente:



CLI FXOS

Verifique os detalhes da captura em **scope packet-capture**:

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

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

Coletar arquivos de captura

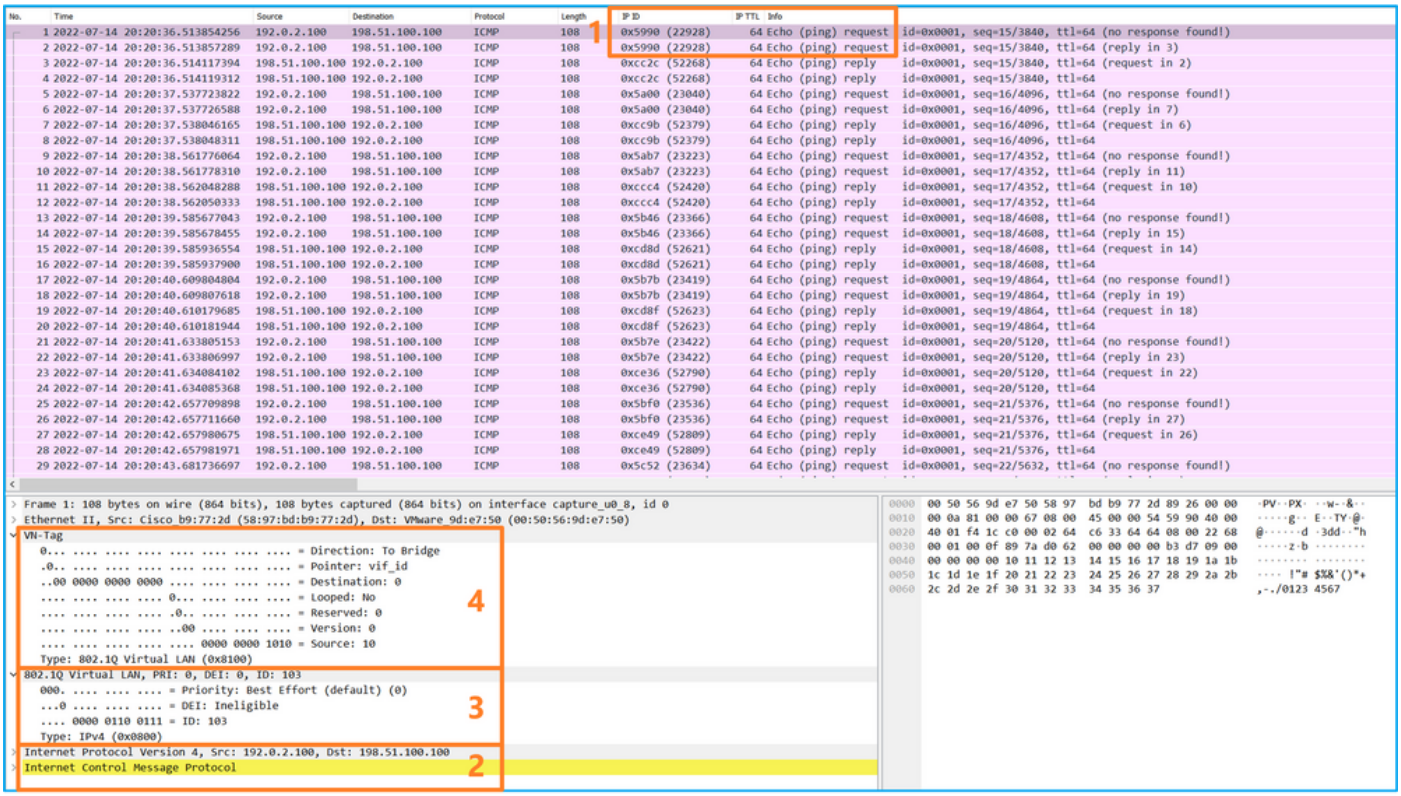
Siga as etapas na seção **Coletar arquivos de captura do switch interno Firepower 4100/9300**.

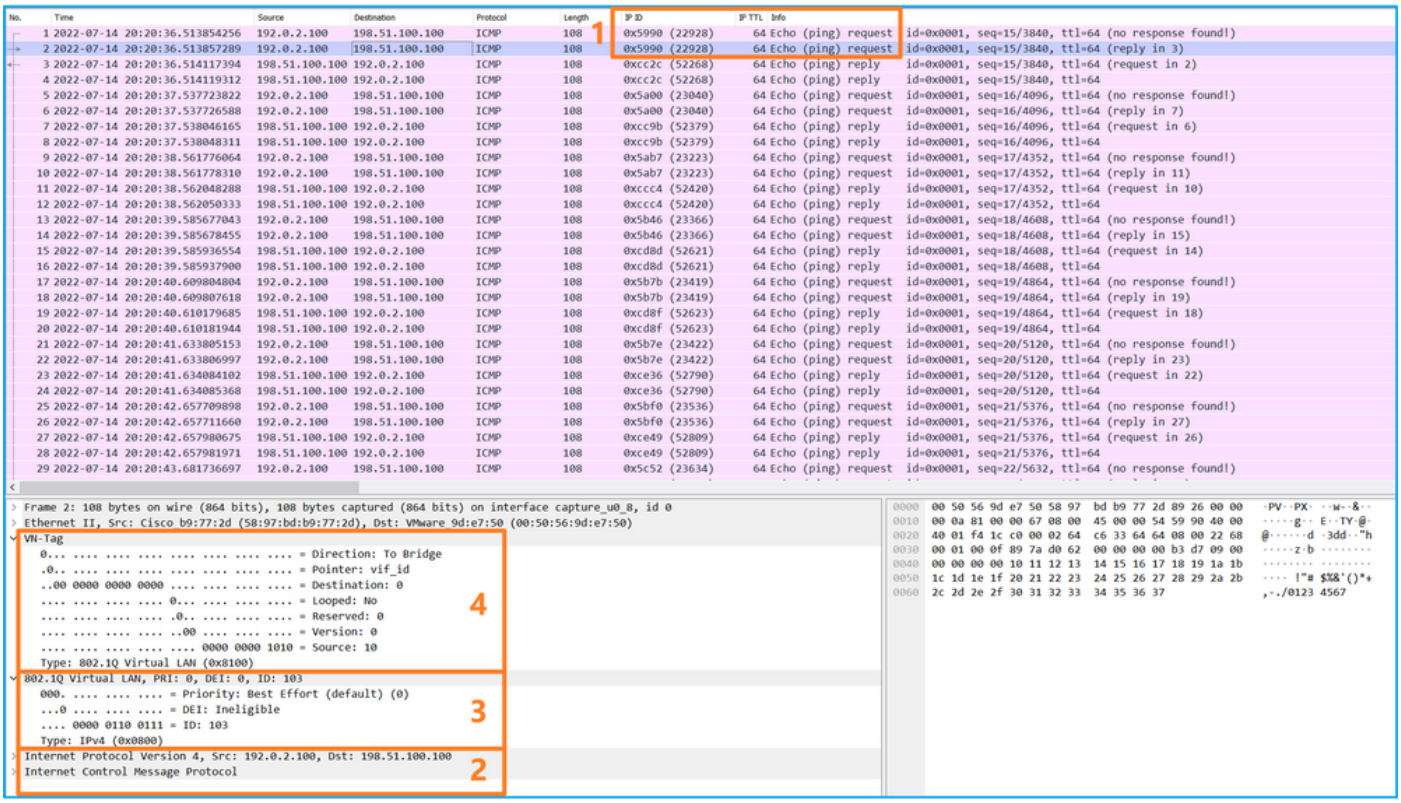
Capturar análise de arquivo

Use um aplicativo leitor de arquivo de captura de pacote para abrir os arquivos de captura. No caso de mais de uma interface de backplane, certifique-se de abrir todos os arquivos de captura para cada interface de backplane. Nesse caso, os pacotes são capturados na interface Ethernet1/9 do painel traseiro.

Selecione o primeiro e o segundo pacotes e verifique os pontos principais:

1. Cada pacote de solicitação de eco ICMP é capturado e mostrado duas vezes.
2. O cabeçalho do pacote original está sem a marca VLAN.
3. O switch interno insere a tag de VLAN de porta adicional **103** que identifica a interface de saída Ethernet1/3.
4. O switch interno insere uma marca VN adicional.

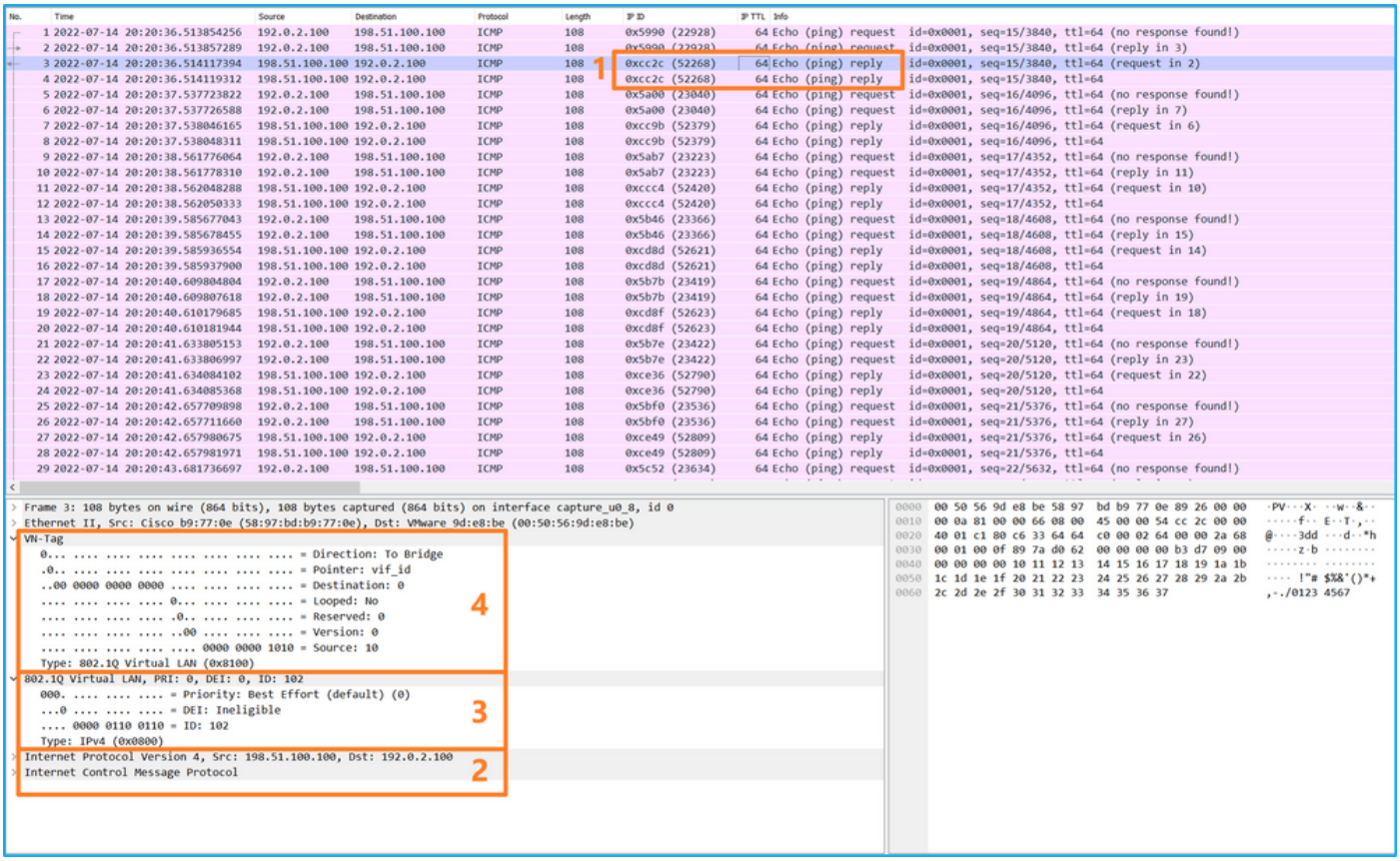




Selecione o terceiro e o quarto pacotes e verifique os pontos principais:

1. Cada resposta de eco ICMP é capturada e exibida duas vezes.

2. O cabeçalho do pacote original está sem a marca VLAN.
3. O switch interno insere a tag de VLAN de porta adicional **102** que identifica a interface de saída Ethernet1/2.
4. O switch interno insere uma marca VN adicional.



Explicação

Quando uma captura de pacote em uma interface de painel traseiro é configurada, o switch captura simultaneamente cada pacote duas vezes. Nesse caso, o switch interno recebe pacotes que já estão marcados pelo aplicativo no módulo de segurança com a marca da VLAN da porta e a marca da VLAN. A marca VLAN identifica a interface de saída que o chassi interno usa para encaminhar os pacotes à rede. A marca de VLAN 103 nos pacotes de solicitação de eco ICMP identifica Ethernet1/3 como a interface de saída, enquanto a marca de VLAN 102 nos pacotes de resposta de eco ICMP identifica Ethernet1/2 como a interface de saída. O switch interno remove a marca VN e a marca VLAN da interface interna antes que os pacotes sejam encaminhados à rede.

Esta tabela resume a tarefa:

Tarefa	Ponto de captura	VLAN de porta interna em pacotes capturados	Direção	Tráfego capturado
Configurar e verificar capturas de pacotes nas interfaces do painel traseiro	Interfaces de backplane	102 103	Somente entrada	Solicitações de eco ICMP do ho 192.0.2.100 para o host 198.51.100.100 Respostas de eco ICMP do hos 198.51.100.100 para o host 192.0.2.100

Capturas de pacotes nas portas do aplicativo e do aplicativo

As capturas de pacotes de porta de aplicativo ou de aplicativo são sempre configuradas nas interfaces do painel traseiro e, adicionalmente, nas interfaces frontais, se o usuário especificar a direção de captura do aplicativo.

Há principalmente 2 casos de uso:

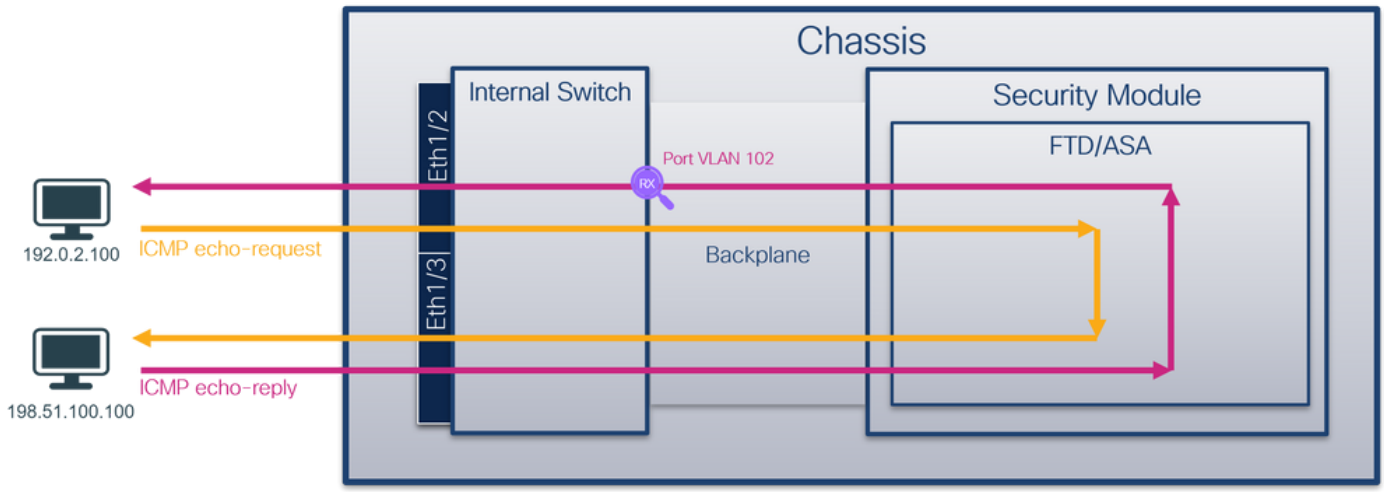
- Configurar capturas de pacotes nas interfaces do painel traseiro para pacotes que deixam uma interface frontal específica. Por exemplo, configure capturas de pacotes na interface Ethernet1/9 do painel traseiro para pacotes que deixam a interface Ethernet1/2.
- Configure capturas simultâneas de pacotes em uma interface frontal específica e nas interfaces de backplane. Por exemplo, configure capturas simultâneas de pacotes na interface Ethernet1/2 e na interface Ethernet1/9 do painel traseiro para pacotes que deixam a interface Ethernet1/2.

Esta seção abrange ambos os casos de uso.

Tarefa 1

Use o FCM e a CLI para configurar e verificar uma captura de pacote na interface do painel traseiro. Os pacotes para os quais a porta de aplicação Ethernet1/2 é identificada como interface de saída são capturados. Nesse caso, as respostas ICMP são capturadas.

Topologia, fluxo de pacotes e pontos de captura

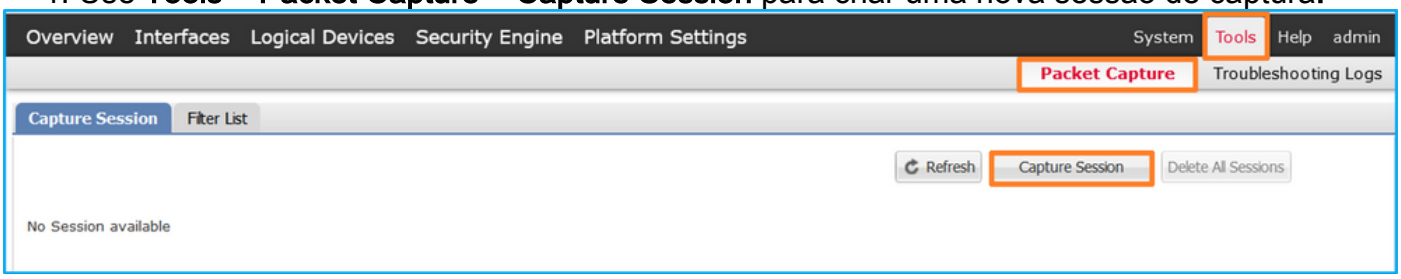


Configuração

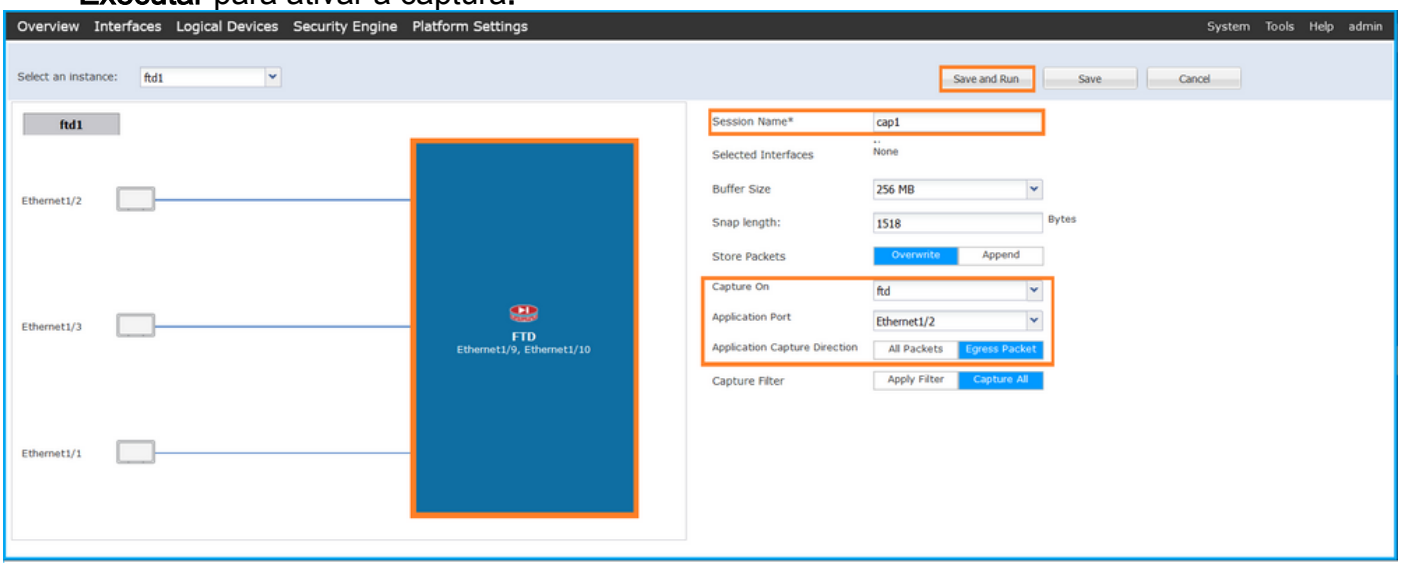
FCM

Siga estas etapas no FCM para configurar uma captura de pacote no aplicativo FTD e na porta Ethernet1/2 do aplicativo:

1. Use **Tools > Packet Capture > Capture Session** para criar uma nova sessão de captura:



2. Selecione o aplicativo **Ethernet1/2** na lista suspensa **Application Port** e selecione **Egress Packet** na **Application Capture Direction**. Forneça o **Nome da Sessão** e clique em **Salvar e Executar** para ativar a captura:



CLI FXOS

Siga estas etapas na CLI FXOS para configurar capturas de pacotes em interfaces de backplane:

1. Identificar o tipo de aplicativo e o identificador:

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

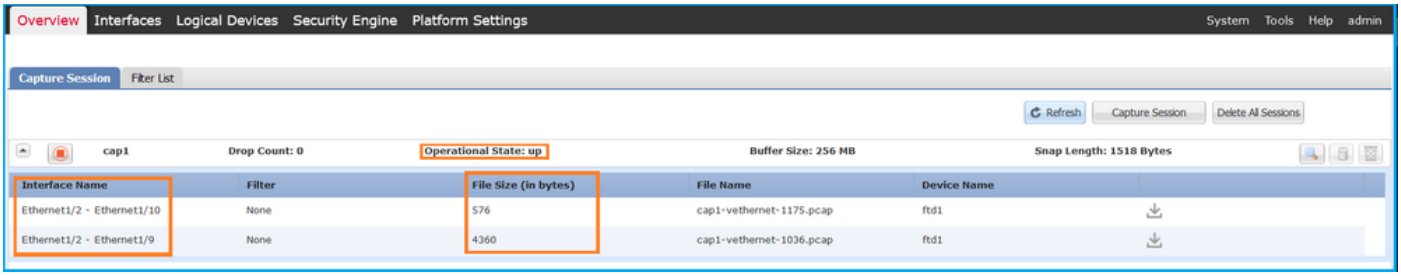
2. Criar uma sessão de captura:

```
firepower# scope packet-capture
firepower /packet-capture # create session cap1
firepower /packet-capture/session* # create app-port 1 112 Ethernet1/2 ftd
firepower /packet-capture/session/app-port* # set app-identifier ftd1
firepower /packet-capture/session/app-port* # set filter ""
firepower /packet-capture/session/app-port* # set subinterface 0
firepower /packet-capture/session/app-port* # up
firepower /packet-capture/session* # commit
firepower /packet-capture/session #
```

Verificação

FCM

Verifique o **nome da interface**, certifique-se de que o **status operacional** esteja ativo e que o **tamanho do arquivo (em bytes)** aumente:



CLI FXOS

Verifique os detalhes da captura em **scope packet-capture**:

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

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

Coletar arquivos de captura

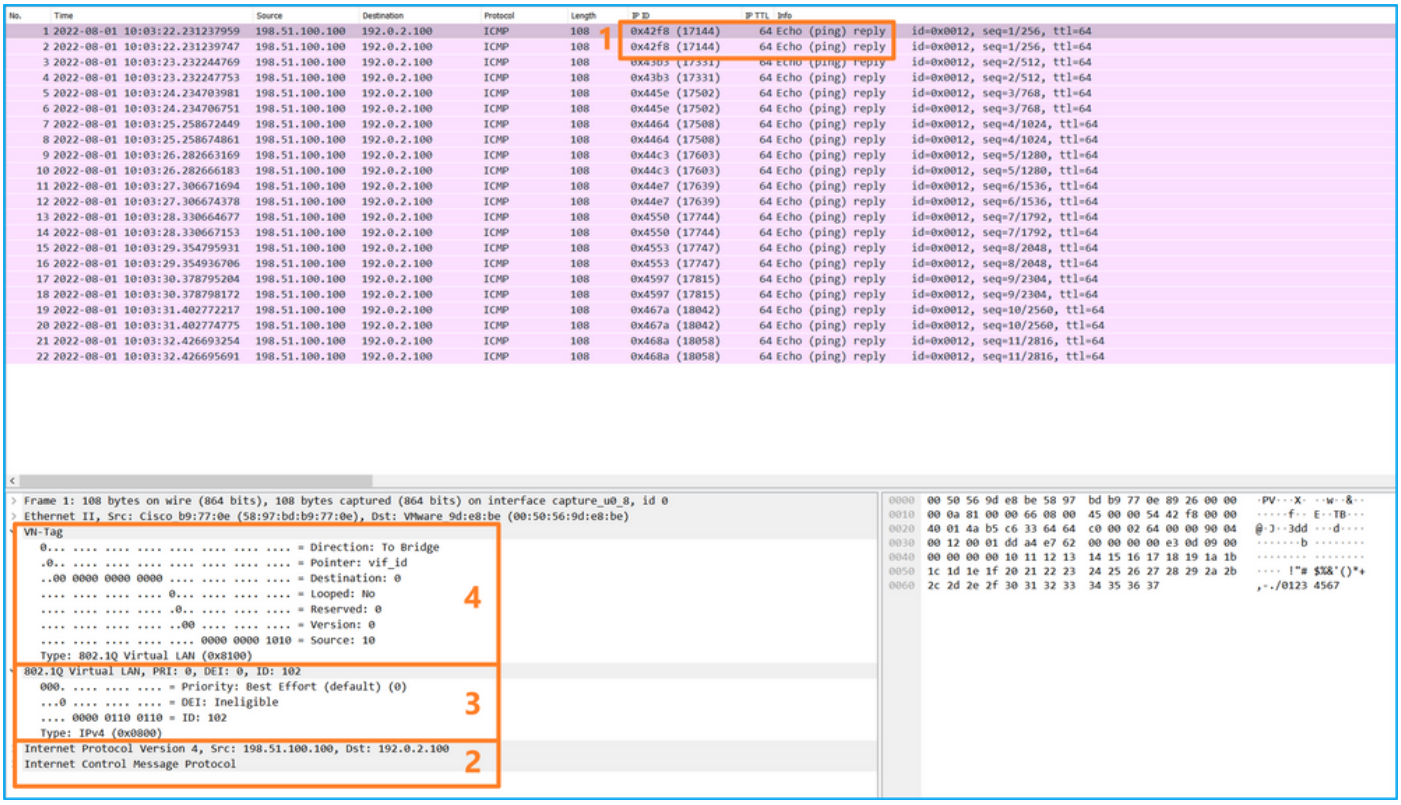
Siga as etapas na seção **Coletar arquivos de captura do switch interno Firepower 4100/9300**.

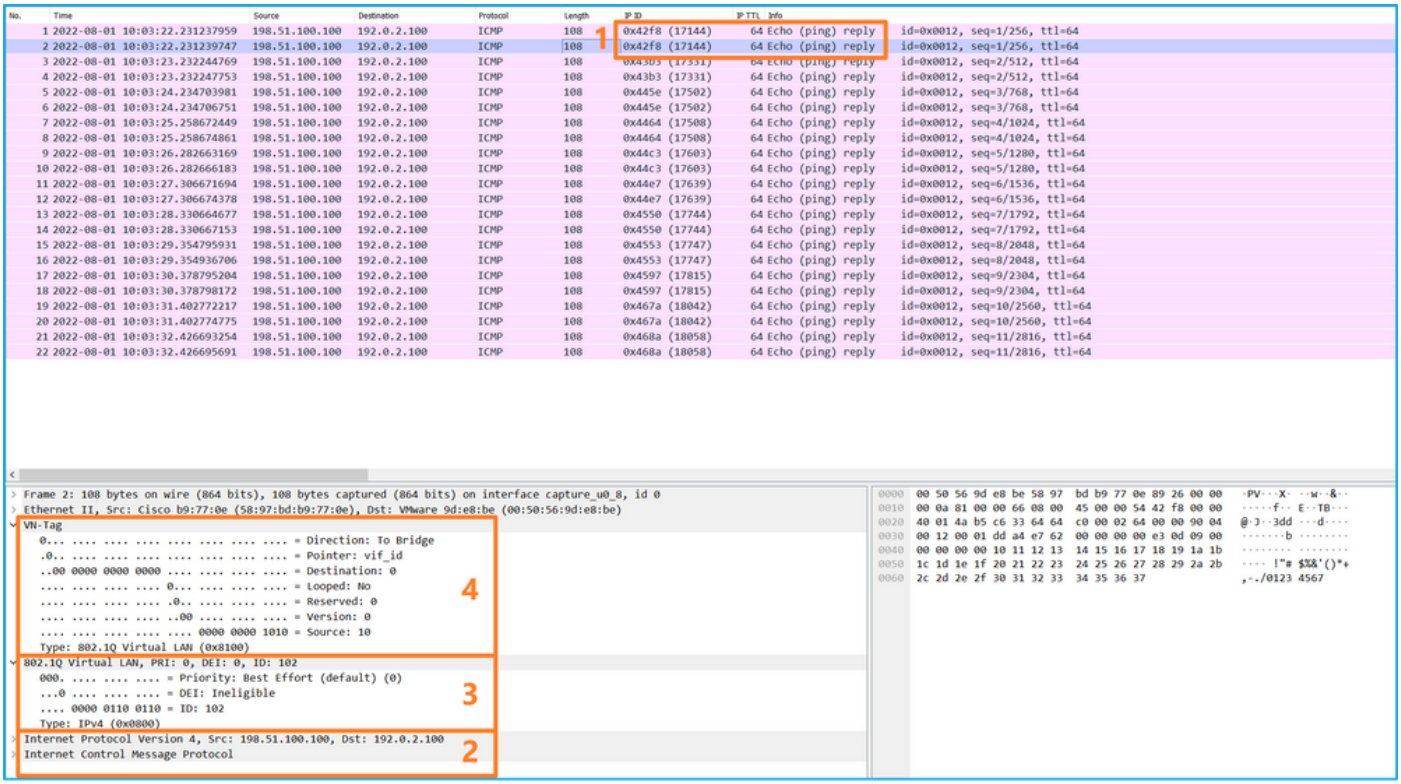
Capturar análise de arquivo

Use um aplicativo leitor de arquivo de captura de pacote para abrir os arquivos de captura. No caso de várias interfaces de backplane, certifique-se de abrir todos os arquivos de captura para cada interface de backplane. Nesse caso, os pacotes são capturados na interface Ethernet1/9 do painel traseiro.

Selecione o primeiro e o segundo pacotes e verifique os pontos principais:

1. Cada resposta de eco ICMP é capturada e exibida duas vezes.
2. O cabeçalho do pacote original está sem a marca VLAN.
3. O switch interno insere a tag de VLAN de porta adicional **102** que identifica a interface de saída Ethernet1/2.
4. O switch interno insere uma marca VN adicional.





Explicação

Nesse caso, a Ethernet1/2 com a porta VLAN tag 102 é a interface de saída para os pacotes de resposta de eco ICMP.

Quando a direção de captura do aplicativo é definida como **Saída** nas opções de captura, os pacotes com a tag de VLAN de porta 102 no cabeçalho Ethernet são capturados nas interfaces de backplane na direção de entrada.

Esta tabela resume a tarefa:

Tarefa	Ponto de captura	VLAN de porta interna em pacotes capturados	Direção	Tráfego capturado
Configurar e verificar capturas na porta Ethernet1/2 do aplicativo e do aplicativo	Interfaces de backplane	102	Somente entrada	Respostas de eco ICMP do ho 198.51.100.100 para o host 192.0.2.100

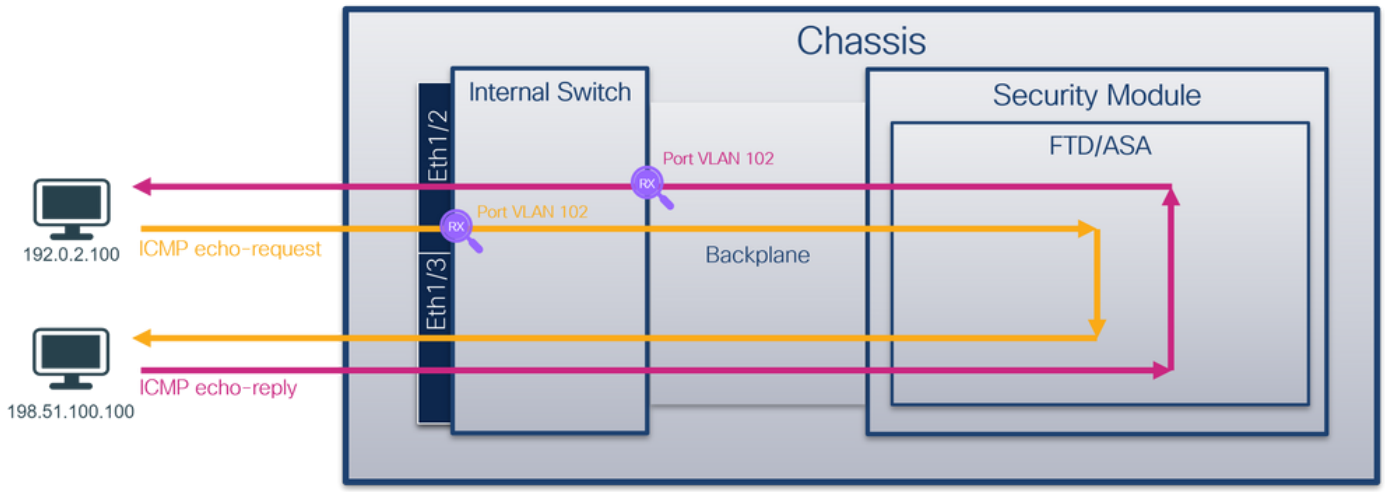
Tarefa 2

Use o FCM e a CLI para configurar e verificar uma captura de pacotes na interface do painel traseiro e na interface Ethernet1/2 da frente.

Capturas de pacotes simultâneas são configuradas em:

- Interface frontal - os pacotes com a porta VLAN 102 na interface Ethernet1/2 são capturados. Os pacotes capturados são solicitações de eco ICMP.
- Interfaces de backplane - pacotes para os quais a Ethernet1/2 é identificada como a interface de saída ou os pacotes com a porta VLAN 102 são capturados. Os pacotes capturados são respostas de eco ICMP.

Topologia, fluxo de pacotes e pontos de captura

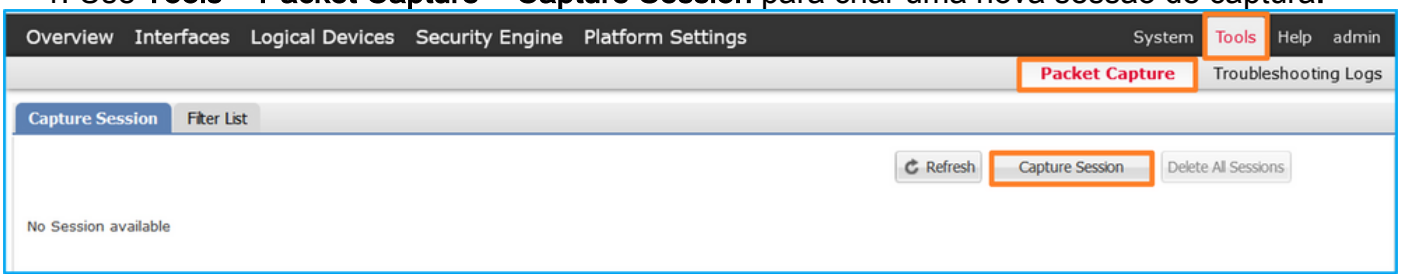


Configuração

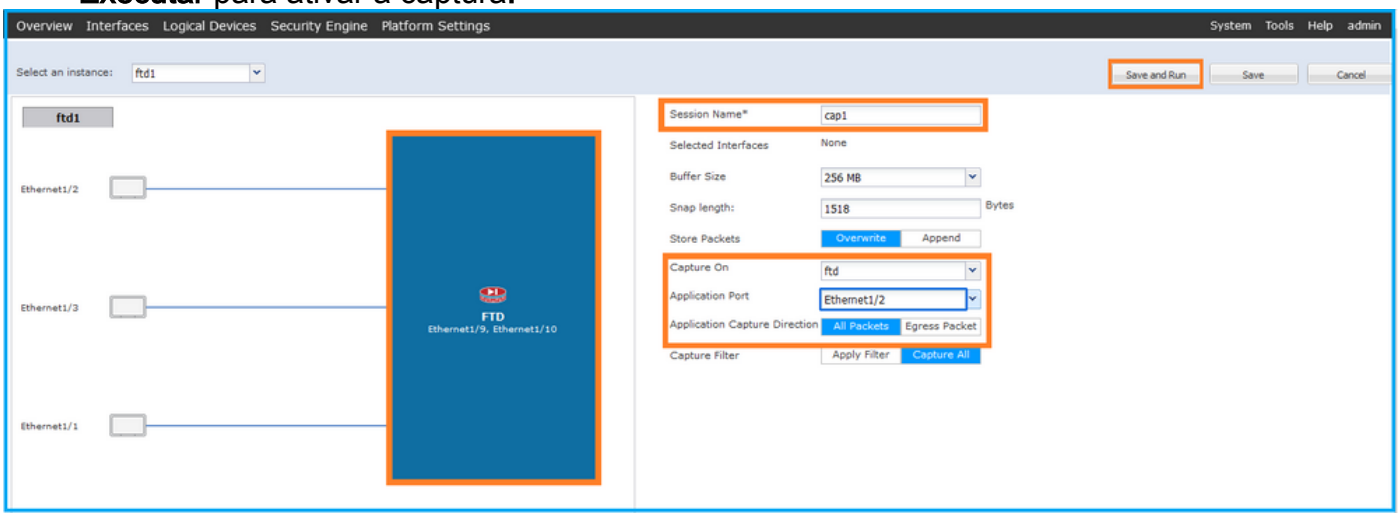
FCM

Siga estas etapas no FCM para configurar uma captura de pacote no aplicativo FTD e na porta Ethernet1/2 do aplicativo:

1. Use **Tools > Packet Capture > Capture Session** para criar uma nova sessão de captura:



2. Selecione o aplicativo FTD, **Ethernet1/2** na lista suspensa **Application Port** e selecione **All Packets** na **Application Capture Direction**. Forneça o **Nome da Sessão** e clique em **Salvar e Executar** para ativar a captura:



CLI FXOS

Siga estas etapas na CLI FXOS para configurar capturas de pacotes em interfaces de backplane:

1. Identificar o tipo de aplicativo e o identificador:

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

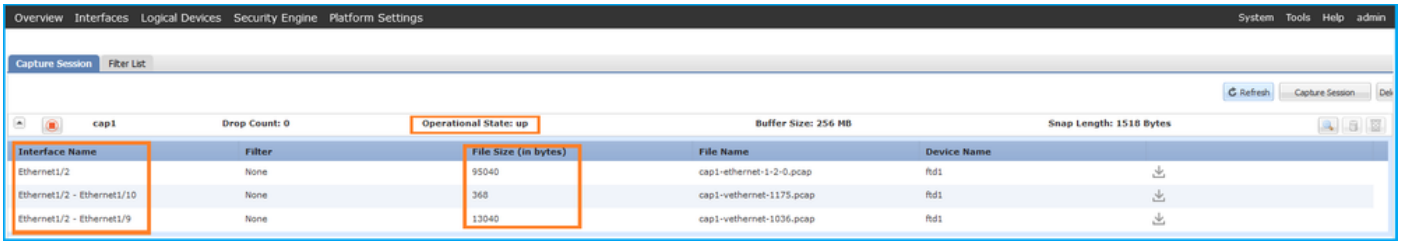
2. Criar uma sessão de captura:

```
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
```

Verificação

FCM

Verifique o **nome da interface**, certifique-se de que o **status operacional** esteja ativo e que o **tamanho do arquivo (em bytes)** aumente:



CLI FXOS

Verifique os detalhes da captura em **scope packet-capture**:

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

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

Coletar arquivos de captura

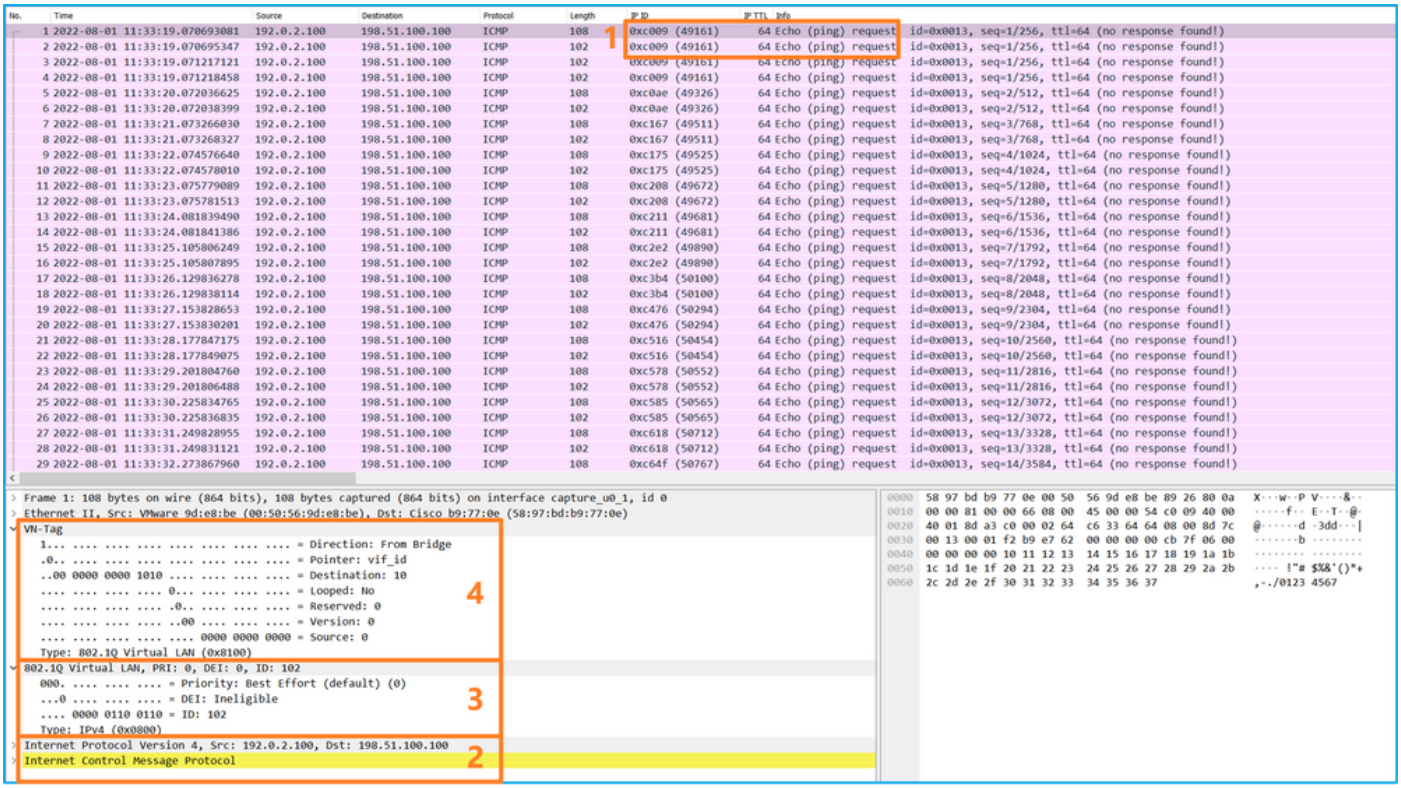
Siga as etapas na seção **Coletar arquivos de captura do switch interno Firepower 4100/9300**.

Capturar análise de arquivo

Use um aplicativo leitor de arquivo de captura de pacote para abrir os arquivos de captura. No caso de várias interfaces de backplane, certifique-se de abrir todos os arquivos de captura para cada interface de backplane. Nesse caso, os pacotes são capturados na interface Ethernet1/9 do painel traseiro.

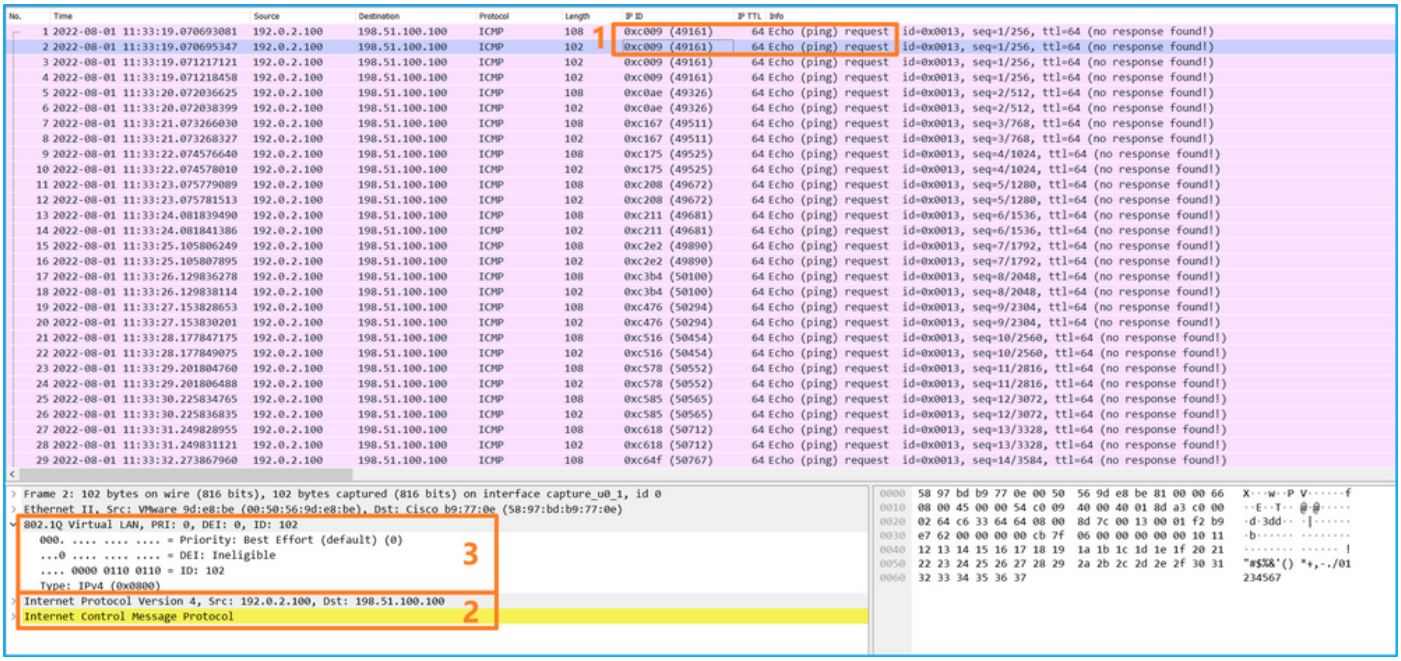
Abra o arquivo de captura para a interface Ethernet1/2, selecione o primeiro pacote e verifique os pontos principais:

1. Somente os pacotes ICMP de solicitação de eco são capturados. Cada pacote é capturado e mostrado 2 vezes.
2. O cabeçalho do pacote original está sem a marca VLAN.
3. O switch interno insere a tag de VLAN de porta adicional **102** que identifica a interface de entrada Ethernet1/2.
4. O switch interno insere uma marca VN adicional.



Selecione o segundo pacote e verifique os pontos principais:

1. Somente os pacotes ICMP de solicitação de eco são capturados. Cada pacote é capturado e mostrado 2 vezes.
2. O cabeçalho do pacote original está sem a marca VLAN.
3. O switch interno insere a tag de VLAN de porta adicional **102** que identifica a interface de entrada Ethernet1/2.

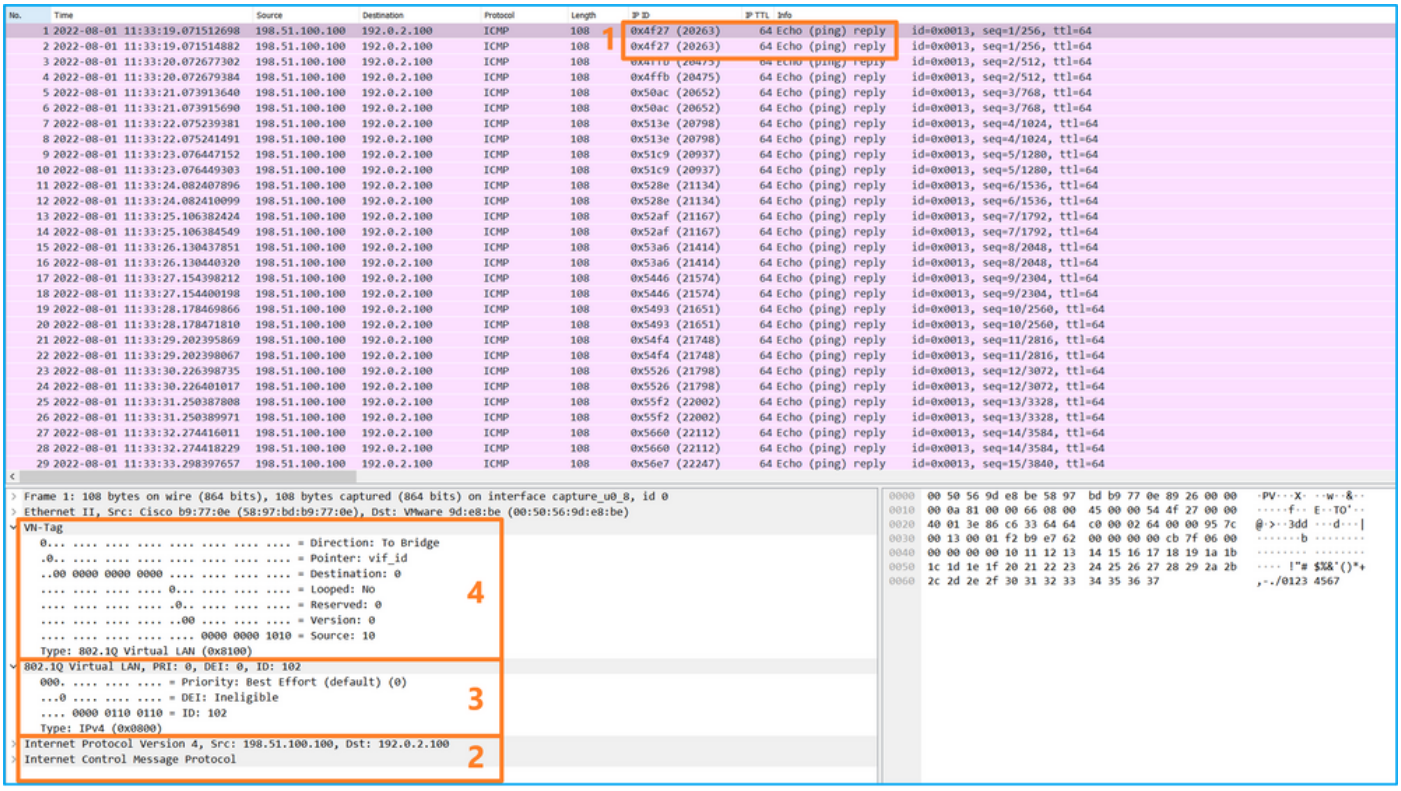


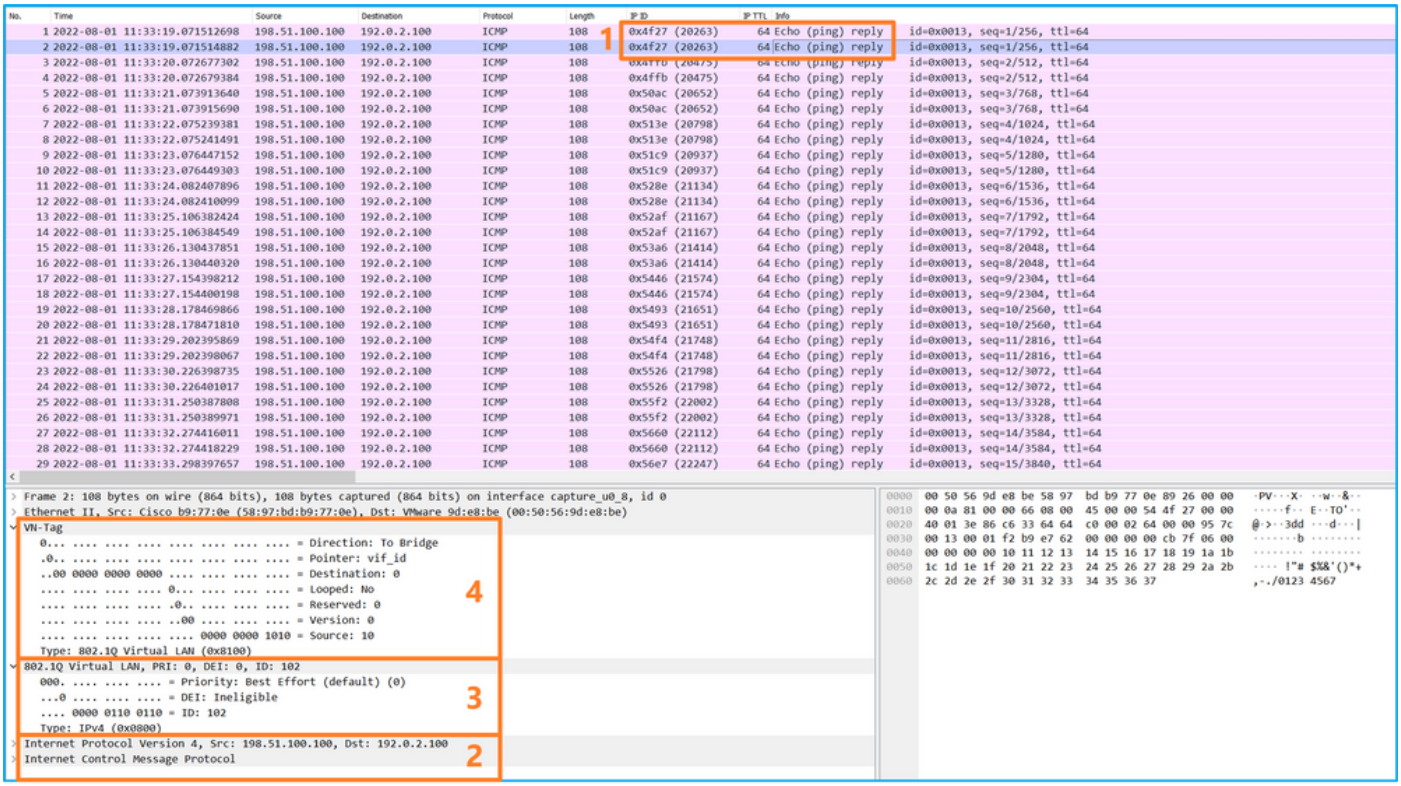
Abra o arquivo de captura para a interface Ethernet1/9, selecione o primeiro e o segundo pacotes e verifique os pontos principais:

1. Cada resposta de eco ICMP é capturada e exibida duas vezes.
2. O cabeçalho do pacote original está sem a marca VLAN.
3. O switch interno insere a tag de VLAN de porta adicional **102** que identifica a interface de

saída Ethernet1/2.

4. O switch interno insere uma marca VN adicional.





Explicação

Se a opção **All Packets** na **Application Capture Direction** estiver selecionada, 2 capturas simultâneas de pacotes relacionadas à porta de aplicativo Ethernet1/2 selecionada serão configuradas: uma captura na interface Ethernet1/2 frontal e uma captura em interfaces de painel traseiro selecionadas.

Quando uma captura de pacote em uma interface frontal é configurada, o switch captura simultaneamente cada pacote duas vezes:

- Após a inserção da marca da porta VLAN.
- Após a inserção da tag VN.

Na ordem de operações, a tag VN é inserida em um estágio posterior à inserção da tag VLAN da porta. Mas no arquivo de captura, o pacote com a marca VN é mostrado antes do pacote com a marca VLAN da porta. Neste exemplo, a marca de VLAN 102 nos pacotes de solicitação de eco ICMP identifica a Ethernet1/2 como a interface de entrada.

Quando uma captura de pacote em uma interface de painel traseiro é configurada, o switch captura simultaneamente cada pacote duas vezes. O switch interno recebe pacotes que já estão marcados pelo aplicativo no módulo de segurança com a marca da porta VLAN e a marca da VLAN. A tag de VLAN de porta identifica a interface de saída que o chassi interno usa para encaminhar os pacotes à rede. Neste exemplo, a marca de VLAN 102 nos pacotes de resposta de eco ICMP identifica a Ethernet1/2 como a interface de saída.

O switch interno remove a marca VN e a marca VLAN da interface interna antes que os pacotes sejam encaminhados à rede.

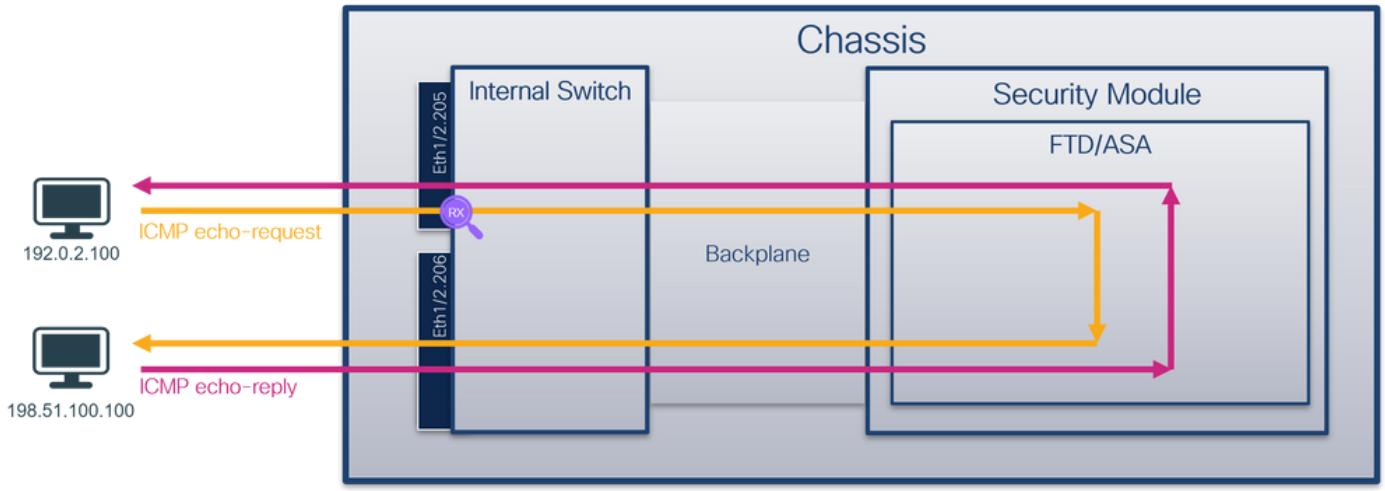
Esta tabela resume a tarefa:

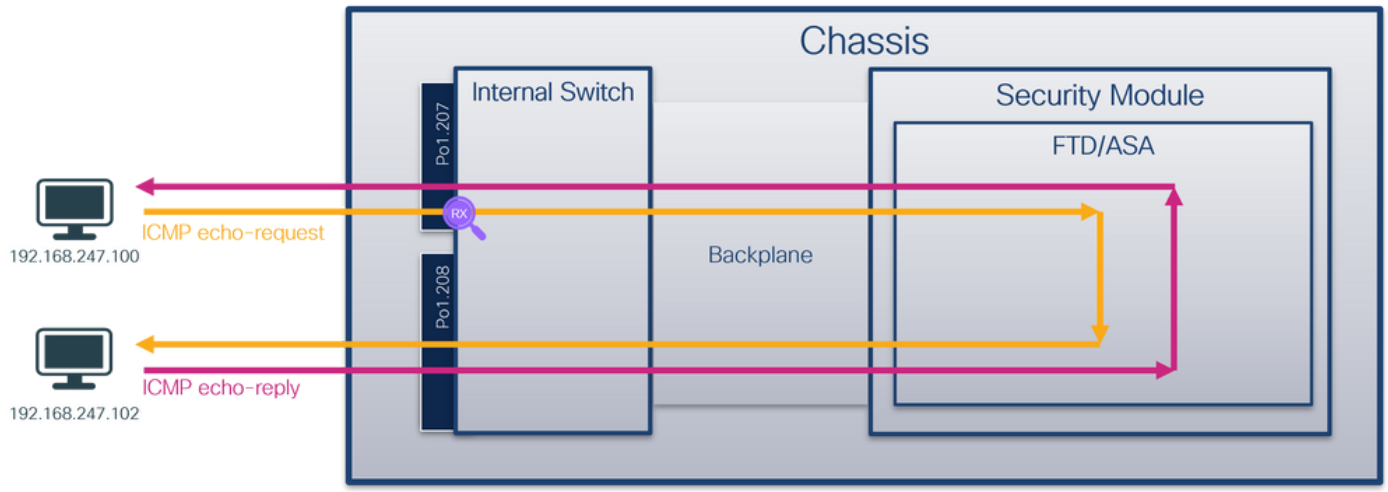
Tarefa	Ponto de captura	VLAN de porta interna em pacotes capturados	Direção	Tráfego capturado
Configurar e verificar capturas na porta Ethernet1/2 do aplicativo e do aplicativo	Interfaces de backplane	102	Somente entrada	Respostas de eco ICMP do h 198.51.100.100 para o host 192.0.2.100
	Interface Ethernet1/2	102	Somente entrada	Solicitações de eco ICMP do 192.0.2.100 para o host 198.51.100.100

Captura de pacotes em uma subinterface de uma interface física ou de canal de porta

Use o FCM e a CLI para configurar e verificar uma captura de pacote na subinterface Ethernet1/2.205 ou na subinterface de canal de porta Portchannel1.207. Subinterfaces e capturas em subinterfaces são suportadas somente para a aplicação FTD no modo de contêiner. Nesse caso, uma captura de pacote em Ethernet1/2.205 e Portchannel1.207 está configurada.

Topologia, fluxo de pacotes e pontos de captura



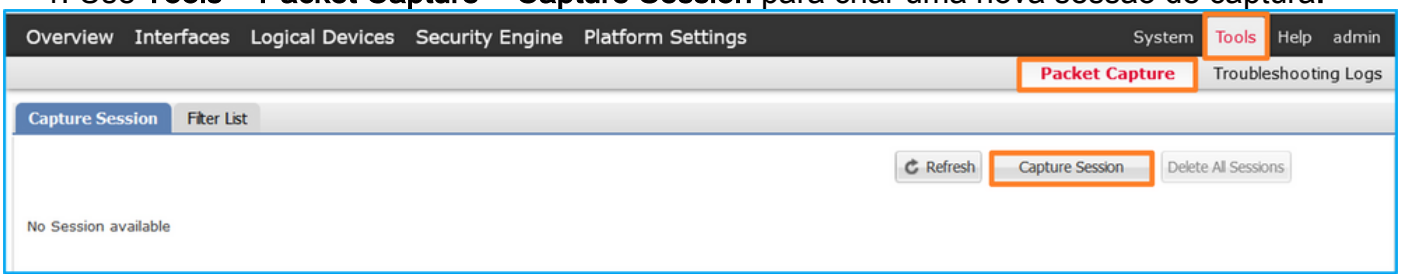


Configuração

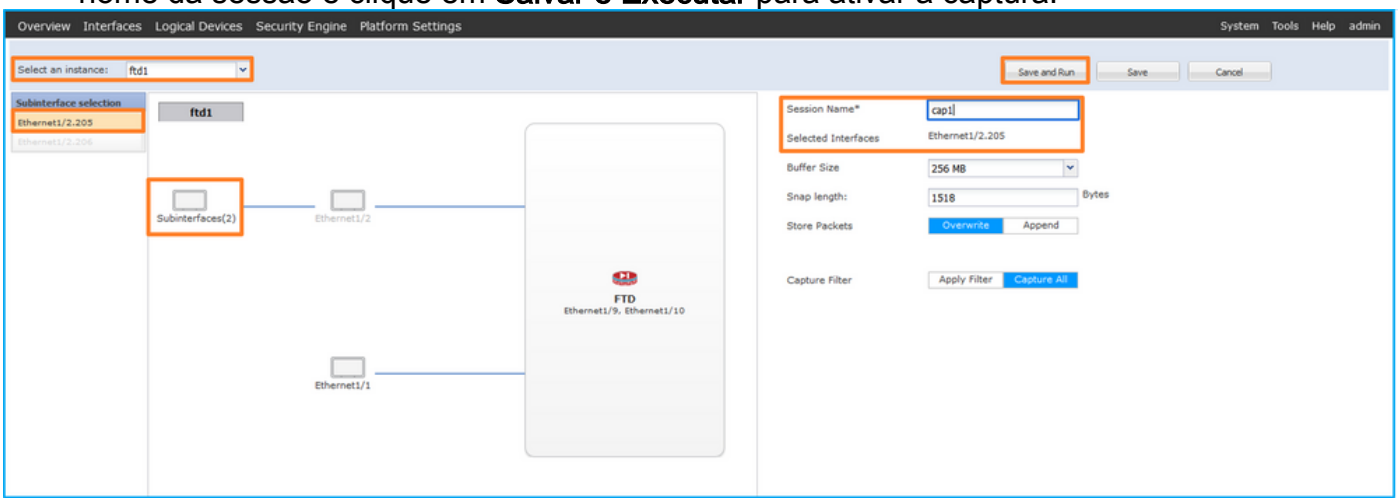
FCM

Siga estas etapas no FCM para configurar uma captura de pacote no aplicativo FTD e na porta Ethernet1/2 do aplicativo:

1. Use **Tools > Packet Capture > Capture Session** para criar uma nova sessão de captura:



2. Selecione a instância de aplicativo específica ftd1, a subinterface Ethernet1/2.205, forneça o nome da sessão e clique em **Salvar e Executar** para ativar a captura:



3. No caso de uma subinterface port-channel, devido ao bug da Cisco ID CSCvq3119, as subinterfaces não são visíveis no FCM. Use a CLI FXOS para configurar capturas em subinterfaces de canal de porta.

CLI FXOS

Siga estas etapas na CLI FXOS para configurar uma captura de pacote nas subinterfaces

Ethernet1/2.205 e Portchannel1.207:

1. Identificar o tipo de aplicativo e o identificador:

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

2. No caso de uma interface port-channel, identifique suas interfaces membro:

```
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. Criar uma sessão de captura:

```
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 #
```

Para subinterfaces port-channel, crie uma captura de pacote para cada interface membro port-channel:

```
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
```

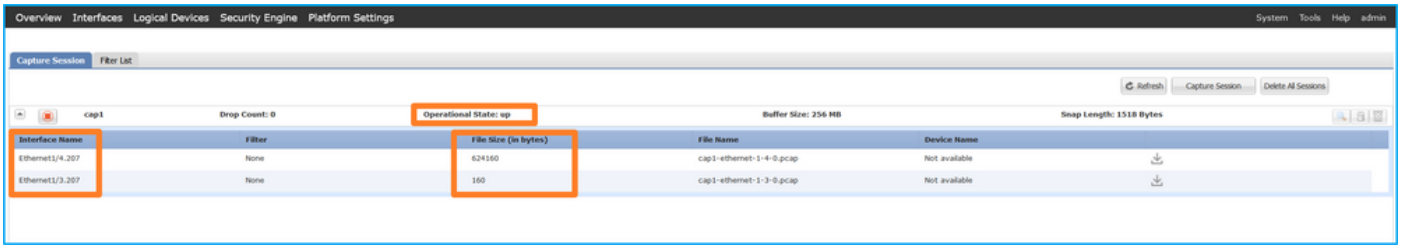
```
firepower /packet-capture/session/phy-port* # set app-identifier ftd1
firepower /packet-capture/session/phy-port* # set subinterface 207
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # enable
firepower /packet-capture/session* # commit
firepower /packet-capture/session #
```

Verificação

FCM

Verifique o **nome da interface**, certifique-se de que o **status operacional** esteja ativo e que o **tamanho do arquivo (em bytes)** aumente:

As capturas de subinterface de canal de porta configuradas no FXOS CLI também são visíveis no FCM; no entanto, eles não podem ser editados:



CLI FXOS

Verifique os detalhes da captura em **scope packet-capture**:

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

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

Canal de porta 1 com interfaces membro Ethernet1/3 e Ethernet1/4:

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

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

Physical ports involved in Packet Capture:
    Slot Id: 1
    Port Id: 3
    Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-3-0.pcap
    Pcapsize: 160  bytes
   Filter:
    Sub Interface: 207
   Application Instance Identifier: ftd1
    Application Name: ftd
   Slot Id: 1
    Port Id: 4
    Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-4-0.pcap
    Pcapsize: 624160  bytes
   Filter:
   Sub Interface: 207
    Application Instance Identifier: ftd1
    Application Name: ftd
```

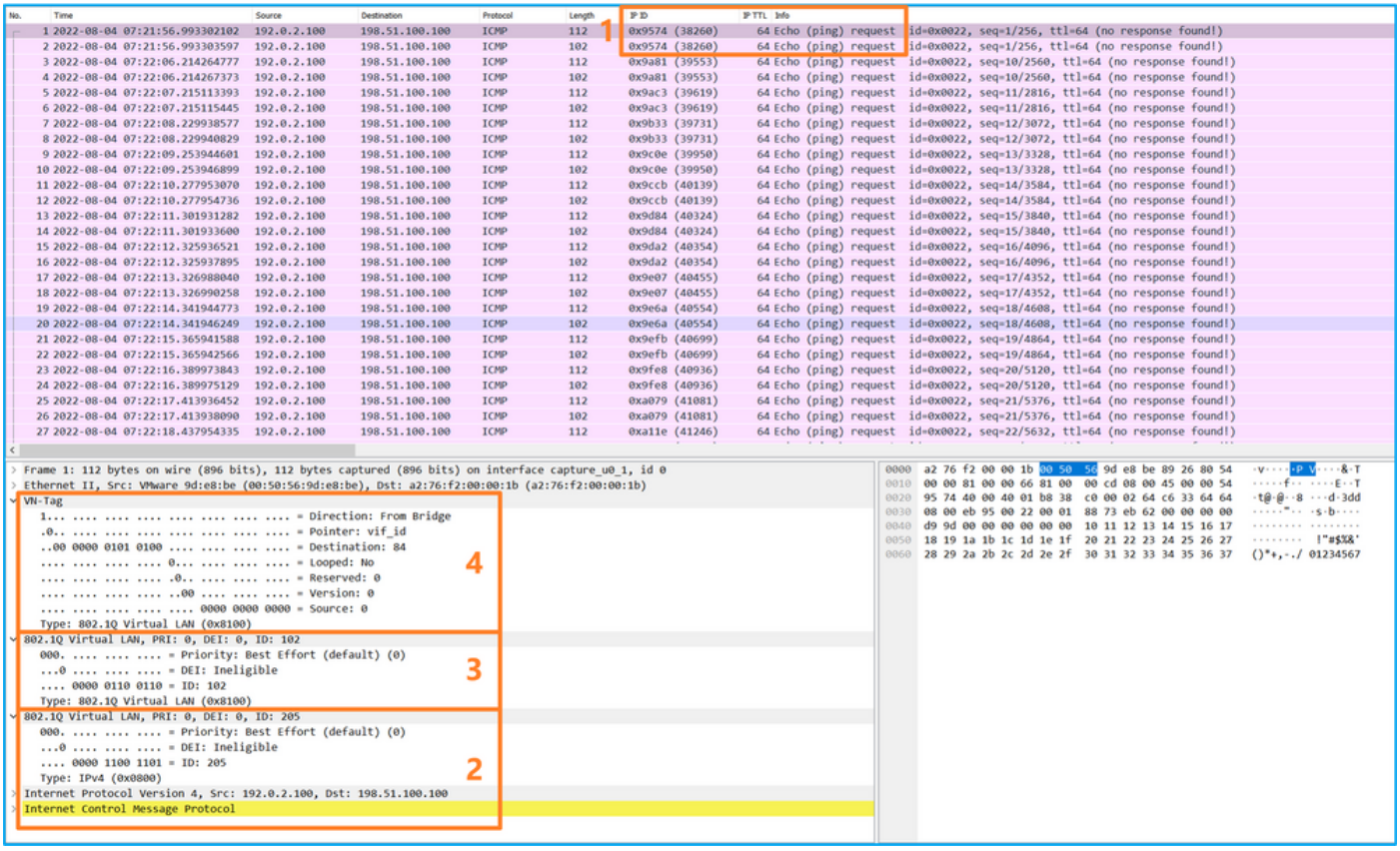
Coletar arquivos de captura

Siga as etapas na seção **Coletar arquivos de captura do switch interno Firepower 4100/9300**.

Capturar análise de arquivo

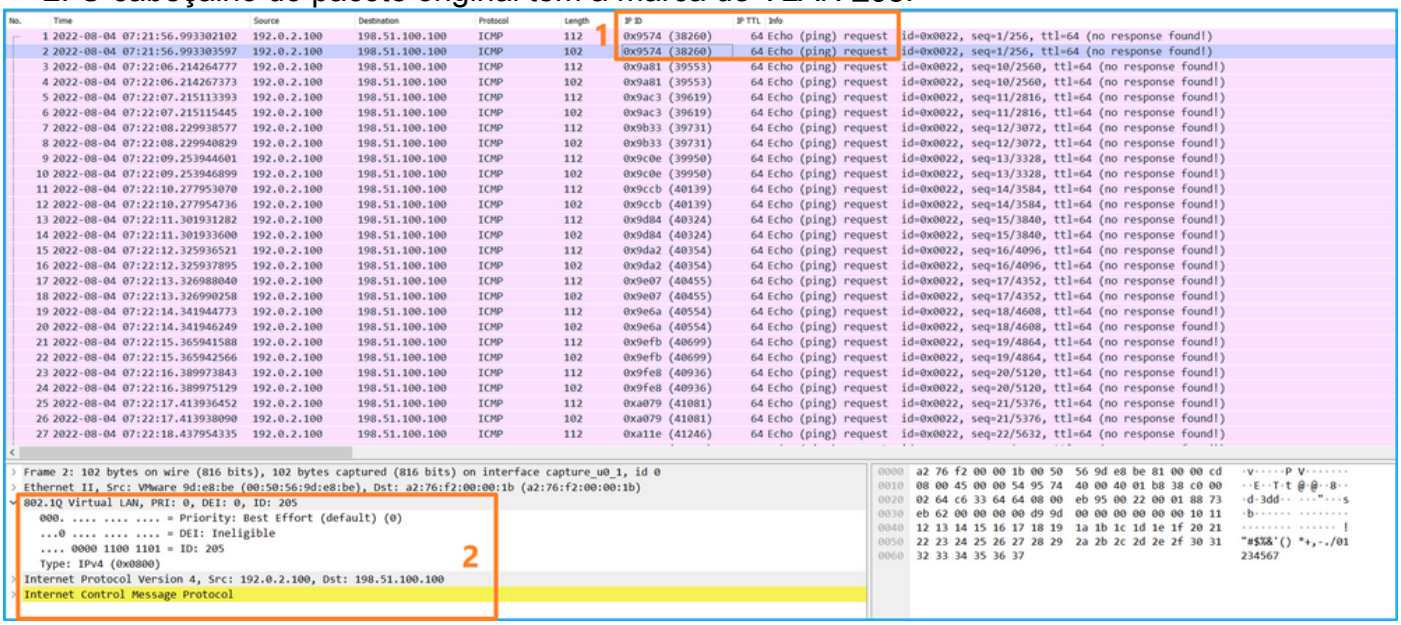
Use um aplicativo leitor de arquivo de captura de pacote para abrir o arquivo de captura. Selecione o primeiro pacote e verifique os pontos principais:

1. Somente os pacotes ICMP de solicitação de eco são capturados. Cada pacote é capturado e mostrado 2 vezes.
2. O cabeçalho do pacote original tem a marca de VLAN **205**.
3. O switch interno insere a tag de VLAN de porta adicional **102** que identifica a interface de entrada Ethernet1/2.
4. O switch interno insere uma marca VN adicional.



Selecione o segundo pacote e verifique os pontos principais:

1. Somente os pacotes ICMP de solicitação de eco são capturados. Cada pacote é capturado e mostrado 2 vezes.
2. O cabeçalho do pacote original tem a marca de VLAN **205**.

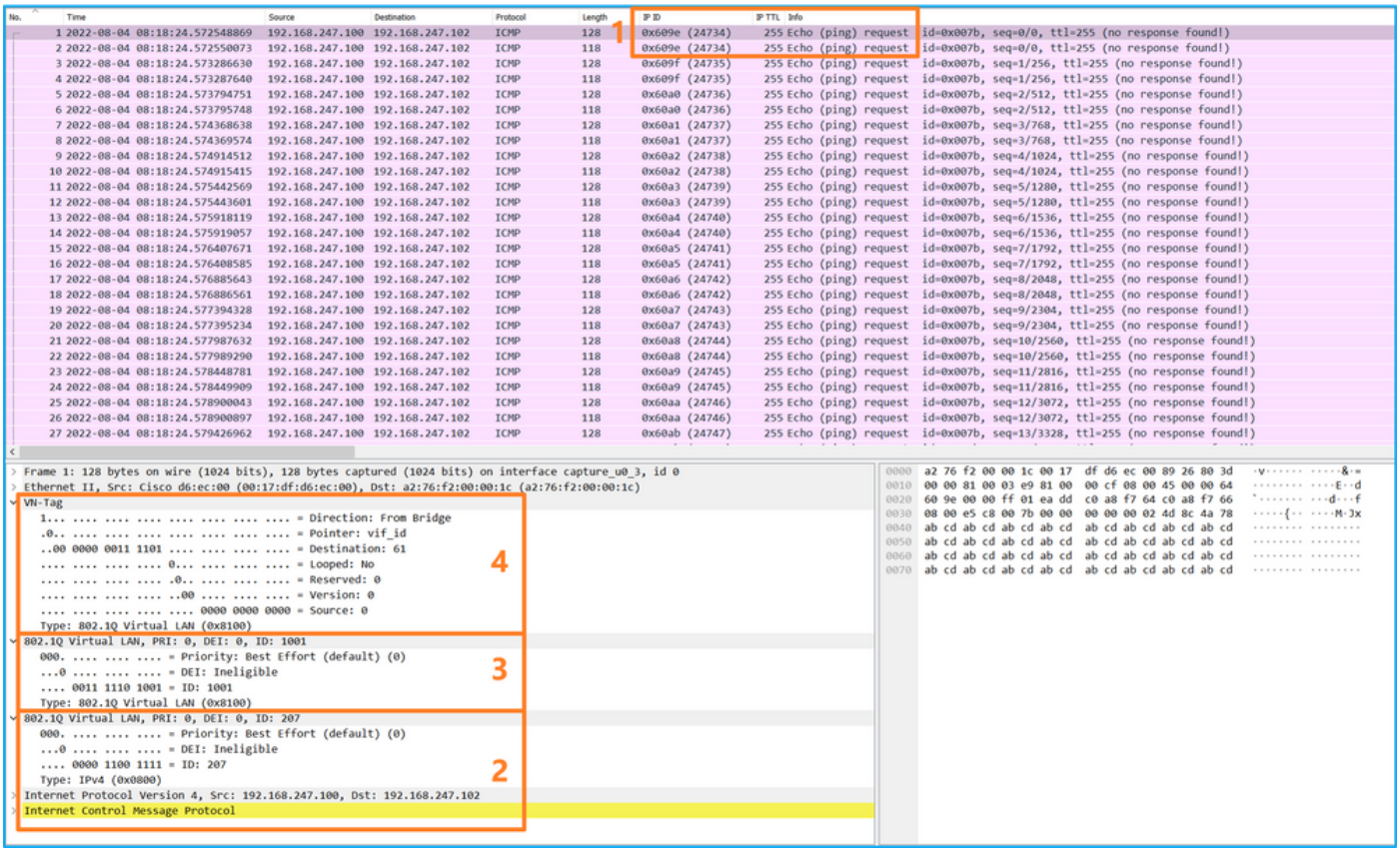


Agora abra os arquivos de captura para Portchannel1.207. Selecione o primeiro pacote e verifique os pontos principais

1. Somente os pacotes ICMP de solicitação de eco são capturados. Cada pacote é capturado e mostrado 2 vezes.
2. O cabeçalho do pacote original tem a marca de VLAN **207**.
3. O switch interno insere uma tag de VLAN de porta adicional **1001** que identifica a interface

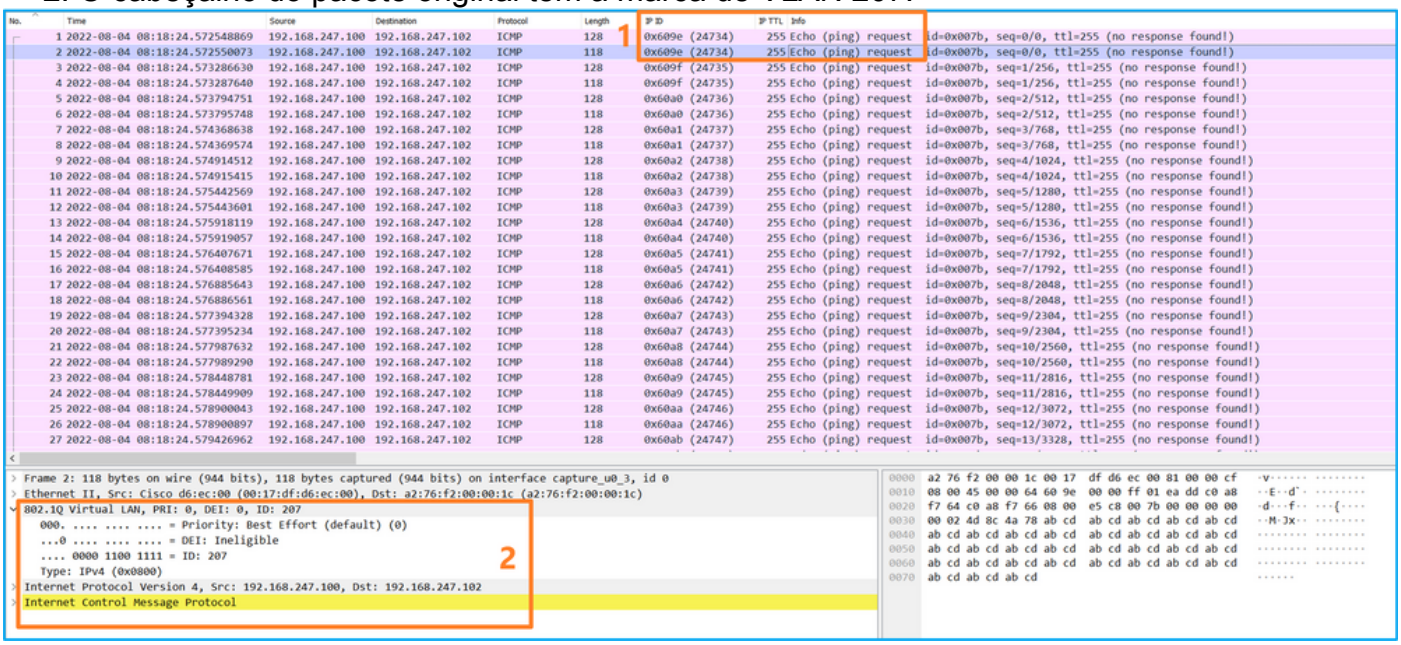
de entrada Portchannel1.

4. O switch interno insere uma marca VN adicional.



Selecione o segundo pacote e verifique os pontos principais:

1. Somente os pacotes ICMP de solicitação de eco são capturados. Cada pacote é capturado e mostrado 2 vezes.
2. O cabeçalho do pacote original tem a marca de VLAN 207.



Explicação

Quando uma captura de pacote em uma interface frontal é configurada, o switch captura simultaneamente cada pacote duas vezes:

- Após a inserção da marca da porta VLAN.
- Após a inserção da tag VN.

Na ordem de operações, a tag VN é inserida em um estágio posterior à inserção da tag VLAN da porta. Mas no arquivo de captura, o pacote com a marca VN é mostrado antes do pacote com a marca VLAN da porta. Além disso, no caso de subinterfaces, nos arquivos de captura, cada segundo pacote não contém a marca da porta VLAN.

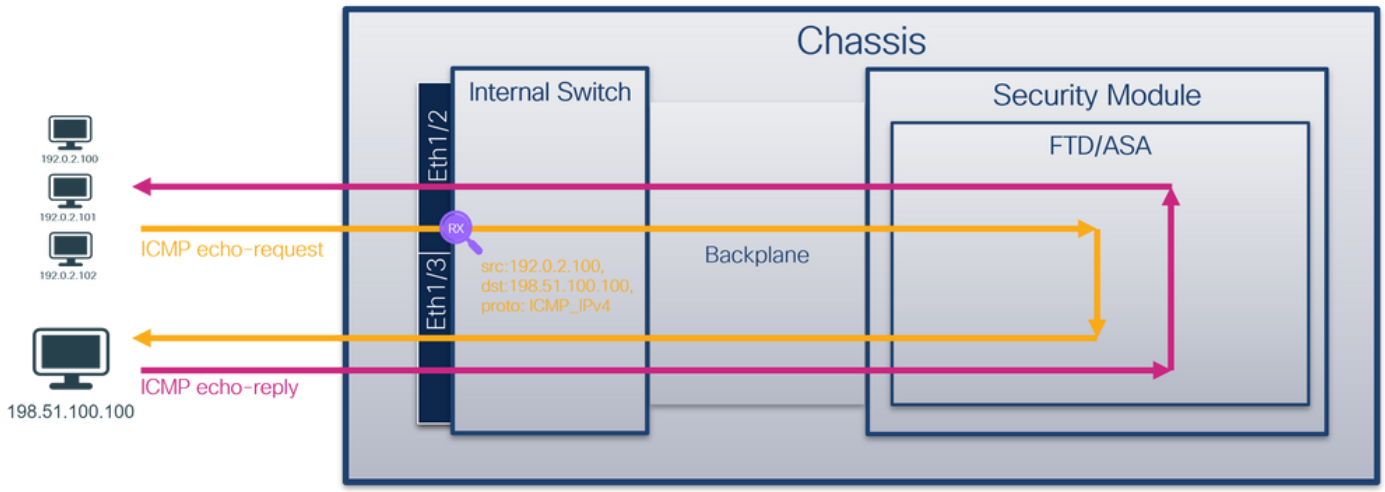
Esta tabela resume a tarefa:

Tarefa	Ponto de captura	VLAN de porta interna em pacotes capturados	Direção	Tráfego capturado
Configurar e verificar uma captura de pacote na subinterface Ethernet1/2.205	Ethernet1/2.205	102	Somente entrada	Solicitações de eco ICMP do hos 192.0.2.100 para o host 198.51.100.100
Configurar e verificar uma captura de pacote na subinterface Portchannel1 com as interfaces membro Ethernet1/3 e Ethernet1/4	Ethernet1/3 Ethernet1/4	1001	Somente entrada	Solicitações de eco ICMP de 192.168.207.100 para o host 192.168.207.102

Filtros de captura de pacotes

Use o FCM e a CLI para configurar e verificar uma captura de pacote na interface Ethernet1/2 com um filtro.

Topologia, fluxo de pacotes e pontos de captura

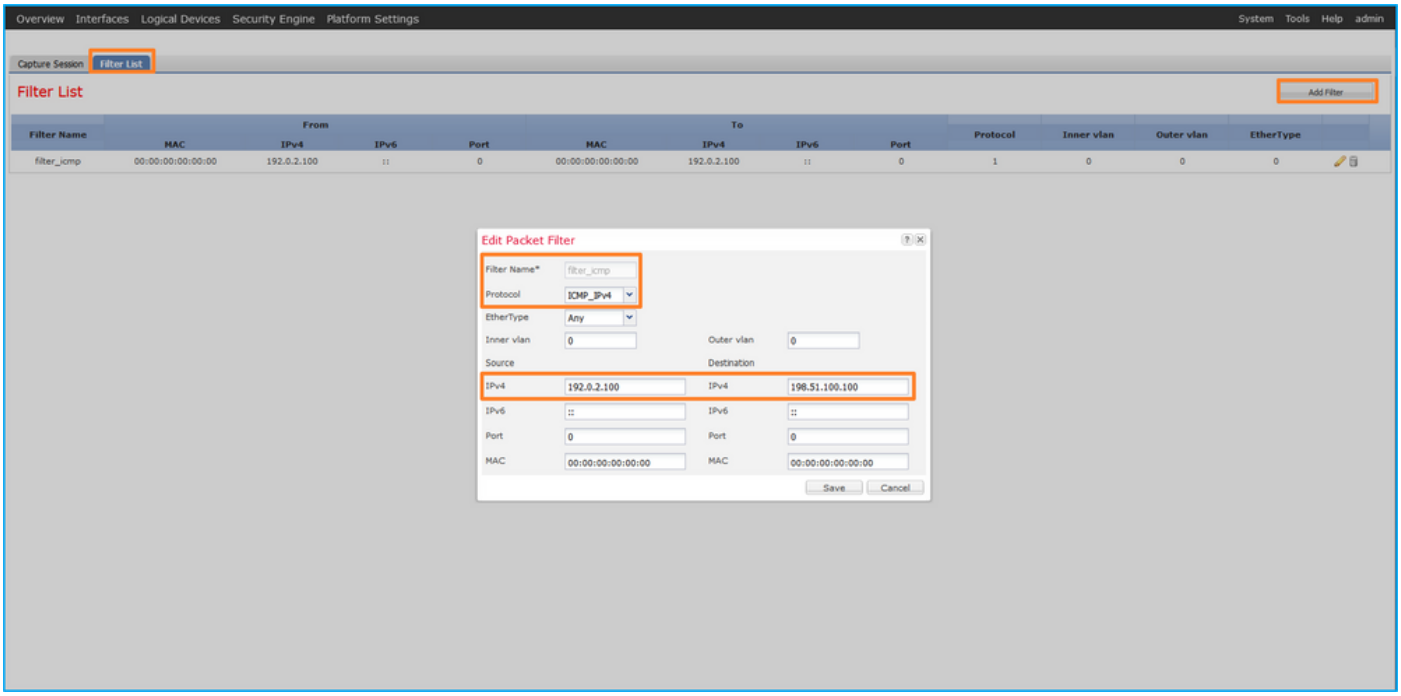


Configuração

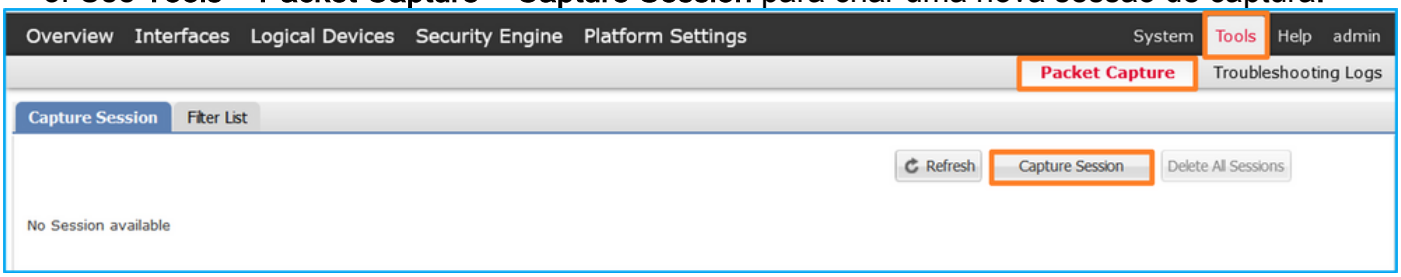
FCM

Siga estas etapas no FCM para configurar um filtro de captura para pacotes de solicitação de eco ICMP do host 192.0.2.100 para o host 198.51.100.100 e aplicá-lo à captura de pacotes na interface Ethernet1/2:

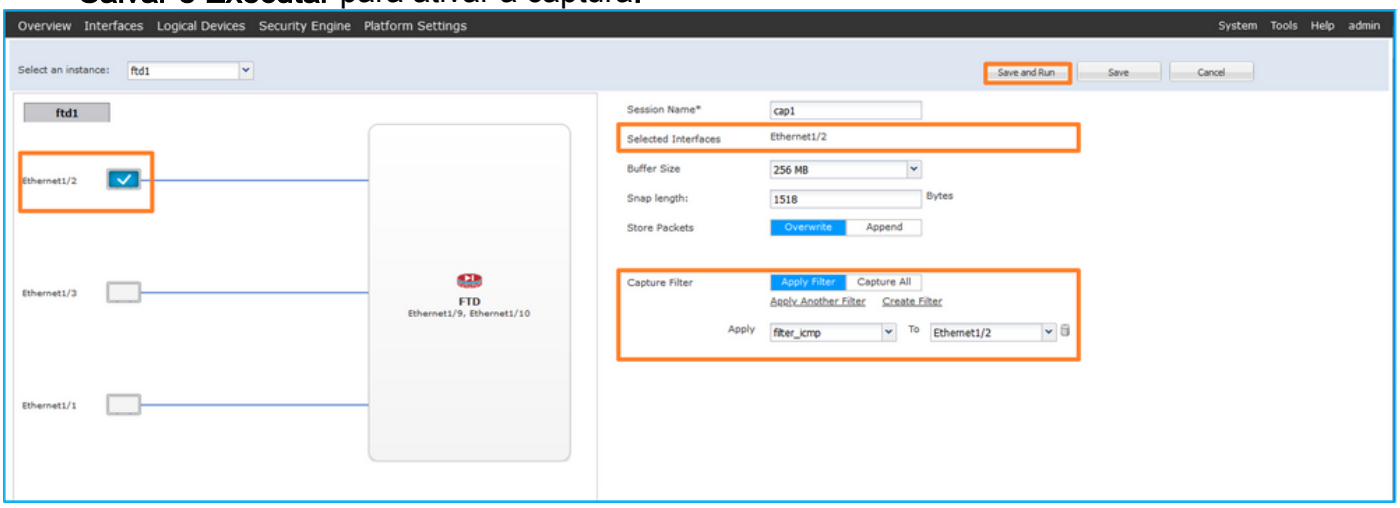
1. Use **Tools > Packet Capture > Filter List > Add Filter** para criar um filtro de captura.
2. Especifique o **Nome do filtro, Protocolo, IPv4 origem, IPv4 destino** e clique em **Salvar:**



3. Use **Tools > Packet Capture > Capture Session** para criar uma nova sessão de captura:



4. Selecione Ethernet1/2, forneça o **Nome da Sessão,** aplique o filtro de captura e clique em **Salvar e Executar** para ativar a captura:



CLI FXOS

Siga estas etapas na CLI FXOS para configurar capturas de pacotes em interfaces de backplane:

1. Identificar o tipo de aplicativo e o identificador:

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

```
Deploy Type Turbo Mode Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ---------- ---------------- --------------- --------------- --
--------- ---------- ------------ --------------- ------------
ftd        ftd1       1          Enabled     Online           7.2.0.82        7.2.0.82
Native      No                      Not Applicable  None
```

2. Identifique o número do protocolo IP em https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml. Nesse caso, o número do protocolo ICMP é 1.

3. Criar uma sessão de captura:

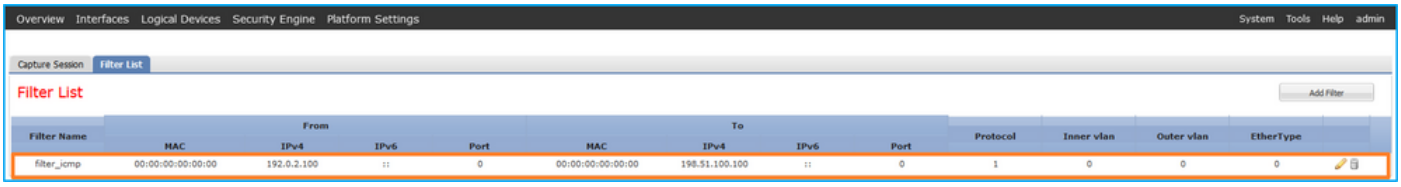
2.

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

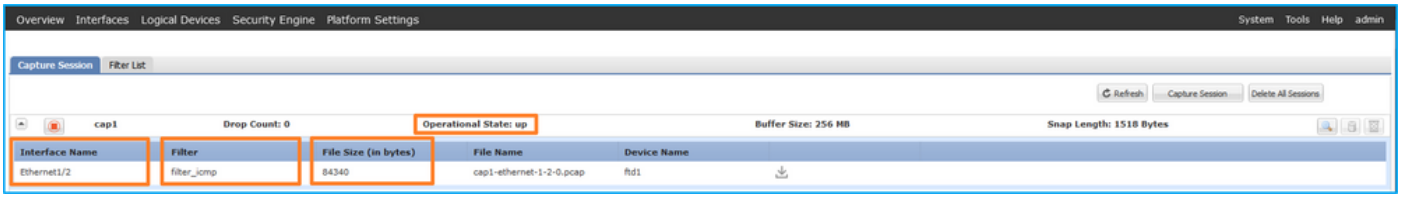
Verificação

FCM

Verifique o **nome da interface**, certifique-se de que o **status operacional** esteja ativo e que o **tamanho do arquivo (em bytes)** aumente:



Verifique o Nome da interface, o **Filtro**, certifique-se de que o **Status operacional** esteja ativo e o Tamanho do arquivo (em bytes) aumente em Ferramentas > Captura de pacote > Capturar sessão:



CLI FXOS

Verifique os detalhes da captura em **scope packet-capture**:

```
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
```

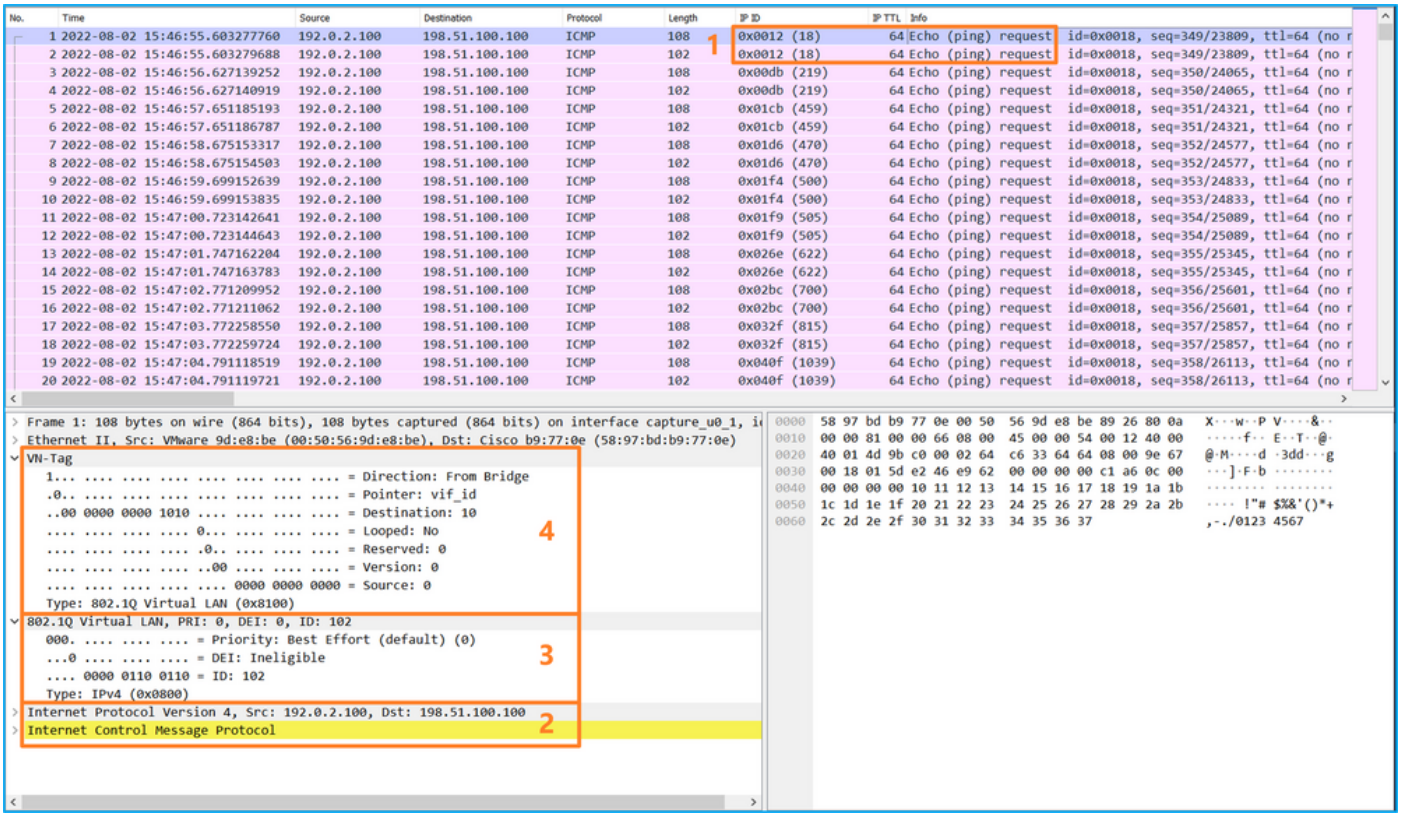
Coletar arquivos de captura

Siga as etapas na seção **Coletar arquivos de captura do switch interno Firepower 4100/9300**.

Capturar análise de arquivo

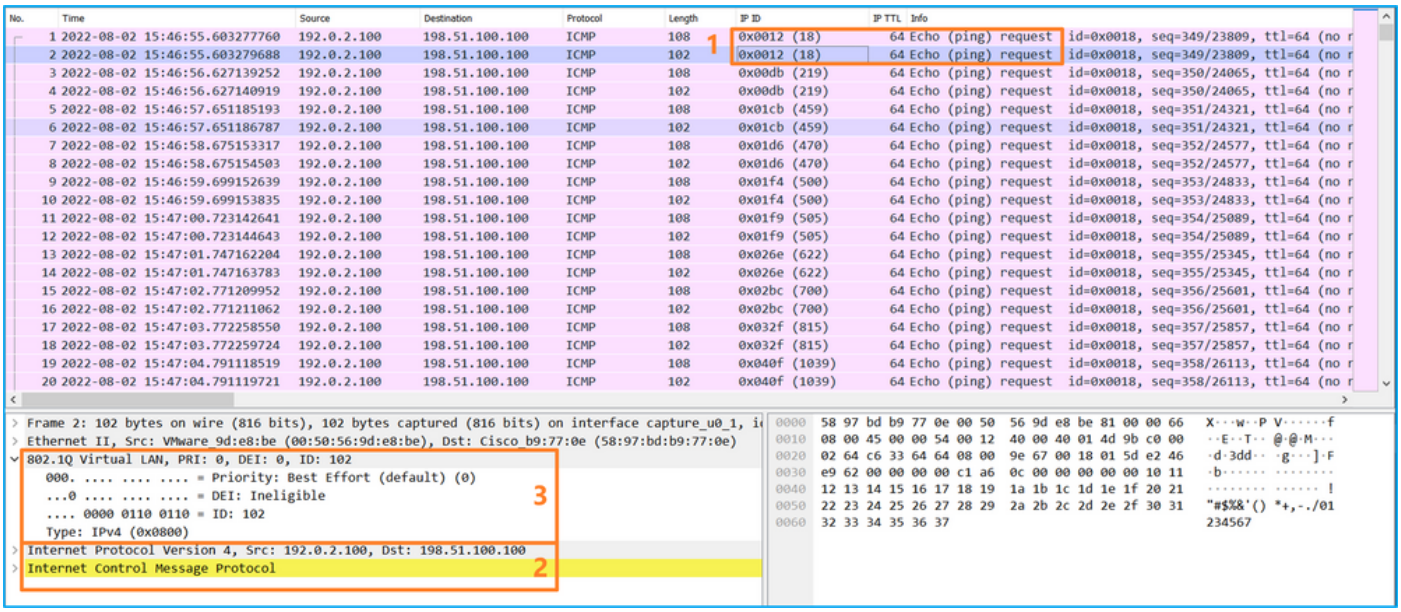
Use um aplicativo leitor de arquivo de captura de pacote para abrir o arquivo de captura. Selecione o primeiro pacote e verifique os pontos principais

1. Somente os pacotes ICMP de solicitação de eco são capturados. Cada pacote é capturado e mostrado 2 vezes.
2. O cabeçalho do pacote original está sem a marca VLAN.
3. O switch interno insere a tag de VLAN de porta adicional **102** que identifica a interface de entrada Ethernet1/2.
4. O switch interno insere uma marca VN adicional.



Selecione o segundo pacote e verifique os pontos principais:

1. Somente os pacotes ICMP de solicitação de eco são capturados. Cada pacote é capturado e mostrado 2 vezes.
2. O cabeçalho do pacote original está sem a marca VLAN.
3. O switch interno insere a tag de VLAN de porta adicional **102** que identifica a interface de entrada Ethernet1/2.



Explicação

Quando uma captura de pacote em uma interface frontal é configurada, o switch captura simultaneamente cada pacote duas vezes:

- Após a inserção da marca da porta VLAN.
- Após a inserção da tag VN.

Na ordem de operações, a tag VN é inserida em um estágio posterior à inserção da tag VLAN da porta. Mas no arquivo de captura, o pacote com a marca VN é mostrado antes do pacote com a marca VLAN da porta.

Quando um filtro de captura é aplicado, somente os pacotes que correspondem ao filtro na direção de entrada são capturados.

Esta tabela resume a tarefa:

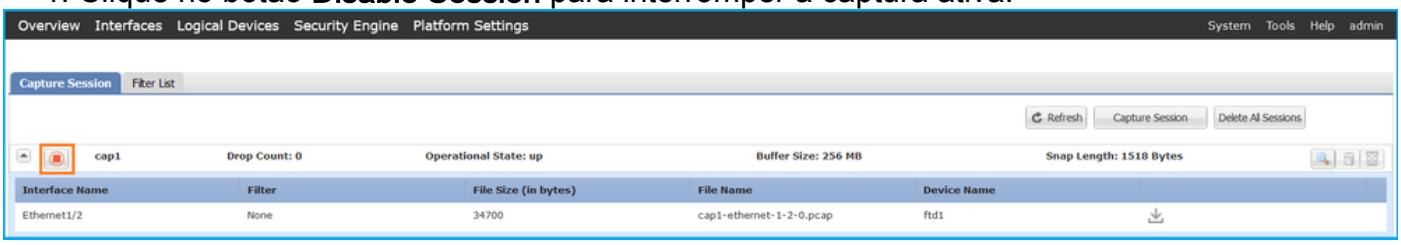
Tarefa	Ponto de captura	VLAN de porta interna em pacotes capturados	Direção	Filtro de usuário	Tráfego capturado
Configurar e verificar uma captura de pacote com um filtro na interface Ethernet1/2 frontal	Ethernet1/2	102	Somente entrada	Protocolo: ICMP Fonte:192.0.2.100 Destino: 198.51.100.100	Solicitações de eco ICMP de 192.0.2.100 para o host 198.51.100.100

Coletar Arquivos De Captura Do Switch Interno Firepower 4100/9300

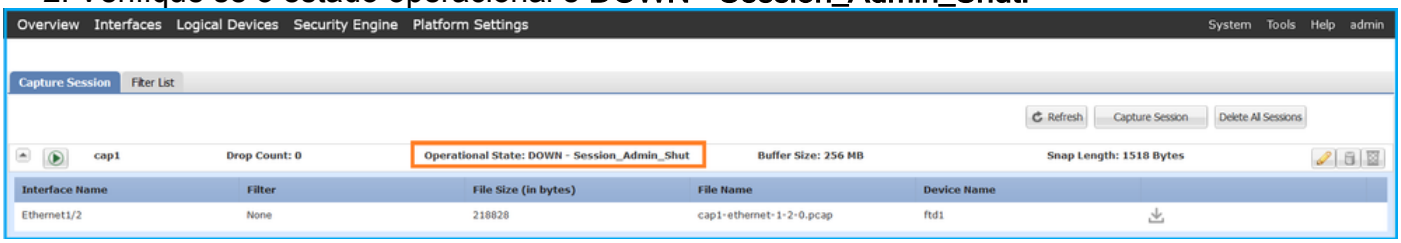
FCM

Siga estas etapas no FCM para coletar arquivos de captura do switch interno:

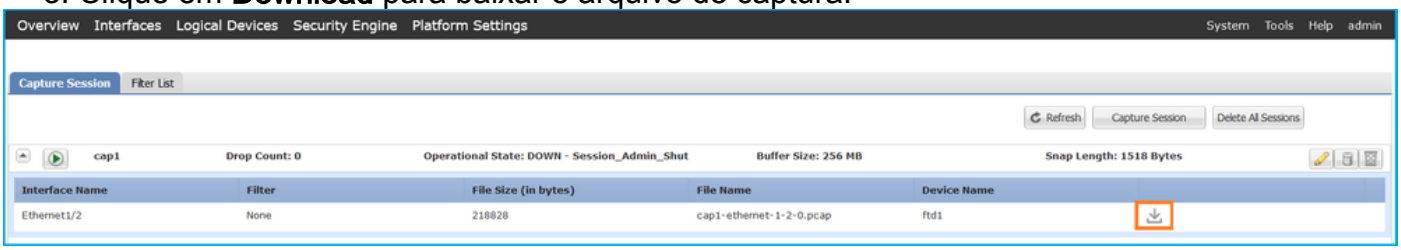
1. Clique no botão **Disable Session** para interromper a captura ativa:



2. Verifique se o estado operacional é **DOWN - Session_Admin_Shut:**



3. Clique em **Download** para baixar o arquivo de captura:



No caso de interfaces port-channel, repita essa etapa para cada interface membro.

CLI FXOS

Siga estas etapas na CLI FXOS para coletar arquivos de captura:

1. Pare a captura ativa:

```
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. Carregue o arquivo de captura do escopo do comando **local-mgmt**:

```
firepower# connect local-mgmt
firepower(local-mgmt)# copy /packet-capture/session-1/cap1-ethernet-1-2-0.pcap ?
 ftp:        Dest File URI
 http:       Dest File URI
 https:      Dest File URI
 scp:        Dest File URI
 sftp:       Dest File URI
 tftp:       Dest File URI
 usbdrive:   Dest File URI
 volatile:   Dest File URI
 workspace:  Dest File URI

firepower(local-mgmt)# copy /packet-capture/session-1/cap1-ethernet-1-2-0.pcap
ftp://ftpuser@10.10.10.1/cap1-ethernet-1-2-0.pcap
Password:
```

No caso de interfaces port-channel, copie o arquivo de captura para cada interface membro.

Diretrizes, limitações e práticas recomendadas para Switch interno Captura do pacote

Para obter diretrizes e limitações relacionadas à captura do switch interno Firepower 4100/9300, consulte o *Guia de configuração do gerenciador de chassi FXOS do Cisco Firepower 4100/9300*

ou oGuia de configuração da CLI FXOS do Cisco Firepower 4100/9300, capítulo Solução de problemas, seção Captura de pacote.

Esta é a lista de práticas recomendadas com base no uso da captura de pacotes em casos de TAC:

- Esteja ciente das diretrizes e limitações.
- Capture pacotes em todas as interfaces de membro de canal de porta e analise todos os arquivos de captura.
- Use filtros de captura.
- Considere o impacto do NAT nos endereços IP do pacote quando um filtro de captura é configurado.
- Aumente ou diminua a **Lente de Ajuste** que especifica o tamanho do quadro caso seja diferente do valor padrão de 1518 bytes. Um tamanho menor resulta em um número maior de pacotes capturados e vice-versa.
- Ajuste o **tamanho do buffer** conforme necessário.
- Esteja ciente da **contagem de queda** na CLI FCM ou FXOS. Quando o limite de tamanho do buffer for atingido, o contador de contagem de queda aumentará.
- Use o filtro **!vntag** no Wireshark para exibir somente pacotes sem a marca VN. Isso é útil para ocultar pacotes marcados com VLAN nos arquivos de captura de pacote da interface frontal.
- Use o filtro **frame.number&1** no Wireshark para exibir apenas quadros ímpares. Isso é útil para ocultar pacotes duplicados nos arquivos de captura de pacotes da interface do painel traseiro.
- No caso de protocolos como o TCP, o Wireshark aplica por padrão regras de colorização que exibem pacotes com condições específicas em cores diferentes. No caso de capturas de switch internas devido a pacotes duplicados em arquivos de captura, o pacote pode ser colorido e marcado de forma falsa-positiva. Se você analisar os arquivos de captura de pacote e aplicar qualquer filtro, exporte os pacotes exibidos para um novo arquivo e abra o novo arquivo.

Configuração e verificação em Firewall seguro 3100

Diferentemente do Firepower 4100/9300, as capturas de switch interno no Secure Firewall 3100 são configuradas na interface de linha de comando do aplicativo através do comando **capture <name> switch**, onde a opção **switch** especifica que as capturas são configuradas no switch interno.

Este é o comando **capture** com a opção **switch**:

```
> 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>
```

As etapas gerais para a configuração da captura de pacotes são as seguintes:

1. Especifique uma interface de entrada:

A configuração de captura do switch aceita o **nome** da interface de entrada. O usuário pode especificar os nomes das interfaces de dados, o uplink interno ou as interfaces de gerenciamento:

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

 management       Name of interface Management1/1
```

2. Especifique o EtherType do quadro ethernet. O EtherType padrão é IP. Os valores da opção **ethernet-type** especificam o EtherType:

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

3. Especifique as condições de correspondência. A opção de **correspondência de** captura especifica os critérios de correspondência:

```
> 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. Especifique outros parâmetros opcionais, como o tamanho do buffer, o comprimento do pacote e assim por diante.
5. Ative a captura. O comando **no capture <name> switch stop** ativa a captura:

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

6. Verifique os detalhes da captura:

- O status administrativo é **enabled**, e o status operacional é **up** e ative.
- O tamanho do arquivo de captura de pacote **Pcapsize** aumenta.
- O número de pacotes capturados na saída de **show capture <cap_name>** é diferente de zero.
- Capturar caminho **Pcapfile.** Os pacotes capturados são salvos automaticamente na **pasta /mnt/disk0/packet-capture/**.
- Capturar condições. O software cria automaticamente filtros de captura com base nas condições de captura.

```
> 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. Pare as capturas quando necessário:

```
> 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. Colete os arquivos de captura. Siga as etapas na seção **Coletar arquivos de captura do switch interno do Secure Firewall 3100**.

Na versão 7.2, a configuração de captura do switch interno não é suportada no FMC ou no FDM. No caso do software ASA versão 9.18(1) e posterior, as capturas de switch interno podem ser configuradas nas versões 7.18.1.x e posteriores do ASDM.

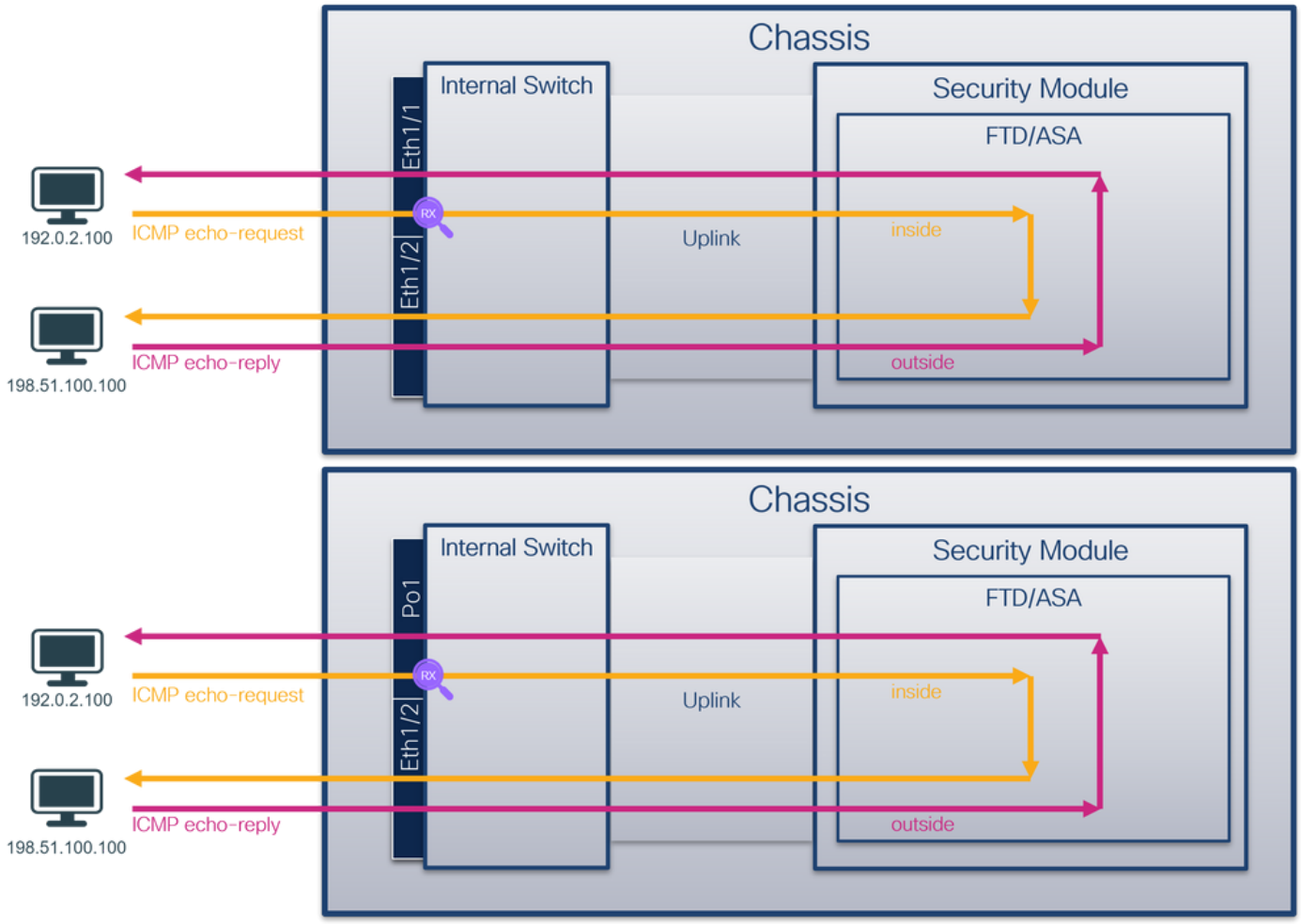
Esses cenários cobrem casos de uso comuns de capturas de switches internos do Secure

Firewall 3100.

Captura de pacotes em uma interface física ou de canal de porta

Use o FTD ou o ASA CLI para configurar e verificar uma captura de pacote na interface Ethernet1/1 ou Portchannel1. Ambas as interfaces têm o nome **if inside**.

Topologia, fluxo de pacotes e pontos de captura



Configuração

Siga estas etapas no ASA ou FTD CLI para configurar uma captura de pacote na interface Ethernet1/1 ou Port-channel1:

1. Verifique o nome se:

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

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

2. Criar uma sessão de captura:

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

3. Ativar a sessão de captura:

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

Verificação

Verifique o nome da sessão de captura, o estado operacional e administrativo, o slot de interface e o identificador. Verifique se o valor de **Pcapsize** em bytes aumenta e se o número de pacotes capturados é diferente de zero:

```
> 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
```

No caso de Port-channel1, a captura é configurada em todas as interfaces membro:

```
> 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
```

As interfaces membro do canal de porta podem ser verificadas no shell de comando FXOS **local-mgmt** através do comando **show portchannel summary**:

```
> connect fxos
…
KSEC-FPR3100-1 connect local-mgmt
KSEC-FPR3100-1(local-mgmt) show portchannel summary
Flags:  D - Down        P - Up in port-channel (members)
I - Individual  H - Hot-standby (LACP only)
s - Suspended   r - Module-removed
S - Switched    R - Routed
U - Up (port-channel)
M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
     Channel
--------------------------------------------------------------------------------
1     Po1(U)      Eth      LACP      Eth1/3(P)    Eth1/4(P)

LACP KeepAlive Timer:
--------------------------------------------------------------------------------
     Channel  PeerKeepAliveTimerFast
--------------------------------------------------------------------------------
1     Po1(U)      False

Cluster LACP Status:
--------------------------------------------------------------------------------
     Channel  ClusterSpanned  ClusterDetach  ClusterUnitID  ClusterSysID
--------------------------------------------------------------------------------
1     Po1(U)      False          False          0            clust
```

Para acessar o FXOS no ASA, execute o comando **connect fxos admin**. No caso de multicontexto, execute o comando no contexto do administrador.

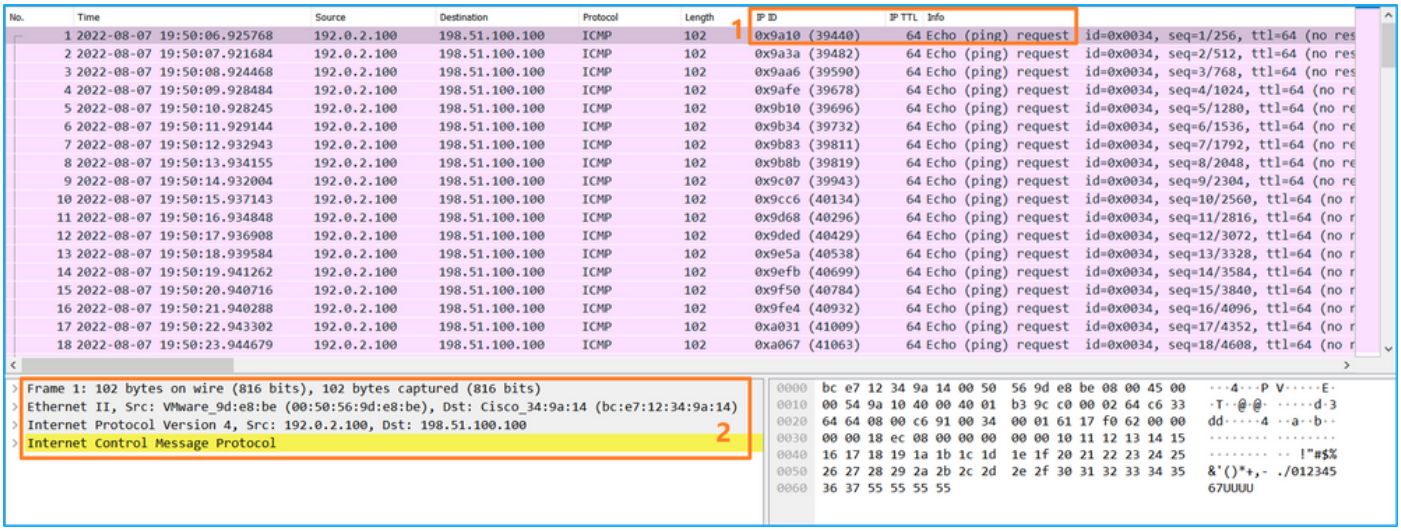
Coletar arquivos de captura

Siga as etapas na seção **Coletar arquivos de captura do switch interno do Secure Firewall 3100**.

Capturar análise de arquivo

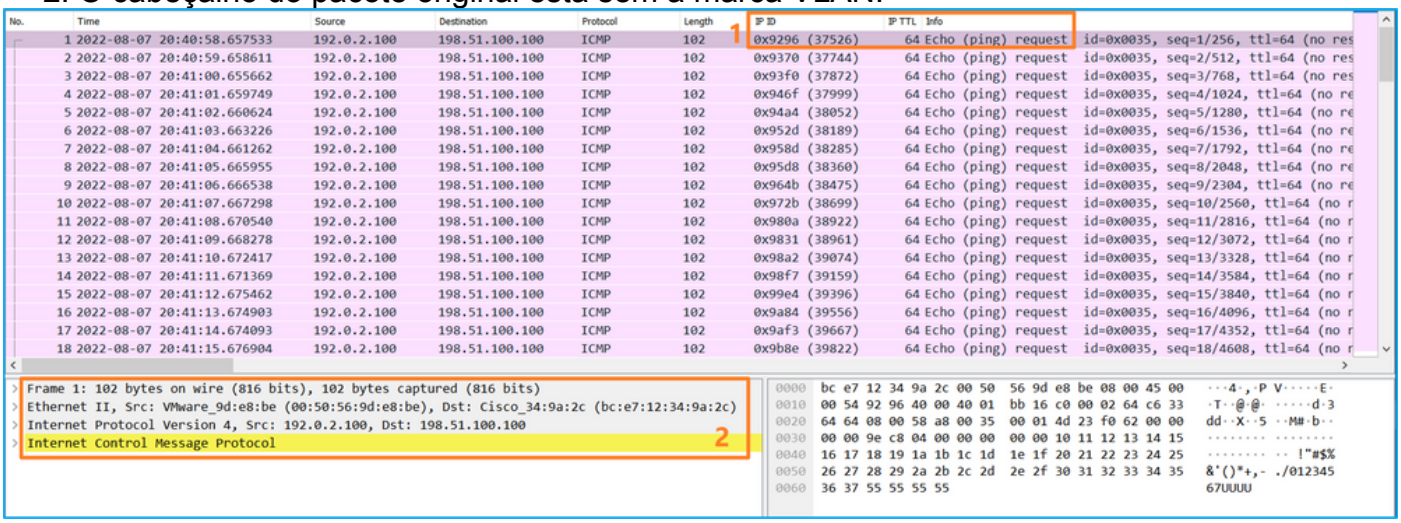
Use um aplicativo leitor de arquivo de captura de pacote para abrir os arquivos de captura para Ethernet1/1. Selecione o primeiro pacote e verifique os pontos principais:

1. Somente os pacotes ICMP de solicitação de eco são capturados.
2. O cabeçalho do pacote original está sem a marca VLAN.



Abra os arquivos de captura para as interfaces membro Portchannel1. Selecione o primeiro pacote e verifique os pontos principais:

1. Somente os pacotes ICMP de solicitação de eco são capturados.
2. O cabeçalho do pacote original está sem a marca VLAN.



Explicação

As capturas do switch são configuradas nas interfaces Ethernet1/1 ou Portchannel1.

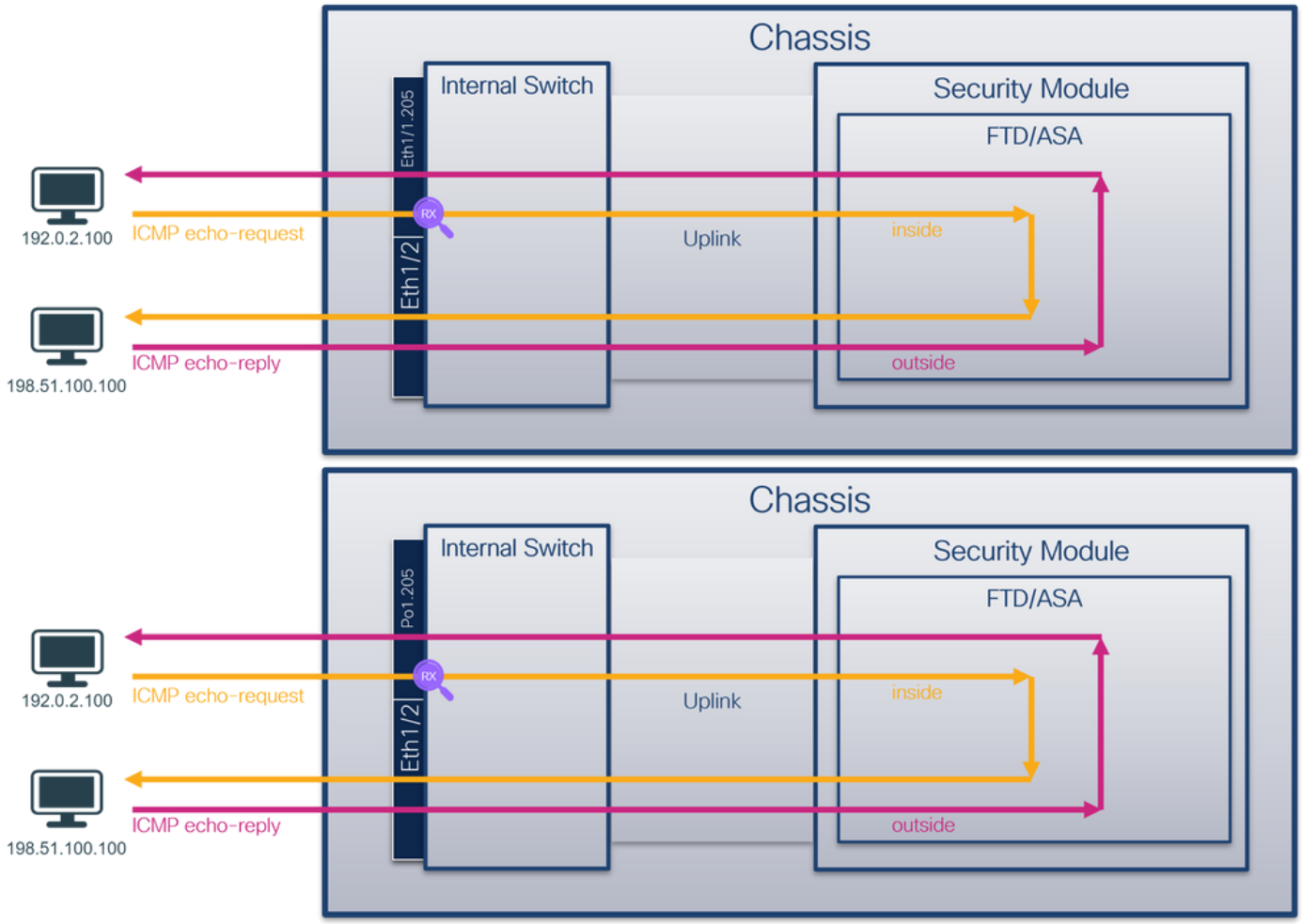
Esta tabela resume a tarefa:

Tarefa	Ponto de captura	Filtro interno	Direção	Tráfego capturado
Configurar e verificar uma captura de pacote na interface Ethernet1/1	Ethernet1/1	Nenhum	Somente entrada	Solicitações de eco ICMP do host 192.0.2.100 para o host 198.51.100
Configurar e verificar uma captura de pacote na interface Portchannel1 com as interfaces membro Ethernet1/3 e Ethernet1/4	Ethernet1/3 Ethernet1/4	Nenhum	Somente entrada	Solicitações de eco ICMP do host 192.0.2.100 para o host 198.51.100

Captura de pacotes em uma subinterface de uma interface física ou de canal de porta

Use o FTD ou o ASA CLI para configurar e verificar uma captura de pacote nas subinterfaces Ethernet1/1.205 ou Portchannel1.205. Ambas as subinterfaces têm o nome **inside**.

Topologia, fluxo de pacotes e pontos de captura



Configuração

Siga estas etapas no ASA ou FTD CLI para configurar uma captura de pacote na interface Ethernet1/1 ou Port-channel1:

1. Verifique o nome se:

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

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

2. Criar uma sessão de captura:

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

3. Ativar a sessão de captura:

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

Verificação

Verifique o nome da sessão de captura, o estado operacional e administrativo, o slot de interface e o identificador. Verifique se o valor de **Pcapsize** em bytes aumenta e se o número de pacotes capturados é diferente de zero:

```
> 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
```

Nesse caso, um filtro com a VLAN externa **Ovlan=205** é criado e aplicado à interface.

No caso de Port-channel1, a captura com um filtro **Ovlan=205** é configurada em todas as interfaces do membro:

```
> 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
```

As interfaces membro do canal de porta podem ser verificadas no shell de comando FXOS **local-mgmt** através do comando **show portchannel summary**:

```
> connect fxos
…
KSEC-FPR3100-1 connect local-mgmt
KSEC-FPR3100-1(local-mgmt) show portchannel summary
Flags:  D - Down        P - Up in port-channel (members)
I - Individual  H - Hot-standby (LACP only)
s - Suspended   r - Module-removed
S - Switched    R - Routed
U - Up (port-channel)
M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
     Channel
--------------------------------------------------------------------------------
1     Po1(U)      Eth      LACP      Eth1/3(P)    Eth1/4(P)

LACP KeepAlive Timer:
--------------------------------------------------------------------------------
     Channel  PeerKeepAliveTimerFast
--------------------------------------------------------------------------------
1     Po1(U)      False

Cluster LACP Status:
--------------------------------------------------------------------------------
     Channel  ClusterSpanned  ClusterDetach  ClusterUnitID  ClusterSysID
--------------------------------------------------------------------------------
1     Po1(U)      False          False          0            clust
```

Para acessar o FXOS no ASA, execute o comando **connect fxos admin**. No caso de multicontexto, execute esse comando no contexto do administrador.

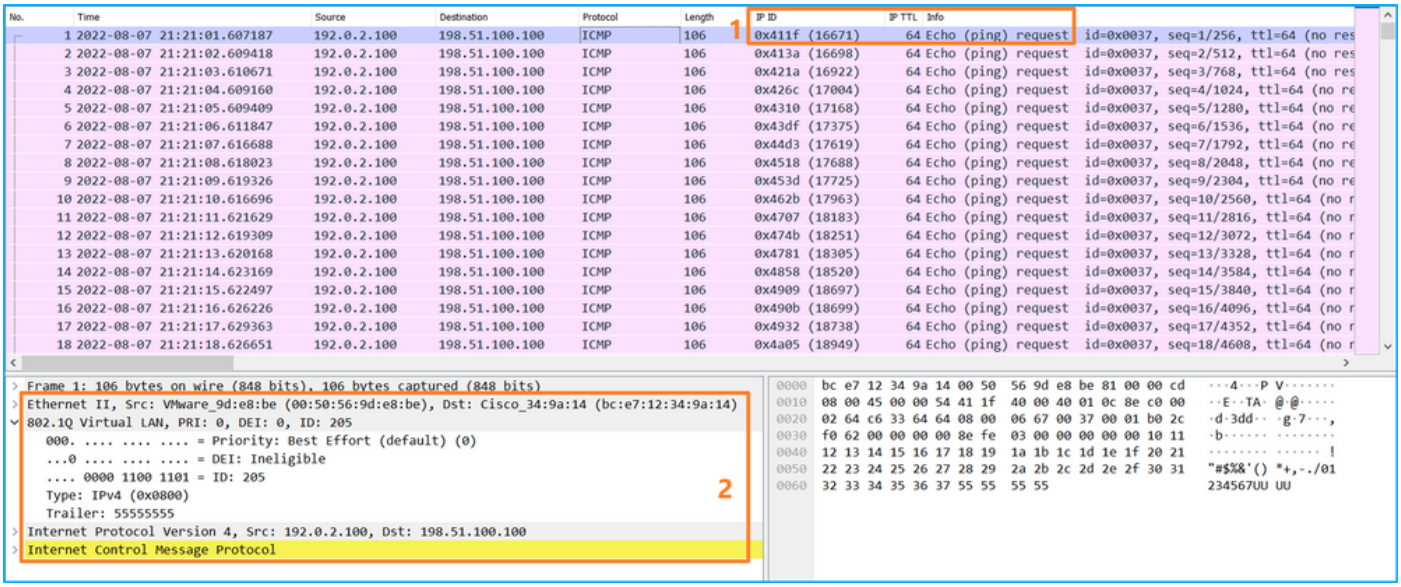
Coletar arquivos de captura

Siga as etapas na seção **Coletar arquivos de captura do switch interno do Secure Firewall 3100**.

Capturar análise de arquivo

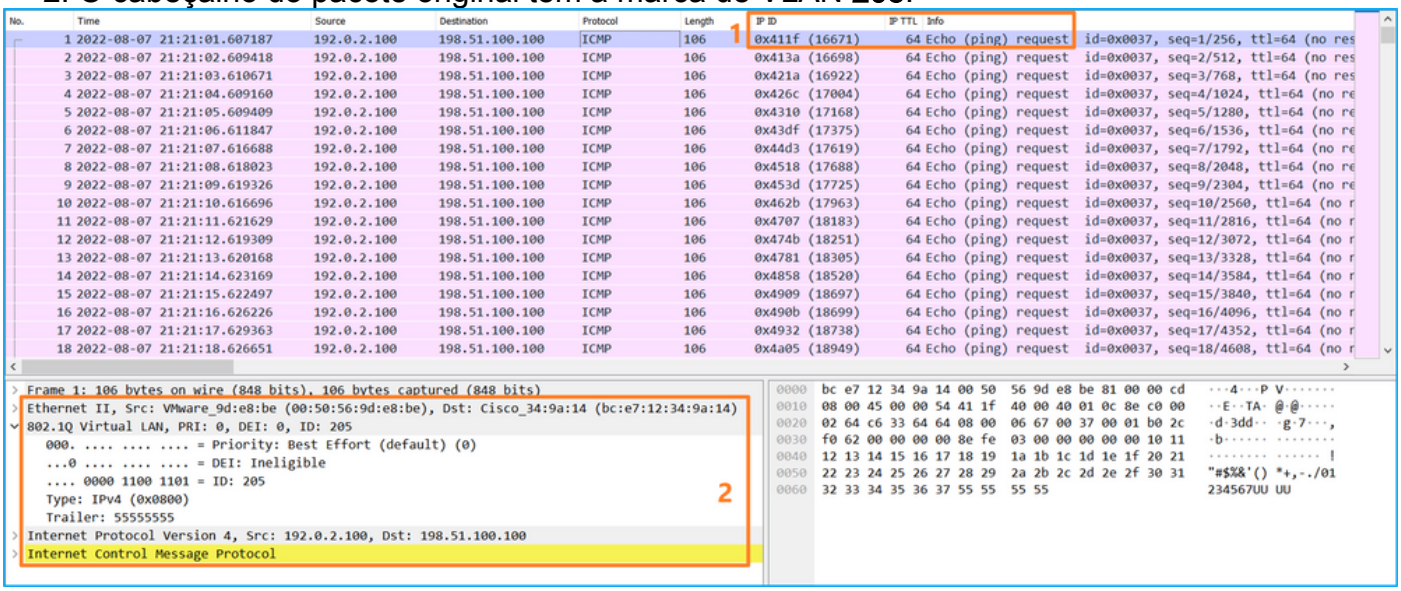
Use um aplicativo leitor de arquivo de captura de pacote para abrir os arquivos de captura para Ethernet1/1.205. Selecione o primeiro pacote e verifique os pontos principais:

1. Somente os pacotes ICMP de solicitação de eco são capturados.
2. O cabeçalho do pacote original tem a marca de VLAN **205**.



Abra os arquivos de captura para as interfaces membro Portchannel1. Selecione o primeiro pacote e verifique os pontos principais:

1. Somente os pacotes ICMP de solicitação de eco são capturados.
2. O cabeçalho do pacote original tem a marca de VLAN **205**.



Explicação

As capturas do switch são configuradas nas subinterfaces Ethernet1/1.205 ou Portchannel1.205 com um filtro que corresponde à VLAN 205 externa.

Esta tabela resume a tarefa:

Tarefa	Ponto de captura	Filtro interno	Direção	Tráfego capturado
Configurar e verificar uma captura de pacote na subinterface Ethernet1/1.205	Ethernet 1/1	VLAN Externa 205	Somente entrada	Solicitações de eco ICMP do host 192.0.2.100 para o host 198.51.100.100
Configurar e verificar uma captura de pacote na subinterface Portchannel1.205 com as interfaces membro Ethernet1/3 e Ethernet1/4	Ethernet 1/3 Ethernet 1/4	VLAN Externa 205	Somente entrada	Solicitações de eco ICMP do host 192.0.2.100 para o host 198.51.100.100

Captura de pacotes em interfaces internas

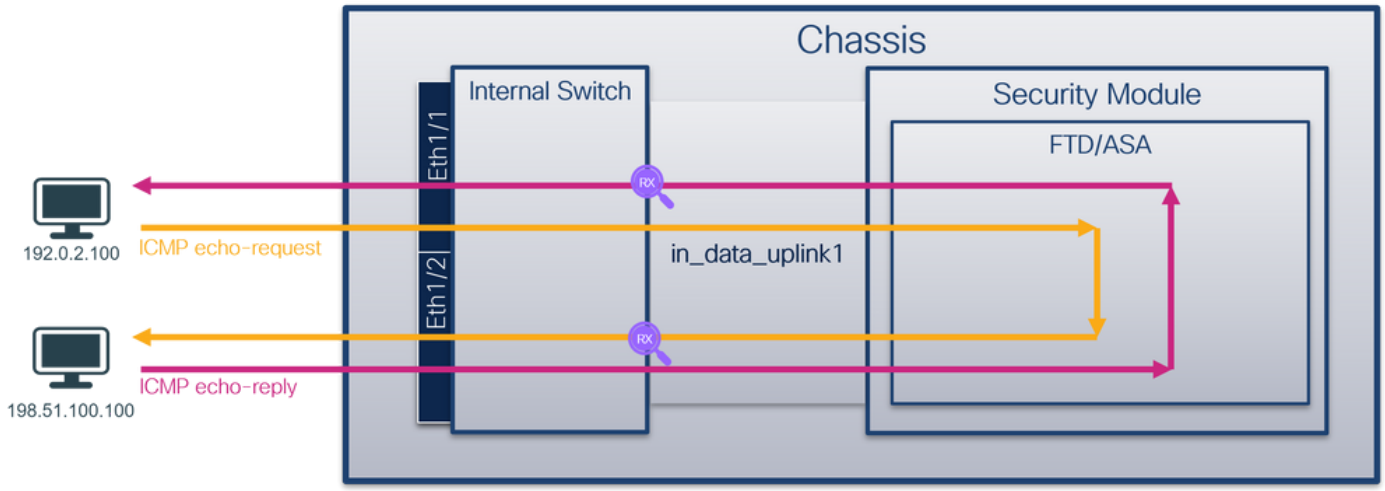
O Secure Firewall tem duas interfaces internas:

- **in_data_uplink1** - conecta o aplicativo ao switch interno.
- **in_mgmt_uplink1** - fornece um caminho de pacote dedicado para conexões de gerenciamento, como SSH para a interface de gerenciamento, ou a conexão de gerenciamento, também conhecida como sftunnel, entre o FMC e o FTD.

Tarefa 1

Use o FTD ou o ASA CLI para configurar e verificar uma captura de pacote na interface de uplink **in_data_uplink1.**

Topologia, fluxo de pacotes e pontos de captura



Configuração

Siga estas etapas no ASA ou FTD CLI para configurar uma captura de pacote na interface **in_data_uplink1**:

1. Criar uma sessão de captura:

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

2. Ativar a sessão de captura:

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

Verificação

Verifique o nome da sessão de captura, o estado operacional e administrativo, o slot de interface e o identificador. Verifique se o valor de **Pcapsize** em bytes aumenta e se o número de pacotes capturados é diferente de zero:

```
>  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
```

Nesse caso, uma captura é criada na interface com um ID interno **18** que é a interface in_data_uplink1 no Secure Firewall 3130. O comando **show portmanager switch status** no shell de comando FXOS **local-mgmt** mostra os IDs da interface:

```
> connect fxos
…
KSEC-FPR3100-1 connect local-mgmt
KSEC-FPR3100-1(local-mgmt) show portmanager switch status
Dev/Port         Mode        Link   Speed  Duplex  Loopback Mode  Port Manager
---------  ----------------  -----  -----  ------  -------------  ------------
0/1             SGMII         Up     1G     Full    None           Link-Up
0/2             SGMII         Up     1G     Full    None           Link-Up
0/3             SGMII         Up     1G     Full    None           Link-Up
0/4             SGMII         Up     1G     Full    None           Link-Up
0/5             SGMII        Down    1G     Half    None           Mac-Link-Down
0/6             SGMII        Down    1G     Half    None           Mac-Link-Down
0/7             SGMII        Down    1G     Half    None           Mac-Link-Down
0/8             SGMII        Down    1G     Half    None           Mac-Link-Down
0/9           1000_BaseX     Down    1G     Full    None           Link-Down
0/10          1000_BaseX     Down    1G     Full    None           Link-Down
0/11          1000_BaseX     Down    1G     Full    None           Link-Down
0/12          1000_BaseX     Down    1G     Full    None           Link-Down
```

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

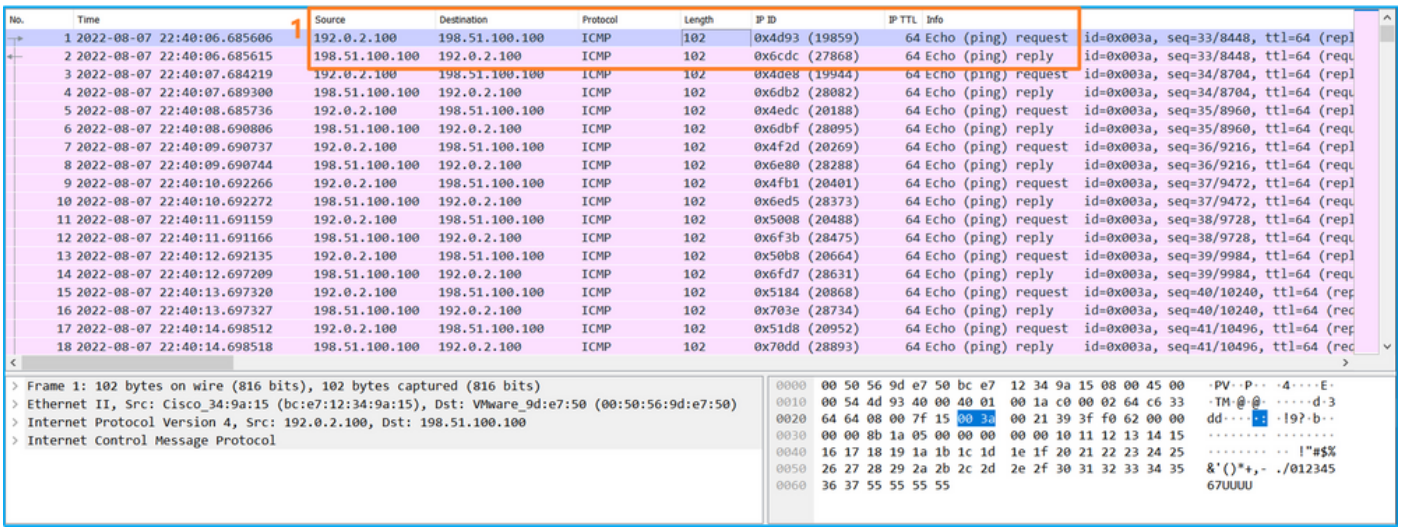
Para acessar o FXOS no ASA, execute o comando **connect fxos admin**. No caso de multicontexto, execute esse comando no contexto do administrador.

Coletar arquivos de captura

Siga as etapas na seção **Coletar arquivos de captura do switch interno do Secure Firewall 3100**.

Capturar análise de arquivo

Use um aplicativo leitor de arquivo de captura de pacote para abrir os arquivos de captura da interface in_data_uplink1. Verifique o ponto-chave - nesse caso, os pacotes ICMP de solicitação de eco e de resposta de eco são capturados. Esses são os pacotes enviados do aplicativo para o switch interno.



Explicação

Quando uma captura de switch na interface de uplink é configurada, somente os pacotes enviados do aplicativo para o switch interno são capturados. Os pacotes enviados ao aplicativo

não são capturados.

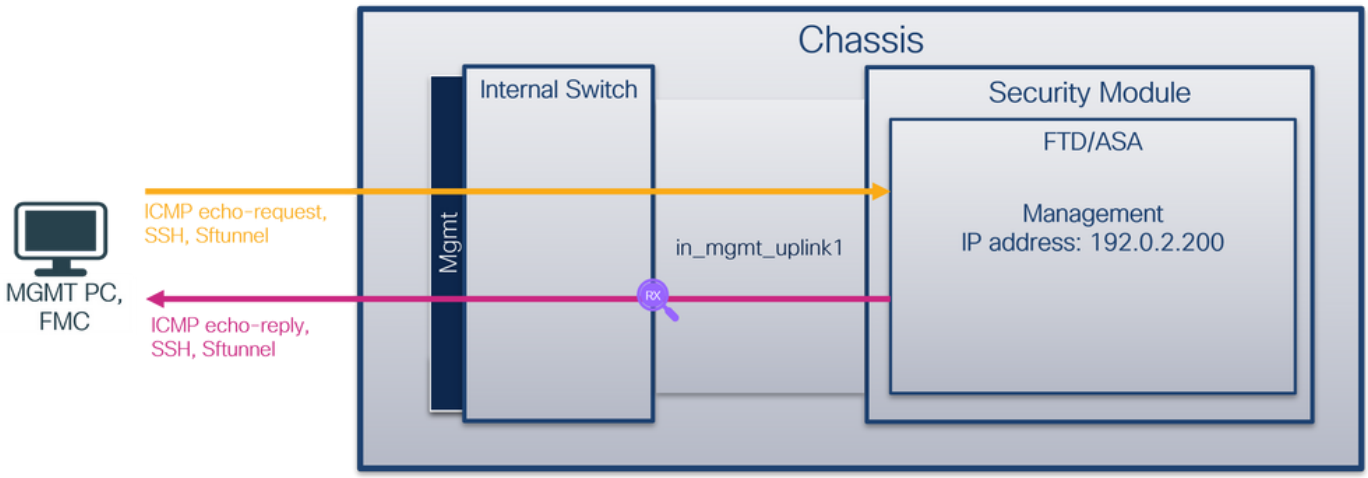
Esta tabela resume a tarefa:

Tarefa	Ponto de captura	Filtro interno	Direção	Tráfego capturado
Configurar e verificar uma captura de pacote na interface de uplink in_data_uplink1	in_data_uplink1	Nenhum	Somente entrada	Solicitações de eco ICMP do hos 192.0.2.100 para o host 198.51.100.100 Respostas de eco ICMP do host 198.51.100.100 para o host 192.0.2.100

Tarefa 2

Use o FTD ou o ASA CLI para configurar e verificar uma captura de pacote na interface de uplink **in_mgmt_uplink1.** Somente os pacotes de conexões do plano de gerenciamento são capturados.

Topologia, fluxo de pacotes e pontos de captura



Configuração

Siga estas etapas no ASA ou FTD CLI para configurar uma captura de pacote na interface **in_mgmt_uplink1**:

1. Criar uma sessão de captura:

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

2. Ativar a sessão de captura:

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

Verificação

Verifique o nome da sessão de captura, o estado operacional e administrativo, o slot de interface e o identificador. Verifique se o valor de **Pcapsize** em bytes aumenta e se o número de pacotes capturados é diferente de zero:

```
> 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
```

Nesse caso, uma captura é criada na interface com um ID interno 19, que é a interface **in_mgmt_uplink1** no Secure Firewall 3130. O comando **show portmanager switch status** no shell de comando FXOS **local-mgmt** mostra os IDs da interface:

```
> connect fxos
…
KSEC-FPR3100-1 connect local-mgmt
KSEC-FPR3100-1(local-mgmt) show portmanager switch status
Dev/Port         Mode        Link   Speed  Duplex  Loopback Mode  Port Manager
---------  ----------------  -----  -----  ------  -------------  ------------
0/1             SGMII         Up     1G     Full    None           Link-Up
0/2             SGMII         Up     1G     Full    None           Link-Up
0/3             SGMII         Up     1G     Full    None           Link-Up
0/4             SGMII         Up     1G     Full    None           Link-Up
0/5             SGMII        Down    1G     Half    None           Mac-Link-Down
0/6             SGMII        Down    1G     Half    None           Mac-Link-Down
0/7             SGMII        Down    1G     Half    None           Mac-Link-Down
0/8             SGMII        Down    1G     Half    None           Mac-Link-Down
```

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

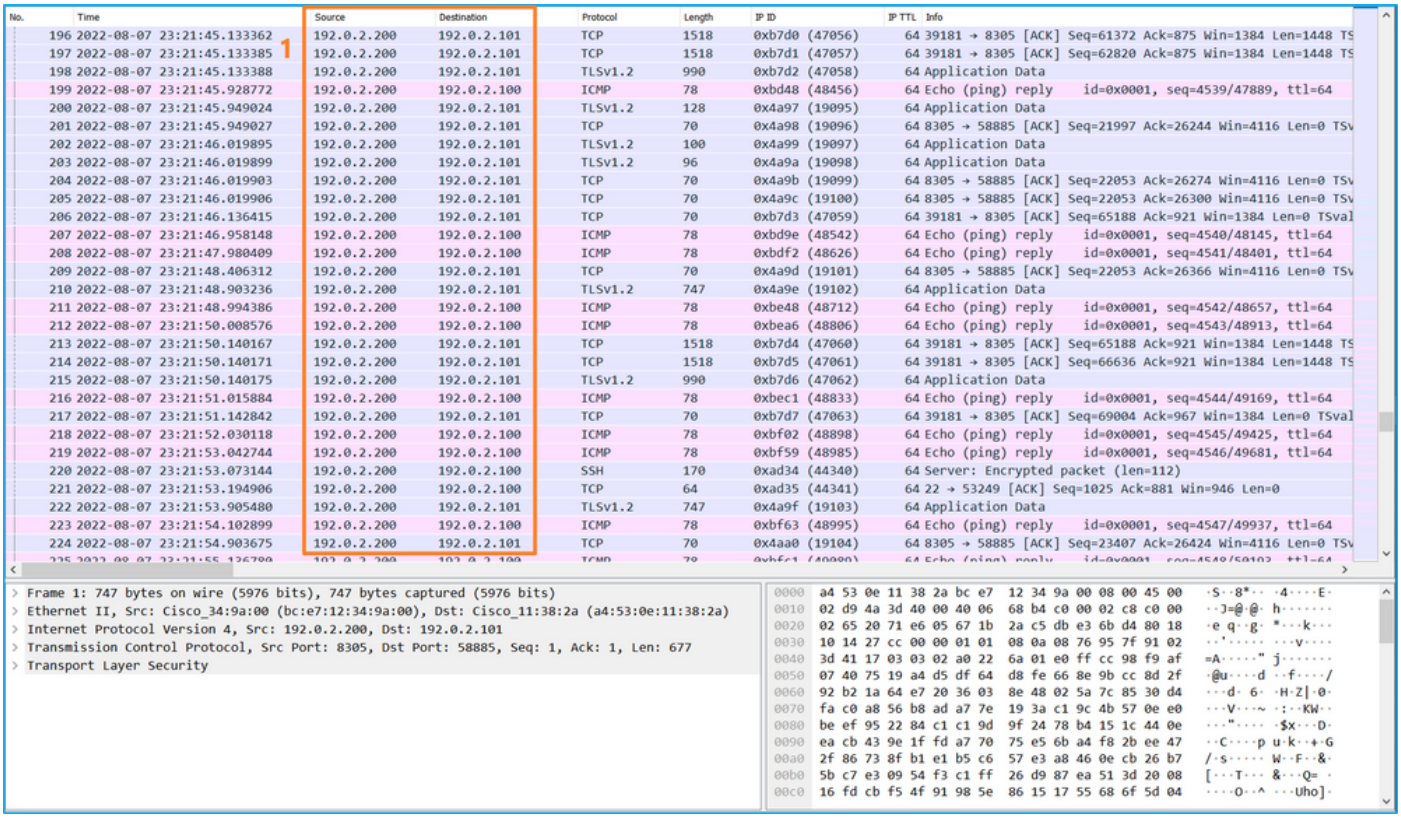
Para acessar o FXOS no ASA, execute o comando **connect fxos admin**. No caso de multicontexto, execute esse comando no contexto do administrador.

Coletar arquivos de captura

Siga as etapas na seção **Coletar arquivos de captura do switch interno do Secure Firewall 3100.**

Capturar análise de arquivo

Use um aplicativo leitor de arquivo de captura de pacote para abrir os arquivos de captura da interface **in_mgmt_uplink1**. Verifique o ponto-chave - nesse caso, somente os pacotes do endereço IP de gerenciamento 192.0.2.200 são mostrados. Exemplos são pacotes SSH, Sftunnel ou ICMP echo reply. Esses são os pacotes enviados da interface de gerenciamento de aplicativos para a rede através do switch interno.



Explicação

Quando uma captura de switch na interface de uplink de gerenciamento é configurada, somente os pacotes de entrada enviados da interface de gerenciamento de aplicativos são capturados. Os pacotes destinados à interface de gerenciamento de aplicativos não são capturados.

Esta tabela resume a tarefa:

Tarefa	Ponto de captura	Filtro interno	Direção	Tráfego capturado
Configurar e verificar uma captura de pacotes na interface de uplink de gerenciamento	in_mgmt_uplink1	Nenhum	Somente entrada (da interface de gerenciamento à rede através do switch interno)	Respostas de eco ICMP do endereço IP gerenciamento FTD 192.0.2.200 para o h 192.0.2.100 Sftunnel do endereço IP de gerenciamen FTD 192.0.2.200 para o endereço IP do 192.0.2.101 SSH do endereço IP de gerenciamento F 192.0.2.200 para o host 192.0.2.100

Filtros de captura de pacotes

Os filtros de captura de pacote do switch interno são configurados da mesma maneira que as capturas de plano de dados. Use as opções **ethernet-type** e **match** para configurar filtros.

Configuração

Siga estas etapas no ASA ou FTD CLI para configurar uma captura de pacote com um filtro que corresponda a quadros ARP ou pacotes ICMP do host 198.51.100.100 na interface Ethernet1/1:

1. Verifique o nome se:

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

2. Crie uma sessão de captura para ARP ou ICMP:

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

> capture capsw switch interface inside match icmp 198.51.100.100
```

Verificação

Verifique o nome da sessão de captura e o filtro. O valor Ethertype é **2054** em decimal e **0x0806** em hexadecimal:

```
> 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
```

Esta é a verificação do filtro para ICMP. O protocolo IP 1 é o ICMP:

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

Total Physical ports involved in Packet Capture: 1

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

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

Total Physical breakout ports involved in Packet Capture: 0

0 packets captured on disk using switch capture

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

Coletar arquivos de captura do switch interno do Secure Firewall 3100

Use o ASA ou o FTD CLI para coletar arquivos de captura do switch interno. No FTD, o arquivo de captura também pode ser exportado através do comando CLI **copy** para destinos acessíveis através das interfaces de dados ou diagnóstico.

Como alternativa, o arquivo pode ser copiado para **/ngfw/var/common** no modo especialista e baixado do FMC através da opção **Download de arquivo**.

No caso de interfaces port-channel, certifique-se de coletar arquivos de captura de pacotes de todas as interfaces membro.

ASA

Siga estas etapas em para coletar arquivos de captura do switch interno no ASA CLI:

1. Pare a captura:

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

2. Verifique se a sessão de captura foi interrompida e observe o nome do arquivo de captura.

```
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. Use o comando CLI **copy** para exportar o arquivo para destinos remotos:

```
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

Siga estas etapas para coletar arquivos de captura do switch interno no FTD CLI e copiá-los para servidores acessíveis via interfaces de dados ou diagnóstico:

1. Vá para o diagnóstico CLI:

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Click 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower> enable
Password: <-- Enter
firepower#
```

2. Pare a captura:

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

3. Verifique se a sessão de captura foi interrompida e observe o nome do arquivo de captura:

```
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. Use o comando CLI **copy** para exportar o arquivo para destinos remotos.

```
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
```

Siga estas etapas em para coletar arquivos de captura do FMC por meio da opção **Download de arquivo**:

1. Pare a captura:

```
> capture capsw switch stop
```

2. Verifique se a sessão de captura foi interrompida e observe o nome do arquivo e o caminho completo do arquivo de captura:

```
> 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
```

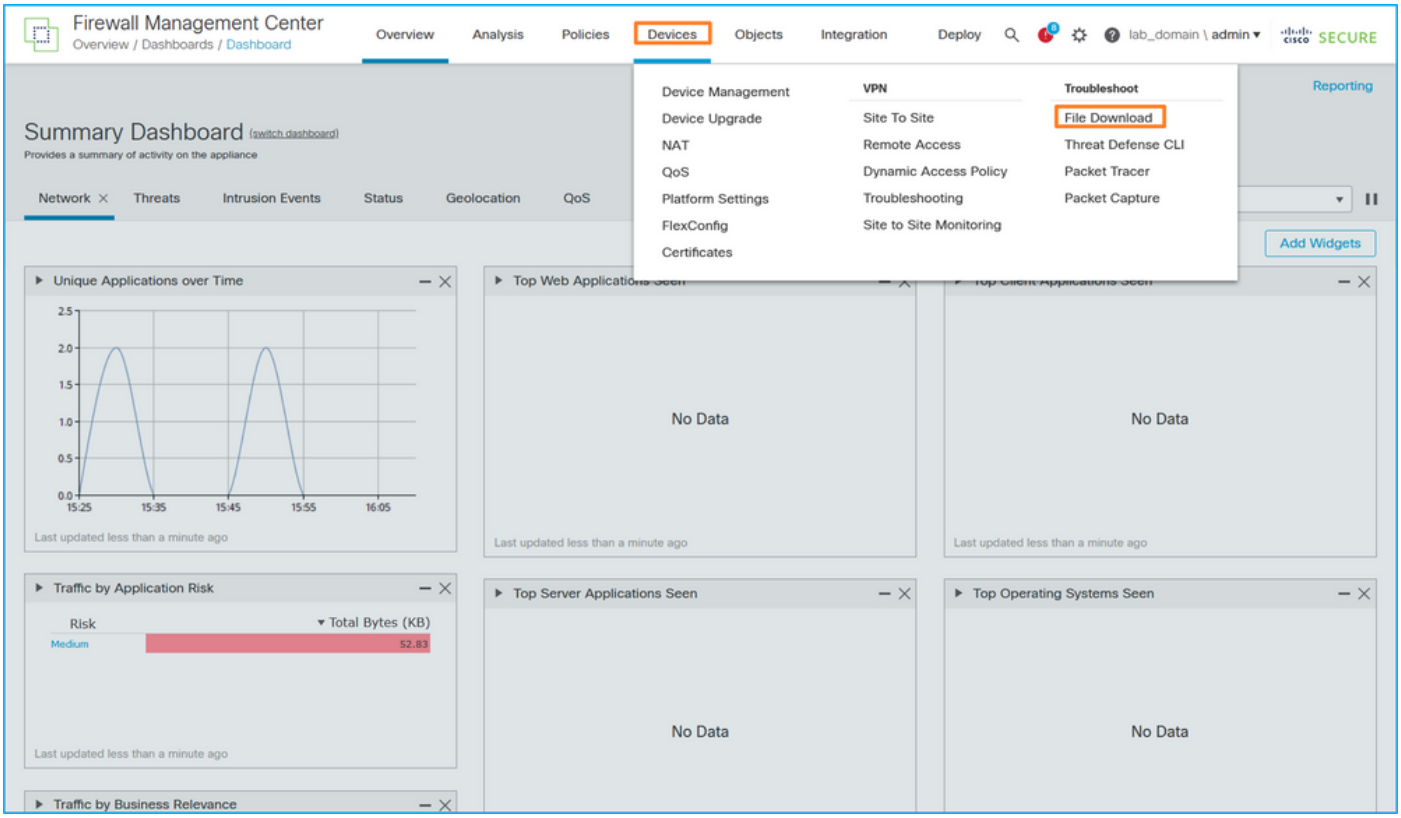
3. Vá para o modo especialista e mude para o modo raiz:

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

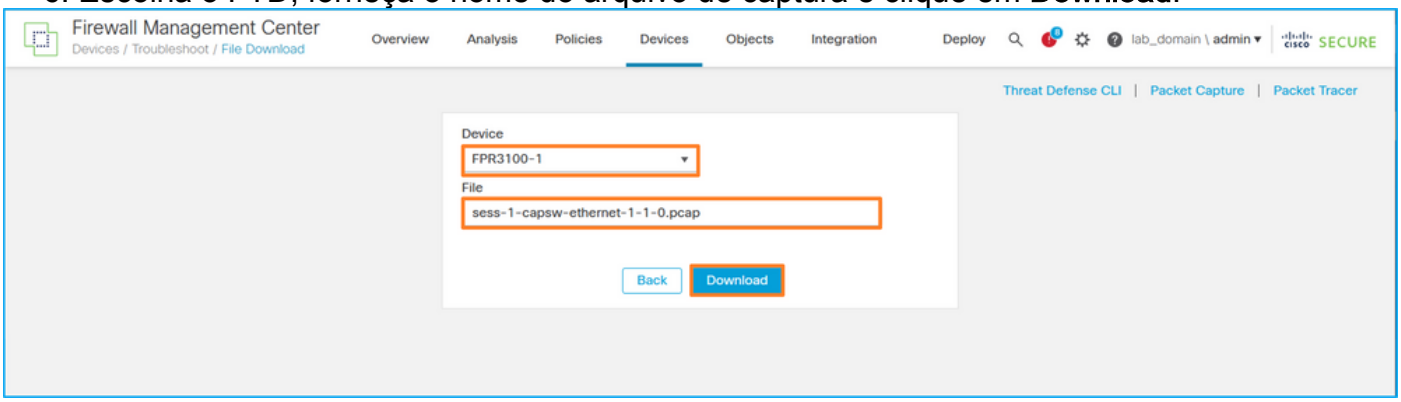
4. Copie o arquivo de captura para **/ngfw/var/common/**:

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

5. No FMC, escolha **Devices > File Download**:



6. Escolha o FTD, forneça o nome do arquivo de captura e clique em **Download**:



Diretrizes, limitações e práticas recomendadas para captura de pacotes de switch interno

Diretrizes e limitações:

- Há suporte para várias sessões de configuração de captura de switch, mas apenas uma sessão de captura de switch pode estar ativa por vez. Uma tentativa de ativar 2 ou mais sessões de captura resulta em um erro "**ERRO: Falha ao habilitar a sessão, pois o limite máximo de 1 sessão ativa de captura de pacotes foi atingido**".
- Uma captura de switch ativo não pode ser excluída.
- As capturas de switch não podem ser lidas no aplicativo. O usuário deve exportar os arquivos.
- Determinadas opções de captura de plano de dados, como **dump, decode, packet-number, trace** e outras, não são suportadas para capturas de switch.
- No caso do ASA multicontexto, as capturas de switch nas interfaces de dados são configuradas em contextos de usuário. As capturas de switch nas interfaces in_data_uplink1 e in_mgmt_uplink1 são suportadas apenas no contexto admin.

Esta é a lista de práticas recomendadas com base no uso da captura de pacotes em casos de TAC:

- Esteja ciente das diretrizes e limitações.
- Use filtros de captura.
- Considere o impacto do NAT nos endereços IP do pacote quando um filtro de captura é configurado.
- Aumente ou diminua o **comprimento do pacote** que especifica o tamanho do quadro, caso ele seja diferente do valor padrão de 1518 bytes. Um tamanho menor resulta em um número maior de pacotes capturados e vice-versa.
- Ajuste o tamanho do **buffer** conforme necessário.
- Esteja ciente da **contagem de queda** na saída do comando **show cap <cap_name> detail**. Quando o limite de tamanho do buffer for atingido, o contador de contagem de queda aumentará.

Informações Relacionadas

- Guias de configuração da CLI do FXOS e do gerenciador de chassi do Firepower 4100/9300
- Guia de introdução do Cisco Secure Firewall 3100
- Referência de comandos FXOS do Cisco Firepower 4100/9300

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.