

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.

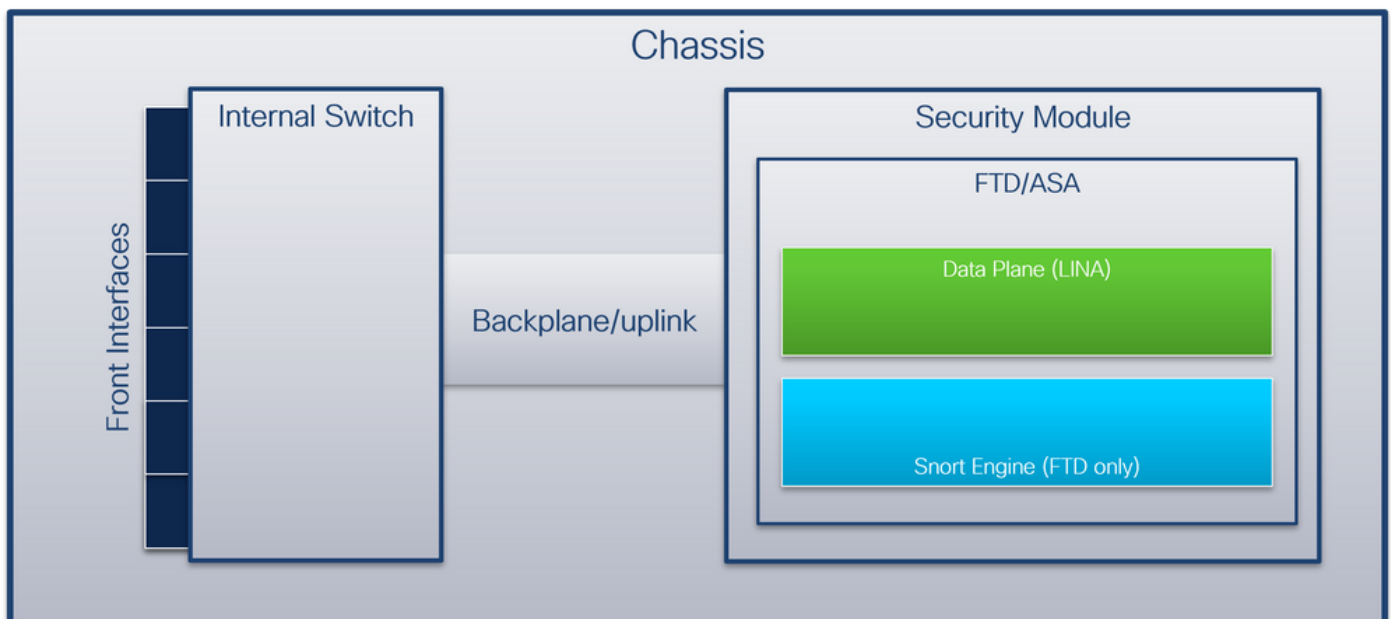
As informações neste documento são baseadas nestas versões de software e hardware:

- 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 aplicação 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 Internal-Data0/0 Internal-Data0/1
Firepower 9300	3	SM1: Ethernet1/9 Ethernet1/10 SM2: Ethernet1/11 Ethernet1/12 SM3: Ethernet1/13 Ethernet1/14	Internal-Data0/0 Internal-Data0/1 Internal-Data0/0 Internal-Data0/1
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-Controlo0/0 "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
  udlld 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

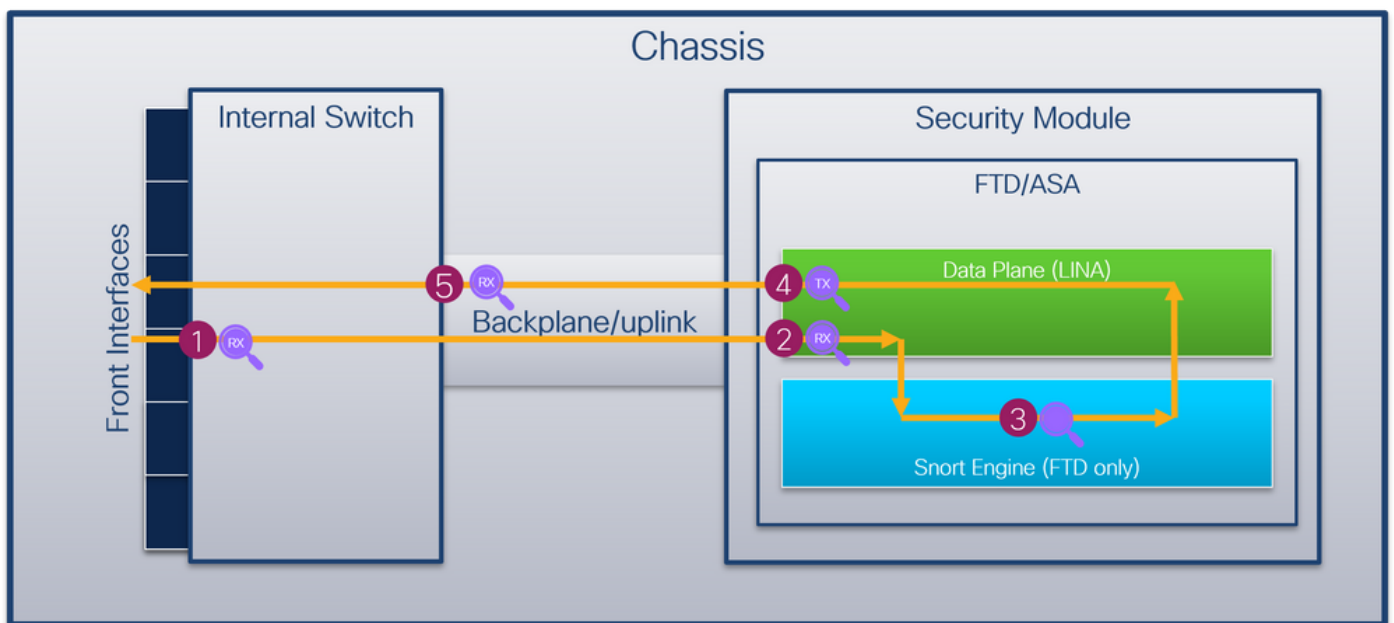
Como no Firepower 4100/9300, a marca de VLAN de porta é usada pelo switch interno para identificar uma interface.

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

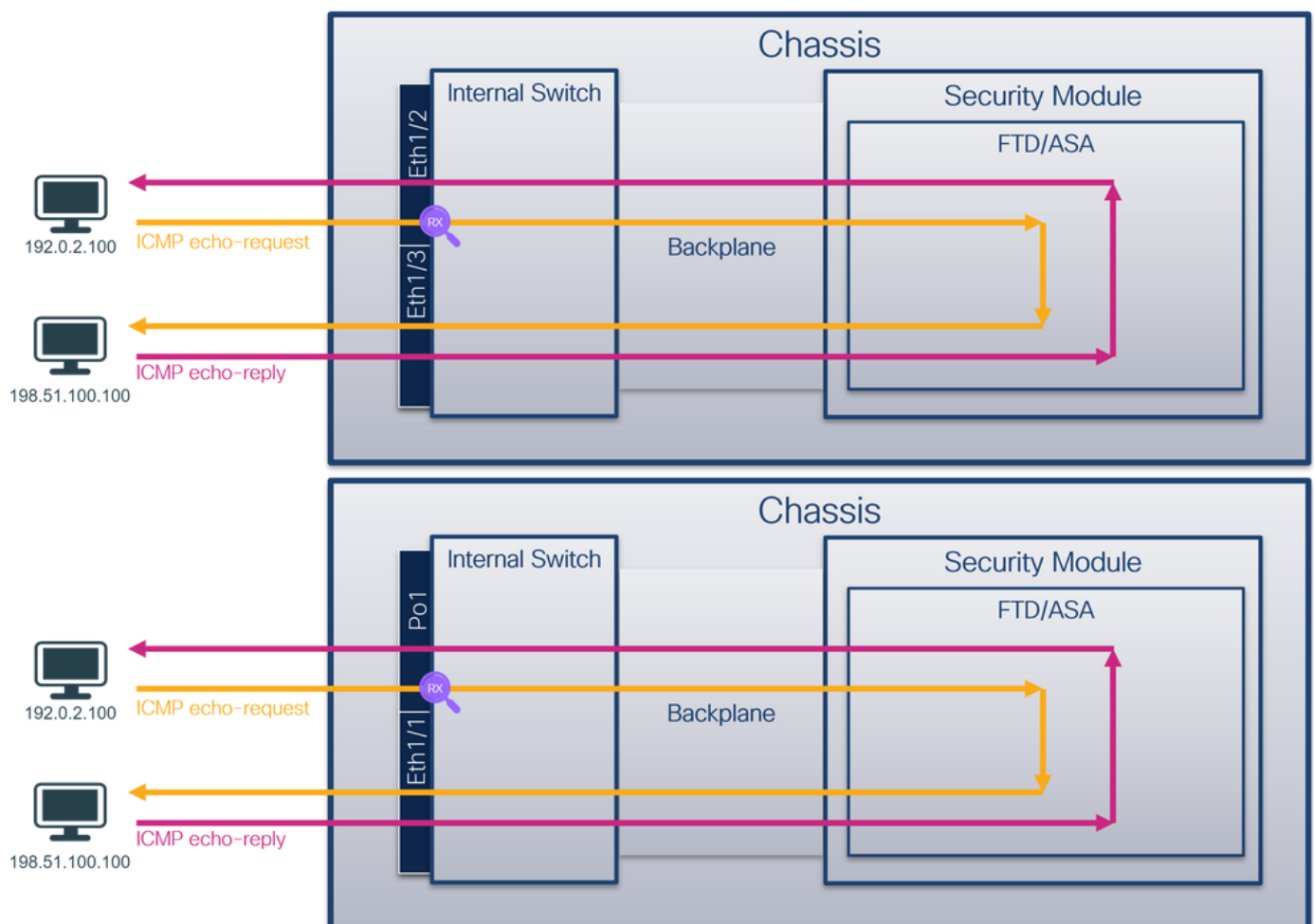
As capturas internas do switch Firepower 4100/9300 podem ser configuradas em **Ferramentas > Captura de pacotes** no FCM ou em **captura de pacote de escopo** no FXOS CLI. Para obter a descrição das opções de captura de pacote, consulte o *Guia de configuração do gerenciador de chassi FXOS do Cisco Firepower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

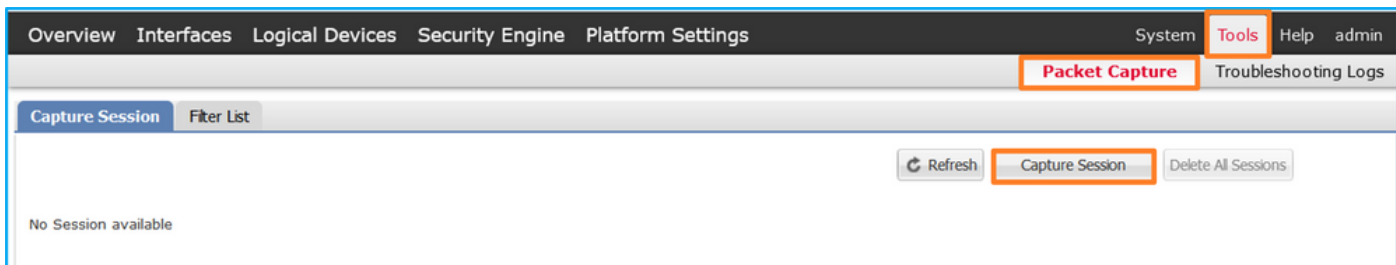


Configuração

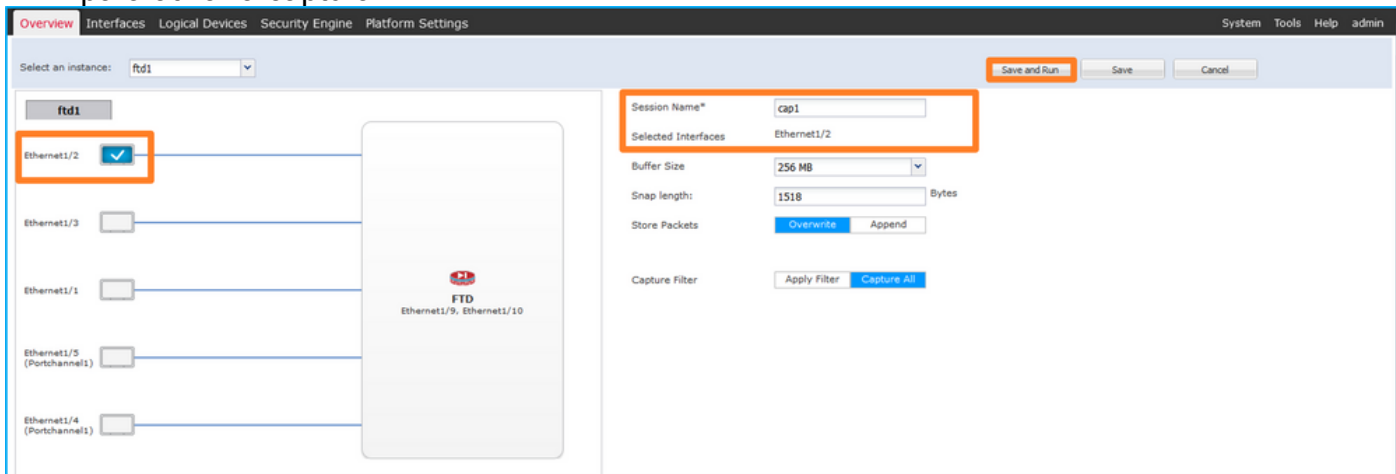
FCM

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

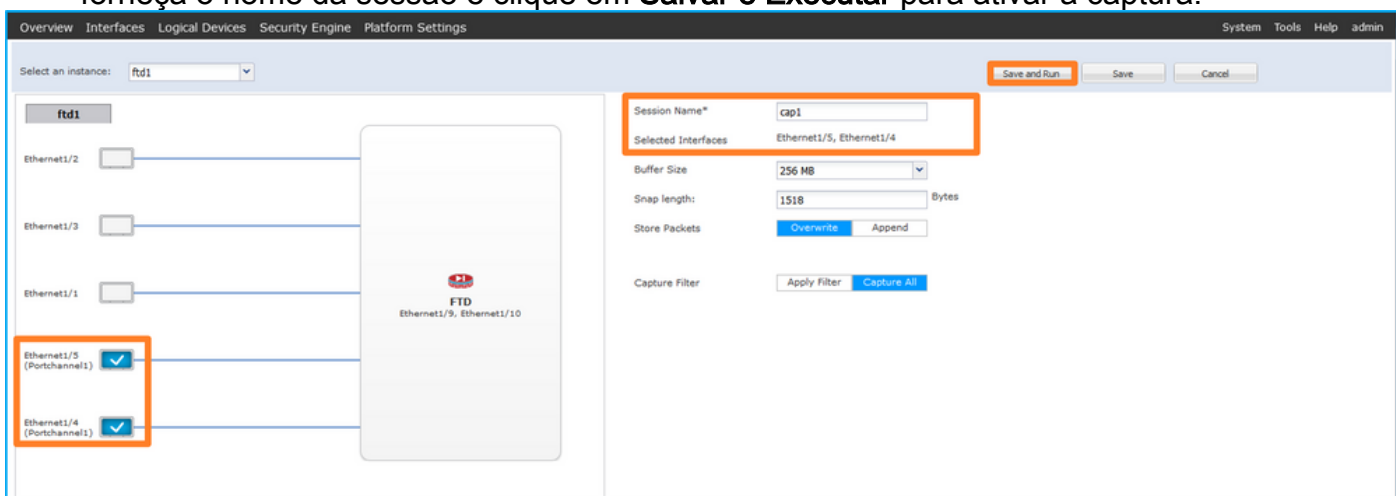
1. Use **Tools > Packet Capture > Capture Session** para criar uma nova sessão de captura:



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 #
```

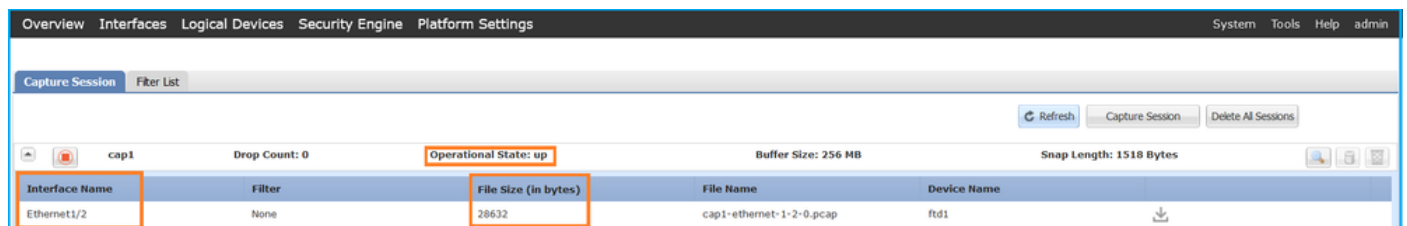
Para interfaces port-channel, uma captura separada para cada interface membro é configurada:

```
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

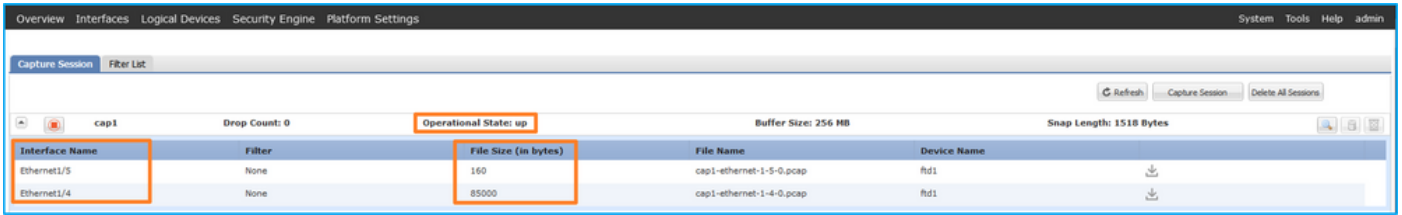
Verifique o nome da interface, certifique-se de que o status operacional esteja ativo e que o tamanho do arquivo (em bytes) aumente:



The screenshot shows the FCM interface with a capture session named 'cap1'. The session is active, with a drop count of 0, a buffer size of 256 MB, and a snap length of 1518 bytes. The operational state is 'up'. A table below the session details shows the captured files:

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

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



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

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.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-07-13 06:23:58.285000930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found)
2	2022-07-13 06:23:58.285082858	192.0.2.100	198.51.100.100	ICMP	102	0x9dec (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found)
3	2022-07-13 06:23:59.309948886	192.0.2.100	198.51.100.100	ICMP	108	0x9ed0 (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found)
4	2022-07-13 06:23:59.3099193731	192.0.2.100	198.51.100.100	ICMP	102	0x9ed0 (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found)
5	2022-07-13 06:24:00.333054190	192.0.2.100	198.51.100.100	ICMP	108	0x9f20 (40736)	64	Echo (ping) request id=0x001a, seq=9/2304, ttl=64 (no response found)
6	2022-07-13 06:24:00.333056014	192.0.2.100	198.51.100.100	ICMP	102	0x9f20 (40736)	64	Echo (ping) request id=0x001a, seq=9/2304, ttl=64 (no response found)
7	2022-07-13 06:24:01.357173530	192.0.2.100	198.51.100.100	ICMP	108	0x9f2d (40749)	64	Echo (ping) request id=0x001a, seq=10/2560, ttl=64 (no response found)
8	2022-07-13 06:24:01.357174708	192.0.2.100	198.51.100.100	ICMP	102	0x9f2d (40749)	64	Echo (ping) request id=0x001a, seq=10/2560, ttl=64 (no response found)
9	2022-07-13 06:24:02.381073741	192.0.2.100	198.51.100.100	ICMP	108	0x9f88 (40840)	64	Echo (ping) request id=0x001a, seq=11/2816, ttl=64 (no response found)
10	2022-07-13 06:24:02.381074999	192.0.2.100	198.51.100.100	ICMP	102	0x9f88 (40840)	64	Echo (ping) request id=0x001a, seq=11/2816, ttl=64 (no response found)
11	2022-07-13 06:24:03.405199041	192.0.2.100	198.51.100.100	ICMP	108	0xa077 (41079)	64	Echo (ping) request id=0x001a, seq=12/3072, ttl=64 (no response found)
12	2022-07-13 06:24:03.405200261	192.0.2.100	198.51.100.100	ICMP	102	0xa077 (41079)	64	Echo (ping) request id=0x001a, seq=12/3072, ttl=64 (no response found)
13	2022-07-13 06:24:04.429155683	192.0.2.100	198.51.100.100	ICMP	108	0xa10f (41231)	64	Echo (ping) request id=0x001a, seq=13/3328, ttl=64 (no response found)
14	2022-07-13 06:24:04.429155683	192.0.2.100	198.51.100.100	ICMP	102	0xa10f (41231)	64	Echo (ping) request id=0x001a, seq=13/3328, ttl=64 (no response found)
15	2022-07-13 06:24:05.453156612	192.0.2.100	198.51.100.100	ICMP	108	0xa16a (41322)	64	Echo (ping) request id=0x001a, seq=14/3584, ttl=64 (no response found)
16	2022-07-13 06:24:05.453158052	192.0.2.100	198.51.100.100	ICMP	102	0xa16a (41322)	64	Echo (ping) request id=0x001a, seq=14/3584, ttl=64 (no response found)
17	2022-07-13 06:24:06.477127687	192.0.2.100	198.51.100.100	ICMP	108	0xa1e9 (41449)	64	Echo (ping) request id=0x001a, seq=15/3840, ttl=64 (no response found)
18	2022-07-13 06:24:06.477129899	192.0.2.100	198.51.100.100	ICMP	102	0xa1e9 (41449)	64	Echo (ping) request id=0x001a, seq=15/3840, ttl=64 (no response found)
19	2022-07-13 06:24:07.501291314	192.0.2.100	198.51.100.100	ICMP	108	0xa1f6 (41462)	64	Echo (ping) request id=0x001a, seq=16/4096, ttl=64 (no response found)
20	2022-07-13 06:24:07.501293041	192.0.2.100	198.51.100.100	ICMP	102	0xa1f6 (41462)	64	Echo (ping) request id=0x001a, seq=16/4096, ttl=64 (no response found)
21	2022-07-13 06:24:08.525089956	192.0.2.100	198.51.100.100	ICMP	108	0xa257 (41559)	64	Echo (ping) request id=0x001a, seq=17/4352, ttl=64 (no response found)
22	2022-07-13 06:24:08.525092088	192.0.2.100	198.51.100.100	ICMP	102	0xa257 (41559)	64	Echo (ping) request id=0x001a, seq=17/4352, ttl=64 (no response found)
23	2022-07-13 06:24:09.549236500	192.0.2.100	198.51.100.100	ICMP	108	0xa2a9 (41641)	64	Echo (ping) request id=0x001a, seq=18/4608, ttl=64 (no response found)
24	2022-07-13 06:24:09.549238564	192.0.2.100	198.51.100.100	ICMP	102	0xa2a9 (41641)	64	Echo (ping) request id=0x001a, seq=18/4608, ttl=64 (no response found)
25	2022-07-13 06:24:10.573110146	192.0.2.100	198.51.100.100	ICMP	108	0xa345 (41797)	64	Echo (ping) request id=0x001a, seq=19/4864, ttl=64 (no response found)
26	2022-07-13 06:24:10.573112504	192.0.2.100	198.51.100.100	ICMP	102	0xa345 (41797)	64	Echo (ping) request id=0x001a, seq=19/4864, ttl=64 (no response found)
27	2022-07-13 06:24:11.597086027	192.0.2.100	198.51.100.100	ICMP	108	0xa349 (41801)	64	Echo (ping) request id=0x001a, seq=20/5120, ttl=64 (no response found)
28	2022-07-13 06:24:11.597088170	192.0.2.100	198.51.100.100	ICMP	102	0xa349 (41801)	64	Echo (ping) request id=0x001a, seq=20/5120, ttl=64 (no response found)
29	2022-07-13 06:24:12.621061022	192.0.2.100	198.51.100.100	ICMP	108	0xa3dc (41948)	64	Echo (ping) request id=0x001a, seq=21/5376, ttl=64 (no response found)


```

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

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.

The screenshot shows a Wireshark capture of ICMP Echo requests. The packet list pane at the top shows 19 packets, all ICMP Echo requests from source 192.0.2.100 to destination 198.51.100.100. The details pane for the selected packet (Frame 2) shows the following structure:

- Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: a2:76:f2:00:25 (a2:76:f2:00:25)
- 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1001
 - 000. = Priority: Best Effort (default) (0)
 - ...0 = DEI: Ineligible
 -0011 1110 1001 = ID: 1001
 - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
- Internet Control Message Protocol

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.

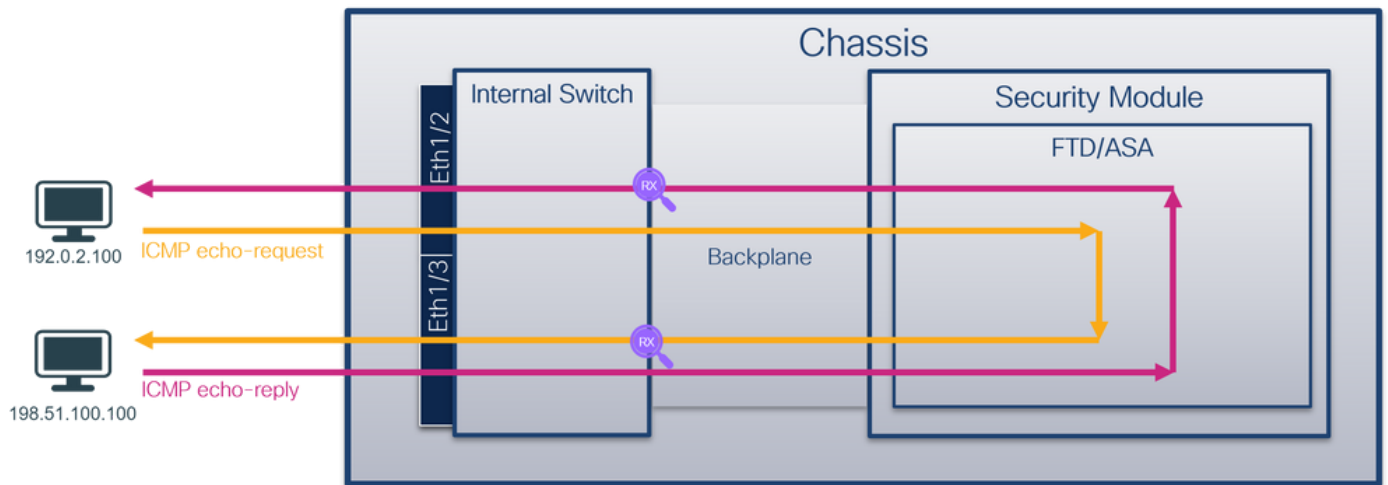
Esta tabela resume a tarefa:

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 host 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 host 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

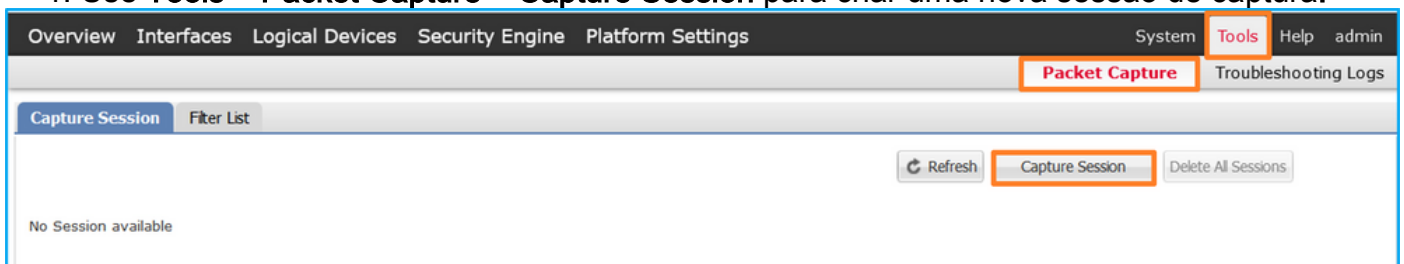


Configuração

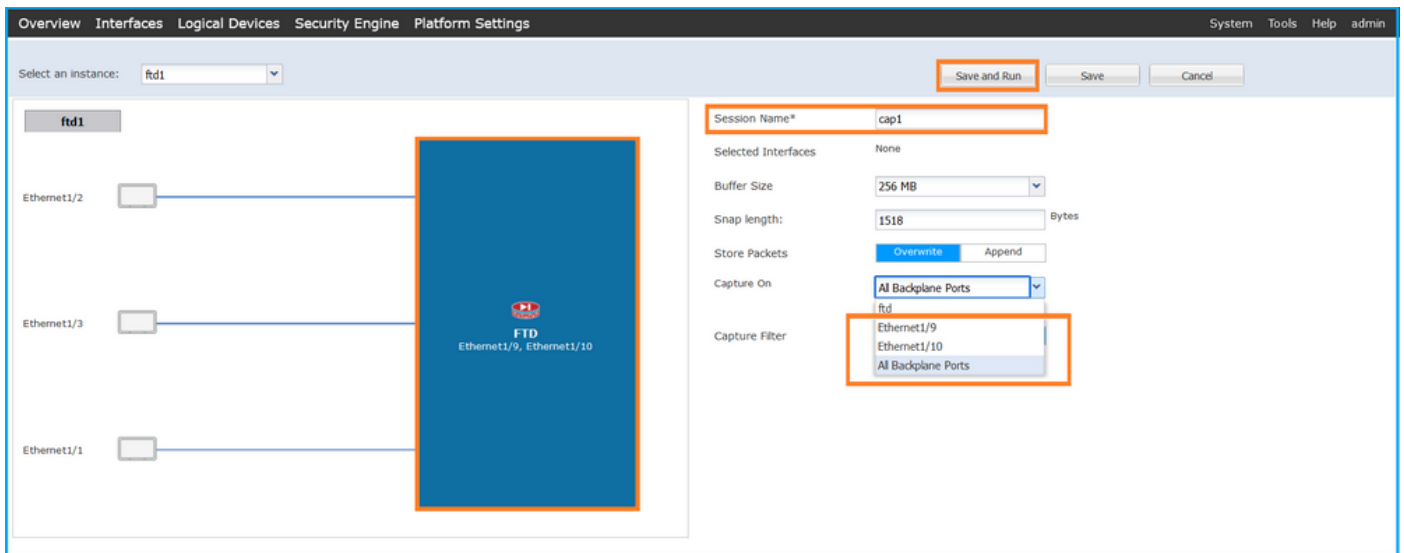
FCM

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:

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

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.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-07-14 20:20:36.513854256	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request
2	2022-07-14 20:20:36.513857289	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request
3	2022-07-14 20:20:36.514119394	198.51.100.100	192.0.2.100	ICMP	108	0xc2c2 (52268)	64	Echo (ping) reply
4	2022-07-14 20:20:36.514119312	198.51.100.100	192.0.2.100	ICMP	108	0xc2c2 (52268)	64	Echo (ping) reply


```

> Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
> Ethernet II, Src: Cisco b9:77:2d:58:97:bd:b9:77:2d, Dst: VMware 9d:e7:50 (00:50:56:9d:e7:50)
  > VN-Tag
    0..... = Direction: To Bridge
    .0..... = Pointer: vif_id
    ..0000 0000 0000..... = Destination: 0
    .....0..... = Looped: No
    .....0..... = Reserved: 0
    .....00..... = Version: 0
    .....0000 0000 1010 = Source: 10
    Type: 802.1Q Virtual LAN (0x8100)
  > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 103
    000..... = Priority: Best Effort (default) (0)
    ..0..... = DEI: Ineligible
    ....0000 0110 0111 = ID: 103
    Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
  > Internet Control Message Protocol
  
```

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-07-14 20:20:36.513854256	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request
2	2022-07-14 20:20:36.513857289	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request
3	2022-07-14 20:20:36.514119394	198.51.100.100	192.0.2.100	ICMP	108	0xc2c2 (52268)	64	Echo (ping) reply
4	2022-07-14 20:20:36.514119312	198.51.100.100	192.0.2.100	ICMP	108	0xc2c2 (52268)	64	Echo (ping) reply


```

> Frame 2: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
> Ethernet II, Src: Cisco b9:77:2d:58:97:bd:b9:77:2d, Dst: VMware 9d:e7:50 (00:50:56:9d:e7:50)
  > VN-Tag
    0..... = Direction: To Bridge
    .0..... = Pointer: vif_id
    ..0000 0000 0000..... = Destination: 0
    .....0..... = Looped: No
    .....0..... = Reserved: 0
    .....00..... = Version: 0
    .....0000 0000 1010 = Source: 10
    Type: 802.1Q Virtual LAN (0x8100)
  > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 103
    000..... = Priority: Best Effort (default) (0)
    ..0..... = DEI: Ineligible
    ....0000 0110 0111 = ID: 103
    Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
  > Internet Control Message Protocol
  
```

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

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

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

The image shows a Wireshark capture of ICMP Echo (ping) traffic. The packet list pane shows a request at 3:02:07-14 and a reply at 3:02:07-14. The packet details pane shows a 'VLAN-Tag' section with '802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102' and 'Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100'. The packet bytes pane shows the raw hex data of the packet.

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 host 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

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:

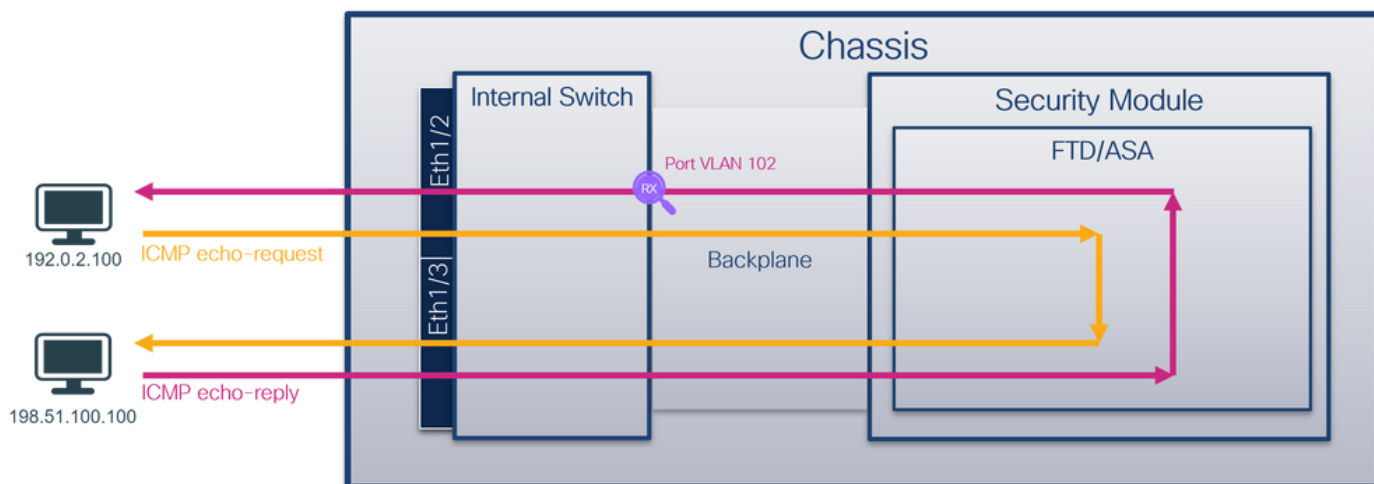
- Configurar capturas de pacotes nas interfaces do painel traseiro para pacotes que deixam uma interface frontal específica. Por exemplo, configure capturas de pacotes na interface Ethernet1/9 do painel traseiro para pacotes que deixam a interface Ethernet1/2.
- Configure capturas simultâneas de pacotes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

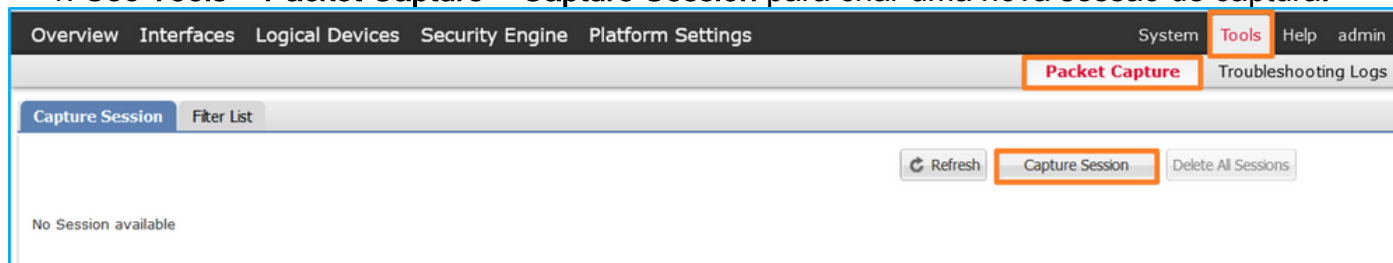


Configuração

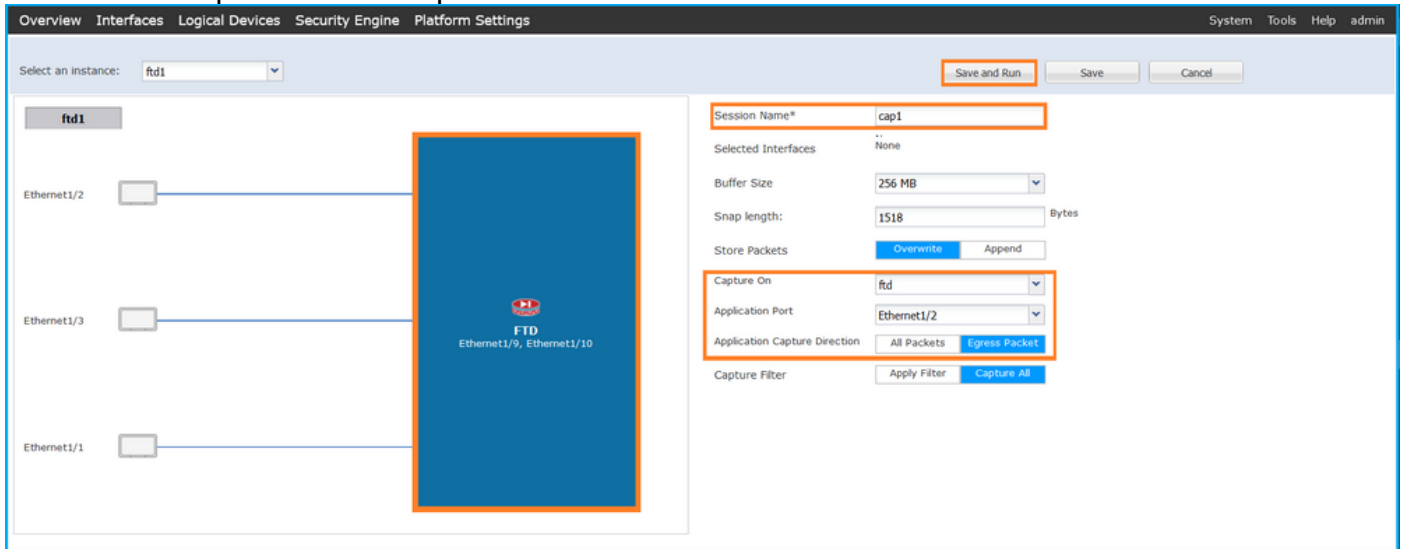
FCM

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:

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

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: 112
Port Name: Ethernet1/2
App Name: ftd
Sub Interface: 0
Application Instance Identifier: ftd1
```

Application ports resolved to:

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

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

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.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 10:03:22.231237959	198.51.100.100	192.0.2.100	ICMP	108	0x42f8 (17144)	64	Echo (ping) reply id=0x0012, seq=1/256, ttl=64
2	2022-08-01 10:03:22.2321239747	198.51.100.100	192.0.2.100	ICMP	108	0x42f8 (17144)	64	Echo (ping) reply id=0x0012, seq=1/256, ttl=64
3	2022-08-01 10:03:23.232244769	198.51.100.100	192.0.2.100	ICMP	108	0x4305 (17331)	64	Echo (ping) reply id=0x0012, seq=2/512, ttl=64
4	2022-08-01 10:03:23.2322447753	198.51.100.100	192.0.2.100	ICMP	108	0x4303 (17331)	64	Echo (ping) reply id=0x0012, seq=2/512, ttl=64
5	2022-08-01 10:03:24.234703981	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64	Echo (ping) reply id=0x0012, seq=3/768, ttl=64
6	2022-08-01 10:03:24.234706751	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64	Echo (ping) reply id=0x0012, seq=3/768, ttl=64
7	2022-08-01 10:03:25.258672449	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64	Echo (ping) reply id=0x0012, seq=4/1024, ttl=64
8	2022-08-01 10:03:25.258674861	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64	Echo (ping) reply id=0x0012, seq=4/1024, ttl=64
9	2022-08-01 10:03:26.282663169	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64	Echo (ping) reply id=0x0012, seq=5/1280, ttl=64
10	2022-08-01 10:03:26.282666183	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64	Echo (ping) reply id=0x0012, seq=5/1280, ttl=64
11	2022-08-01 10:03:27.306671694	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64	Echo (ping) reply id=0x0012, seq=6/1536, ttl=64
12	2022-08-01 10:03:27.306674378	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64	Echo (ping) reply id=0x0012, seq=6/1536, ttl=64
13	2022-08-01 10:03:28.330664677	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64	Echo (ping) reply id=0x0012, seq=7/1792, ttl=64
14	2022-08-01 10:03:28.330667153	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64	Echo (ping) reply id=0x0012, seq=7/1792, ttl=64
15	2022-08-01 10:03:29.354795931	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply id=0x0012, seq=8/2048, ttl=64
16	2022-08-01 10:03:29.354936706	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply id=0x0012, seq=8/2048, ttl=64
17	2022-08-01 10:03:30.378795204	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64	Echo (ping) reply id=0x0012, seq=9/2304, ttl=64
18	2022-08-01 10:03:30.378798172	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64	Echo (ping) reply id=0x0012, seq=9/2304, ttl=64
19	2022-08-01 10:03:31.402772217	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64	Echo (ping) reply id=0x0012, seq=10/2560, ttl=64
20	2022-08-01 10:03:31.402774775	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64	Echo (ping) reply id=0x0012, seq=10/2560, ttl=64
21	2022-08-01 10:03:32.426693254	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64	Echo (ping) reply id=0x0012, seq=11/2816, ttl=64
22	2022-08-01 10:03:32.426695691	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64	Echo (ping) reply id=0x0012, seq=11/2816, ttl=64


```

> Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
> Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VMware 9d:e8:be (00:50:56:9d:e8:be)
  0000  00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00  .PV...X...w-&...
  0010  00 0a 81 00 00 66 08 00 45 00 00 54 42 f8 00 00  ....f...E...TB...
  0020  40 01 4a b5 c6 33 64 64 c0 00 02 64 00 00 90 04  @...3dd...d...
  0030  00 12 00 01 dd a4 e7 62 00 00 00 00 e3 0d 09 00  ....:.....b.....
  0040  00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b  .........
  0050  1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b  ....!%$%()*+...
  0060  2c 2d 2e 2f 30 31 32 33 34 35 36 37              ,.-/0123 4567
  
```

```

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

The screenshot displays a network traffic capture. The top section is a table of packets, where the first column is 'No.', the second is 'Time', the third is 'Source', the fourth is 'Destination', the fifth is 'Protocol', the sixth is 'Length', the seventh is 'IP ID', the eighth is 'IP TTL', and the ninth is 'Info'. The packets are all ICMP Echo (ping) replies. The bottom section shows a detailed view of a packet frame, with fields like Ethernet II, VLAN-Tag, 802.1Q Virtual LAN, and Internet Protocol Version 4. Orange boxes and numbers 1, 2, 3, and 4 highlight specific fields in both views.

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	Soment Respostas de eco ICMP do host e 198.51.100.100 para o host entrada 192.0.2.100

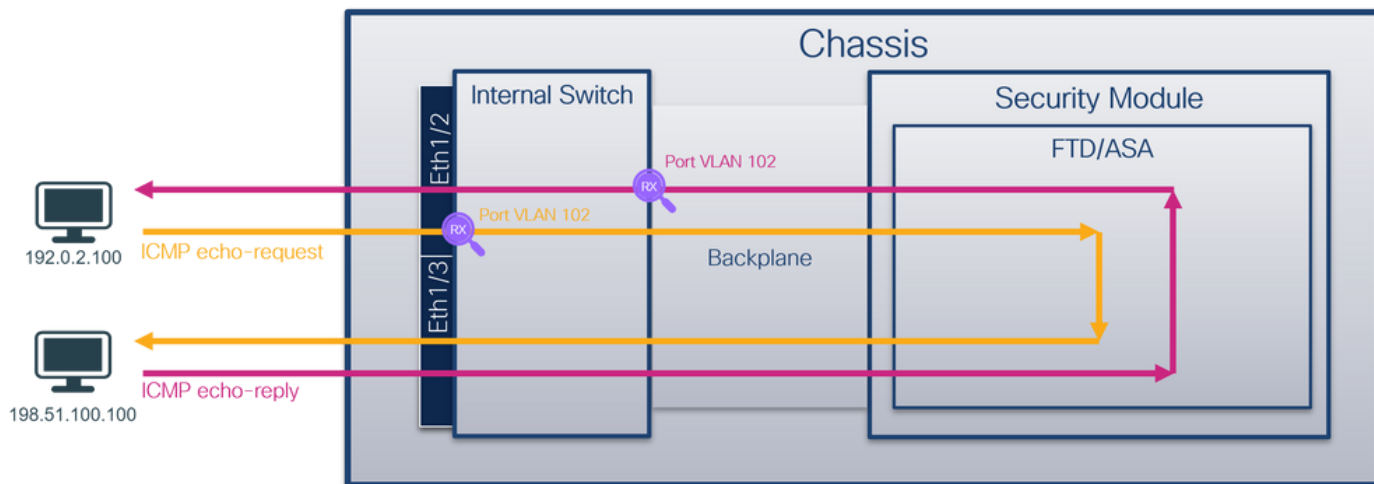
Tarefa 2

Use o FCM e uma 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

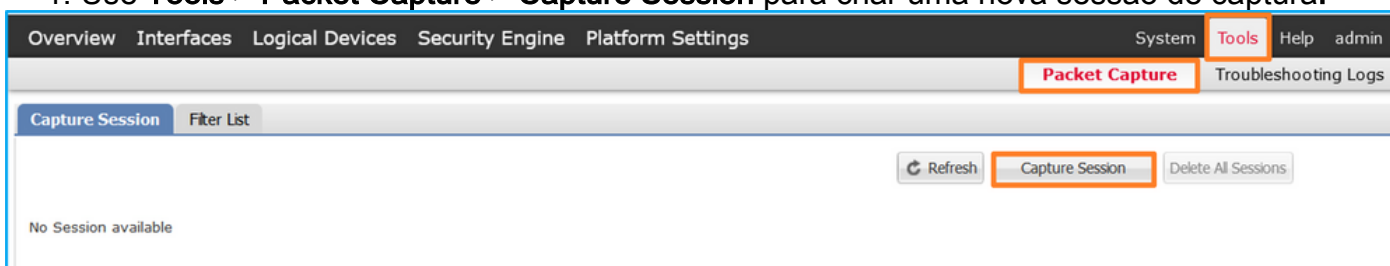


Configuração

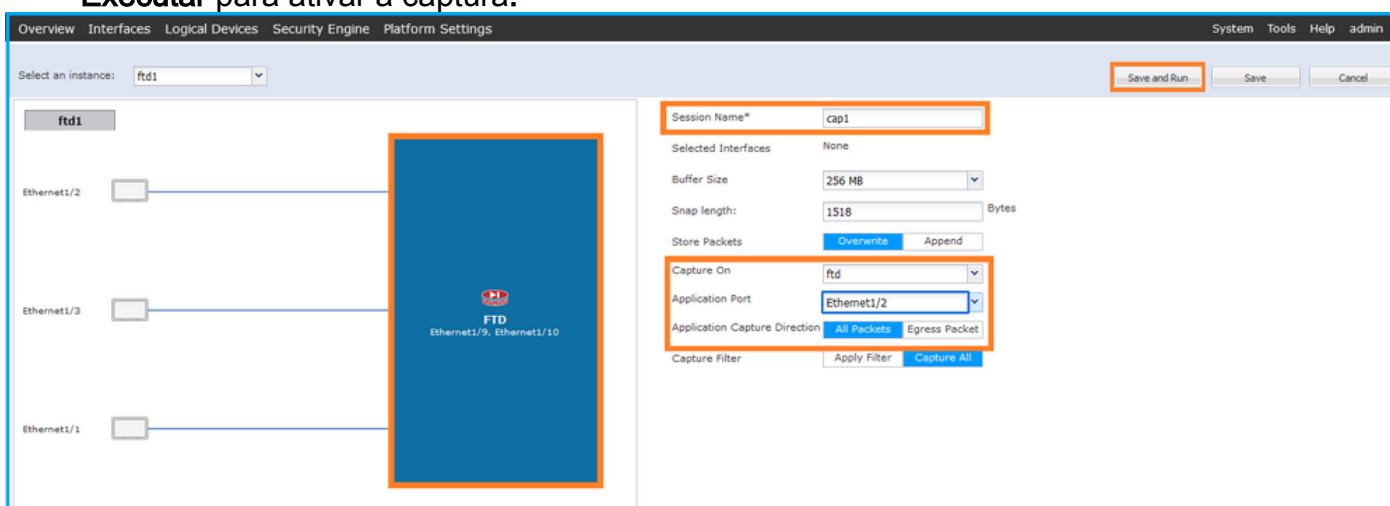
FCM

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:

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/2	None	95040	cap1-ethernet-1-2-0.pcap	fd1
Ethernet1/2 - Ethernet1/10	None	368	cap1-vethernet-1175.pcap	fd1
Ethernet1/2 - Ethernet1/9	None	13040	cap1-vethernet-1036.pcap	fd1

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.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 11:33:19.070693081	192.0.2.100	198.51.100.100	ICMP	108	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
2	2022-08-01 11:33:19.070695347	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
3	2022-08-01 11:33:19.071217121	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
4	2022-08-01 11:33:19.071218458	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
5	2022-08-01 11:33:20.072036625	192.0.2.100	198.51.100.100	ICMP	108	0xc0ae (49326)	64	Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found)
6	2022-08-01 11:33:20.072038399	192.0.2.100	198.51.100.100	ICMP	102	0xc0ae (49326)	64	Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found)
7	2022-08-01 11:33:21.073266930	192.0.2.100	198.51.100.100	ICMP	108	0xc167 (49511)	64	Echo (ping) request id=0x0013, seq=3/768, ttl=64 (no response found)
8	2022-08-01 11:33:21.073268327	192.0.2.100	198.51.100.100	ICMP	102	0xc167 (49511)	64	Echo (ping) request id=0x0013, seq=3/768, ttl=64 (no response found)
9	2022-08-01 11:33:22.074576640	192.0.2.100	198.51.100.100	ICMP	108	0xc175 (49525)	64	Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found)
10	2022-08-01 11:33:22.074578010	192.0.2.100	198.51.100.100	ICMP	102	0xc175 (49525)	64	Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found)
11	2022-08-01 11:33:23.075799089	192.0.2.100	198.51.100.100	ICMP	108	0xc208 (49672)	64	Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found)
12	2022-08-01 11:33:23.07581513	192.0.2.100	198.51.100.100	ICMP	102	0xc208 (49672)	64	Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found)
13	2022-08-01 11:33:24.081839490	192.0.2.100	198.51.100.100	ICMP	108	0xc211 (49681)	64	Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found)
14	2022-08-01 11:33:24.081841386	192.0.2.100	198.51.100.100	ICMP	102	0xc211 (49681)	64	Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found)
15	2022-08-01 11:33:25.105806249	192.0.2.100	198.51.100.100	ICMP	108	0xc2e2 (49890)	64	Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found)
16	2022-08-01 11:33:25.105807895	192.0.2.100	198.51.100.100	ICMP	102	0xc2e2 (49890)	64	Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found)
17	2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	ICMP	108	0xc3b4 (50100)	64	Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found)
18	2022-08-01 11:33:26.129838114	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100)	64	Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found)
19	2022-08-01 11:33:27.153828653	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found)
20	2022-08-01 11:33:27.153830201	192.0.2.100	198.51.100.100	ICMP	102	0xc476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found)
21	2022-08-01 11:33:28.17847175	192.0.2.100	198.51.100.100	ICMP	108	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found)
22	2022-08-01 11:33:28.17849075	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found)
23	2022-08-01 11:33:29.201804760	192.0.2.100	198.51.100.100	ICMP	108	0xc578 (50552)	64	Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found)
24	2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	102	0xc578 (50552)	64	Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found)
25	2022-08-01 11:33:30.225834765	192.0.2.100	198.51.100.100	ICMP	108	0xc585 (50565)	64	Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found)
26	2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (50565)	64	Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found)
27	2022-08-01 11:33:31.249828955	192.0.2.100	198.51.100.100	ICMP	108	0xc618 (50712)	64	Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found)
28	2022-08-01 11:33:31.249831121	192.0.2.100	198.51.100.100	ICMP	102	0xc618 (50712)	64	Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found)
29	2022-08-01 11:33:32.273867960	192.0.2.100	198.51.100.100	ICMP	108	0xc64f (50767)	64	Echo (ping) request id=0x0013, seq=14/3584, ttl=64 (no response found)

Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_1, id 0
 Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)

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

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

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

```

0000 58 97 bd b9 77 0e 00 50 56 9d e8 be 89 26 80 0a  X...w...P V...&..
0010 00 00 81 00 00 66 08 00 45 00 00 54 c0 09 40 00  ..E...T...@....
0020 40 01 8d a3 c0 00 02 64 c6 33 64 00 00 8d 7c    @.....d .3dd...|
0030 00 13 00 01 f2 b9 e7 62 00 00 00 00 cb 7f 06 00  ....b.....
0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b  .........
0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b  ..*558()*+...
0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37           ,./01234567
  
```

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.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 11:33:19.070693081	192.0.2.100	198.51.100.100	ICMP	108	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
2	2022-08-01 11:33:19.070695347	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
3	2022-08-01 11:33:19.071217121	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
4	2022-08-01 11:33:19.071218458	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
5	2022-08-01 11:33:20.072036625	192.0.2.100	198.51.100.100	ICMP	108	0xc0ae (49326)	64	Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found)
6	2022-08-01 11:33:20.072038399	192.0.2.100	198.51.100.100	ICMP	102	0xc0ae (49326)	64	Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found)
7	2022-08-01 11:33:21.073266930	192.0.2.100	198.51.100.100	ICMP	108	0xc167 (49511)	64	Echo (ping) request id=0x0013, seq=3/768, ttl=64 (no response found)
8	2022-08-01 11:33:21.073268327	192.0.2.100	198.51.100.100	ICMP	102	0xc167 (49511)	64	Echo (ping) request id=0x0013, seq=3/768, ttl=64 (no response found)
9	2022-08-01 11:33:22.074576640	192.0.2.100	198.51.100.100	ICMP	108	0xc175 (49525)	64	Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found)
10	2022-08-01 11:33:22.074578010	192.0.2.100	198.51.100.100	ICMP	102	0xc175 (49525)	64	Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found)
11	2022-08-01 11:33:23.075799089	192.0.2.100	198.51.100.100	ICMP	108	0xc208 (49672)	64	Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found)
12	2022-08-01 11:33:23.07581513	192.0.2.100	198.51.100.100	ICMP	102	0xc208 (49672)	64	Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found)
13	2022-08-01 11:33:24.081839490	192.0.2.100	198.51.100.100	ICMP	108	0xc211 (49681)	64	Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found)
14	2022-08-01 11:33:24.081841386	192.0.2.100	198.51.100.100	ICMP	102	0xc211 (49681)	64	Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found)
15	2022-08-01 11:33:25.105806249	192.0.2.100	198.51.100.100	ICMP	108	0xc2e2 (49890)	64	Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found)
16	2022-08-01 11:33:25.105807895	192.0.2.100	198.51.100.100	ICMP	102	0xc2e2 (49890)	64	Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found)
17	2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	ICMP	108	0xc3b4 (50100)	64	Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found)
18	2022-08-01 11:33:26.129838114	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100)	64	Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found)
19	2022-08-01 11:33:27.153828653	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found)
20	2022-08-01 11:33:27.153830201	192.0.2.100	198.51.100.100	ICMP	102	0xc476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found)
21	2022-08-01 11:33:28.17847175	192.0.2.100	198.51.100.100	ICMP	108	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found)
22	2022-08-01 11:33:28.17849075	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found)
23	2022-08-01 11:33:29.201804760	192.0.2.100	198.51.100.100	ICMP	108	0xc578 (50552)	64	Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found)
24	2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	102	0xc578 (50552)	64	Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found)
25	2022-08-01 11:33:30.225834765	192.0.2.100	198.51.100.100	ICMP	108	0xc585 (50565)	64	Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found)
26	2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (50565)	64	Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found)
27	2022-08-01 11:33:31.249828955	192.0.2.100	198.51.100.100	ICMP	108	0xc618 (50712)	64	Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found)
28	2022-08-01 11:33:31.249831121	192.0.2.100	198.51.100.100	ICMP	102	0xc618 (50712)	64	Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found)
29	2022-08-01 11:33:32.273867960	192.0.2.100	198.51.100.100	ICMP	108	0xc64f (50767)	64	Echo (ping) request id=0x0013, seq=14/3584, ttl=64 (no response found)

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

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

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

```

0000 58 97 bd b9 77 0e 00 50 56 9d e8 be 81 00 00 66  X...w...P V.....f
0010 00 00 45 00 00 54 c0 09 40 00 00 40 01 8d a3 c0  ..E...T...@....
0020 02 64 c6 33 64 00 00 8d 7c 00 13 00 01 f2 b9 e7 62 00 00 00 00 cb 7f 06 00 11  ..b.....
0030 e7 62 00 00 00 00 cb 7f 06 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37  ..*558()*+.../01234567
  
```

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.

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

1 0x4f27 (20263) 64 Echo (ping) reply id=0x0013, seq=1/256, ttl=64

2 0x4f27 (20263) 64 Echo (ping) reply id=0x0013, seq=1/256, ttl=64

3 0xa170 (20475) 64 Echo (ping) reply id=0x0013, seq=2/512, ttl=64

4 0x4ffb (20475) 64 Echo (ping) reply id=0x0013, seq=2/512, ttl=64

5 0x50ac (20652) 64 Echo (ping) reply id=0x0013, seq=3/768, ttl=64

6 0x50ac (20652) 64 Echo (ping) reply id=0x0013, seq=3/768, ttl=64

7 0x513e (20798) 64 Echo (ping) reply id=0x0013, seq=4/1024, ttl=64

8 0x513e (20798) 64 Echo (ping) reply id=0x0013, seq=4/1024, ttl=64

9 0x51c9 (20937) 64 Echo (ping) reply id=0x0013, seq=5/1280, ttl=64

10 0x51c9 (20937) 64 Echo (ping) reply id=0x0013, seq=5/1280, ttl=64

11 0x528e (21134) 64 Echo (ping) reply id=0x0013, seq=6/1536, ttl=64

12 0x528e (21134) 64 Echo (ping) reply id=0x0013, seq=6/1536, ttl=64

13 0x52af (21167) 64 Echo (ping) reply id=0x0013, seq=7/1792, ttl=64

14 0x52af (21167) 64 Echo (ping) reply id=0x0013, seq=7/1792, ttl=64

15 0x53a6 (21414) 64 Echo (ping) reply id=0x0013, seq=8/2048, ttl=64

16 0x53a6 (21414) 64 Echo (ping) reply id=0x0013, seq=8/2048, ttl=64

17 0x5446 (21574) 64 Echo (ping) reply id=0x0013, seq=9/2304, ttl=64

18 0x5446 (21574) 64 Echo (ping) reply id=0x0013, seq=9/2304, ttl=64

19 0x5493 (21651) 64 Echo (ping) reply id=0x0013, seq=10/2560, ttl=64

20 0x5493 (21651) 64 Echo (ping) reply id=0x0013, seq=10/2560, ttl=64

21 0x54f4 (21748) 64 Echo (ping) reply id=0x0013, seq=11/2816, ttl=64

22 0x54f4 (21748) 64 Echo (ping) reply id=0x0013, seq=11/2816, ttl=64

23 0x5526 (21798) 64 Echo (ping) reply id=0x0013, seq=12/3072, ttl=64

24 0x5526 (21798) 64 Echo (ping) reply id=0x0013, seq=12/3072, ttl=64

25 0x55f2 (22002) 64 Echo (ping) reply id=0x0013, seq=13/3328, ttl=64

26 0x55f2 (22002) 64 Echo (ping) reply id=0x0013, seq=13/3328, ttl=64

27 0x5660 (22112) 64 Echo (ping) reply id=0x0013, seq=14/3584, ttl=64

28 0x5660 (22112) 64 Echo (ping) reply id=0x0013, seq=14/3584, ttl=64

29 0x56e7 (22247) 64 Echo (ping) reply id=0x0013, seq=15/3840, ttl=64

0000 00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00 --PV...X...w-&...
0010 00 0a 81 00 00 66 08 00 45 00 00 54 4f 27 00 00F...E...TO...
0020 40 01 3e 86 c6 33 64 64 c0 00 02 64 00 00 95 7c @->...3dd...d...|
0030 00 13 00 01 f2 b9 e7 62 00 00 00 00 cb 7f 06 00b...
0040 00 00 00 00 11 12 13 14 15 16 17 18 19 1a 1b
0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2bl"*\$%&'()*+
0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,.-./0123 4567 ,.-./0123 4567

4 0x8100 802.1Q Virtual LAN (0x8100)

3 0x0800 Type: IPv4 (0x0800)

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

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.

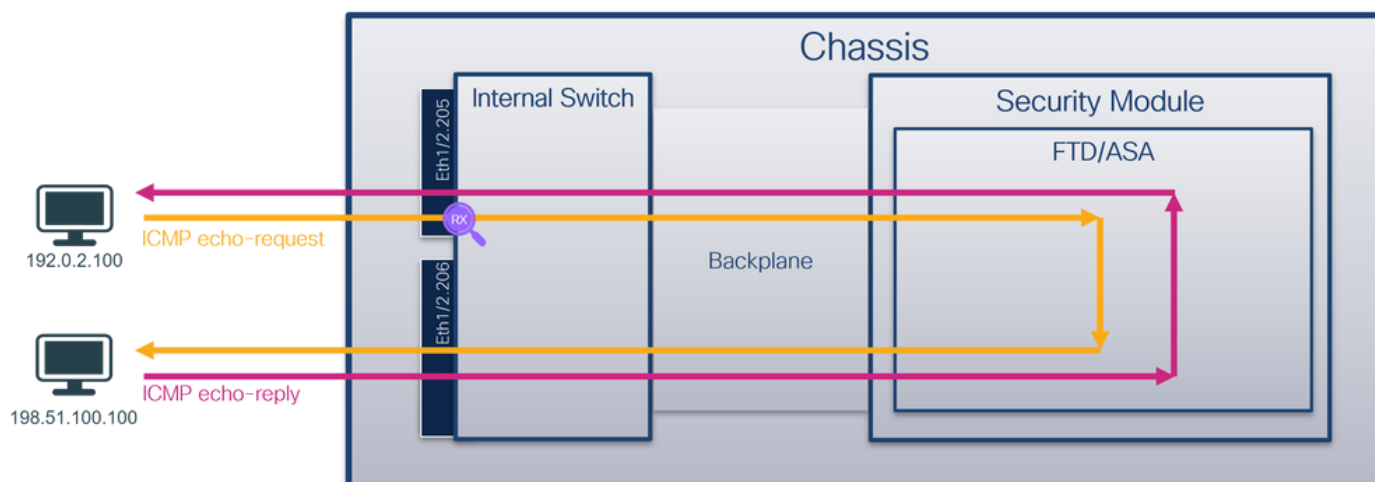
Esta tabela resume a tarefa:

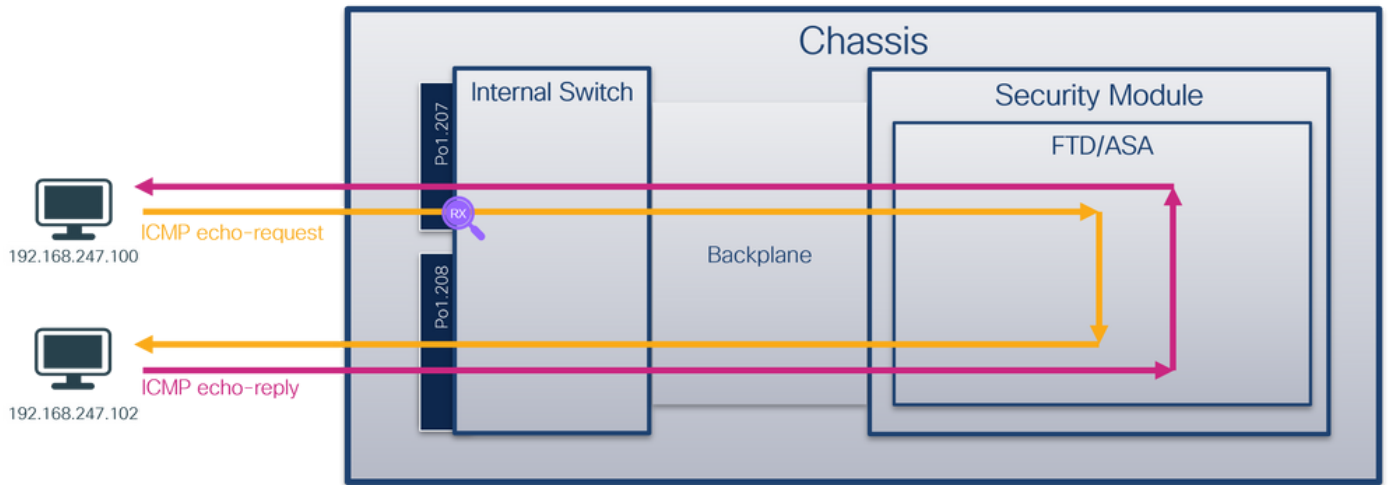
Tarefa	Ponto de captura	VLAN de porta interna em pacotes capturados	Direção	Tráfego capturado
Configurar e verificar capturas na porta Ethernet1/2 do aplicativo e do aplicativo	Interfaces de backplane	102	Somente entrada	Respostas de eco ICMP do host 198.51.100.100 para o host 192.0.2.100
	Interface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



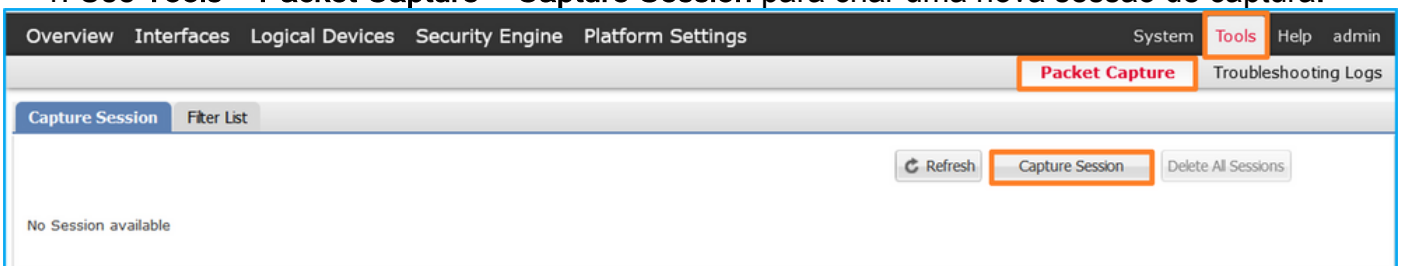


Configuração

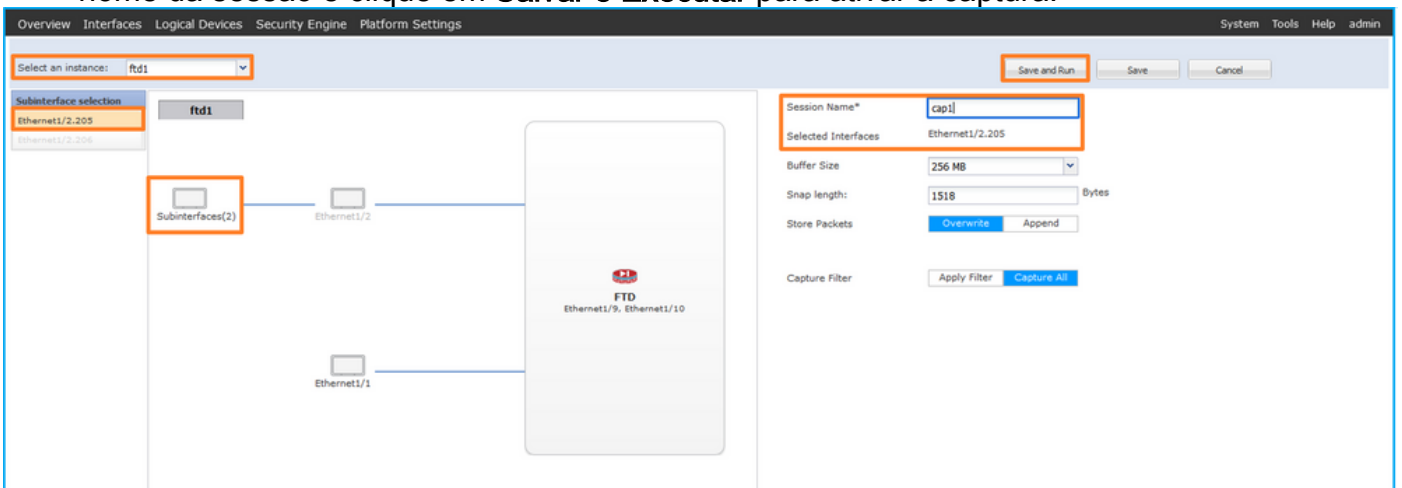
FCM

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 [CSCvg3119](#), 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:

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/2/205	None	233992	cap1-ethernet-1-2-0.pcap	fd1

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

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/4/207	None	624160	cap1-ethernet-1-4-0.pcap	Not available
Ethernet1/3/207	None	160	cap1-ethernet-1-3-0.pcap	Not available

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.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-04 07:21:56.993302102	192.0.2.100	198.51.100.100	ICMP	112	0x9574 (38260)	64	Echo (ping) request id=0x0022, seq=1/256, ttl=64 (no response found)
2	2022-08-04 07:21:56.993303597	192.0.2.100	198.51.100.100	ICMP	102	0x9574 (38260)	64	Echo (ping) request id=0x0022, seq=1/256, ttl=64 (no response found)
3	2022-08-04 07:22:06.214264777	192.0.2.100	198.51.100.100	ICMP	112	0x9a81 (39553)	64	Echo (ping) request id=0x0022, seq=10/2560, ttl=64 (no response found)
4	2022-08-04 07:22:06.214267373	192.0.2.100	198.51.100.100	ICMP	102	0x9a81 (39553)	64	Echo (ping) request id=0x0022, seq=10/2560, ttl=64 (no response found)
5	2022-08-04 07:22:07.215113393	192.0.2.100	198.51.100.100	ICMP	112	0x9ac3 (39619)	64	Echo (ping) request id=0x0022, seq=11/2816, ttl=64 (no response found)
6	2022-08-04 07:22:07.215115445	192.0.2.100	198.51.100.100	ICMP	102	0x9ac3 (39619)	64	Echo (ping) request id=0x0022, seq=11/2816, ttl=64 (no response found)
7	2022-08-04 07:22:08.229938577	192.0.2.100	198.51.100.100	ICMP	112	0x9b33 (39731)	64	Echo (ping) request id=0x0022, seq=12/3072, ttl=64 (no response found)
8	2022-08-04 07:22:08.229940829	192.0.2.100	198.51.100.100	ICMP	102	0x9b33 (39731)	64	Echo (ping) request id=0x0022, seq=12/3072, ttl=64 (no response found)
9	2022-08-04 07:22:09.253944601	192.0.2.100	198.51.100.100	ICMP	112	0x9c0e (39950)	64	Echo (ping) request id=0x0022, seq=13/3328, ttl=64 (no response found)
10	2022-08-04 07:22:09.253946899	192.0.2.100	198.51.100.100	ICMP	102	0x9c0e (39950)	64	Echo (ping) request id=0x0022, seq=13/3328, ttl=64 (no response found)
11	2022-08-04 07:22:10.277953070	192.0.2.100	198.51.100.100	ICMP	112	0x9ccb (40139)	64	Echo (ping) request id=0x0022, seq=14/3584, ttl=64 (no response found)
12	2022-08-04 07:22:10.277954736	192.0.2.100	198.51.100.100	ICMP	102	0x9ccb (40139)	64	Echo (ping) request id=0x0022, seq=14/3584, ttl=64 (no response found)
13	2022-08-04 07:22:11.301931282	192.0.2.100	198.51.100.100	ICMP	112	0x9d84 (40324)	64	Echo (ping) request id=0x0022, seq=15/3840, ttl=64 (no response found)
14	2022-08-04 07:22:11.301933600	192.0.2.100	198.51.100.100	ICMP	102	0x9d84 (40324)	64	Echo (ping) request id=0x0022, seq=15/3840, ttl=64 (no response found)
15	2022-08-04 07:22:12.325936521	192.0.2.100	198.51.100.100	ICMP	112	0x9da2 (40354)	64	Echo (ping) request id=0x0022, seq=16/4096, ttl=64 (no response found)
16	2022-08-04 07:22:12.325937895	192.0.2.100	198.51.100.100	ICMP	102	0x9da2 (40354)	64	Echo (ping) request id=0x0022, seq=16/4096, ttl=64 (no response found)
17	2022-08-04 07:22:13.326988040	192.0.2.100	198.51.100.100	ICMP	112	0x9e07 (40455)	64	Echo (ping) request id=0x0022, seq=17/4352, ttl=64 (no response found)
18	2022-08-04 07:22:13.326990258	192.0.2.100	198.51.100.100	ICMP	102	0x9e07 (40455)	64	Echo (ping) request id=0x0022, seq=17/4352, ttl=64 (no response found)
19	2022-08-04 07:22:14.341944773	192.0.2.100	198.51.100.100	ICMP	112	0x9e6a (40554)	64	Echo (ping) request id=0x0022, seq=18/4608, ttl=64 (no response found)
20	2022-08-04 07:22:14.341946249	192.0.2.100	198.51.100.100	ICMP	102	0x9e6a (40554)	64	Echo (ping) request id=0x0022, seq=18/4608, ttl=64 (no response found)
21	2022-08-04 07:22:15.365941588	192.0.2.100	198.51.100.100	ICMP	112	0x9efb (40699)	64	Echo (ping) request id=0x0022, seq=19/4864, ttl=64 (no response found)
22	2022-08-04 07:22:15.365942566	192.0.2.100	198.51.100.100	ICMP	102	0x9efb (40699)	64	Echo (ping) request id=0x0022, seq=19/4864, ttl=64 (no response found)
23	2022-08-04 07:22:16.389973843	192.0.2.100	198.51.100.100	ICMP	112	0x9f08 (40936)	64	Echo (ping) request id=0x0022, seq=20/5120, ttl=64 (no response found)
24	2022-08-04 07:22:16.389975129	192.0.2.100	198.51.100.100	ICMP	102	0x9f08 (40936)	64	Echo (ping) request id=0x0022, seq=20/5120, ttl=64 (no response found)
25	2022-08-04 07:22:17.413936452	192.0.2.100	198.51.100.100	ICMP	112	0xa079 (41081)	64	Echo (ping) request id=0x0022, seq=21/5376, ttl=64 (no response found)
26	2022-08-04 07:22:17.413938090	192.0.2.100	198.51.100.100	ICMP	102	0xa079 (41081)	64	Echo (ping) request id=0x0022, seq=21/5376, ttl=64 (no response found)
27	2022-08-04 07:22:18.437954335	192.0.2.100	198.51.100.100	ICMP	112	0xa11e (41246)	64	Echo (ping) request id=0x0022, seq=22/5632, ttl=64 (no response found)

```

> Frame 11: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface capture_u0_1, id 0
> Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: a2:76:f2:00:00:1b (a2:76:f2:00:00:1b)
  > VNI-Tag
    1. .... = Direction: From Bridge
    ..0. .... = Pointer: vif_id
    ..00 0000 0101 0100 .... = Destination: 84
    ....0. .... = Looped: No
    ....0. .... = Reserved: 0
    ....00 .... = Version: 0
    ....0000 0000 0000 = Source: 0
    Type: 802.1Q Virtual LAN (0x8100)
  > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
    000. .... = Priority: Best Effort (default) (0)
    ..0 .... = DEI: Ineligible
    ....0000 0110 0110 = ID: 102
    Type: 802.1Q Virtual LAN (0x8100)
  > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 205
    000. .... = Priority: Best Effort (default) (0)
    ..0 .... = DEI: Ineligible
    ....0000 1100 1101 = ID: 205
    Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
  > Internet Control Message Protocol
  
```

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.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-04 07:21:56.993302102	192.0.2.100	198.51.100.100	ICMP	112	0x9574 (38260)	64	Echo (ping) request id=0x0022, seq=1/256, ttl=64 (no response found)
2	2022-08-04 07:21:56.993303597	192.0.2.100	198.51.100.100	ICMP	102	0x9574 (38260)	64	Echo (ping) request id=0x0022, seq=1/256, ttl=64 (no response found)
3	2022-08-04 07:22:06.214264777	192.0.2.100	198.51.100.100	ICMP	112	0x9a81 (39553)	64	Echo (ping) request id=0x0022, seq=10/2560, ttl=64 (no response found)
4	2022-08-04 07:22:06.214267373	192.0.2.100	198.51.100.100	ICMP	102	0x9a81 (39553)	64	Echo (ping) request id=0x0022, seq=10/2560, ttl=64 (no response found)
5	2022-08-04 07:22:07.215113393	192.0.2.100	198.51.100.100	ICMP	112	0x9ac3 (39619)	64	Echo (ping) request id=0x0022, seq=11/2816, ttl=64 (no response found)
6	2022-08-04 07:22:07.215115445	192.0.2.100	198.51.100.100	ICMP	102	0x9ac3 (39619)	64	Echo (ping) request id=0x0022, seq=11/2816, ttl=64 (no response found)
7	2022-08-04 07:22:08.229938577	192.0.2.100	198.51.100.100	ICMP	112	0x9b33 (39731)	64	Echo (ping) request id=0x0022, seq=12/3072, ttl=64 (no response found)
8	2022-08-04 07:22:08.229940829	192.0.2.100	198.51.100.100	ICMP	102	0x9b33 (39731)	64	Echo (ping) request id=0x0022, seq=12/3072, ttl=64 (no response found)
9	2022-08-04 07:22:09.253944601	192.0.2.100	198.51.100.100	ICMP	112	0x9c0e (39950)	64	Echo (ping) request id=0x0022, seq=13/3328, ttl=64 (no response found)
10	2022-08-04 07:22:09.253946899	192.0.2.100	198.51.100.100	ICMP	102	0x9c0e (39950)	64	Echo (ping) request id=0x0022, seq=13/3328, ttl=64 (no response found)
11	2022-08-04 07:22:10.277953070	192.0.2.100	198.51.100.100	ICMP	112	0x9ccb (40139)	64	Echo (ping) request id=0x0022, seq=14/3584, ttl=64 (no response found)
12	2022-08-04 07:22:10.277954736	192.0.2.100	198.51.100.100	ICMP	102	0x9ccb (40139)	64	Echo (ping) request id=0x0022, seq=14/3584, ttl=64 (no response found)
13	2022-08-04 07:22:11.301931282	192.0.2.100	198.51.100.100	ICMP	112	0x9d84 (40324)	64	Echo (ping) request id=0x0022, seq=15/3840, ttl=64 (no response found)
14	2022-08-04 07:22:11.301933600	192.0.2.100	198.51.100.100	ICMP	102	0x9d84 (40324)	64	Echo (ping) request id=0x0022, seq=15/3840, ttl=64 (no response found)
15	2022-08-04 07:22:12.325936521	192.0.2.100	198.51.100.100	ICMP	112	0x9da2 (40354)	64	Echo (ping) request id=0x0022, seq=16/4096, ttl=64 (no response found)
16	2022-08-04 07:22:12.325937895	192.0.2.100	198.51.100.100	ICMP	102	0x9da2 (40354)	64	Echo (ping) request id=0x0022, seq=16/4096, ttl=64 (no response found)
17	2022-08-04 07:22:13.326988040	192.0.2.100	198.51.100.100	ICMP	112	0x9e07 (40455)	64	Echo (ping) request id=0x0022, seq=17/4352, ttl=64 (no response found)
18	2022-08-04 07:22:13.326990258	192.0.2.100	198.51.100.100	ICMP	102	0x9e07 (40455)	64	Echo (ping) request id=0x0022, seq=17/4352, ttl=64 (no response found)
19	2022-08-04 07:22:14.341944773	192.0.2.100	198.51.100.100	ICMP	112	0x9e6a (40554)	64	Echo (ping) request id=0x0022, seq=18/4608, ttl=64 (no response found)
20	2022-08-04 07:22:14.341946249	192.0.2.100	198.51.100.100	ICMP	102	0x9e6a (40554)	64	Echo (ping) request id=0x0022, seq=18/4608, ttl=64 (no response found)
21	2022-08-04 07:22:15.365941588	192.0.2.100	198.51.100.100	ICMP	112	0x9efb (40699)	64	Echo (ping) request id=0x0022, seq=19/4864, ttl=64 (no response found)
22	2022-08-04 07:22:15.365942566	192.0.2.100	198.51.100.100	ICMP	102	0x9efb (40699)	64	Echo (ping) request id=0x0022, seq=19/4864, ttl=64 (no response found)
23	2022-08-04 07:22:16.389973843	192.0.2.100	198.51.100.100	ICMP	112	0x9f08 (40936)	64	Echo (ping) request id=0x0022, seq=20/5120, ttl=64 (no response found)
24	2022-08-04 07:22:16.389975129	192.0.2.100	198.51.100.100	ICMP	102	0x9f08 (40936)	64	Echo (ping) request id=0x0022, seq=20/5120, ttl=64 (no response found)
25	2022-08-04 07:22:17.413936452	192.0.2.100	198.51.100.100	ICMP	112	0xa079 (41081)	64	Echo (ping) request id=0x0022, seq=21/5376, ttl=64 (no response found)
26	2022-08-04 07:22:17.413938090	192.0.2.100	198.51.100.100	ICMP	102	0xa079 (41081)	64	Echo (ping) request id=0x0022, seq=21/5376, ttl=64 (no response found)
27	2022-08-04 07:22:18.437954335	192.0.2.100	198.51.100.100	ICMP	112	0xa11e (41246)	64	Echo (ping) request id=0x0022, seq=22/5632, ttl=64 (no response found)

```

> Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture_u0_1, id 0
> Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: a2:76:f2:00:00:1b (a2:76:f2:00:00:1b)
  > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 205
    000. .... = Priority: Best Effort (default) (0)
    ..0 .... = DEI: Ineligible
    ....0000 1100 1101 = ID: 205
    Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
  > Internet Control Message Protocol
  
```

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.

Frame 1: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface capture_u0_3, id 0
Ethernet II, Src: Cisco d6iec:00 (00:17:df:d6:ec:00), Dst: a2:76:f2:00:00:1c (a2:76:f2:00:00:1c)

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

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

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

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

Seleção 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.

Frame 2: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface capture_u0_3, id 0
Ethernet II, Src: Cisco d6iec:00 (00:17:df:d6:ec:00), Dst: a2:76:f2:00:00:1c (a2:76:f2:00:00:1c)

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

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

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.

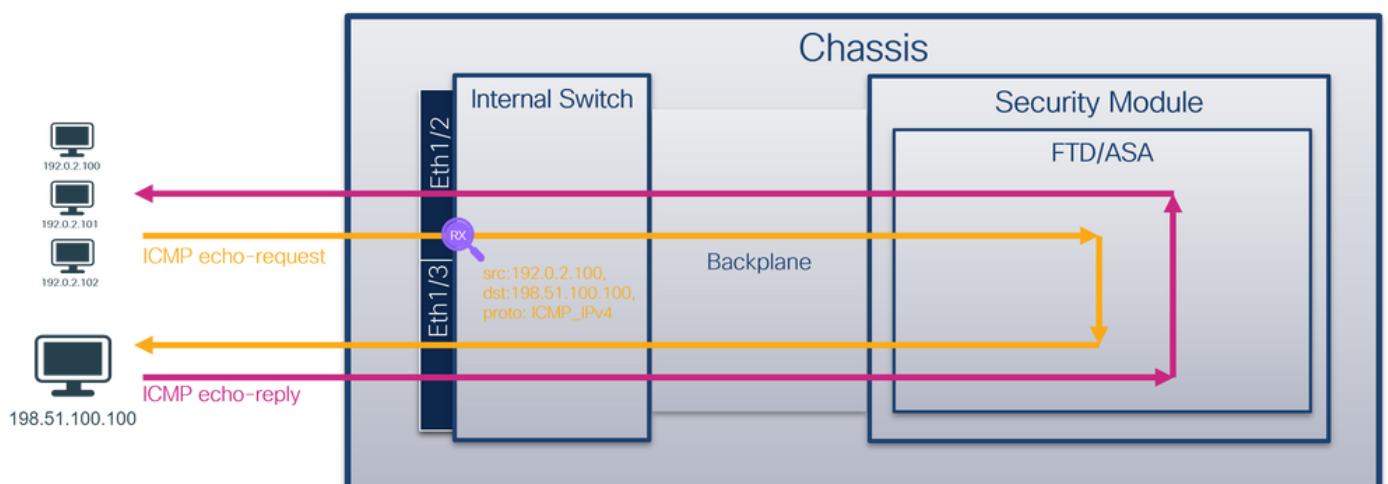
Esta tabela resume a tarefa:

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	Soment e 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 com as interfaces membro Ethernet1/3 e Ethernet1/4	Ethernet1/3 Ethernet1/4	1001	Soment e 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

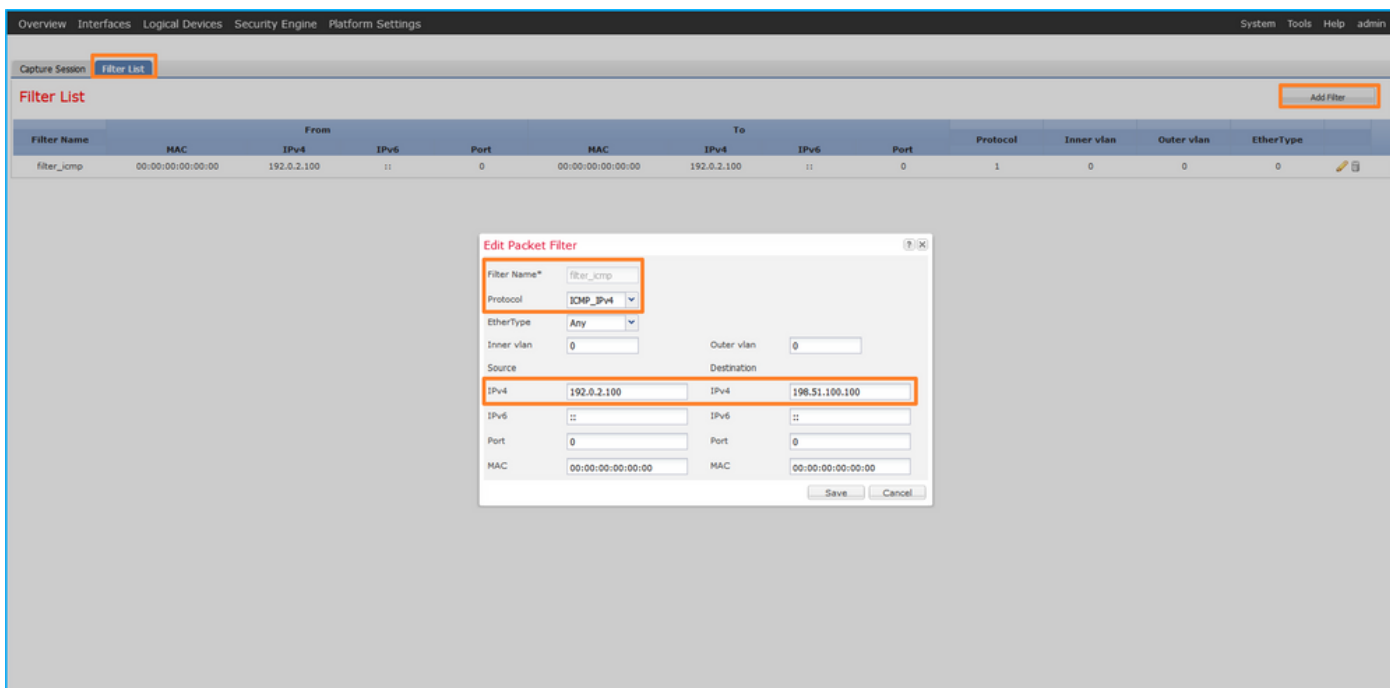


Configuração

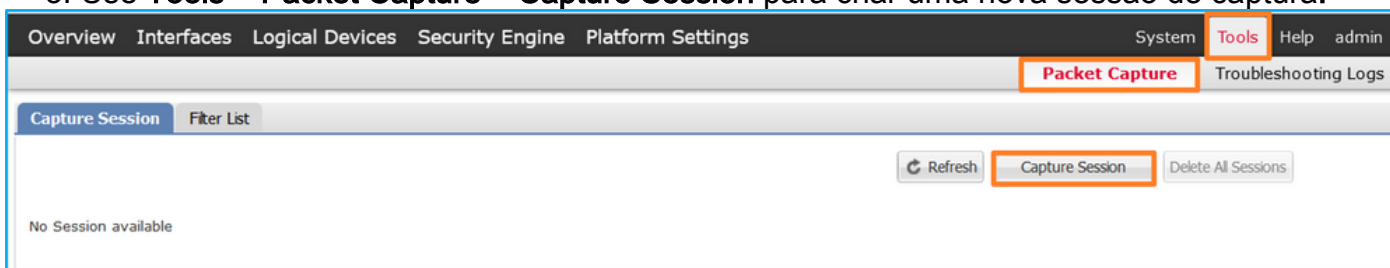
FCM

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:

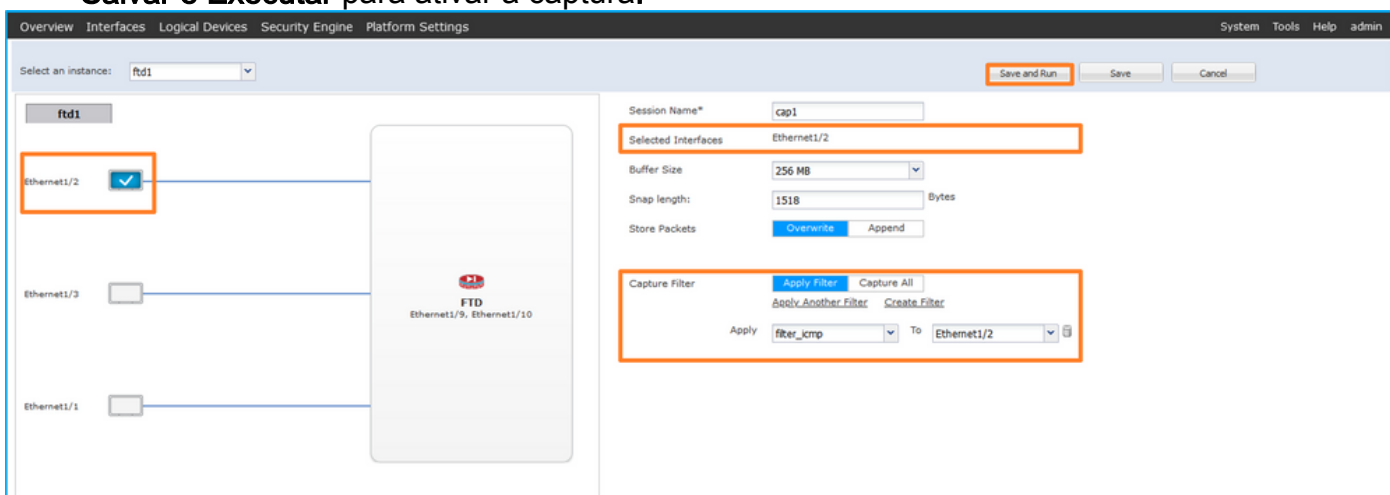
1. Use **Tools > Packet Capture > Filter List > Add Filter** para criar um filtro de captura.
2. Especifique o **Nome do filtro, Protocolo, IPv4 origem, IPv4 destino** e clique em **Salvar**:



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:

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

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:

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

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.

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

Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_1, i
 Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)

VN-Tag

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

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

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

Seleção 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.

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

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

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

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

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

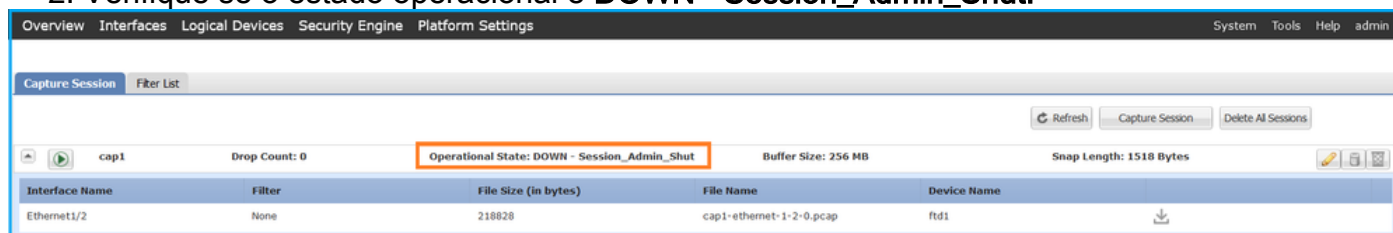
FCM

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 o Guia 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 ativo.
- 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.

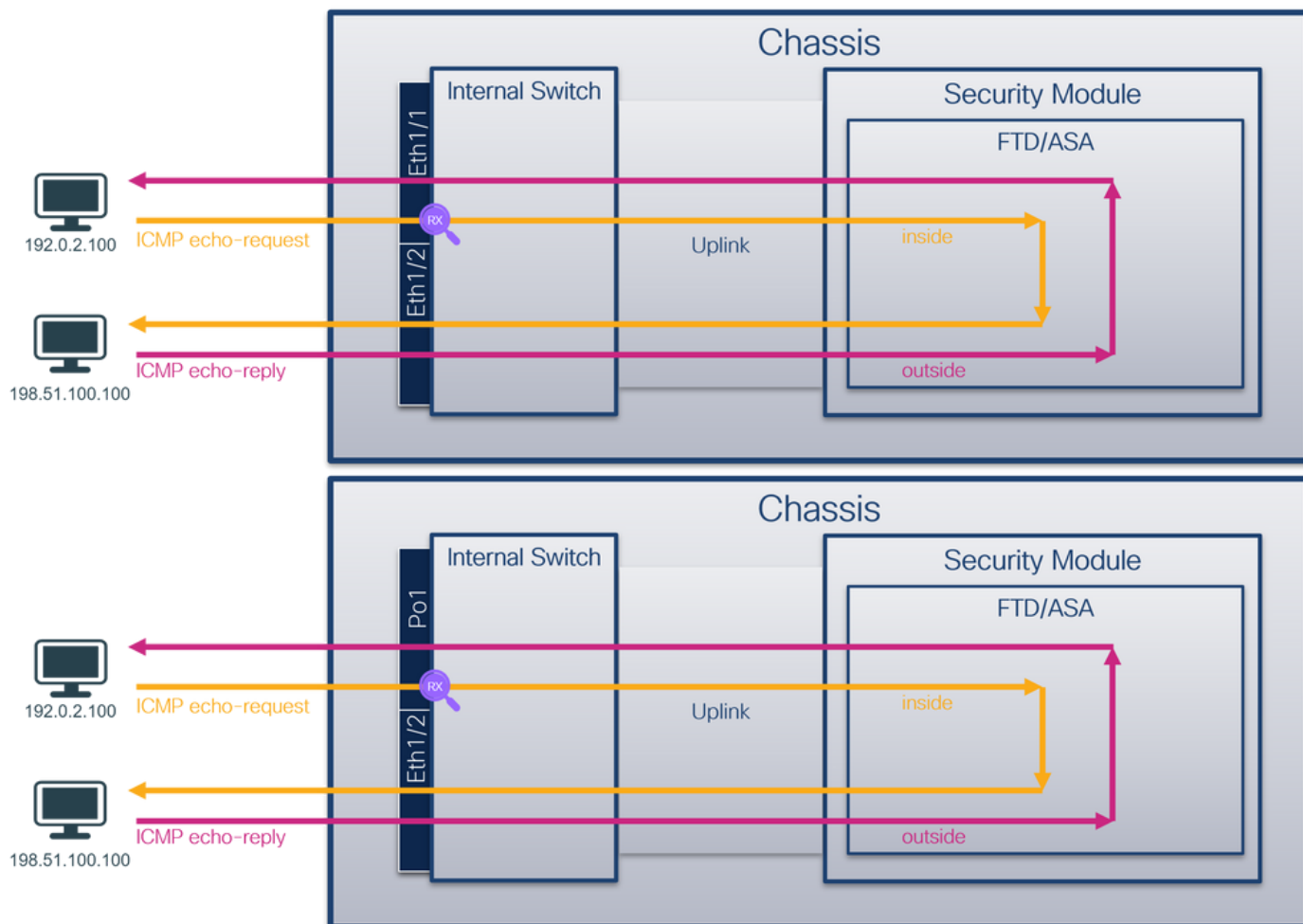
Esses cenários cobrem casos de uso comuns de capturas de switches internos do Secure

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.

No.	Time	Source	Destination	Protocol	Length	IP ID	TTL	Info
1	2022-08-07 19:50:06.925768	192.0.2.100	198.51.100.100	ICMP	102	0x9a10 (39440)	64	Echo (ping) request id=0x0034, seq=1/256, ttl=64 (no res
2	2022-08-07 19:50:07.921684	192.0.2.100	198.51.100.100	ICMP	102	0x9a3a (39482)	64	Echo (ping) request id=0x0034, seq=2/512, ttl=64 (no res
3	2022-08-07 19:50:08.924468	192.0.2.100	198.51.100.100	ICMP	102	0x9aa6 (39590)	64	Echo (ping) request id=0x0034, seq=3/768, ttl=64 (no res
4	2022-08-07 19:50:09.928484	192.0.2.100	198.51.100.100	ICMP	102	0x9afe (39678)	64	Echo (ping) request id=0x0034, seq=4/1024, ttl=64 (no re
5	2022-08-07 19:50:10.928245	192.0.2.100	198.51.100.100	ICMP	102	0x9b10 (39696)	64	Echo (ping) request id=0x0034, seq=5/1280, ttl=64 (no re
6	2022-08-07 19:50:11.929144	192.0.2.100	198.51.100.100	ICMP	102	0x9b34 (39732)	64	Echo (ping) request id=0x0034, seq=6/1536, ttl=64 (no re
7	2022-08-07 19:50:12.932943	192.0.2.100	198.51.100.100	ICMP	102	0x9b83 (39811)	64	Echo (ping) request id=0x0034, seq=7/1792, ttl=64 (no re
8	2022-08-07 19:50:13.934155	192.0.2.100	198.51.100.100	ICMP	102	0x9b8b (39819)	64	Echo (ping) request id=0x0034, seq=8/2048, ttl=64 (no re
9	2022-08-07 19:50:14.932804	192.0.2.100	198.51.100.100	ICMP	102	0x9c07 (39943)	64	Echo (ping) request id=0x0034, seq=9/2304, ttl=64 (no re
10	2022-08-07 19:50:15.937143	192.0.2.100	198.51.100.100	ICMP	102	0x9cc6 (40134)	64	Echo (ping) request id=0x0034, seq=10/2560, ttl=64 (no r
11	2022-08-07 19:50:16.934848	192.0.2.100	198.51.100.100	ICMP	102	0x9d68 (40296)	64	Echo (ping) request id=0x0034, seq=11/2816, ttl=64 (no r
12	2022-08-07 19:50:17.936908	192.0.2.100	198.51.100.100	ICMP	102	0x9ded (40429)	64	Echo (ping) request id=0x0034, seq=12/3072, ttl=64 (no r
13	2022-08-07 19:50:18.939584	192.0.2.100	198.51.100.100	ICMP	102	0x9e5a (40538)	64	Echo (ping) request id=0x0034, seq=13/3328, ttl=64 (no r
14	2022-08-07 19:50:19.941262	192.0.2.100	198.51.100.100	ICMP	102	0x9ef6 (40699)	64	Echo (ping) request id=0x0034, seq=14/3584, ttl=64 (no r
15	2022-08-07 19:50:20.940716	192.0.2.100	198.51.100.100	ICMP	102	0x9ffb (40874)	64	Echo (ping) request id=0x0034, seq=15/3840, ttl=64 (no r
16	2022-08-07 19:50:21.940288	192.0.2.100	198.51.100.100	ICMP	102	0x9fe4 (40932)	64	Echo (ping) request id=0x0034, seq=16/4096, ttl=64 (no r
17	2022-08-07 19:50:22.943307	192.0.2.100	198.51.100.100	ICMP	102	0xa031 (41009)	64	Echo (ping) request id=0x0034, seq=17/4352, ttl=64 (no r
18	2022-08-07 19:50:23.944679	192.0.2.100	198.51.100.100	ICMP	102	0xa067 (41063)	64	Echo (ping) request id=0x0034, seq=18/4608, ttl=64 (no r

Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)		0000	bc e7 12 34 9a 14 00 50 56 9d e8 be 08 00 45 00P.V.....E-
Ethernet II, Src: VMware_9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco_34:9a:14 (bc:e7:12:34:9a:14)		0010	00 54 9a 10 40 00 40 01 b3 9c c0 00 02 64 c6 33	.T.@.@.....d:3
Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100		0020	64 64 08 00 c6 91 00 34 00 01 61 17 f0 62 00 00	dd...4...a-b-
Internet Control Message Protocol		0030	00 00 18 ec 08 00 00 00 00 00 10 11 12 13 14 15
		0040	16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25!""#%&
		0050	26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35	&'()*+,-./012345
		0060	36 37 55 55 55 55	67UUUU

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.

No.	Time	Source	Destination	Protocol	Length	IP ID	TTL	Info
1	2022-08-07 20:40:58.657533	192.0.2.100	198.51.100.100	ICMP	102	0x9296 (37526)	64	Echo (ping) request id=0x0035, seq=1/256, ttl=64 (no res
2	2022-08-07 20:40:59.658611	192.0.2.100	198.51.100.100	ICMP	102	0x9370 (37744)	64	Echo (ping) request id=0x0035, seq=2/512, ttl=64 (no res
3	2022-08-07 20:41:00.655662	192.0.2.100	198.51.100.100	ICMP	102	0x93f0 (37872)	64	Echo (ping) request id=0x0035, seq=3/768, ttl=64 (no res
4	2022-08-07 20:41:01.659749	192.0.2.100	198.51.100.100	ICMP	102	0x946f (37999)	64	Echo (ping) request id=0x0035, seq=4/1024, ttl=64 (no re
5	2022-08-07 20:41:02.660624	192.0.2.100	198.51.100.100	ICMP	102	0x94a4 (38052)	64	Echo (ping) request id=0x0035, seq=5/1280, ttl=64 (no re
6	2022-08-07 20:41:03.663226	192.0.2.100	198.51.100.100	ICMP	102	0x952d (38189)	64	Echo (ping) request id=0x0035, seq=6/1536, ttl=64 (no re
7	2022-08-07 20:41:04.661262	192.0.2.100	198.51.100.100	ICMP	102	0x958d (38285)	64	Echo (ping) request id=0x0035, seq=7/1792, ttl=64 (no re
8	2022-08-07 20:41:05.665955	192.0.2.100	198.51.100.100	ICMP	102	0x95d8 (38360)	64	Echo (ping) request id=0x0035, seq=8/2048, ttl=64 (no re
9	2022-08-07 20:41:06.666538	192.0.2.100	198.51.100.100	ICMP	102	0x964b (38475)	64	Echo (ping) request id=0x0035, seq=9/2304, ttl=64 (no re
10	2022-08-07 20:41:07.667298	192.0.2.100	198.51.100.100	ICMP	102	0x972b (38699)	64	Echo (ping) request id=0x0035, seq=10/2560, ttl=64 (no r
11	2022-08-07 20:41:08.670540	192.0.2.100	198.51.100.100	ICMP	102	0x980a (38922)	64	Echo (ping) request id=0x0035, seq=11/2816, ttl=64 (no r
12	2022-08-07 20:41:09.668278	192.0.2.100	198.51.100.100	ICMP	102	0x9831 (38961)	64	Echo (ping) request id=0x0035, seq=12/3072, ttl=64 (no r
13	2022-08-07 20:41:10.672417	192.0.2.100	198.51.100.100	ICMP	102	0x98a2 (39074)	64	Echo (ping) request id=0x0035, seq=13/3328, ttl=64 (no r
14	2022-08-07 20:41:11.671369	192.0.2.100	198.51.100.100	ICMP	102	0x98f7 (39159)	64	Echo (ping) request id=0x0035, seq=14/3584, ttl=64 (no r
15	2022-08-07 20:41:12.675462	192.0.2.100	198.51.100.100	ICMP	102	0x99e4 (39396)	64	Echo (ping) request id=0x0035, seq=15/3840, ttl=64 (no r
16	2022-08-07 20:41:13.674993	192.0.2.100	198.51.100.100	ICMP	102	0x9a84 (39556)	64	Echo (ping) request id=0x0035, seq=16/4096, ttl=64 (no r
17	2022-08-07 20:41:14.674093	192.0.2.100	198.51.100.100	ICMP	102	0x9af3 (39667)	64	Echo (ping) request id=0x0035, seq=17/4352, ttl=64 (no r
18	2022-08-07 20:41:15.676904	192.0.2.100	198.51.100.100	ICMP	102	0x9b8e (39822)	64	Echo (ping) request id=0x0035, seq=18/4608, ttl=64 (no r

Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)		0000	bc e7 12 34 9a 2c 00 50 56 9d e8 be 08 00 45 00P.V.....E-
Ethernet II, Src: VMware_9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco_34:9a:2c (bc:e7:12:34:9a:2c)		0010	00 54 92 96 40 00 40 01 bb 16 c0 00 02 64 c6 33	.T.@.@.....d:3
Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100		0020	64 64 08 00 58 a8 00 35 00 01 4d 23 f0 62 00 00	dd-X.5...MH.b-
Internet Control Message Protocol		0030	00 00 9e c8 04 00 00 00 00 00 10 11 12 13 14 15
		0040	16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25!""#%&
		0050	26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35	&'()*+,-./012345
		0060	36 37 55 55 55 55	67UUUU

Explicação

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

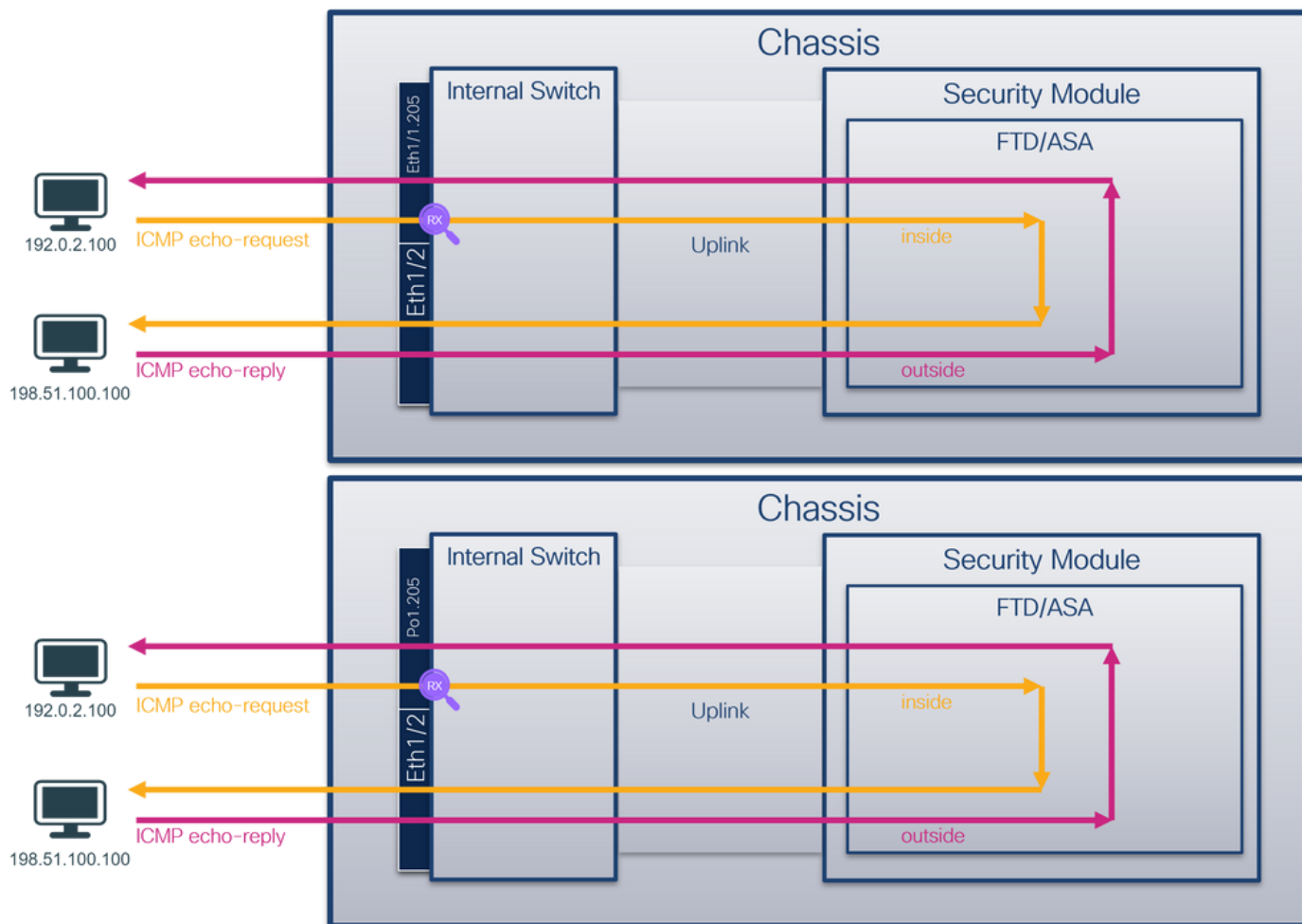
Esta tabela resume a tarefa:

Tarefa	Ponto de captura	Filtro interno	Direção	Tráfego capturado
Configurar e verificar uma captura de pacote na interface Ethernet1/1	Ethernet1/1	Nenhum	Soment e 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 interface Portchannel1 com as interfaces membro Ethernet1/3 e Ethernet1/4	Ethernet1/3 Ethernet1/4	Nenhum	Soment e entrada	Solicitações de eco ICMP do host 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 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:          caps-1-1
```

```
Packet Capture Filter Info
```

```
Name:          caps-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.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-07 21:21:01.607187	192.0.2.100	198.51.100.100	ICMP	106	0x411f (16671)	64	Echo (ping) request id=0x0037, seq=1/256, ttl=64 (no res
2	2022-08-07 21:21:02.609418	192.0.2.100	198.51.100.100	ICMP	106	0x413a (16698)	64	Echo (ping) request id=0x0037, seq=2/512, ttl=64 (no res
3	2022-08-07 21:21:03.610671	192.0.2.100	198.51.100.100	ICMP	106	0x421a (16922)	64	Echo (ping) request id=0x0037, seq=3/768, ttl=64 (no res
4	2022-08-07 21:21:04.609160	192.0.2.100	198.51.100.100	ICMP	106	0x426c (17004)	64	Echo (ping) request id=0x0037, seq=4/1024, ttl=64 (no res
5	2022-08-07 21:21:05.609409	192.0.2.100	198.51.100.100	ICMP	106	0x4310 (17168)	64	Echo (ping) request id=0x0037, seq=5/1280, ttl=64 (no res
6	2022-08-07 21:21:06.611847	192.0.2.100	198.51.100.100	ICMP	106	0x43df (17375)	64	Echo (ping) request id=0x0037, seq=6/1536, ttl=64 (no res
7	2022-08-07 21:21:07.616688	192.0.2.100	198.51.100.100	ICMP	106	0x44d3 (17619)	64	Echo (ping) request id=0x0037, seq=7/1792, ttl=64 (no res
8	2022-08-07 21:21:08.618023	192.0.2.100	198.51.100.100	ICMP	106	0x4518 (17688)	64	Echo (ping) request id=0x0037, seq=8/2048, ttl=64 (no res
9	2022-08-07 21:21:09.619326	192.0.2.100	198.51.100.100	ICMP	106	0x453d (17725)	64	Echo (ping) request id=0x0037, seq=9/2304, ttl=64 (no res
10	2022-08-07 21:21:10.616696	192.0.2.100	198.51.100.100	ICMP	106	0x462b (17963)	64	Echo (ping) request id=0x0037, seq=10/2560, ttl=64 (no res
11	2022-08-07 21:21:11.621629	192.0.2.100	198.51.100.100	ICMP	106	0x4707 (18183)	64	Echo (ping) request id=0x0037, seq=11/2816, ttl=64 (no res
12	2022-08-07 21:21:12.619309	192.0.2.100	198.51.100.100	ICMP	106	0x474b (18251)	64	Echo (ping) request id=0x0037, seq=12/3072, ttl=64 (no res
13	2022-08-07 21:21:13.620168	192.0.2.100	198.51.100.100	ICMP	106	0x4781 (18305)	64	Echo (ping) request id=0x0037, seq=13/3328, ttl=64 (no res
14	2022-08-07 21:21:14.623169	192.0.2.100	198.51.100.100	ICMP	106	0x4858 (18520)	64	Echo (ping) request id=0x0037, seq=14/3584, ttl=64 (no res
15	2022-08-07 21:21:15.622497	192.0.2.100	198.51.100.100	ICMP	106	0x4909 (18697)	64	Echo (ping) request id=0x0037, seq=15/3840, ttl=64 (no res
16	2022-08-07 21:21:16.626226	192.0.2.100	198.51.100.100	ICMP	106	0x490b (18699)	64	Echo (ping) request id=0x0037, seq=16/4096, ttl=64 (no res
17	2022-08-07 21:21:17.629363	192.0.2.100	198.51.100.100	ICMP	106	0x4932 (18738)	64	Echo (ping) request id=0x0037, seq=17/4352, ttl=64 (no res
18	2022-08-07 21:21:18.626651	192.0.2.100	198.51.100.100	ICMP	106	0x4a05 (18949)	64	Echo (ping) request id=0x0037, seq=18/4608, ttl=64 (no res


```

> Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
> Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco_34:9a:14 (bc:e7:12:34:9a:14)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 205
  000. .... = Priority: Best Effort (default) (0)
  ...0 .... = DEI: Ineligible
  ... 0000 1100 1101 = ID: 205
  Type: IPv4 (0x0800)
  Trailer: 55555555
> Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
> Internet Control Message Protocol
  
```

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.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-07 21:21:01.607187	192.0.2.100	198.51.100.100	ICMP	106	0x411f (16671)	64	Echo (ping) request id=0x0037, seq=1/256, ttl=64 (no res
2	2022-08-07 21:21:02.609418	192.0.2.100	198.51.100.100	ICMP	106	0x413a (16698)	64	Echo (ping) request id=0x0037, seq=2/512, ttl=64 (no res
3	2022-08-07 21:21:03.610671	192.0.2.100	198.51.100.100	ICMP	106	0x421a (16922)	64	Echo (ping) request id=0x0037, seq=3/768, ttl=64 (no res
4	2022-08-07 21:21:04.609160	192.0.2.100	198.51.100.100	ICMP	106	0x426c (17004)	64	Echo (ping) request id=0x0037, seq=4/1024, ttl=64 (no res
5	2022-08-07 21:21:05.609409	192.0.2.100	198.51.100.100	ICMP	106	0x4310 (17168)	64	Echo (ping) request id=0x0037, seq=5/1280, ttl=64 (no res
6	2022-08-07 21:21:06.611847	192.0.2.100	198.51.100.100	ICMP	106	0x43df (17375)	64	Echo (ping) request id=0x0037, seq=6/1536, ttl=64 (no res
7	2022-08-07 21:21:07.616688	192.0.2.100	198.51.100.100	ICMP	106	0x44d3 (17619)	64	Echo (ping) request id=0x0037, seq=7/1792, ttl=64 (no res
8	2022-08-07 21:21:08.618023	192.0.2.100	198.51.100.100	ICMP	106	0x4518 (17688)	64	Echo (ping) request id=0x0037, seq=8/2048, ttl=64 (no res
9	2022-08-07 21:21:09.619326	192.0.2.100	198.51.100.100	ICMP	106	0x453d (17725)	64	Echo (ping) request id=0x0037, seq=9/2304, ttl=64 (no res
10	2022-08-07 21:21:10.616696	192.0.2.100	198.51.100.100	ICMP	106	0x462b (17963)	64	Echo (ping) request id=0x0037, seq=10/2560, ttl=64 (no res
11	2022-08-07 21:21:11.621629	192.0.2.100	198.51.100.100	ICMP	106	0x4707 (18183)	64	Echo (ping) request id=0x0037, seq=11/2816, ttl=64 (no res
12	2022-08-07 21:21:12.619309	192.0.2.100	198.51.100.100	ICMP	106	0x474b (18251)	64	Echo (ping) request id=0x0037, seq=12/3072, ttl=64 (no res
13	2022-08-07 21:21:13.620168	192.0.2.100	198.51.100.100	ICMP	106	0x4781 (18305)	64	Echo (ping) request id=0x0037, seq=13/3328, ttl=64 (no res
14	2022-08-07 21:21:14.623169	192.0.2.100	198.51.100.100	ICMP	106	0x4858 (18520)	64	Echo (ping) request id=0x0037, seq=14/3584, ttl=64 (no res
15	2022-08-07 21:21:15.622497	192.0.2.100	198.51.100.100	ICMP	106	0x4909 (18697)	64	Echo (ping) request id=0x0037, seq=15/3840, ttl=64 (no res
16	2022-08-07 21:21:16.626226	192.0.2.100	198.51.100.100	ICMP	106	0x490b (18699)	64	Echo (ping) request id=0x0037, seq=16/4096, ttl=64 (no res
17	2022-08-07 21:21:17.629363	192.0.2.100	198.51.100.100	ICMP	106	0x4932 (18738)	64	Echo (ping) request id=0x0037, seq=17/4352, ttl=64 (no res
18	2022-08-07 21:21:18.626651	192.0.2.100	198.51.100.100	ICMP	106	0x4a05 (18949)	64	Echo (ping) request id=0x0037, seq=18/4608, ttl=64 (no res


```

> Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
> Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco_34:9a:14 (bc:e7:12:34:9a:14)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 205
  000. .... = Priority: Best Effort (default) (0)
  ...0 .... = DEI: Ineligible
  ... 0000 1100 1101 = ID: 205
  Type: IPv4 (0x0800)
  Trailer: 55555555
> Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
> Internet Control Message Protocol
  
```

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	Soment e Solicitações de eco ICMP do host 192.0.2.100 para o host entrada 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	Soment e Solicitações de eco ICMP do host 192.0.2.100 para o host entrada 198.51.100.100

Captura de pacotes em interfaces internas

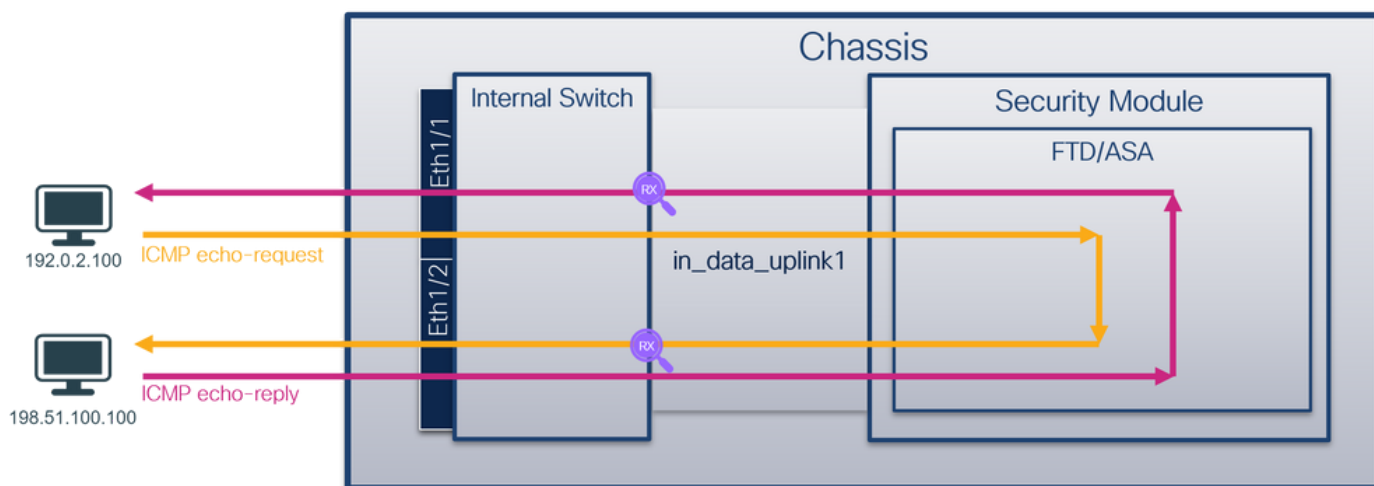
O Secure Firewall tem duas interfaces internas:

- **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.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP-TTL	Info
1	2022-08-07 22:40:06.685606	192.0.2.100	198.51.100.100	ICMP	102	0x4d93 (19859)	64	Echo (ping) request id=0x003a, seq=33/8448, ttl=64 (repl
2	2022-08-07 22:40:06.685615	198.51.100.100	192.0.2.100	ICMP	102	0x6cdc (27868)	64	Echo (ping) reply id=0x003a, seq=33/8448, ttl=64 (requ
3	2022-08-07 22:40:07.684219	192.0.2.100	198.51.100.100	ICMP	102	0x40e8 (19944)	64	Echo (ping) request id=0x003a, seq=34/8704, ttl=64 (repl
4	2022-08-07 22:40:07.689300	198.51.100.100	192.0.2.100	ICMP	102	0x6db2 (28082)	64	Echo (ping) reply id=0x003a, seq=34/8704, ttl=64 (requ
5	2022-08-07 22:40:08.685736	192.0.2.100	198.51.100.100	ICMP	102	0x4edc (20188)	64	Echo (ping) request id=0x003a, seq=35/8960, ttl=64 (repl
6	2022-08-07 22:40:08.690806	198.51.100.100	192.0.2.100	ICMP	102	0x6dbf (28095)	64	Echo (ping) reply id=0x003a, seq=35/8960, ttl=64 (requ
7	2022-08-07 22:40:09.690737	192.0.2.100	198.51.100.100	ICMP	102	0x4f2d (20269)	64	Echo (ping) request id=0x003a, seq=36/9216, ttl=64 (repl
8	2022-08-07 22:40:09.690744	198.51.100.100	192.0.2.100	ICMP	102	0x6e80 (28288)	64	Echo (ping) reply id=0x003a, seq=36/9216, ttl=64 (requ
9	2022-08-07 22:40:10.692266	192.0.2.100	198.51.100.100	ICMP	102	0x4fb1 (20401)	64	Echo (ping) request id=0x003a, seq=37/9472, ttl=64 (repl
10	2022-08-07 22:40:10.692272	198.51.100.100	192.0.2.100	ICMP	102	0x6ed5 (28373)	64	Echo (ping) reply id=0x003a, seq=37/9472, ttl=64 (requ
11	2022-08-07 22:40:11.691159	192.0.2.100	198.51.100.100	ICMP	102	0x5008 (20488)	64	Echo (ping) request id=0x003a, seq=38/9728, ttl=64 (requ
12	2022-08-07 22:40:11.691166	198.51.100.100	192.0.2.100	ICMP	102	0x6f3b (28475)	64	Echo (ping) reply id=0x003a, seq=38/9728, ttl=64 (requ
13	2022-08-07 22:40:12.692135	192.0.2.100	198.51.100.100	ICMP	102	0x50b8 (20664)	64	Echo (ping) request id=0x003a, seq=39/9984, ttl=64 (requ
14	2022-08-07 22:40:12.692209	198.51.100.100	192.0.2.100	ICMP	102	0x6fd7 (28631)	64	Echo (ping) reply id=0x003a, seq=39/9984, ttl=64 (requ
15	2022-08-07 22:40:13.697320	192.0.2.100	198.51.100.100	ICMP	102	0x5184 (20868)	64	Echo (ping) request id=0x003a, seq=40/10240, ttl=64 (req
16	2022-08-07 22:40:13.697327	198.51.100.100	192.0.2.100	ICMP	102	0x703e (28734)	64	Echo (ping) reply id=0x003a, seq=40/10240, ttl=64 (rec
17	2022-08-07 22:40:14.698512	192.0.2.100	198.51.100.100	ICMP	102	0x51d8 (20952)	64	Echo (ping) request id=0x003a, seq=41/10496, ttl=64 (req
18	2022-08-07 22:40:14.698518	198.51.100.100	192.0.2.100	ICMP	102	0x70dd (28893)	64	Echo (ping) reply id=0x003a, seq=41/10496, ttl=64 (rec

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

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.

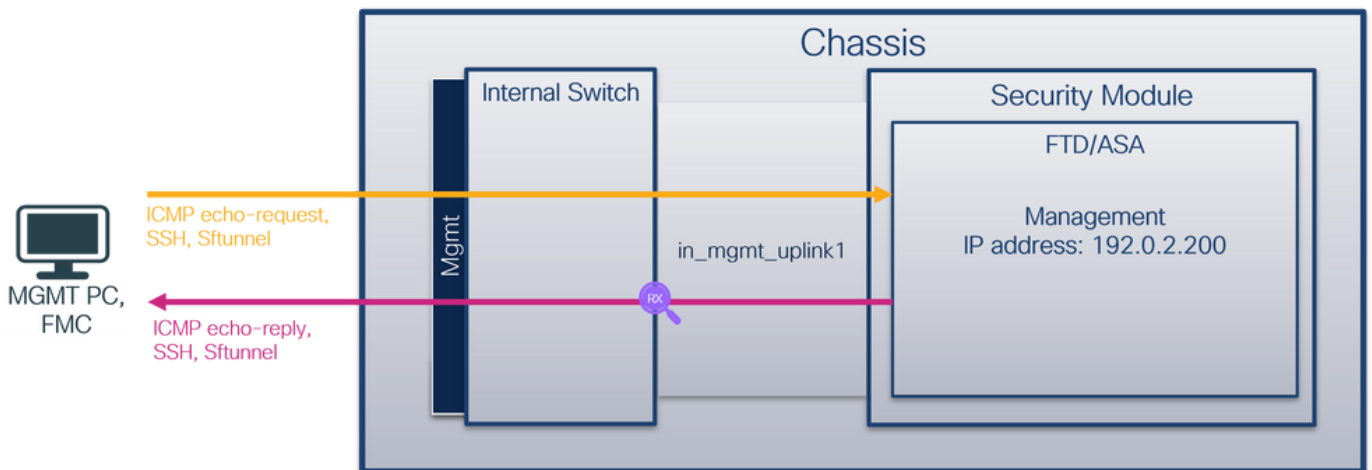
Esta tabela resume a tarefa:

Tarefa	Ponto de captura	Filtro interno	Direção	Tráfego capturado
Configurar e verificar uma captura de pacote na interface de uplink <code>in_data_uplink1</code>	<code>in_data_uplink1</code>	Nenhum	Somente entrada	Solicitações de eco ICMP do host 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.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
196	2022-08-07 23:21:45.133362	192.0.2.200	192.0.2.101	TCP	1518	0xb7d0 (47056)	64	39181 → 8305 [ACK] Seq=61372 Ack=875 Win=1384 Len=1448 TS
197	2022-08-07 23:21:45.133385	192.0.2.200	192.0.2.101	TCP	1518	0xb7d1 (47057)	64	39181 → 8305 [ACK] Seq=62820 Ack=875 Win=1384 Len=1448 TS
198	2022-08-07 23:21:45.133388	192.0.2.200	192.0.2.101	TLSv1.2	990	0xb7d2 (47058)	64	Application Data
199	2022-08-07 23:21:45.928772	192.0.2.200	192.0.2.100	ICMP	78	0xbd48 (48456)	64	Echo (ping) reply id=0x0001, seq=4539/47889, ttl=64
200	2022-08-07 23:21:45.949024	192.0.2.200	192.0.2.101	TLSv1.2	128	0x4a97 (19095)	64	Application Data
201	2022-08-07 23:21:45.949027	192.0.2.200	192.0.2.101	TCP	70	0x4a98 (19096)	64	8305 → 58885 [ACK] Seq=21997 Ack=26244 Win=4116 Len=0 TSv
202	2022-08-07 23:21:46.019895	192.0.2.200	192.0.2.101	TLSv1.2	100	0x4a99 (19097)	64	Application Data
203	2022-08-07 23:21:46.019899	192.0.2.200	192.0.2.101	TLSv1.2	96	0x4a9a (19098)	64	Application Data
204	2022-08-07 23:21:46.019903	192.0.2.200	192.0.2.101	TCP	70	0x4a9b (19099)	64	8305 → 58885 [ACK] Seq=22053 Ack=26274 Win=4116 Len=0 TSv
205	2022-08-07 23:21:46.019906	192.0.2.200	192.0.2.101	TCP	70	0x4a9c (19100)	64	8305 → 58885 [ACK] Seq=22053 Ack=26300 Win=4116 Len=0 TSv
206	2022-08-07 23:21:46.136415	192.0.2.200	192.0.2.101	TCP	70	0xb7d3 (47059)	64	39181 → 8305 [ACK] Seq=65188 Ack=921 Win=1384 Len=0 TSval
207	2022-08-07 23:21:46.958148	192.0.2.200	192.0.2.100	ICMP	78	0xbd9e (48542)	64	Echo (ping) reply id=0x0001, seq=4540/48145, ttl=64
208	2022-08-07 23:21:47.980409	192.0.2.200	192.0.2.100	ICMP	78	0xbd9f (48543)	64	Echo (ping) reply id=0x0001, seq=4541/48146, ttl=64
209	2022-08-07 23:21:48.406312	192.0.2.200	192.0.2.101	TCP	70	0x4a9d (19101)	64	8305 → 58885 [ACK] Seq=22053 Ack=26366 Win=4116 Len=0 TSv
210	2022-08-07 23:21:48.903236	192.0.2.200	192.0.2.101	TLSv1.2	747	0x4a9e (19102)	64	Application Data
211	2022-08-07 23:21:48.994386	192.0.2.200	192.0.2.100	ICMP	78	0xbe48 (48712)	64	Echo (ping) reply id=0x0001, seq=4542/48657, ttl=64
212	2022-08-07 23:21:50.008576	192.0.2.200	192.0.2.100	ICMP	78	0xbe49 (48713)	64	Echo (ping) reply id=0x0001, seq=4543/48658, ttl=64
213	2022-08-07 23:21:50.140167	192.0.2.200	192.0.2.101	TCP	1518	0xb7d4 (47060)	64	39181 → 8305 [ACK] Seq=65188 Ack=921 Win=1384 Len=1448 TS
214	2022-08-07 23:21:50.140171	192.0.2.200	192.0.2.101	TCP	1518	0xb7d5 (47061)	64	39181 → 8305 [ACK] Seq=66636 Ack=921 Win=1384 Len=1448 TS
215	2022-08-07 23:21:50.140175	192.0.2.200	192.0.2.101	TLSv1.2	990	0xb7d6 (47062)	64	Application Data
216	2022-08-07 23:21:51.015884	192.0.2.200	192.0.2.100	ICMP	78	0xbec1 (48833)	64	Echo (ping) reply id=0x0001, seq=4544/49169, ttl=64
217	2022-08-07 23:21:51.142842	192.0.2.200	192.0.2.101	TCP	70	0xbfd7 (47063)	64	39181 → 8305 [ACK] Seq=69004 Ack=967 Win=1384 Len=0 TSval
218	2022-08-07 23:21:52.030118	192.0.2.200	192.0.2.100	ICMP	78	0xbfd0 (48898)	64	Echo (ping) reply id=0x0001, seq=4545/49425, ttl=64
219	2022-08-07 23:21:53.042744	192.0.2.200	192.0.2.100	ICMP	78	0xbfd1 (48899)	64	Echo (ping) reply id=0x0001, seq=4546/49681, ttl=64
220	2022-08-07 23:21:53.073144	192.0.2.200	192.0.2.100	SSH	170	0xad34 (44340)	64	Server: Encrypted packet (len=112)
221	2022-08-07 23:21:53.194906	192.0.2.200	192.0.2.100	TCP	64	0xad35 (44341)	64	22 → 53249 [ACK] Seq=1025 Ack=881 Win=946 Len=0
222	2022-08-07 23:21:53.905480	192.0.2.200	192.0.2.101	TLSv1.2	747	0x4a9f (19103)	64	Application Data
223	2022-08-07 23:21:54.102899	192.0.2.200	192.0.2.100	ICMP	78	0xbf63 (48995)	64	Echo (ping) reply id=0x0001, seq=4547/49937, ttl=64
224	2022-08-07 23:21:54.903675	192.0.2.200	192.0.2.101	TCP	70	0x4aa0 (19104)	64	8305 → 58885 [ACK] Seq=23407 Ack=26424 Win=4116 Len=0 TSv
225	2022-08-07 23:21:55.136700	192.0.2.200	192.0.2.100	TCP	70	0xbf64 (48996)	64	Echo (ping) reply id=0x0001, seq=4548/50103, ttl=64

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 de gerenciamento FTD 192.0.2.200 para o host 192.0.2.100 Sftunnel do endereço IP de gerenciamento FTD 192.0.2.200 para o endereço IP do host 192.0.2.101 SSH do endereço IP de gerenciamento FTD 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:          caps-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/:

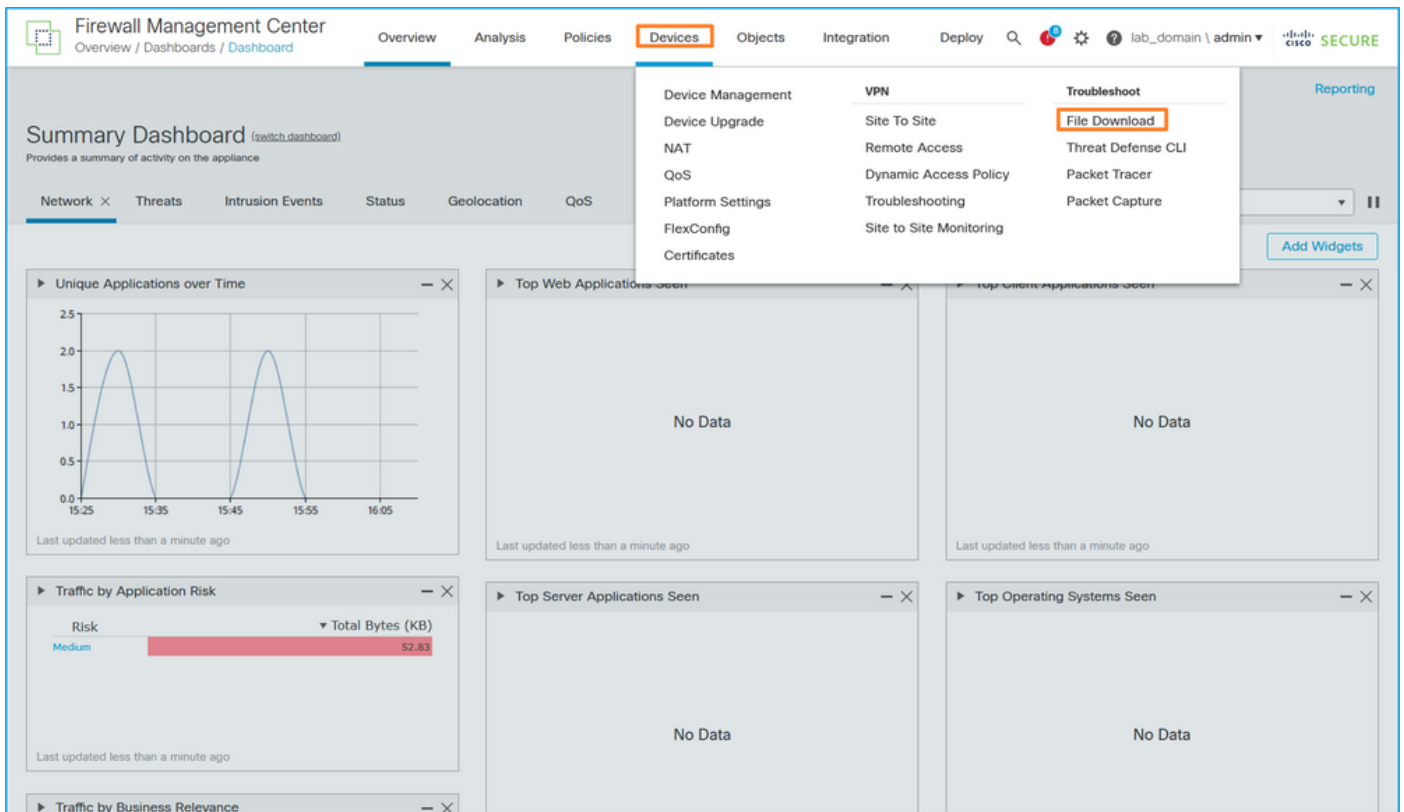
```
root@KSEC-FPR3100-1:/home/admin cp /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap /ngfw/var/common/
```

```
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.