

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

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[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 firewall seguro 1200/3100/4200](#)

[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](#)

[Captura de pacotes nas interfaces da porta do switch L2](#)

[Captura de pacotes em chassis de várias instâncias](#)

[Coletar Arquivos de Captura do Switch Interno com Firewall Seguro](#)

[Diretrizes, limitações e práticas recomendadas para captura de pacotes de switch interno](#)

[Informações Relacionadas](#)

Introdução

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

Pré-requisitos

Requisitos

Conhecimento básico do produto, análise de captura.

Componentes Utilizados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

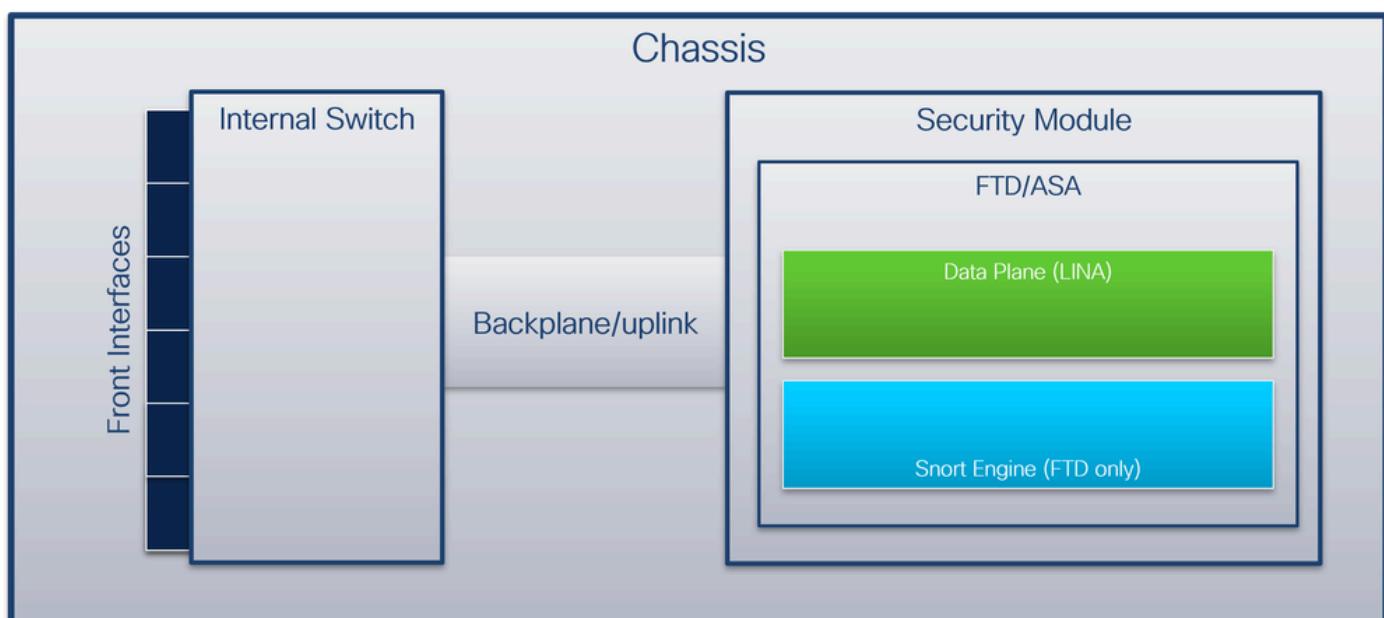
As informações neste documento são baseadas nestas versões de software e hardware:

- Firewall seguro 1200, 3100, 4200
- Firepower 4100/9300
- Sistema operacional Cisco Secure eXtensible (FXOS) 2.12.0.x, 2.17(0.x)
- Defesa contra ameaças do Cisco Secure Firewall (FTD) 7.2.0.x, 7.4.1-172, 7.7.0.89
- Cisco Secure Firewall Management Center (FMC) 7.2.0.x, 7.4.1-172, 7.7.0.89
- Dispositivo de segurança adaptável (ASA) 9.18(1)x, 9.20(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 1200/3100/4200 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 nos 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 as 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.
- Uplink de gerenciamento - uma interface interna exclusiva para o Secure Firewall 3100/4200 que fornece caminho de tráfego de gerenciamento entre o switch interno e o aplicativo.
- Interface de gerenciamento - uma interface física no chassi.
- Interfaces de dados - interfaces alocadas para o aplicativo usadas para encaminhar o tráfego.

No caso do Secure Firewall 3100/4200, os dados, o gerenciamento e as interfaces de uplink são mapeados para portas de switch internas específicas.

 Note: Para o Secure Firewall 1200, as interfaces de dados e uplink são mapeadas para portas de switch internas específicas. A porta de gerenciamento, no entanto, é uma interface fora de banda e não faz parte do switch interno.

O mapeamento pode ser verificado na saída do comando FXOS local-mgmt shell show portmanager switch status.

Neste exemplo, a porta 0/17 é a interface de gerenciamento do chassi, a porta 0/18 é a interface de backplane/uplink e a porta 0/19 é a interface de uplink de gerenciamento.

```
<#root>  
firepower-3140#  
connect local-mgmt  
  
Warning: network service is not available when entering 'connect local-mgmt'  
firepower-3140(local-mgmt)#  
  
show portmanager switch status
```

Dev/Port	Mode	Link	Speed	Duplex	Loopback	Autoneg	FEC	Link Scan	Port Man
0/1	SGMII	Up	1G	Full	None	No	None	None	Link-Up
0/2	SGMII	Up	1G	Full	None	No	None	None	Link-Up
0/3	SGMII	Down	1G	Full	n/a	No	None	None	Force-Lin
0/4	SGMII	Down	1G	Full	n/a	No	None	None	Force-Lin
0/5	SGMII	Down	1G	Full	n/a	No	None	None	Force-Lin
0/6	SGMII	Down	1G	Full	n/a	No	None	None	Force-Lin
0/7	SGMII	Down	1G	Full	n/a	No	None	None	Force-Lin

0/8	SGMII	Down	1G	Full	n/a	No	None	None	Force-Li
0/9	SR_LR	Down	25G	Full	n/a	No	None	None	Force-Li
0/10	SR_LR	Down	25G	Full	n/a	No	None	None	Force-Li
0/11	1000_BaseXDown	1G	Full	n/a	No	None	None	None	Force-Li
0/12	1000_BaseXDown	1G	Full	n/a	No	None	None	None	Force-Li
0/13	1000_BaseXDown	1G	Full	n/a	No	None	None	None	Force-Li
0/14	1000_BaseXDown	1G	Full	n/a	No	None	None	None	Force-Li
0/15	1000_BaseXDown	1G	Full	n/a	No	None	None	None	Force-Li
0/16	1000_BaseXDown	1G	Full	n/a	No	None	None	None	Force-Li
0/17	1000_BaseX	Up	1G	Full	None	No	None	None	Link-Up
0/18	KR2	Up	50G						
Full	None	No		None	None	Link-Up			
0/19	KR	Up	25G						
Full	None	No	25G	None	None	Link-Up			
0/20	KR	Up		Full	None	No	None	None	Link-Up

Esta tabela mostra as interfaces de backplane no Firepower 4100/9300 e as interfaces de uplink de dados no Secure Firewall 1200/3100/4200:

Platform	Número de módulos de segurança suportados	Interface de backplane/uplink	Porta do switch interno mapeada para backplane/uplink	Interface de aplicativo mapeada
Firepower 4100 (exceto Firepower 4110/4112)	1	SM1: Ethernet1/9 Ethernet1/10	N/A	Internal-Data0/0 Internal-Data0/1
Firepower 4110/4112	1	Ethernet1/9	N/A	Internal-Data0/0 Internal-Data0/1
Firepower 9300	3	SM1: Ethernet1/9 Ethernet1/10 SM2: Ethernet1/11 Ethernet1/12	N/A	Internal-Data0/0 Internal-Data0/1 Internal-Data0/0 Internal-Data0/1 Internal-Data0/0

		SM3: Ethernet1/13 Ethernet1/14		Internal-Data0/1
Firewall seguro 1210	1	in_data_uplink1	Porta 9	Internal-Data0/1
Firewall seguro 1220	1	in_data_uplink1 in_data_uplink2 in_data_uplink3	Porta 11 Porta 12 Porta 13	Internal-Data0/1 Internal-Data0/2 Internal-Data0/3
Firewall seguro 1230	1	in_data_uplink1	Porta 13	Internal-Data0/1
Firewall seguro 1240		in_data_uplink2 in_data_uplink3	Porta 14 Porta 15	Internal-Data0/2 Internal-Data0/3
Firewall seguro 1250	1	in_data_uplink1	Porta 13	Internal-Data0/1
Firewall seguro 3100	1	in_data_uplink1	Porta 18	Internal-Data0/1
Firewall seguro 4200	1	in_data_uplink1 in_data_uplink2 (somente 4245)	Porta 11 Porta 12 (somente 4245)	Internal-Data0/1 Internal-Data0/2 (somente 4245)

Esta tabela mostra interfaces de gerenciamento e interfaces de uplink de gerenciamento no Secure Firewall 1200/3100/4200:

Platform	Interface de gerenciamento do chassi	Porta de switch interna mapeada para a interface de gerenciamento do chassi	Porta de switch interna mapeada para interface de uplink de gerenciamento	Interface de aplicativo mapeada
Firewall	Gerenciamento1	Não mapeado para	N/A	N/A

seguro 1210		nenhuma porta de switch interna		
Firewall seguro 1200 (exceto 1210)	Gerenciamento1	Não mapeado para nenhuma porta de switch interna	N/A	N/A
Firewall seguro 3100	Gerenciamento1	Porta 0/17	Porta 0/19	in_mgmt_uplink1
Firewall seguro 4200	Gerenciamento1 Gerenciamento2	Porta 0/9 Porta 0/10	Porta 0/13 Porta 0/14	in_mgmt_uplink1 in_mgmt_uplink2

No caso do Firepower 4100/9300 com 2 interfaces de painel traseiro por módulo ou do Secure Firewall 4245 com 2 interfaces de uplink de dados, o switch interno e os aplicativos nos módulos executam o balanceamento de carga de tráfego nas duas interfaces.

- Módulo de segurança, mecanismo de segurança ou blade - o módulo em que aplicativos como FTD ou ASA estão instalados. O Firepower 9300 suporta até 3 módulos de segurança.
- Interface de aplicativo mapeada - os nomes das interfaces de backplane ou uplink em aplicativos, como FTD ou ASA.

Além disso, o Secure Firewall 1200 apresenta uma nova arquitetura com três interfaces de uplink de dados. O switch interno e o aplicativo executam balanceamento de carga nessas interfaces.

Use o comando show interface detail para verificar interfaces internas:

```
<#root>
>
show interface detail | grep Interface
```

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

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

```

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

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

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

```

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:

```

<#root>
firepower#
connect fxos

...
firepower(fxos)#
show run int e1/2

```

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

version 5.0(3)N2(4.120)

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

switchport trunk native vlan 102

  speed 1000
  duplex full
  udld disable
  no shutdown
```

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 1200/3100/4200

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

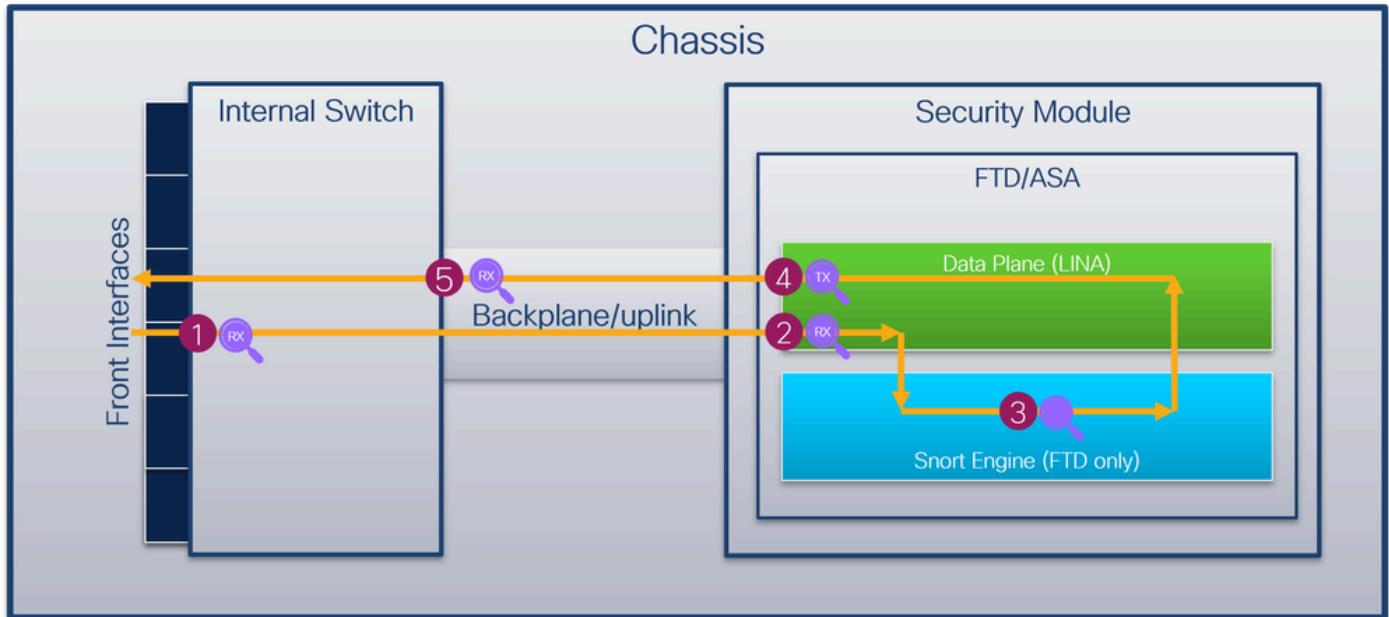
A marca da porta VLAN é compartilhada com o aplicativo. O aplicativo insere as respectivas marcas de VLAN de interface de saída em cada pacote. Quando um pacote do aplicativo é recebido pelo switch interno na interface de uplink, o switch lê a marca VLAN da interface de saída, identifica a interface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

Fluxo de pacotes e pontos de captura

Firepower 4100/9300 e Secure Firewall 3100

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:



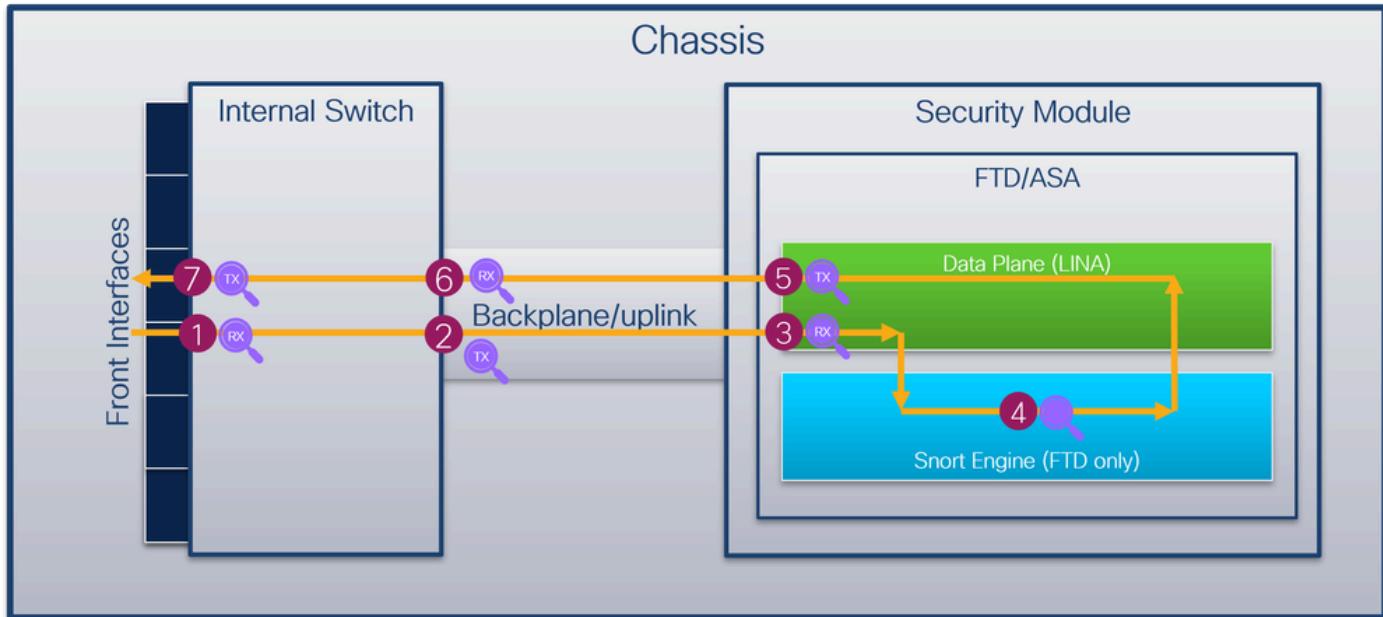
Os pontos de captura são:

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 de 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.

Firewall seguro 1200/4200

Os firewalls Secure Firewall 1200/4200 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 chassis 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 saída da interface interna do painel traseiro do switch.
3. Ponto de captura de ingresso da interface do plano de dados
4. Ponto de captura de Snort
5. Ponto de captura de saída da interface do plano de dados
6. 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.
7. Ponto de captura de saída da interface frontal do switch interno.

O switch interno suporta opcionalmente capturas bidirecionais - de entrada e de saída. Por padrão, o switch interno captura pacotes na direção de entrada.

 Note: A interface de gerenciamento no Secure Firewall 1200 é uma interface fora de banda e não faz parte do switch interno. Por esse motivo, a captura do tráfego da interface de gerenciamento no nível do switch não é suportada no Secure Firewall 1200.

Configuração e verificação no Firepower 4100/9300

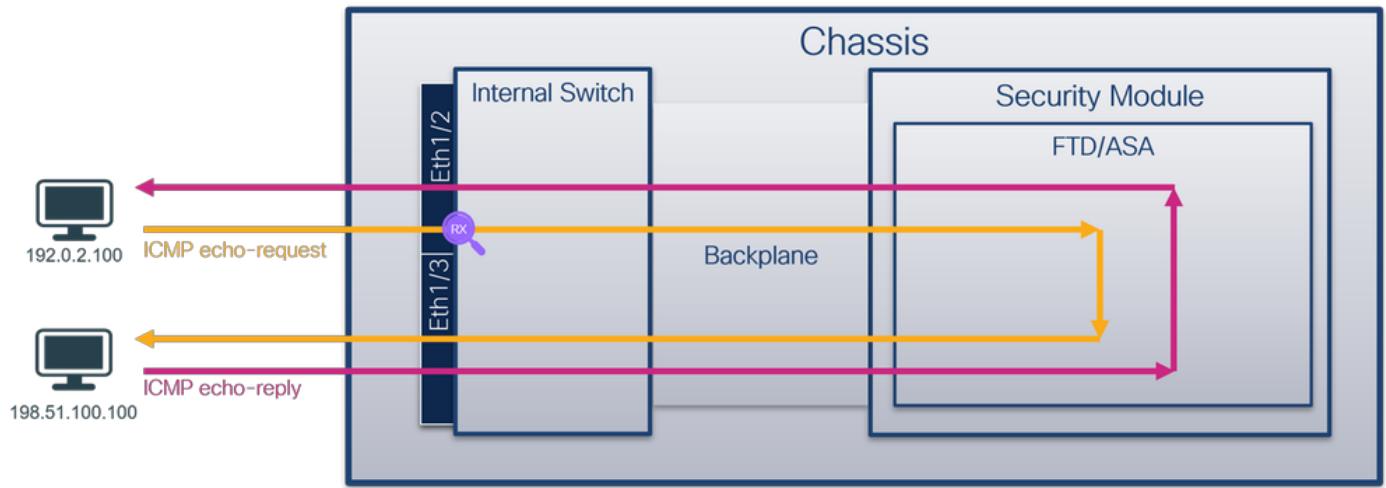
As capturas internas do switch Firepower 4100/9300 podem ser configuradas em Ferramentas > Captura de pacotes no FCM ou em captura de pacote de escopo no FXOS CLI. Para obter a descrição das opções de captura de pacote, consulte o Guia de configuração do gerenciador de chassi FXOS do Cisco Firepower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

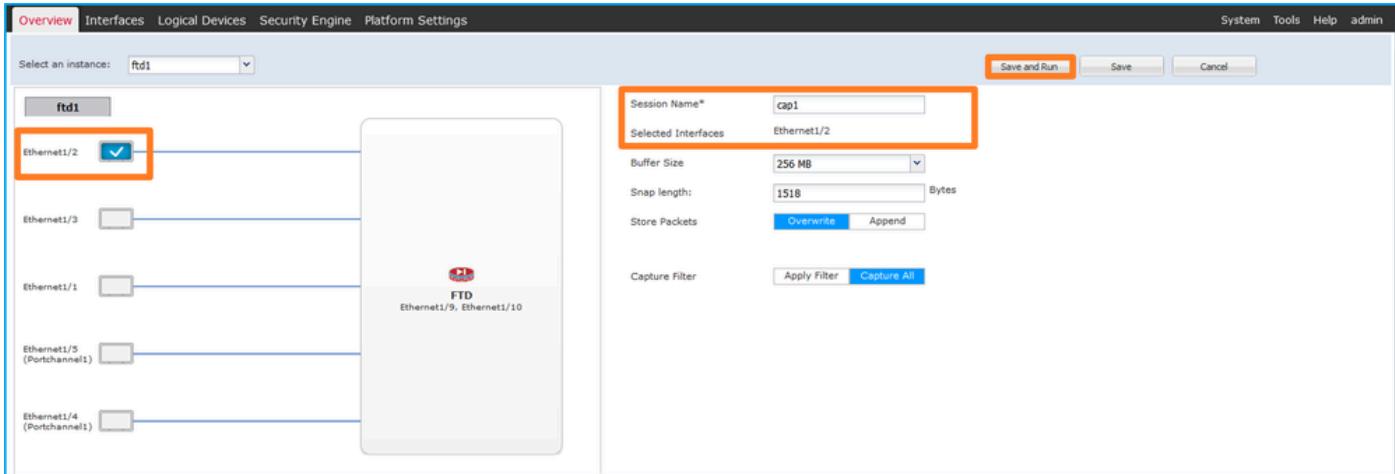
Execute estas etapas no FCM para configurar uma captura de pacote nas interfaces Ethernet1/2 ou Portchannel1:

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

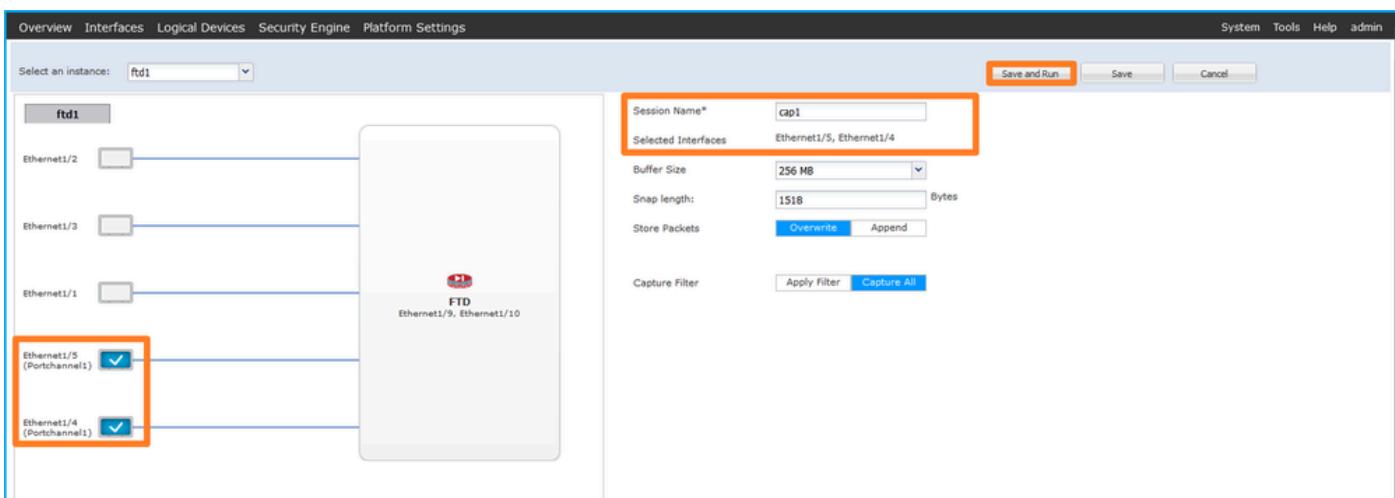
A interface 'Capture Session' no FCM:

- Barra superior: Overview, Interfaces, Logical Devices, Security Engine, Platform Settings, System, Tools, Help, admin. O link 'Tools' e o sub-menu 'Packet Capture' estão destacados.
- Barra de navegação: Capture Session (destacado), Filter List.
- Conteúdo principal: 'No Session available'.
- Botões na barra inferior: Refresh, Capture Session (destacado), Delete All Sessions.

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

Execute 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:

```
<#root>
```

```
firepower#
```

```
scope ssa
```

```
firepower /ssa #
```

```
show app-instance
```

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version	Deploy Type
ftd	ftd1						

1	Enabled	Online	7.2.0.82	7.2.0.82	Native	No
---	---------	--------	----------	----------	--------	----

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

```
<#root>

firepower#
connect fxos

<output skipped>
firepower(fxos)#

show port-channel summary

Flags: D - Down      P - Up in port-channel (members)
      I - Individual H - Hot-standby (LACP only)
      S - Suspended   r - Module-removed
      S - Switched    R - Routed
      U - Up (port-channel)
      M - Not in use. Min-links not met
-----
Group Port-      Type     Protocol Member Ports
      Channel
-----
1      Po1(SU)      Eth      LACP      Eth1/4(P)      Eth1/5(P)
```

3. Criar uma sessão de captura:

```
<#root>

firepower#
scope packet-capture

firepower /packet-capture #
create session cap1

firepower /packet-capture/session* #
create phy-port Eth1/2

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

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

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

firepower /packet-capture/session* #
enable

firepower /packet-capture/session* #
commit

firepower /packet-capture/session #
```

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

```
<#root>

firepower#
scope packet-capture

firepower /packet-capture #
create session cap1

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

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

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

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

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

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

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

```

set app-identifier ftd1

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

up

firepower /packet-capture/session* #

enable

firepower /packet-capture/session* #

commit

firepower /packet-capture/session #

```

Verificação

FCM

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

Interface Name	File Size (in bytes)	File Name	Device Name
Ethernet1/2	28632	cap1-ethernet-1-2-0.pcap	ftd1

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

Interface Name	File Size (in bytes)	File Name	Device Name
Ethernet1/5	160	cap1-ethernet-1-5-0.pcap	ftd1
Ethernet1/4	85000	cap1-ethernet-1-4-0.pcap	ftd1

CLI FXOS

Verifique os detalhes da captura em scope packet-capture:

```

<#root>

firepower#
scope packet-capture

firepower /packet-capture #
show session cap1

```

Traffic Monitoring Session:

Packet Capture Session Name: cap1

Session: 1

Admin State: Enabled

Oper State: Up

Oper State Reason: Active

Config Success: Yes

Config Fail Reason:

Append Flag: Overwrite

Session Mem Usage: 256 MB

Session Pcap Snap Len: 1518 Bytes

Error Code: 0

Drop Count: 0

Physical ports involved in Packet Capture:

Slot Id: 1

Port Id: 2

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

Pcapsize: 75136 bytes

Filter:

Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

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

<#root>

firepower#

scope packet-capture

firepower /packet-capture #

```
show session cap1
```

Traffic Monitoring Session:

Packet Capture Session Name: cap1

Session: 1

Admin State: Enabled

Oper State: Up

Oper State Reason: Active

Config Success: Yes

Config Fail Reason:

Append Flag: Overwrite

Session Mem Usage: 256 MB

Session Pcap Snap Len: 1518 Bytes

Error Code: 0

Drop Count: 0

Physical ports involved in Packet Capture:

slot Id: 1

Port Id: 4

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

Pcapsize: 310276 bytes

Filter:

Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

slot Id: 1

Port Id: 5

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

Pcapsize: 160 bytes

Filter:

Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

Coletar arquivos de captura

Execute 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 06:23:58.285080930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found!)
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 06:23:59.30948886	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 06:23:59.309193731	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 06:24:02.381074991	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 06:24:03.405199841	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 06:24:04.429156831	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 06:24:11.597086207	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	0000 58 97 bd b9 77 00 50 56 9d e8 be 89 26 80 0a X--w-P V---&-
> Ethernet II, Src: VMware_9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)	0010 00 00 81 00 00 66 08 00 45 80 00 54 9d ec 40 08 E---t-B-
✓ VN-Tag	0020 40 01 af c0 c0 00 02 64 c6 33 64 64 08 00 4e a2 @---d-3dd-N-
1.... = Direction: From Bridge	0030 00 1a 00 07 f4 64 ce 62 00 00 00 20 a2 07 00 ---d-b---
0.. = Pointer: vif_id	0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b ---!
..00 0000 0000 1010 = Destination: 10	0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b !"#\$88()*
.... 0.. = Looped: No	0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,./0123 4567
....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: 102	
000 = Priority: Best Effort (default) (0)	
...0 = DEI: Ineligible	
.... 0000 0010 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.

No.	Time	Source	Destination	Protocol	Length	IP ID	TTL	Info
1	2022-07-13 06:23:58.285080930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found!)
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 06:23:59.309048886	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 06:23:59.309193731	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 06:24:01.357174708	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 06:24:04.429156831	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 06:24:07.501293081	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 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)								
Ethernet II, Src: VMware_9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)								
0000... 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								

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.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-05 23:07:31.865872877	192.0.2.100	198.51.100.100	ICMP	108	0x322e (12846)	64	Echo (ping) request
2	2022-08-05 23:07:31.865875131	192.0.2.100	198.51.100.100	ICMP	102	0x322e (12846)	64	Echo (ping) request
3	2022-08-05 23:07:32.86714598	192.0.2.100	198.51.100.100	ICMP	108	0x32b9 (12985)	64	Echo (ping) request
4	2022-08-05 23:07:32.867145852	192.0.2.100	198.51.100.100	ICMP	102	0x32b9 (12985)	64	Echo (ping) request
5	2022-08-05 23:07:33.881902485	192.0.2.100	198.51.100.100	ICMP	108	0x32d8 (13016)	64	Echo (ping) request
6	2022-08-05 23:07:33.881904191	192.0.2.100	198.51.100.100	ICMP	102	0x32d8 (13016)	64	Echo (ping) request
7	2022-08-05 23:07:34.883049425	192.0.2.100	198.51.100.100	ICMP	108	0x3373 (13171)	64	Echo (ping) request
8	2022-08-05 23:07:34.883051649	192.0.2.100	198.51.100.100	ICMP	102	0x3373 (13171)	64	Echo (ping) request
9	2022-08-05 23:07:35.883478016	192.0.2.100	198.51.100.100	ICMP	108	0x3427 (13351)	64	Echo (ping) request
10	2022-08-05 23:07:35.883479190	192.0.2.100	198.51.100.100	ICMP	102	0x3427 (13351)	64	Echo (ping) request
11	2022-08-05 23:07:36.888741625	192.0.2.100	198.51.100.100	ICMP	108	0x34de (13534)	64	Echo (ping) request
12	2022-08-05 23:07:36.8889742853	192.0.2.100	198.51.100.100	ICMP	102	0x34de (13534)	64	Echo (ping) request
13	2022-08-05 23:07:37.913770117	192.0.2.100	198.51.100.100	ICMP	108	0x354c (13644)	64	Echo (ping) request
14	2022-08-05 23:07:37.913772219	192.0.2.100	198.51.100.100	ICMP	102	0x354c (13644)	64	Echo (ping) request
15	2022-08-05 23:07:38.937829879	192.0.2.100	198.51.100.100	ICMP	108	0x3602 (13826)	64	Echo (ping) request
16	2022-08-05 23:07:38.937831215	192.0.2.100	198.51.100.100	ICMP	102	0x3602 (13826)	64	Echo (ping) request
17	2022-08-05 23:07:39.961786128	192.0.2.100	198.51.100.100	ICMP	108	0x36ed (14061)	64	Echo (ping) request
18	2022-08-05 23:07:39.961787284	192.0.2.100	198.51.100.100	ICMP	102	0x36ed (14061)	64	Echo (ping) request
19	2022-08-05 23:07:40.985773090	192.0.2.100	198.51.100.100	ICMP	108	0x37d5 (14293)	64	Echo (ping) request

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.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-05 23:07:31.865872877	192.0.2.100	198.51.100.100	ICMP	108	0x322e (12846)	64	Echo (ping) request
2	2022-08-05 23:07:31.865875131	192.0.2.100	198.51.100.100	ICMP	102	0x322e (12846)	64	Echo (ping) request
3	2022-08-05 23:07:32.867144598	192.0.2.100	198.51.100.100	ICMP	108	0x32b9 (12985)	64	Echo (ping) request
4	2022-08-05 23:07:32.867145852	192.0.2.100	198.51.100.100	ICMP	102	0x32b9 (12985)	64	Echo (ping) request
5	2022-08-05 23:07:33.881982485	192.0.2.100	198.51.100.100	ICMP	108	0x32d0 (13016)	64	Echo (ping) request
6	2022-08-05 23:07:33.881904191	192.0.2.100	198.51.100.100	ICMP	102	0x32d8 (13016)	64	Echo (ping) request
7	2022-08-05 23:07:34.883049425	192.0.2.100	198.51.100.100	ICMP	108	0x3373 (13171)	64	Echo (ping) request
8	2022-08-05 23:07:34.883051649	192.0.2.100	198.51.100.100	ICMP	102	0x3373 (13171)	64	Echo (ping) request
9	2022-08-05 23:07:35.883478016	192.0.2.100	198.51.100.100	ICMP	108	0x3427 (13351)	64	Echo (ping) request
10	2022-08-05 23:07:35.883479190	192.0.2.100	198.51.100.100	ICMP	102	0x3427 (13351)	64	Echo (ping) request
11	2022-08-05 23:07:36.889741625	192.0.2.100	198.51.100.100	ICMP	108	0x34de (13534)	64	Echo (ping) request
12	2022-08-05 23:07:36.889742853	192.0.2.100	198.51.100.100	ICMP	102	0x34de (13534)	64	Echo (ping) request
13	2022-08-05 23:07:37.913770117	192.0.2.100	198.51.100.100	ICMP	108	0x354c (13644)	64	Echo (ping) request
14	2022-08-05 23:07:37.913772219	192.0.2.100	198.51.100.100	ICMP	102	0x354c (13644)	64	Echo (ping) request
15	2022-08-05 23:07:38.937829879	192.0.2.100	198.51.100.100	ICMP	108	0x3602 (13826)	64	Echo (ping) request
16	2022-08-05 23:07:38.937831215	192.0.2.100	198.51.100.100	ICMP	102	0x3602 (13826)	64	Echo (ping) request
17	2022-08-05 23:07:39.961786128	192.0.2.100	198.51.100.100	ICMP	108	0x36ed (14061)	64	Echo (ping) request
18	2022-08-05 23:07:39.961787284	192.0.2.100	198.51.100.100	ICMP	102	0x36ed (14061)	64	Echo (ping) request
19	2022-08-05 23:07:40.985773090	192.0.2.100	198.51.100.100	ICMP	108	0x37d5 (14293)	64	Echo (ping) request

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.

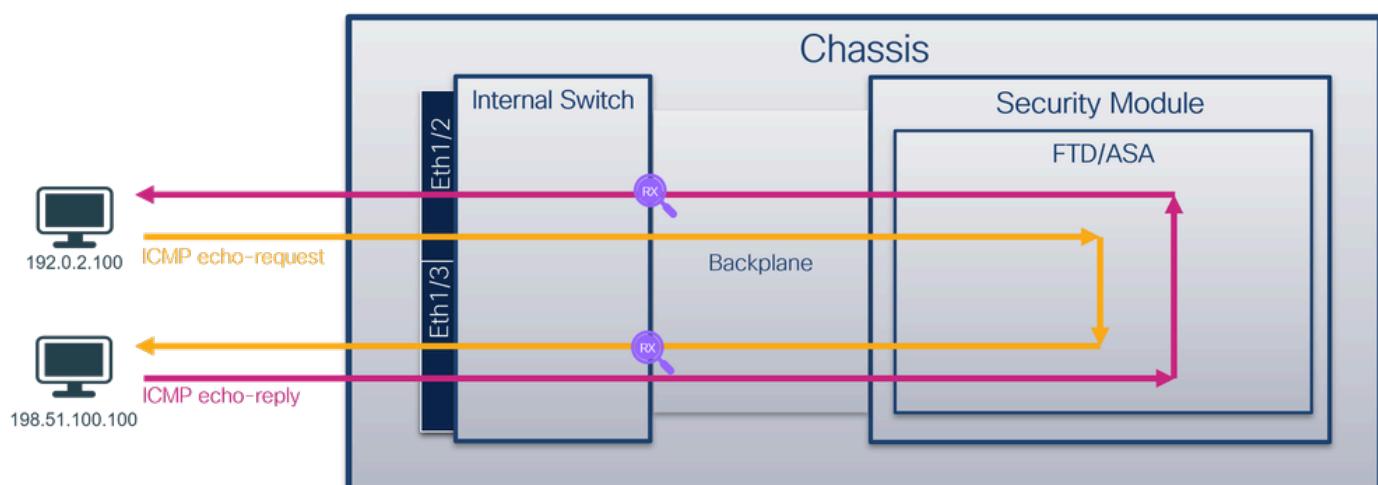
Esta tabela resume a tarefa:

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

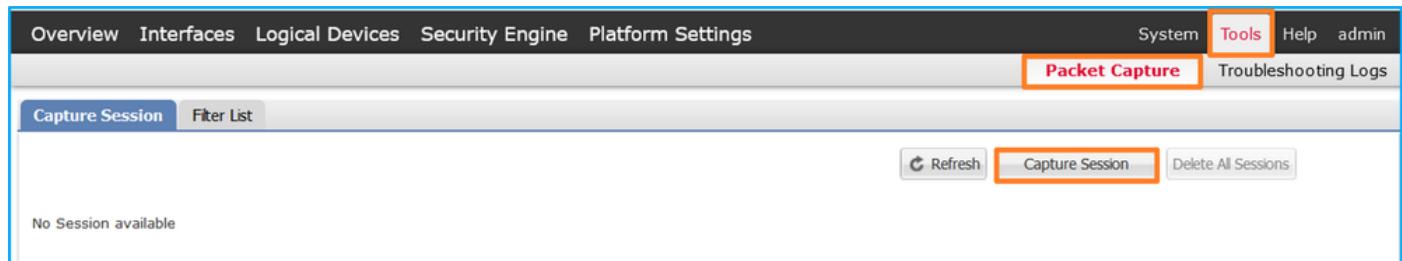


Configuração

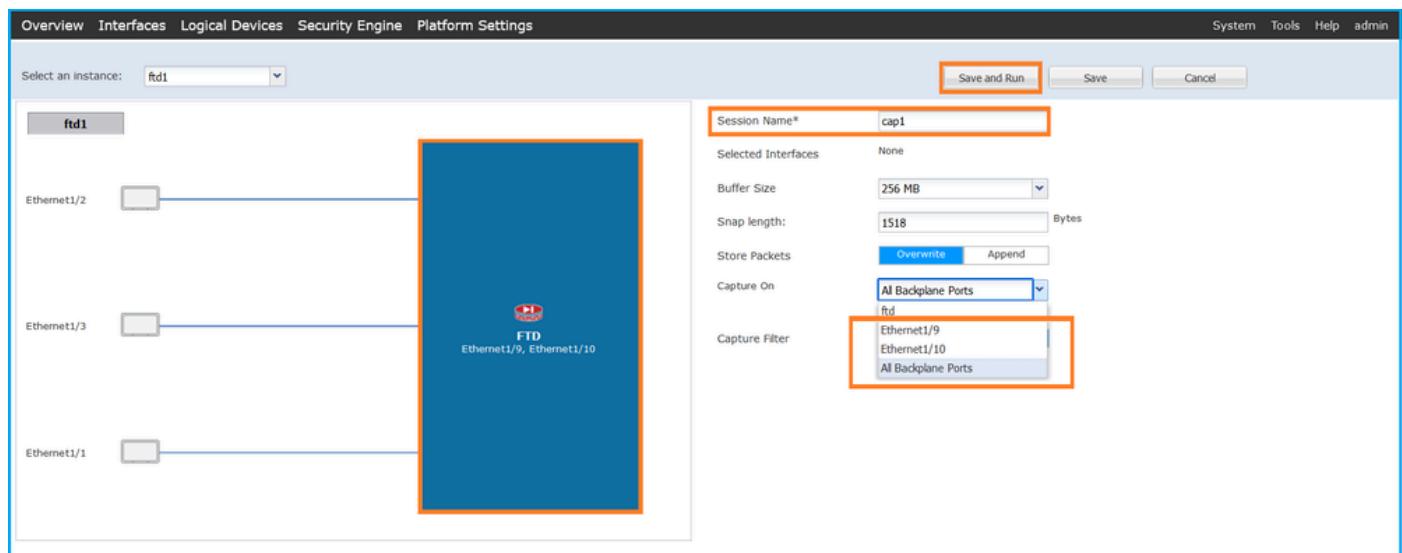
FCM

Execute estas etapas no FCM para configurar capturas de pacotes nas interfaces do painel traseiro:

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

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

1. Identificar o tipo de aplicativo e o identificador:

```
<#root>
```

```
firepower#
```

```
scope ssa
```

```

firepower /ssa#
show app-instance

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

```

2. Criar uma sessão de captura:

```

<#root>

firepower#
scope packet-capture

firepower /packet-capture #
create session cap1

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

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

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

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

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

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

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

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

```

up

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

enable

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

commit

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

Verificação

FCM

Verifique o nome da interface, assegure-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:

```
<#root>
```

```
firepower#
```

```
scope packet-capture
```

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

```
show session cap1
```

Traffic Monitoring Session:

```
Packet Capture Session Name: cap1
```

```
Session: 1
```

```
Admin State: Enabled
```

Oper State: Up

Oper State Reason: Active

Config Success: Yes

Config Fail Reason:

Append Flag: Overwrite

Session Mem Usage: 256 MB

Session Pcap Snap Len: 1518 Bytes

Error Code: 0

Drop Count: 0

Physical ports involved in Packet Capture:

Slot Id: 1

Port Id: 10

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

Pcapsize: 1017424 bytes

Filter:

Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

Slot Id: 1

Port Id: 9

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

Pcapsize: 1557432 bytes

Filter:

Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

Coletar arquivos de captura

Execute 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	ID	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 id=0x0001, seq=15/3840, ttl=64 (no response found!)
2	2022-07-14 20:20:36.513859028	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (reply in 3)
3	2022-07-14 20:20:36.514117394	198.51.100.100	192.0.2.100	ICMP	108	0xcc2c (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 2)
4	2022-07-14 20:20:36.514119312	198.51.100.100	192.0.2.100	ICMP	108	0xcc2c (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64
5	2022-07-14 20:20:37.537723822	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040)	64	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (no response found!)
6	2022-07-14 20:20:37.537726588	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040)	64	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (reply in 7)
7	2022-07-14 20:20:37.538046165	198.51.100.100	192.0.2.100	ICMP	108	0xcc9b (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 6)
8	2022-07-14 20:20:37.538048311	198.51.100.100	192.0.2.100	ICMP	108	0xcc9b (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64
9	2022-07-14 20:20:38.561776064	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (no response found!)
10	2022-07-14 20:20:38.561778310	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (reply in 11)
11	2022-07-14 20:20:38.562048288	198.51.100.100	192.0.2.100	ICMP	108	0x5ab7 (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 10)
12	2022-07-14 20:20:38.562059333	198.51.100.100	192.0.2.100	ICMP	108	0xccc4 (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64
13	2022-07-14 20:20:39.585677043	192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366)	64	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (no response found!)
14	2022-07-14 20:20:39.585678455	192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366)	64	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (reply in 15)
15	2022-07-14 20:20:39.585936554	198.51.100.100	192.0.2.100	ICMP	108	0xcd8d (52621)	64	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64 (request in 14)
16	2022-07-14 20:20:39.585937900	198.51.100.100	192.0.2.100	ICMP	108	0xcd8d (52621)	64	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64
17	2022-07-14 20:20:40.609804804	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (23419)	64	Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (no response found!)
18	2022-07-14 20:20:40.609807618	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (23419)	64	Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (reply in 19)
19	2022-07-14 20:20:40.609808180	198.51.100.100	192.0.2.100	ICMP	108	0xcd8f (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64 (request in 18)
20	2022-07-14 20:20:40.610181944	198.51.100.100	192.0.2.100	ICMP	108	0xcd8f (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64
21	2022-07-14 20:20:41.633805153	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (no response found!)
22	2022-07-14 20:20:41.633806997	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (reply in 23)
23	2022-07-14 20:20:41.634084102	198.51.100.100	192.0.2.100	ICMP	108	0xce36 (52790)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64 (request in 22)
24	2022-07-14 20:20:41.634085368	198.51.100.100	192.0.2.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64
25	2022-07-14 20:20:42.657709898	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (no response found!)
26	2022-07-14 20:20:42.657711660	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (reply in 27)
27	2022-07-14 20:20:42.657709875	198.51.100.100	192.0.2.100	ICMP	108	0xce49 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64 (request in 26)
28	2022-07-14 20:20:42.657981971	198.51.100.100	192.0.2.100	ICMP	108	0xce49 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64
29	2022-07-14 20:20:43.681736697	192.0.2.100	198.51.100.100	ICMP	108	0x5c52 (23634)	64	Echo (ping) request id=0x0001, seq=22/5632, ttl=64 (no response found!)

> 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 9de:e7:50 (00:50:56:9d:e7:50)								
VN-Tag								
0... = Direction: To Bridge								
..0... = Pointer: vif_id								
..00 0000 0000 0000 = Destination: 0								
.... 0... = Looped: No								
.... 0... = Reserved: 0								
.... 0... = Version: 0								
.... 0000 0000 1010 = Source: 10								
Type: 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.
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	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 id=0x0001, seq=15/3840, ttl=64 (no response found!)
2	2022-07-14 20:20:36.514117394	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (reply in 3)
3	2022-07-14 20:20:36.514117394	198.51.100.100	192.0.2.100	ICMP	108	1 0xcc2c (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 2)
4	2022-07-14 20:20:36.514117392	198.51.100.100	192.0.2.100	ICMP	108	0xcc2c (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 2)
5	2022-07-14 20:20:37.537723822	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040)	64	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (no response found!)
6	2022-07-14 20:20:37.537726588	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040)	64	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (no response found!)
7	2022-07-14 20:20:37.538046165	198.51.100.100	192.0.2.100	ICMP	108	0xcc9b (52279)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 6)
8	2022-07-14 20:20:37.538048311	198.51.100.100	192.0.2.100	ICMP	108	0xcc9b (52279)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 6)
9	2022-07-14 20:20:38.561776064	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (no response found!)
10	2022-07-14 20:20:38.561778310	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (no response found!)
11	2022-07-14 20:20:38.562048288	198.51.100.100	192.0.2.100	ICMP	108	0xcccc (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 10)
12	2022-07-14 20:20:38.562050333	198.51.100.100	192.0.2.100	ICMP	108	0xcccc (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 10)
13	2022-07-14 20:20:39.585677843	192.0.2.100	198.51.100.100	ICMP	108	0x5b40 (23366)	64	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (no response found!)
14	2022-07-14 20:20:39.585678455	192.0.2.100	198.51.100.100	ICMP	108	0x5b40 (23366)	64	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (no response found!)
15	2022-07-14 20:20:39.585678554	198.51.100.100	192.0.2.100	ICMP	108	0xccd8d (52621)	64	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64 (request in 14)
16	2022-07-14 20:20:39.585937900	198.51.100.100	192.0.2.100	ICMP	108	0xccd8d (52621)	64	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64 (request in 14)
17	2022-07-14 20:20:40.609884804	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (23419)	64	Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (no response found!)
18	2022-07-14 20:20:40.609887618	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (23419)	64	Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (no response found!)
19	2022-07-14 20:20:40.610179685	198.51.100.100	192.0.2.100	ICMP	108	0xcd8f (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64 (request in 18)
20	2022-07-14 20:20:40.610181944	198.51.100.100	192.0.2.100	ICMP	108	0xcd8f (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64 (request in 18)
21	2022-07-14 20:20:41.633805153	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (no response found!)
22	2022-07-14 20:20:41.633806997	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (no response found!)
23	2022-07-14 20:20:41.634084102	198.51.100.100	192.0.2.100	ICMP	108	0xce36 (52790)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64 (request in 22)
24	2022-07-14 20:20:41.634085368	198.51.100.100	192.0.2.100	ICMP	108	0xce36 (52790)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64 (request in 22)
25	2022-07-14 20:20:42.657709988	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (no response found!)
26	2022-07-14 20:20:42.657711660	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (no response found!)
27	2022-07-14 20:20:42.657711660	198.51.100.100	192.0.2.100	ICMP	108	0xce49 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64 (request in 26)
28	2022-07-14 20:20:42.657981971	198.51.100.100	192.0.2.100	ICMP	108	0xce49 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64 (request in 26)
29	2022-07-14 20:20:43.681736697	192.0.2.100	198.51.100.100	ICMP	108	0x5c52 (23634)	64	Echo (ping) request id=0x0001, seq=22/5632, ttl=64 (no response found!)

Frame 3: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_vo_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)

VN-Tag
0... = Direction: To Bridge
. = Pointer: vif_id
..0 00 0000 0000 0000 = Destination: 0
.... 0... = Looped: No
....0... = Reserved: 0
....0... = Version: 0
..... 0000 0000 1010 = Source: 10
Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
000 = Priority: Best Effort (default) (0)
....0 = DEI: Ineligible
....0000 0110 0110 = ID: 102
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100
Internet Control Message Protocol

0000 00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00 ·PV··X··W·&·
0000 00 0a 81 00 00 66 00 00 45 00 00 54 cc 2c 00 00 ·f··E·T··
0020 40 01 c1 80 c6 33 64 64 c0 00 02 64 00 00 2a 68 @...3dd··d·h
0030 00 01 00 0f 89 7a d0 62 00 00 00 b3 d7 09 00 z·b
0040 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 ··!# \$88'()*+
0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,..../0123 4567

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:

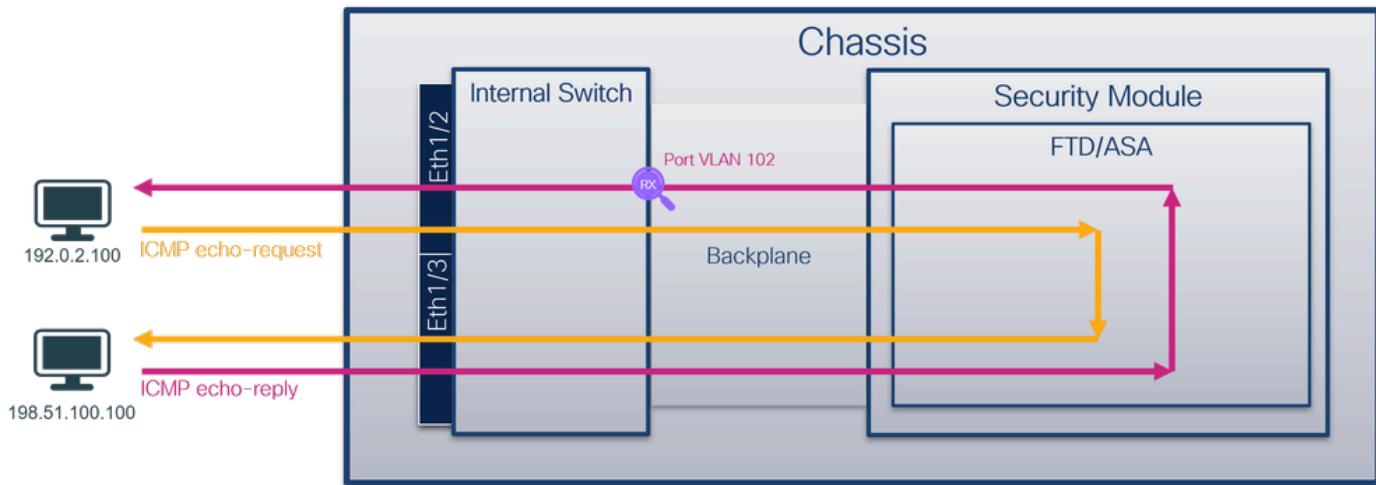
- Configurar capturas de pacotes nas interfaces do painel traseiro para pacotes que deixam uma interface frontal específica. Por exemplo, configure capturas de pacotes na interface Ethernet1/9 do painel traseiro para pacotes que deixam a interface Ethernet1/2.
- Configure capturas simultâneas de pacotes em uma interface frontal específica e nas interfaces do painel traseiro. 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 a interface de saída são capturados. Nesse caso, as respostas ICMP são capturadas.

Topologia, fluxo de pacotes e pontos de captura



Configuração

FCM

Execute 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:

The screenshot shows the Firepower Management Platform interface. The top navigation bar includes tabs for Overview, Interfaces, Logical Devices, Security Engine, Platform Settings, System, Tools (which is highlighted with a red box), Help, and admin. Below the navigation bar, there's a sub-navigation bar with 'Capture Session' (highlighted with a red box) and 'Filter List'. On the right side of this bar are buttons for Refresh, Capture Session (highlighted with a red box), and Delete All Sessions. The main content area displays a message 'No Session available'.

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:

The screenshot shows the 'Capture Session' configuration dialog. On the left, there's a network diagram for instance 'ftd1' showing three interfaces: Ethernet1/2, Ethernet1/3, and Ethernet1/1. A blue box highlights the central configuration area. In this area, the 'Session Name*' field is set to 'cap1'. Under 'Selected Interfaces', 'None' is selected. The 'Buffer Size' is set to '256 MB'. 'Snap length:' is set to '1518 Bytes'. Under 'Store Packets', 'Overwrite' is selected. The 'Capture On' dropdown is set to 'ftd'. The 'Application Port' dropdown is set to 'Ethernet1/2'. The 'Application Capture Direction' dropdown is set to 'Egress Packet' (highlighted with a red box). At the bottom, there are 'Capture Filter' options for 'Apply Filter' and 'Capture All'. Buttons for 'Save and Run' (highlighted with a red box), 'Save', and 'Cancel' are at the top right.

CLI FXOS

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

1. Identificar o tipo de aplicativo e o identificador:

```
<#root>
firepower#
scope ssa

firepower /ssa#
show app-instance
```

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version	Deploy Type
ftd	ftd1		Enabled	Online	7.2.0.82	7.2.0.82	Native

2. Criar uma sessão de captura:

```
<#root>

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, assegure-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:

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

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

Traffic Monitoring Session:

Packet Capture Session Name: cap1

Session: 1

Admin State: Enabled

Oper State: Up

Oper State Reason: Active

Config Success: Yes

Config Fail Reason:

Append Flag: Overwrite

Session Mem Usage: 256 MB

Session Pcap Snap Len: 1518 Bytes

Error Code: 0

Drop Count: 0

Application ports involved in Packet Capture:

Slot Id: 1

Link Name: l12

Port Name: Ethernet1/2

App Name: ftd
Sub Interface: 0

Application Instance Identifier: ftd1

Application ports resolved to:

Name: vnic1

Eq Slot Id: 1

Eq Port Id: 9

Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1036.pcap

Pcapsize: 53640 bytes

vlan: 102

Filter:

Name: vnic2

Eq Slot Id: 1

Eq Port Id: 10

Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1175.pcap

Pcapsize: 1824 bytes

vlan: 102

Filter:

Coletar arquivos de captura

Execute 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 10:03:22.231237959	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	0x4303 (17331)	64	Echo (ping) reply id=0x0012, seq=2/512, ttl=64
4	2022-08-01 10:03:23.232244769	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 10:03:25.258672449	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 10:03:28.3306664677	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 10:03:28.3306667153	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	0000 00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00 ·PV··X··w··8··
Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VMware 9d:e8:be (00:50:56:9d:e8:be)	0010 00 0a 81 00 00 66 08 00 45 00 00 54 42 f8 00 00 ···f··E··TB···
VN-Tag	0020 40 01 4a b5 c6 33 64 64 c0 00 02 64 00 00 90 04 @ J-3dd ·d···
0..... = Direction: To Bridge	0030 00 12 00 01 dd a4 e7 d2 00 00 00 e3 0d 09 00 ..b.....
.0... = Pointer: vif_id	0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b ..!# \$38'(')*
..00 0000 0000 0000 .. = Destination: 0	0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ,,.0123 4567
..... = Looped: No	0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37
..... = Reserved: 0	
..... = Version: 0	
..... = 0000 0000 1010 = Source: 10	
Type: 802.1Q Virtual LAN (0x8100)	
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102	
000 = Priority: Best Effort (default) (0)	
...0 = DEI: Ineligible	
.... 0000 0110 0110 .. = ID: 102	
Type: IPv4 (0x0800)	
Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100	
Internet Control Message Protocol	

Explicação

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

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

Esta tabela resume a tarefa:

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

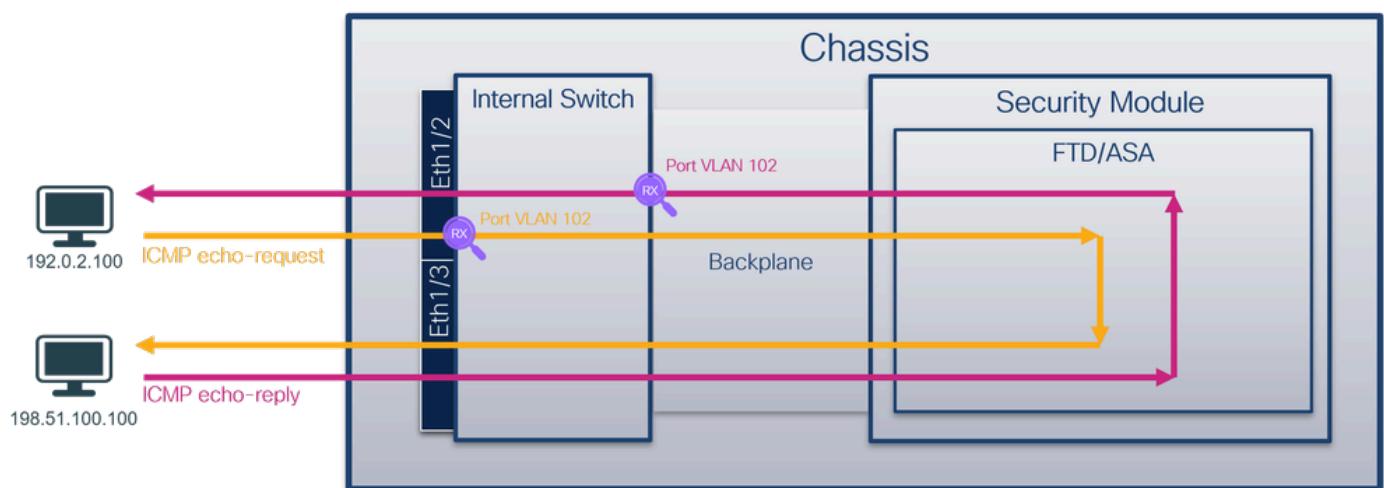
Tarefa 2

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

Capturas de pacotes simultâneas são configuradas em:

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

Topologia, fluxo de pacotes e pontos de captura



Configuração

FCM

Execute 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:

The screenshot shows the Firepower Management Platform's navigation bar with links for Overview, Interfaces, Logical Devices, Security Engine, Platform Settings, System, Tools, Help, and admin. Below the navigation bar, there are tabs for Capture Session and Filter List, with 'Capture Session' being the active tab. A red box highlights the 'Tools' menu item. In the main content area, there are buttons for Refresh, Capture Session (which is also highlighted with a red box), and Delete All Sessions. A message 'No Session available' is displayed.

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:

The screenshot shows the 'Capture Session' configuration screen. On the left, there is a network diagram for instance 'ftd1' showing interfaces Ethernet1/2, Ethernet1/3, and Ethernet1/1. On the right, the configuration panel has fields for Session Name (set to 'cap1'), Selected Interfaces (None), Buffer Size (256 MB), Snap length (1518 Bytes), Store Packets (Overwrite), and a 'Capture On' dropdown set to 'ftd'. Below that is an 'Application Port' dropdown set to 'Ethernet1/2'. Under 'Application Capture Direction', 'All Packets' is selected. At the bottom are 'Capture Filter' buttons for 'Apply Filter' and 'Capture All'. The 'Save and Run' button is highlighted with a red box.

CLI FXOS

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

1. Identificar o tipo de aplicativo e o identificador:

```
<#root>
firepower#
scope ssa

firepower /ssa#
show app-instance
```

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

2. Criar uma sessão de captura:

```
<#root>

firepower#
scope packet-capture

firepower /packet-capture #
create session cap1

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

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

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

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

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

firepower /packet-capture/session* #
enable

firepower /packet-capture/session* #
commit

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

Verificação

FCM

Verifique o nome da interface, assegure-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:

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

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

Traffic Monitoring Session:

Packet Capture Session Name: cap1

Session: 1

Admin State: Enabled

Oper State: Up

Oper State Reason: Active

Config Success: Yes

Config Fail Reason:

Append Flag: Overwrite

Session Mem Usage: 256 MB

Session Pcap Snap Len: 1518 Bytes

Error Code: 0

Drop Count: 0

Physical ports involved in Packet Capture:

Slot Id: 1

Port Id: 2

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

Pcapsize: 410444 bytes

Filter:

Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

Application ports involved in Packet Capture:

slot Id: 1

Link Name: link12

Port Name: Ethernet1/2

App Name: ftd

Sub Interface: 0

Application Instance Identifier: ftd1

Application ports resolved to:

Name: vnic1

Eq Slot Id: 1

Eq Port Id: 9

Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1036.pcap

Pcapsize: 128400 bytes

Vlan: 102

Filter:

Name: vnic2

Eq Slot Id: 1

Eq Port Id: 10

Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1175.pcap

Pcapsize: 2656 bytes

Vlan: 102

Filter:

Coletar arquivos de captura

Execute 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	ID	TTL	Info
1	2022-08-01 11:33:19.078693081	192.0.2.100	198.51.100.100	ICMP	108	0x0c089 (49161)	64	Echo (ping) request
2	2022-08-01 11:33:19.078695347	192.0.2.100	198.51.100.100	ICMP	102	0x0c089 (49161)	64	Echo (ping) request
3	2022-08-01 11:33:19.071217121	192.0.2.100	198.51.100.100	ICMP	102	0x0c089 (49161)	64	Echo (ping) request
4	2022-08-01 11:33:19.071218458	192.0.2.100	198.51.100.100	ICMP	102	0x0c089 (49161)	64	Echo (ping) request
5	2022-08-01 11:33:19.07208236625	192.0.2.100	198.51.100.100	ICMP	108	0x0c8ae (49326)	64	Echo (ping) request
6	2022-08-01 11:33:20.0720839845	192.0.2.100	198.51.100.100	ICMP	102	0x0c8ae (49326)	64	Echo (ping) request
7	2022-08-01 11:33:21.0732682209	192.0.2.100	198.51.100.100	ICMP	108	0x1c167 (49511)	64	Echo (ping) request
8	2022-08-01 11:33:21.073268249	192.0.2.100	198.51.100.100	ICMP	102	0x1c167 (49511)	64	Echo (ping) request
9	2022-08-01 11:33:22.074576640	192.0.2.100	198.51.100.100	ICMP	108	0x1c175 (49525)	64	Echo (ping) request
10	2022-08-01 11:33:22.074578010	192.0.2.100	198.51.100.100	ICMP	102	0x1c175 (49525)	64	Echo (ping) request
11	2022-08-01 11:33:23.075779089	192.0.2.100	198.51.100.100	ICMP	108	0xc208 (49672)	64	Echo (ping) request
12	2022-08-01 11:33:23.075781513	192.0.2.100	198.51.100.100	ICMP	102	0xc208 (49672)	64	Echo (ping) request
13	2022-08-01 11:33:24.081813949	192.0.2.100	198.51.100.100	ICMP	108	0xc211 (49681)	64	Echo (ping) request
14	2022-08-01 11:33:24.081841386	192.0.2.100	198.51.100.100	ICMP	102	0xc211 (49681)	64	Echo (ping) request
15	2022-08-01 11:33:25.105806249	192.0.2.100	198.51.100.100	ICMP	108	0xc2e2 (49890)	64	Echo (ping) request
16	2022-08-01 11:33:25.105807895	192.0.2.100	198.51.100.100	ICMP	102	0xc2e2 (49890)	64	Echo (ping) request
17	2022-08-01 11:33:26.129836273	192.0.2.100	198.51.100.100	ICMP	108	0xc3b4 (50100)	64	Echo (ping) request
18	2022-08-01 11:33:26.129838114	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100)	64	Echo (ping) request
19	2022-08-01 11:33:27.153828653	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294)	64	Echo (ping) request
20	2022-08-01 11:33:27.153830201	192.0.2.100	198.51.100.100	ICMP	102	0xc476 (50294)	64	Echo (ping) request
21	2022-08-01 11:33:28.177847175	192.0.2.100	198.51.100.100	ICMP	108	0xc516 (50454)	64	Echo (ping) request
22	2022-08-01 11:33:28.177849755	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (50454)	64	Echo (ping) request
23	2022-08-01 11:33:29.201804760	192.0.2.100	198.51.100.100	ICMP	108	0xc578 (50552)	64	Echo (ping) request
24	2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	102	0xc578 (50552)	64	Echo (ping) request
25	2022-08-01 11:33:30.225834765	192.0.2.100	198.51.100.100	ICMP	108	0xc585 (50565)	64	Echo (ping) request
26	2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (50565)	64	Echo (ping) request
27	2022-08-01 11:33:31.249828095	192.0.2.100	198.51.100.100	ICMP	108	0xc618 (50712)	64	Echo (ping) request
28	2022-08-01 11:33:31.249831121	192.0.2.100	198.51.100.100	ICMP	102	0xc618 (50712)	64	Echo (ping) request
29	2022-08-01 11:33:32.273876960	192.0.2.100	198.51.100.100	ICMP	108	0xc64f (50767)	64	Echo (ping) request

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	0x0c09 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found!)
2	2022-08-01 11:33:19.070695437	192.0.2.100	198.51.100.100	ICMP	102	0x0c09 (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	0x0c09 (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	0x0c09 (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	0x0c0a (49326)	64	Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found!)
6	2022-08-01 11:33:20.072038899	192.0.2.100	198.51.100.100	ICMP	102	0x0c0a (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	0x16f (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	0x16f (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	0x175 (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	0x175 (49525)	64	Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found!)
11	2022-08-01 11:33:23.075779089	192.0.2.100	198.51.100.100	ICMP	108	0x1e0 (49672)	64	Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found!)
12	2022-08-01 11:33:23.075781513	192.0.2.100	198.51.100.100	ICMP	102	0x1e0 (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	0x211 (49681)	64	Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found!)
14	2022-08-01 11:33:24.081841186	192.0.2.100	198.51.100.100	ICMP	102	0x211 (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	0x2e0 (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	0x2e0 (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	0x3b8 (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	0x3b8 (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	0x476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found!)
20	2022-08-01 11:33:27.153830281	192.0.2.100	198.51.100.100	ICMP	102	0x476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found!)
21	2022-08-01 11:33:28.177847175	192.0.2.100	198.51.100.100	ICMP	108	0x516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found!)
22	2022-08-01 11:33:28.177849075	192.0.2.100	198.51.100.100	ICMP	102	0x516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found!)
23	2022-08-01 11:33:28.190847660	192.0.2.100	198.51.100.100	ICMP	108	0x578 (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	0x578 (50552)	64	Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found!)
25	2022-08-01 11:33:30.225837465	192.0.2.100	198.51.100.100	ICMP	108	0x598 (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	0x598 (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	0x618 (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	0x618 (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!)

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.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 11:33:19.071512698	198.51.100.100	192.0.2.100	ICMP	108	1 0x4f27 (20263)	64	Echo (ping) reply id=0x0013, seq=1/256, ttl=64
2	2022-08-01 11:33:19.071514882	198.51.100.100	192.0.2.100	ICMP	108	0x4f27 (20263)	64	Echo (ping) reply id=0x0013, seq=1/256, ttl=64
3	2022-08-01 11:33:20.072677302	198.51.100.100	192.0.2.100	ICMP	108	0x41f0 (20475)	64	Echo (ping) reply id=0x0013, seq=2/512, ttl=64
4	2022-08-01 11:33:20.072679384	198.51.100.100	192.0.2.100	ICMP	108	0xdffb (20475)	64	Echo (ping) reply id=0x0013, seq=2/512, ttl=64
5	2022-08-01 11:33:21.073913640	198.51.100.100	192.0.2.100	ICMP	108	0x50ac (20652)	64	Echo (ping) reply id=0x0013, seq=3/768, ttl=64
6	2022-08-01 11:33:21.073915690	198.51.100.100	192.0.2.100	ICMP	108	0x50ac (20652)	64	Echo (ping) reply id=0x0013, seq=3/768, ttl=64
7	2022-08-01 11:33:22.075239381	198.51.100.100	192.0.2.100	ICMP	108	0x513e (20798)	64	Echo (ping) reply id=0x0013, seq=4/1024, ttl=64
8	2022-08-01 11:33:22.075241491	198.51.100.100	192.0.2.100	ICMP	108	0x513e (20798)	64	Echo (ping) reply id=0x0013, seq=4/1024, ttl=64
9	2022-08-01 11:33:23.076447152	198.51.100.100	192.0.2.100	ICMP	108	0x51c9 (20937)	64	Echo (ping) reply id=0x0013, seq=5/1280, ttl=64
10	2022-08-01 11:33:23.076449303	198.51.100.100	192.0.2.100	ICMP	108	0x51c9 (20937)	64	Echo (ping) reply id=0x0013, seq=5/1280, ttl=64
11	2022-08-01 11:33:24.082407896	198.51.100.100	192.0.2.100	ICMP	108	0x528e (21134)	64	Echo (ping) reply id=0x0013, seq=6/1536, ttl=64
12	2022-08-01 11:33:24.082410099	198.51.100.100	192.0.2.100	ICMP	108	0x528e (21134)	64	Echo (ping) reply id=0x0013, seq=6/1536, ttl=64
13	2022-08-01 11:33:25.106382424	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64	Echo (ping) reply id=0x0013, seq=7/1792, ttl=64
14	2022-08-01 11:33:25.106384549	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64	Echo (ping) reply id=0x0013, seq=7/1792, ttl=64
15	2022-08-01 11:33:26.130437851	198.51.100.100	192.0.2.100	ICMP	108	0x5346 (21414)	64	Echo (ping) reply id=0x0013, seq=8/2048, ttl=64
16	2022-08-01 11:33:26.130440320	198.51.100.100	192.0.2.100	ICMP	108	0x5346 (21414)	64	Echo (ping) reply id=0x0013, seq=8/2048, ttl=64
17	2022-08-01 11:33:27.075241491	198.51.100.100	192.0.2.100	ICMP	108	0x5446 (21574)	64	Echo (ping) reply id=0x0013, seq=9/2304, ttl=64
18	2022-08-01 11:33:27.154400918	198.51.100.100	192.0.2.100	ICMP	108	0x5446 (21574)	64	Echo (ping) reply id=0x0013, seq=9/2304, ttl=64
19	2022-08-01 11:33:28.178469866	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64	Echo (ping) reply id=0x0013, seq=10/2560, ttl=64
20	2022-08-01 11:33:28.178471810	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64	Echo (ping) reply id=0x0013, seq=10/2560, ttl=64
21	2022-08-01 11:33:29.202395869	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21748)	64	Echo (ping) reply id=0x0013, seq=11/2816, ttl=64
22	2022-08-01 11:33:29.202398067	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21748)	64	Echo (ping) reply id=0x0013, seq=11/2816, ttl=64
23	2022-08-01 11:33:30.226398735	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64	Echo (ping) reply id=0x0013, seq=12/3072, ttl=64
24	2022-08-01 11:33:30.226401017	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64	Echo (ping) reply id=0x0013, seq=12/3072, ttl=64
25	2022-08-01 11:33:31.259387088	198.51.100.100	192.0.2.100	ICMP	108	0x55f2 (22002)	64	Echo (ping) reply id=0x0013, seq=13/3328, ttl=64
26	2022-08-01 11:33:31.259389971	198.51.100.100	192.0.2.100	ICMP	108	0x55f2 (22002)	64	Echo (ping) reply id=0x0013, seq=13/3328, ttl=64
27	2022-08-01 11:33:32.274416011	198.51.100.100	192.0.2.100	ICMP	108	0x5660 (22112)	64	Echo (ping) reply id=0x0013, seq=14/3584, ttl=64
28	2022-08-01 11:33:32.274418229	198.51.100.100	192.0.2.100	ICMP	108	0x5660 (22112)	64	Echo (ping) reply id=0x0013, seq=14/3584, ttl=64
29	2022-08-01 11:33:33.298397657	198.51.100.100	192.0.2.100	ICMP	108	0x5667 (22247)	64	Echo (ping) reply id=0x0013, seq=15/3840, ttl=64

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 chassis interno usa para

encaminhar os pacotes para a 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.

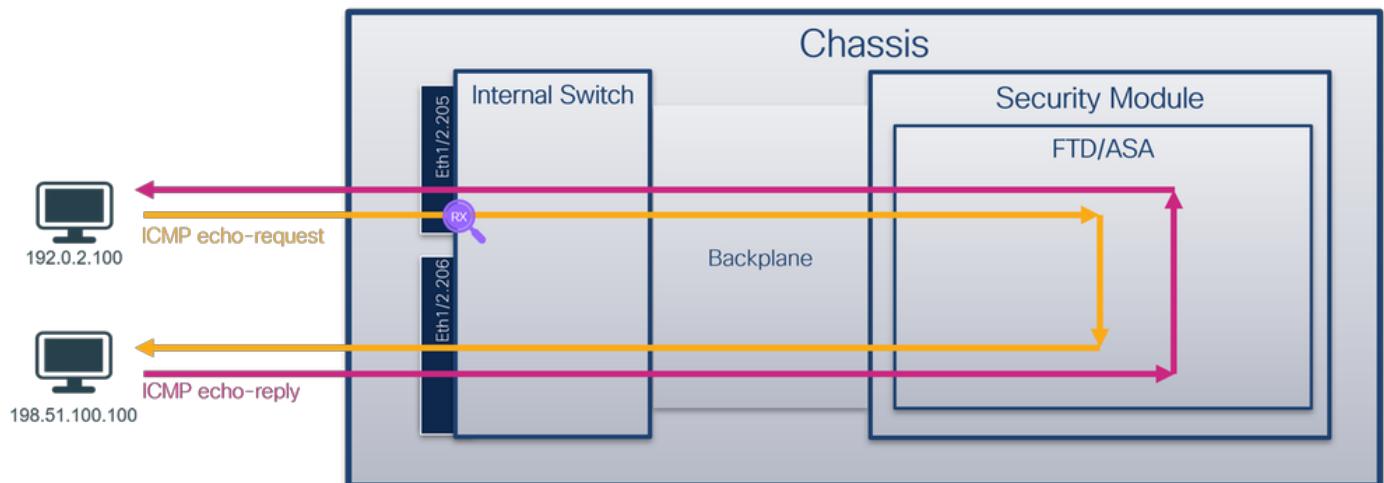
Esta tabela resume a tarefa:

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

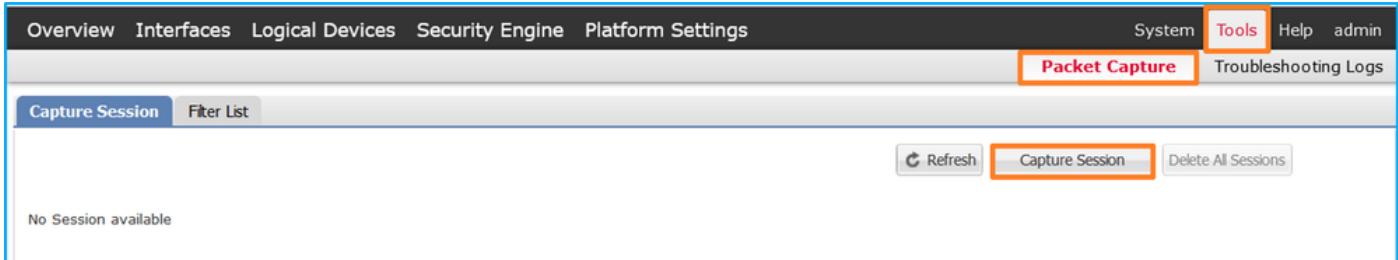


Configuração

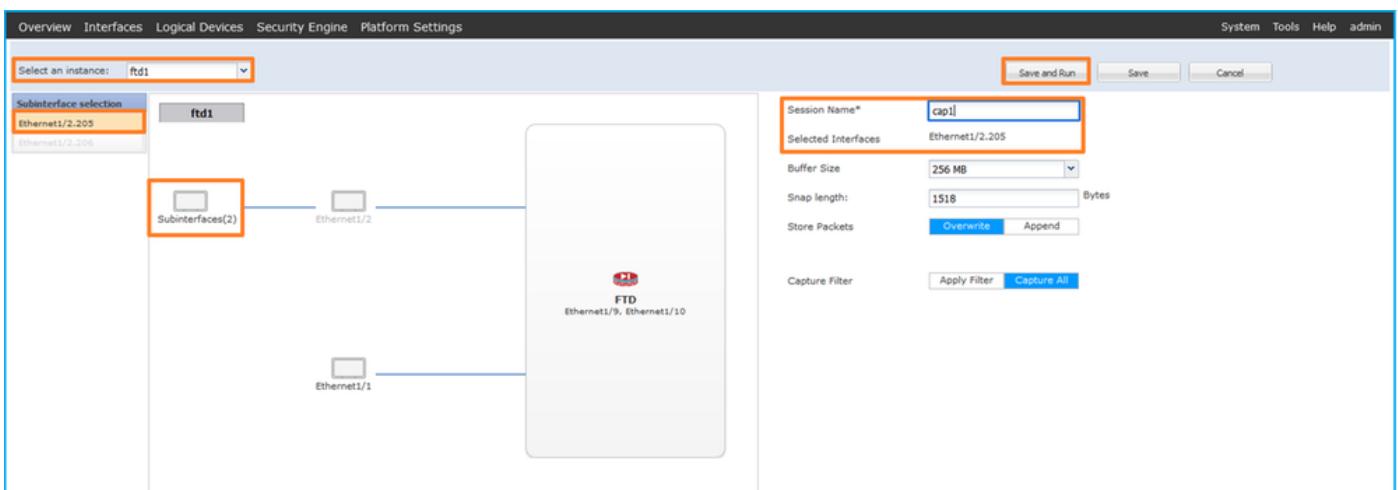
FCM

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

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



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



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

CLI FXOS

Execute 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:

```
<#root>  
firepower#  
scope ssa  
  
firepower /ssa #  
show app-instance
```

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version	Deploy Version	Type
ftd	ftd1							
1	ftd2	1	Enabled	Online	7.2.0.82	7.2.0.82	Container	No Container

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

```
<#root>

firepower#
connect fxos

<output skipped>
firepower(fxos)#

show port-channel summary

Flags: D - Down          P - Up in port-channel (members)
      I - Individual    H - Hot-standby (LACP only)
      S - Suspended      r - Module-removed
      S - Switched       R - Routed
      U - Up (port-channel)
      M - Not in use. Min-links not met
-----
Group Port-      Type      Protocol Member Ports
      Channel
-----
1      Po1(SU)     Eth       LACP      Eth1/3(P)   Eth1/3(P)
```

3. Criar uma sessão de captura:

```
<#root>

firepower#
scope packet-capture

firepower /packet-capture #
create session cap1

firepower /packet-capture/session* #
create phy-port Eth1/2

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

```

set app ftd

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

firepower /packet-capture/session/phy-port* #
set subinterface 205

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

firepower /packet-capture/session* #
enable

firepower /packet-capture/session* #
commit

firepower /packet-capture/session #

```

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

```

<#root>

firepower#
scope packet-capture

firepower /packet-capture #
create filter vlan207

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

firepower /packet-capture/filter* #
up

firepower /packet-capture* #
create session cap1

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

```

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

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

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

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

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

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

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

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

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

firepower /packet-capture/session* #
enable

firepower /packet-capture/session* #
commit

firepower /packet-capture/session #
```

Verificação

FCM

Verifique o nome da interface, assegure-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	firepower
Ethernet1/2.206	None			

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
Ethernet1/4.208	None	160	cap1-ethernet-1-4-0.pcap	Not available
Ethernet1/4.209	None			

CLI FXOS

Verifique os detalhes da captura em scope packet-capture:

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

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

Traffic Monitoring Session:

```
Packet Capture Session Name: cap1
```

```
Session: 1
```

```
Admin State: Enabled
```

```
Oper State: Up
```

```
Oper State Reason: Active
```

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

Physical ports involved in Packet Capture:

Slot Id: 1

Port Id: 2

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

Pcapsize: 9324 bytes

Filter:

Sub Interface: 205

Application Instance Identifier: ftd1

Application Name: ftd

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

<#root>

firepower#

scope packet-capture

firepower /packet-capture # show session cap1

Traffic Monitoring Session:

Packet Capture Session Name: cap1

Session: 1

Admin State: Enabled

Oper State: Up

Oper State Reason: Active

Config Success: Yes

Config Fail Reason:

Append Flag: Overwrite

Session Mem Usage: 256 MB

Session Pcap Snap Len: 1518 Bytes

Error Code: 0
Drop Count: 0

Physical ports involved in Packet Capture:

Slot Id: 1

Port Id: 3

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

Pcapsize: 160 bytes

Filter:

Sub Interface: 207

Application Instance Identifier: ftd1

Application Name: ftd

Slot Id: 1

Port Id: 4

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

Pcapsize: 624160 bytes

Filter:

Sub Interface: 207

Application Instance Identifier: ftd1

Application Name: ftd

Coletar arquivos de captura

Execute 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	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	0x9aa81 (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	0x9aa81 (39553)	64	Echo (ping) request id=0x0022, seq=10/2560, ttl=64 (no response found!)
5	2022-08-04 07:22:07.151113393	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 07:22:07.151113395	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	0xb9b33 (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	0xb9b33 (39731)	64	Echo (ping) request id=0x0022, seq=12/3072, ttl=64 (no response found!)
9	2022-08-04 07:22:09.253944661	192.0.2.100	198.51.100.100	ICMP	112	0x9cc0e (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	0x9cc0e (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	102	0xd9d84 (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	0xd9d84 (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 07:22:12.325937805	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	0x9e0f7 (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	0x9e0f7 (40455)	64	Echo (ping) request id=0x0022, seq=17/4352, ttl=64 (no response found!)
19	2022-08-04 07:22:14.341946249	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	0x9fe8 (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	0x9fe8 (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 07:22:17.413938099	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 1: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface capture_u0_1, id 0	Ethernet II, Src: VMware_9de8be (00:50:56:9d:e8:be), Dst: a2:76:f2:00:00:1b (a2:76:f2:00:00:1b)	0000 a2 76 f2 00 00 1b 00 50 56 9d e8 be 00 26 80 54 v .+p.v ..& T
VN-Tag	0010 00 00 81 00 00 66 81 00 00 cd 08 00 45 00 00 54 f .. E-T	
1.... = Direction: From Bridge	0020 95 74 40 00 40 01 b4 38 c0 00 02 64 c6 33 64 64 t@ @.B d3d	
.0... = Pointer: vif_id	0030 08 00 eb 95 00 22 00 01 88 73 eb 62 00 00 00 00 ..s b..	
..00 0000 0101 0100 = Destination: 84	0040 d9 94 00 00 00 00 00 00 10 11 12 13 14 15 16 17 ..I\$33..	
.... 0... = Looped: No	0050 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 ..L\$33..	
....0.... = Reserved: 0	0060 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 (*)+,-./ 01234567	
.....0000 0000 0000 ..0000 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		
....00 0010 0110 = ID: 102		
Type: 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		

Seleciona 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 07:21:56.993302102	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 07:22:06.214264777	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	0x9a83 (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	0x9a83 (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 07:22:10.253946899	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 07:22:10.277953078	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 07:22:11.301933606	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 07:22:13.326988049	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	0x9e64 (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	0x9e64 (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	0x9f8b (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	0x9f8b (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 07:22:17.413936899	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_u_0_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

- Somente os pacotes ICMP de solicitação de eco são capturados. Cada pacote é capturado e mostrado 2 vezes.
- O cabeçalho do pacote original tem a marca de VLAN 207.
- O switch interno insere uma tag de VLAN de porta adicional 1001 que identifica a interface de entrada Portchannel1.
- O switch interno insere uma marca VN adicional.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info	
1	2022-08-04 08:18:24.572548869	192.168.247.100	192.168.247.102	ICMP	128	0x6f09e (24734)	255	Echo (ping) request	id=0x007b, seq=0/0, ttl=255 (no response found!)
2	2022-08-04 08:18:24.572550073	192.168.247.100	192.168.247.102	ICMP	118	0x6f09e (24734)	255	Echo (ping) request	id=0x007b, seq=0/0, ttl=255 (no response found!)
3	2022-08-04 08:18:24.573286630	192.168.247.100	192.168.247.102	ICMP	128	0x6f09f (24735)	255	Echo (ping) request	id=0x007b, seq=1/256, ttl=255 (no response found!)
4	2022-08-04 08:18:24.573287640	192.168.247.100	192.168.247.102	ICMP	118	0x6f09f (24735)	255	Echo (ping) request	id=0x007b, seq=1/256, ttl=255 (no response found!)
5	2022-08-04 08:18:24.573794751	192.168.247.100	192.168.247.102	ICMP	128	0x6f0a0 (24736)	255	Echo (ping) request	id=0x007b, seq=2/512, ttl=255 (no response found!)
6	2022-08-04 08:18:24.573795748	192.168.247.100	192.168.247.102	ICMP	118	0x6f0a0 (24736)	255	Echo (ping) request	id=0x007b, seq=2/512, ttl=255 (no response found!)
7	2022-08-04 08:18:24.574368638	192.168.247.100	192.168.247.102	ICMP	128	0x6f0a0 (24737)	255	Echo (ping) request	id=0x007b, seq=3/768, ttl=255 (no response found!)
8	2022-08-04 08:18:24.574368538	192.168.247.100	192.168.247.102	ICMP	118	0x6f0a0 (24737)	255	Echo (ping) request	id=0x007b, seq=3/768, ttl=255 (no response found!)
9	2022-08-04 08:18:24.574914512	192.168.247.100	192.168.247.102	ICMP	128	0x6f0a2 (24738)	255	Echo (ping) request	id=0x007b, seq=4/1024, ttl=255 (no response found!)
10	2022-08-04 08:18:24.574915415	192.168.247.100	192.168.247.102	ICMP	118	0x6f0a2 (24738)	255	Echo (ping) request	id=0x007b, seq=4/1024, ttl=255 (no response found!)
11	2022-08-04 08:18:24.575442569	192.168.247.100	192.168.247.102	ICMP	128	0x6f0a3 (24739)	255	Echo (ping) request	id=0x007b, seq=5/1280, ttl=255 (no response found!)
12	2022-08-04 08:18:24.575443601	192.168.247.100	192.168.247.102	ICMP	118	0x6f0a3 (24739)	255	Echo (ping) request	id=0x007b, seq=5/1280, ttl=255 (no response found!)
13	2022-08-04 08:18:24.575918119	192.168.247.100	192.168.247.102	ICMP	128	0x6f0a4 (24740)	255	Echo (ping) request	id=0x007b, seq=6/1536, ttl=255 (no response found!)
14	2022-08-04 08:18:24.575919057	192.168.247.100	192.168.247.102	ICMP	118	0x6f0a4 (24740)	255	Echo (ping) request	id=0x007b, seq=7/1792, ttl=255 (no response found!)
15	2022-08-04 08:18:24.576407671	192.168.247.100	192.168.247.102	ICMP	128	0x6f0a5 (24741)	255	Echo (ping) request	id=0x007b, seq=8/2160, ttl=255 (no response found!)
16	2022-08-04 08:18:24.576408585	192.168.247.100	192.168.247.102	ICMP	118	0x6f0a5 (24741)	255	Echo (ping) request	id=0x007b, seq=8/2160, ttl=255 (no response found!)
17	2022-08-04 08:18:24.576488563	192.168.247.100	192.168.247.102	ICMP	128	0x6f0a6 (24742)	255	Echo (ping) request	id=0x007b, seq=8/2848, ttl=255 (no response found!)
18	2022-08-04 08:18:24.576886561	192.168.247.100	192.168.247.102	ICMP	118	0x6f0a6 (24742)	255	Echo (ping) request	id=0x007b, seq=9/2304, ttl=255 (no response found!)
19	2022-08-04 08:18:24.577394328	192.168.247.100	192.168.247.102	ICMP	128	0x6f0a7 (24743)	255	Echo (ping) request	id=0x007b, seq=9/2304, ttl=255 (no response found!)
20	2022-08-04 08:18:24.577395234	192.168.247.100	192.168.247.102	ICMP	118	0x6f0a7 (24743)	255	Echo (ping) request	id=0x007b, seq=10/2560, ttl=255 (no response found!)
21	2022-08-04 08:18:24.577987632	192.168.247.100	192.168.247.102	ICMP	128	0x6f0a8 (24744)	255	Echo (ping) request	id=0x007b, seq=10/2560, ttl=255 (no response found!)
22	2022-08-04 08:18:24.577989290	192.168.247.100	192.168.247.102	ICMP	118	0x6f0a8 (24744)	255	Echo (ping) request	id=0x007b, seq=10/2560, ttl=255 (no response found!)
23	2022-08-04 08:18:24.578448781	192.168.247.100	192.168.247.102	ICMP	128	0x6f0a9 (24745)	255	Echo (ping) request	id=0x007b, seq=11/2816, ttl=255 (no response found!)
24	2022-08-04 08:18:24.578449999	192.168.247.100	192.168.247.102	ICMP	118	0x6f0a9 (24745)	255	Echo (ping) request	id=0x007b, seq=11/2816, ttl=255 (no response found!)
25	2022-08-04 08:18:24.578900043	192.168.247.100	192.168.247.102	ICMP	128	0x6f0aa (24746)	255	Echo (ping) request	id=0x007b, seq=12/3072, ttl=255 (no response found!)
26	2022-08-04 08:18:24.578900997	192.168.247.100	192.168.247.102	ICMP	118	0x6f0aa (24746)	255	Echo (ping) request	id=0x007b, seq=12/3072, ttl=255 (no response found!)
27	2022-08-04 08:18:24.579426962	192.168.247.100	192.168.247.102	ICMP	128	0x6f0ab (24747)	255	Echo (ping) request	id=0x007b, seq=13/3328, ttl=255 (no response found!)

Frame 1: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface capture_u_0_3, id 0

Ethernet II, Src: Cisco d6:ec:00 (00:17:df:d6:ec:00), Dst: a2:76:f2:00:00:1c (a2:76:f2:00:00:1c)

✓ VNI-Tag

1.... = Direction: From Bridge

.0.... = Pointen: vif_id

..0 000 0001 0011 1101 = Destination: 61

.... 000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 = Looped: No

.... 000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 = Reserved: 0

.... 000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 = Version: 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 1100 1101 = 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

Seleciona 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 1: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface capture_w0_3, id 0

Frame 2: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface capture_w0_3, id 0

Ethernet II, Src: Cisco d6:ec: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: 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:

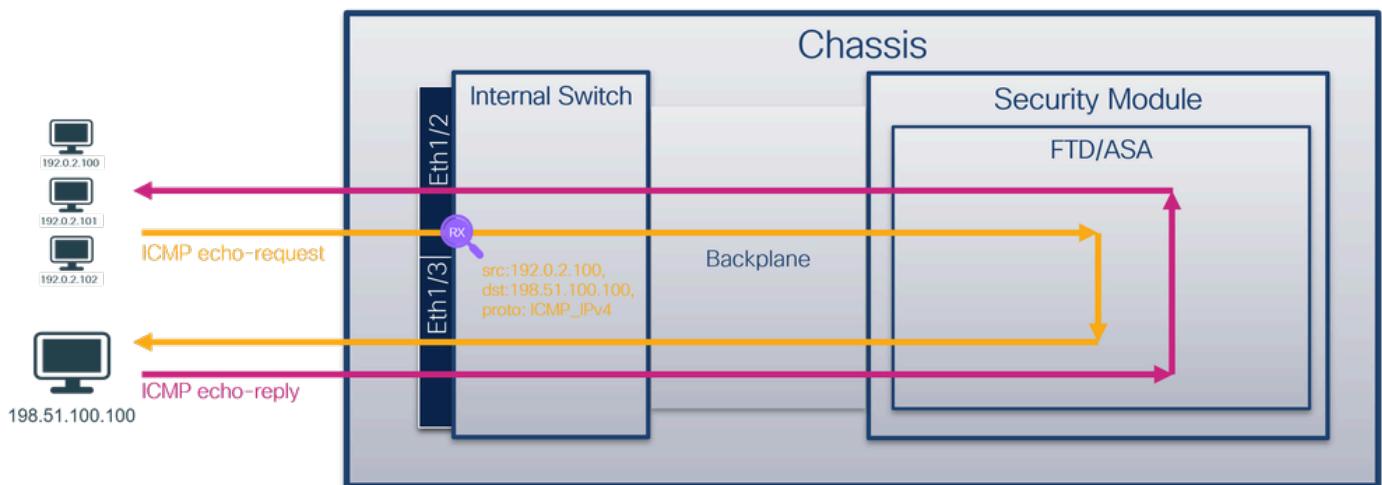
Tarefa	Ponto de captura	VLAN de porta interna em pacotes capturados	Direção	Tráfego capturado
Configurar e verificar uma captura de pacote na subinterface Ethernet1/2.205	Ethernet1/2.205	102	Somente entrada	Solicitações de eco ICMP do host 192.0.2.100 para o host 198.51.100.100
Configurar e verificar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

uma captura de pacote na subinterface Portchannel1 com as interfaces membro Ethernet1/3 e Ethernet1/4	Ethernet1/4		entrada 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:

Capture Session **Filter List**

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

Edit Packet Filter

Filter Name*: filter_icmp
Protocol: ICMP_IPv4
EtherType: Any
Inner vlan: 0 Outer vlan: 0
Source: IPv4 192.0.2.100 Destination: IPv4 198.51.100.100
IPv6 :: IPv6 ::
Port: 0 Port: 0
MAC: 00:00:00:00:00:00 MAC: 00:00:00:00:00:00

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

Overview Interfaces Logical Devices Security Engine Platform Settings System **Tools** Help admin

Packet Capture

Capture Session **Filter List**

Refresh Capture Session Delete All Sessions

No Session available

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

Select an instance: ftd1

Session Name*: cap1
Selected Interfaces: Ethernet1/2
Buffer Size: 256 MB
Snap length: 1518 Bytes
Store Packets: Overwrite Append

Capture Filter: **filter_icmp** To: **Ethernet1/2**

CLI FXOS

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

1. Identificar o tipo de aplicativo e o identificador:

```
<#root>

firepower#
scope ssa

firepower /ssa#
show app-instance

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

2. 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:

```
<#root>

firepower#
scope packet-capture

firepower /packet-capture #
create filter filter_icmp

firepower /packet-capture/filter* #
set destip 198.51.100.100

firepower /packet-capture/filter* #
set protocol 1

firepower /packet-capture/filter* #
set srcip 192.0.2.100

firepower /packet-capture/filter* #
exit

firepower /packet-capture* #
```

```

create session cap1

firepower /packet-capture/session* #

create phy-port Ethernet1/2

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

set app ftd

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

set app-identifier ftd1

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

set filter filter_icmp

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

exit

firepower /packet-capture/session* #

enable

firepower /packet-capture/session* #

commit

firepower /packet-capture/session #

```

Verificação

FCM

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

Filter List													Add Filter
Filter Name	From				To				Protocol	Inner vlan	Outer vlan	EtherType	
	HAC	IPv4	IPv6	Port	HAC	IPv4	IPv6	Port					
filter_icmp	00:00:00:00:00:00	192.0.2.100		11	0	00:00:00:00:00:00	198.51.100.100	11	0	3	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:



CLI FXOS

Verifique os detalhes da captura em scope packet-capture:

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

firepower /packet-capture #
show filter detail
```

Configure a filter for packet capture:

```
Name: filter_icmp
```

```
Protocol: 1
```

```
Ivlan: 0
Ovlan: 0
```

```
src Ip: 192.0.2.100
```

```
Dest Ip: 198.51.100.100
```

```
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0
Src Ipv6: ::

Dest Ipv6: ::

firepower /packet-capture #

show session cap1
```

Traffic Monitoring Session:

```
Packet Capture Session Name: cap1
```

```
Session: 1
```

Admin State: Enabled

Oper State: Up

Oper State Reason: Active

Config Success: Yes

Config Fail Reason:

Append Flag: Overwrite

Session Mem Usage: 256 MB

Session Pcap Snap Len: 1518 Bytes

Error Code: 0

Drop Count: 0

Physical ports involved in Packet Capture:

slot Id: 1

Port Id: 2

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

Pcapsize: 213784 bytes

Filter: filter_icmp

Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

Coletar arquivos de captura

Execute 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.

- 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 entrada Ethernet1/2.
- O switch interno insere uma marca VN adicional.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-02 15:46:55.603277760	192.0.2.100	198.51.100.100	ICMP	108	1 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, interface Cisco b9:77:0e (58:97:bd:b9:77:0e)
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
.....0... = Looped: No
.....0... = Reserved: 0
.....0... = Version: 0
.....00... = 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:

- Somente os pacotes ICMP de solicitação de eco são capturados. Cada pacote é capturado e mostrado 2 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 entrada Ethernet1/2.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-02 15:46:55.603277760	192.0.2.100	198.51.100.100	ICMP	108	1 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, interface Cisco b9:77:0e (58:97:bd:b9:77:0e)
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
.....0... = Looped: No
.....0... = Reserved: 0
.....0... = Version: 0
.....00... = 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

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 do host 192.0.2.100 para o host 198.51.100.100

Coletar Arquivos De Captura Do Switch Interno Firepower 4100/9300

FCM

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

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

The screenshot shows the FCM interface with the 'Capture Session' tab selected. At the top, there are buttons for Refresh, Capture Session, and Delete All Sessions. Below that is a summary row with session ID 'cap1', drop count '0', operational state 'up', buffer size '256 MB', and snap length '1518 Bytes'. A table below lists captured packets with columns: Interface Name, Filter, File Size (in bytes), File Name, and Device Name. One entry is shown: 'Ethernet1/2' with 'None' filter, file size 34700, file name 'cap1-ethernet-1-2-0.pcap', and device name 'ftd1'. There are also icons for download and delete.

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

Capture Session Filter List

Operational State: DOWN - Session_Admin_Shut

File Size (in bytes): 218828

Device Name: ftd1

3. Clique em Download para fazer download do arquivo de captura:

Capture Session Filter List

Operational State: DOWN - Session_Admin_Shut

File Size (in bytes): 218828

Device Name: ftd1

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

CLI FXOS

Execute estas etapas na CLI do FXOS para coletar arquivos de captura:

1. Pare a captura ativa:

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

firepower /packet-capture #
scope session cap1

firepower /packet-capture/session #
disable

firepower /packet-capture/session* #
commit

firepower /packet-capture/session #
up

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

Traffic Monitoring Session:
Packet Capture Session Name:

```
cap1
```

```
Session: 1
```

```
Admin State: Disabled
```

```
Oper State: Down
```

```
Oper State Reason: Admin Disable
```

```
Config Success: Yes
```

```
Config Fail Reason:
```

```
Append Flag: Overwrite
```

```
Session Mem Usage: 256 MB
```

```
Session Pcap Snap Len: 1518 Bytes
```

```
Error Code: 0
```

```
Drop Count: 0
```

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

```
Slot Id: 1
```

```
Port Id: 2
```

```
Pcapfile:
```

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

```
Pcapsize: 115744 bytes
```

```
Filter:
```

```
Sub Interface: 0
```

```
Application Instance Identifier: ftd1
```

```
Application Name: ftd
```

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

```
<#root>
```

```
firepower#
```

```
connect local-mgmt
```

```
firepower(local-mgmt)#
```

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

```
ftp: Dest File URI
```

```
http: Dest File URI
```

```
https: Dest File URI
```

```
scp: Dest File URI
```

```
sftp: Dest File URI
```

```
tftp: Dest File URI
```

```
usbdrive: Dest File URI
```

```
volatile: Dest File URI
```

```
workspace: Dest File URI
```

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

Password:

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

Diretrizes, Limitações e Práticas Recomendadas para Captura de Pacotes de Switch Interno

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 membro do 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 no Secure Firewall 1200/3100/4200

Diferentemente do Firepower 4100/9300, as capturas de switch interno no Secure Firewall 1200/3100/4200 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`:

```
<#root>

> capture cap_sw switch

?

buffer      Configure size of capture buffer, default is 256MB
ether-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:

```
<#root>

>

capture capswh 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
```

O Secure Firewall 1200/4200 suporta capturas bidirecionais. O valor padrão é ingresso, a menos

que especificado de outra forma:

```
<#root>
>
capture capi switch interface inside direction

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

Além disso, o Secure Firewall 4245 tem 2 interfaces de uplink de gerenciamento e dados internos:

```
<#root>
>
capture capsw switch interface

eventing      Name of interface Management1/2
in_data_uplink1 Capture packets on internal data uplink1 interface
in_data_uplink2 Capture packets on internal data uplink2 interface
in_mgmt_uplink1 Capture packets on internal mgmt uplink1 interface
in_mgmt_uplink2 Capture packets on internal mgmt uplink2 interface
management     Name of interface Management1/1
```

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

```
<#root>
>
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:

```
<#root>
>
capture capsw switch interface inside match ?

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

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

```
<#root>
>
capture capsw switch interface inside match ip

>
no capture capsw switch stop
```

6. Verifique os detalhes da captura:

- O status administrativo é enabled, e o status operacional é up e ative.
- O tamanho do arquivo de captura de pacote Pcapsize aumenta.

- O número de pacotes capturados na saída de show capture <cap_name> é diferente de zero.
- Capturar caminho Pcapfile. Os pacotes capturados são salvos automaticamente na pasta /mnt/disk0/packet-capture/.
- Capturar condições. O software cria automaticamente filtros de captura com base nas condições de captura.

```
<#root>
```

```
>
```

```
show capture capsw
```

```
27 packet captured on disk using switch capture
```

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

```
>
```

```
show capture capsw detail
```

```
Packet Capture info
```

```
Name: capsw
```

```
Session: 1
```

```
Admin State: enabled
```

```
Oper State: up
```

```
Oper State Reason: Active
```

```
Config Success: yes
```

```
Config Fail Reason:
```

```
Append Flag: overwrite
```

```
Session Mem Usage: 256
```

```
Session Pcap Snap Len: 1518
```

```
Error Code: 0
```

```
Drop Count: 0
```

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

```
Physical port:
```

```
Slot Id: 1
```

```
Port Id: 1
```

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

```
Pcapsize: 18838
```

Filter: caps-w-1-1

Packet Capture Filter Info

Name: caps-w-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:

```
<#root>  
>  
capture caps-w switch stop
```

```
>  
show capture caps-w detail
```

Packet Capture info

Name: caps-w

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:              caps-w-1-1

Packet Capture Filter Info
Name:                caps-w-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. Execute as etapas na seção Coletar arquivos de captura do switch interno do firewall seguro.

No software Secure Firewall versão 7.7, 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.

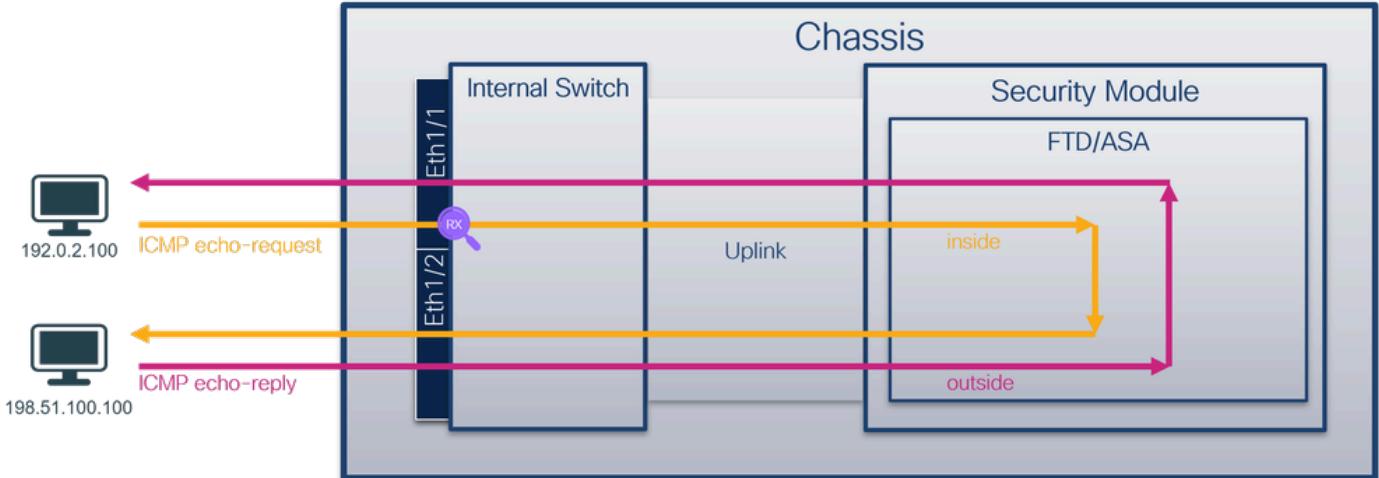
Esses cenários cobrem casos de uso comuns de capturas de switches internos do Secure Firewall 1200/3100/4200.

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

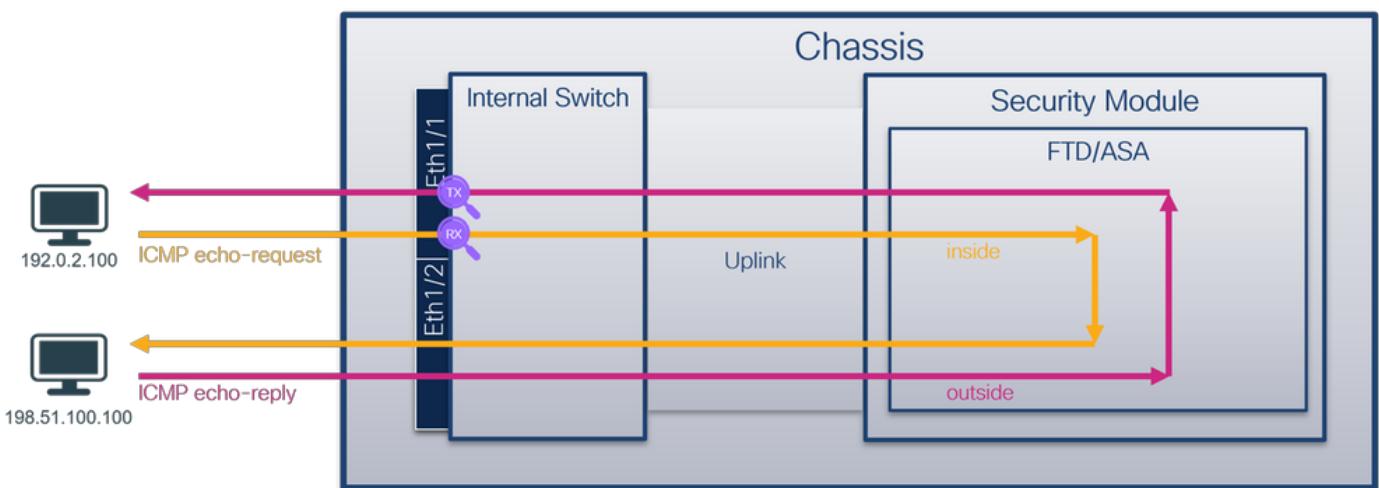
Use o FTD ou o ASA CLI para configurar e verificar uma captura de pacote na interface Ethernet1/1 ou Portchannel1. Ambas as interfaces têm o nome if inside.

Topologia, fluxo de pacotes e pontos de captura

Firewall seguro 3100:



Firewall seguro 1200/4200:



Configuração

Execute 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:

```
<#root>
```

```
>
```

```
show nameif
```

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

```
<#root>
```

```
>

show nameif

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

2. Criar uma sessão de captura

```
<#root>

>

capture capsw switch interface inside
```

O Secure Firewall 1200/4200 suporta direcionalidade de captura:

```
<#root>

> capture capsw switch interface inside direction ?

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

> capture capsw switch interface inside direction both
```

3. Habilitar a sessão de captura:

```
<#root>

> 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:

```
<#root>
```

>

```
show capture capsw detail
```

Packet Capture info

Name: capsw

Session: 1

Admin State: enabled

Oper State: up

Oper State Reason: Active

Config Success: yes

Config Fail Reason:

Append Flag: overwrite

Session Mem Usage: 256

Session Pcap Snap Len: 1518

Error Code: 0

Drop Count: 0

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1

Port Id: 1

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

Pcapsize: 12653

Filter: capsw-1-1

Packet Capture Filter Info

Name: capsw-1-1

Protocol: 0

Ivlan: 0

Ovlan: 0

Src Ip: 0.0.0.0

Dest Ip: 0.0.0.0

Src Ipv6: ::

Dest Ipv6: ::

Src MAC: 00:00:00:00:00:00

Dest MAC: 00:00:00:00:00:00

Src Port: 0

Dest Port: 0

Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

```
79 packets captured on disk using switch capture
```

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

```
Firewall seguro 1200/4200:
```

```
<#root>  
>  
show cap caps w detail
```

```
Packet Capture info
```

```
Name: caps w  
  
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-caps w-ethernet-1-1-0.pcap  
Pcapsize: 0
```

```
Direction: both
```

```
Drop: disable  
Filter: caps w-1-1
```

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

```
Dest Ip:          0.0.0.0
Src Ipv6:         :: 
Dest Ipv6:         :: 
Src MAC:          00:00:00:00:00:00
Dest MAC:          00:00:00:00:00:00
Src Port:          0
Dest Port:         0
Ethertype:        0
```

Total Physical breakout ports involved in Packet Capture: 0

```
33 packet captured on disk using switch capture
```

Reading of capture file from disk is not supported

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

```
<#root>
```

```
>
```

```
show capture capsw detail
```

Packet Capture info

```
Name:           capsw
```

```
Session:        1
```

```
Admin State:    enabled
```

```
Oper State:     up
```

```
Oper State Reason: Active
```

```
Config Success: yes
```

```
Config Fail Reason:
```

```
Append Flag:    overwrite
```

```
Session Mem Usage: 256
```

```
Session Pcap Snap Len: 1518
```

```
Error Code:     0
```

```
Drop Count:     0
```

Total Physical ports involved in Packet Capture: 2

Physical port:

```
Slot Id:        1
```

```
Port Id:        4
```

```
Pcapfile:          /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-4-0.pcap
Pcapsize:         28824

Filter:           caps-w-1-4
```

Packet Capture Filter Info

Name:	caps-w-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:           caps-w-1-3
```

Packet Capture Filter Info

Name:	caps-w-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:

```
<#root>
>
connect fxos

...
firewall#
connect local-mgmt

firewall(local-mgmt)#
show portchannel summary

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

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

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

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

Execute as etapas na seção Coletar arquivos de captura do switch interno do firewall seguro.

Capturar análise de arquivo

Use um aplicativo leitor de arquivo de captura de pacote para abrir os arquivos de captura para Ethernet1/1. Neste exemplo, a captura de pacotes no Secure Firewall 3100 é analisada. 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	1 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	2 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	3 0x9aae (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	4 0x9afe (39678)	64	Echo (ping) request id=0x0034, seq=4/1024, ttl=64 (no res)
5	2022-08-07 19:50:10.928245	192.0.2.100	198.51.100.100	ICMP	102	5 0x9b10 (39696)	64	Echo (ping) request id=0x0034, seq=5/1280, ttl=64 (no res)
6	2022-08-07 19:50:11.929144	192.0.2.100	198.51.100.100	ICMP	102	6 0x9b34 (39732)	64	Echo (ping) request id=0x0034, seq=6/1536, ttl=64 (no res)
7	2022-08-07 19:50:12.932943	192.0.2.100	198.51.100.100	ICMP	102	7 0x9b83 (39811)	64	Echo (ping) request id=0x0034, seq=7/1792, ttl=64 (no res)
8	2022-08-07 19:50:13.934155	192.0.2.100	198.51.100.100	ICMP	102	8 0x9b19 (39819)	64	Echo (ping) request id=0x0034, seq=8/2048, ttl=64 (no res)
9	2022-08-07 19:50:14.932004	192.0.2.100	198.51.100.100	ICMP	102	9 0x9c07 (39943)	64	Echo (ping) request id=0x0034, seq=9/2304, ttl=64 (no res)
10	2022-08-07 19:50:15.937143	192.0.2.100	198.51.100.100	ICMP	102	10 0x9c6 (40134)	64	Echo (ping) request id=0x0034, seq=10/2560, ttl=64 (no res)
11	2022-08-07 19:50:16.934848	192.0.2.100	198.51.100.100	ICMP	102	11 0x9d68 (40296)	64	Echo (ping) request id=0x0034, seq=11/2816, ttl=64 (no res)
12	2022-08-07 19:50:17.936908	192.0.2.100	198.51.100.100	ICMP	102	12 0x9ded (40429)	64	Echo (ping) request id=0x0034, seq=12/3072, ttl=64 (no res)
13	2022-08-07 19:50:18.939584	192.0.2.100	198.51.100.100	ICMP	102	13 0x9e5a (40538)	64	Echo (ping) request id=0x0034, seq=13/3328, ttl=64 (no res)
14	2022-08-07 19:50:19.941262	192.0.2.100	198.51.100.100	ICMP	102	14 0x9efb (40699)	64	Echo (ping) request id=0x0034, seq=14/3584, ttl=64 (no res)
15	2022-08-07 19:50:20.940716	192.0.2.100	198.51.100.100	ICMP	102	15 0x9f50 (40784)	64	Echo (ping) request id=0x0034, seq=15/3840, ttl=64 (no res)
16	2022-08-07 19:50:21.940288	192.0.2.100	198.51.100.100	ICMP	102	16 0x9f4e (40932)	64	Echo (ping) request id=0x0034, seq=16/4096, ttl=64 (no res)
17	2022-08-07 19:50:22.943302	192.0.2.100	198.51.100.100	ICMP	102	17 0xa031 (41009)	64	Echo (ping) request id=0x0034, seq=17/4352, ttl=64 (no res)
18	2022-08-07 19:50:23.944679	192.0.2.100	198.51.100.100	ICMP	102	18 0xa067 (41063)	64	Echo (ping) request id=0x0034, seq=18/4608, ttl=64 (no res)

Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
 > Ethernet II, Src: VMware_9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco_34:9a:14 (bc:e7:12:34:9a:14)
 > Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
 > Internet Control Message Protocol

0000 bc e7 12 34 9a 14 00 50 56 9d e8 be 08 00 45 00 ...4...P V....E.
 0010 00 54 9a 10 40 00 40 01 b3 9c c0 00 02 64 c6 33 -T-@...d-3
 0020 64 64 08 00 c6 91 00 34 00 01 61 17 f0 62 00 00 dd...4...a-b..
 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 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	1 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	2 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	3 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	4 0x946f (37999)	64	Echo (ping) request id=0x0035, seq=4/1024, ttl=64 (no res)
5	2022-08-07 20:41:02.660624	192.0.2.100	198.51.100.100	ICMP	102	5 0x94a4 (38052)	64	Echo (ping) request id=0x0035, seq=5/1280, ttl=64 (no res)
6	2022-08-07 20:41:03.663226	192.0.2.100	198.51.100.100	ICMP	102	6 0x952d (38189)	64	Echo (ping) request id=0x0035, seq=6/1536, ttl=64 (no res)
7	2022-08-07 20:41:04.661262	192.0.2.100	198.51.100.100	ICMP	102	7 0x958d (38285)	64	Echo (ping) request id=0x0035, seq=7/1792, ttl=64 (no res)
8	2022-08-07 20:41:05.665955	192.0.2.100	198.51.100.100	ICMP	102	8 0x95d8 (38360)	64	Echo (ping) request id=0x0035, seq=8/2048, ttl=64 (no res)
9	2022-08-07 20:41:06.666538	192.0.2.100	198.51.100.100	ICMP	102	9 0x964b (38475)	64	Echo (ping) request id=0x0035, seq=9/2304, ttl=64 (no res)
10	2022-08-07 20:41:07.667298	192.0.2.100	198.51.100.100	ICMP	102	10 0x972b (38699)	64	Echo (ping) request id=0x0035, seq=10/2560, ttl=64 (no res)
11	2022-08-07 20:41:08.670540	192.0.2.100	198.51.100.100	ICMP	102	11 0x980a (38922)	64	Echo (ping) request id=0x0035, seq=11/2816, ttl=64 (no res)
12	2022-08-07 20:41:09.668278	192.0.2.100	198.51.100.100	ICMP	102	12 0x9831 (38961)	64	Echo (ping) request id=0x0035, seq=12/3072, ttl=64 (no res)
13	2022-08-07 20:41:10.672417	192.0.2.100	198.51.100.100	ICMP	102	13 0x98a2 (39074)	64	Echo (ping) request id=0x0035, seq=13/3328, ttl=64 (no res)
14	2022-08-07 20:41:11.671369	192.0.2.100	198.51.100.100	ICMP	102	14 0x98f7 (39159)	64	Echo (ping) request id=0x0035, seq=14/3584, ttl=64 (no res)
15	2022-08-07 20:41:12.675462	192.0.2.100	198.51.100.100	ICMP	102	16 0x99e4 (39396)	64	Echo (ping) request id=0x0035, seq=15/3840, ttl=64 (no res)
16	2022-08-07 20:41:13.674903	192.0.2.100	198.51.100.100	ICMP	102	17 0x9a84 (39556)	64	Echo (ping) request id=0x0035, seq=16/4096, ttl=64 (no res)
17	2022-08-07 20:41:14.674093	192.0.2.100	198.51.100.100	ICMP	102	18 0x9af3 (39667)	64	Echo (ping) request id=0x0035, seq=17/4352, ttl=64 (no res)
18	2022-08-07 20:41:15.676904	192.0.2.100	198.51.100.100	ICMP	102	19 0xb8e (39822)	64	Echo (ping) request id=0x0035, seq=18/4608, ttl=64 (no res)

Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
 > Ethernet II, Src: VMware_9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco_34:9a:2c (bc:e7:12:34:9a:2c)
 > Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
 > Internet Control Message Protocol

0000 bc e7 12 34 9a 2c 00 50 56 9d e8 be 08 00 45 00 ...4...P V....E.
 0010 00 54 92 96 40 00 40 01 bb 1c c0 00 02 64 c6 33 -T-@...d-3
 0020 64 64 08 00 58 a8 00 35 00 01 4d 23 f0 62 00 00 dd...X-5...M-b..
 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 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	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 Ethernet1/3 e Ethernet1/4	Ethernet1/3 Ethernet1/4	Nenhum	Somente entrada*	Solicitações de eco ICMP do host 192.0.2.100 para o host 198.51.100.100

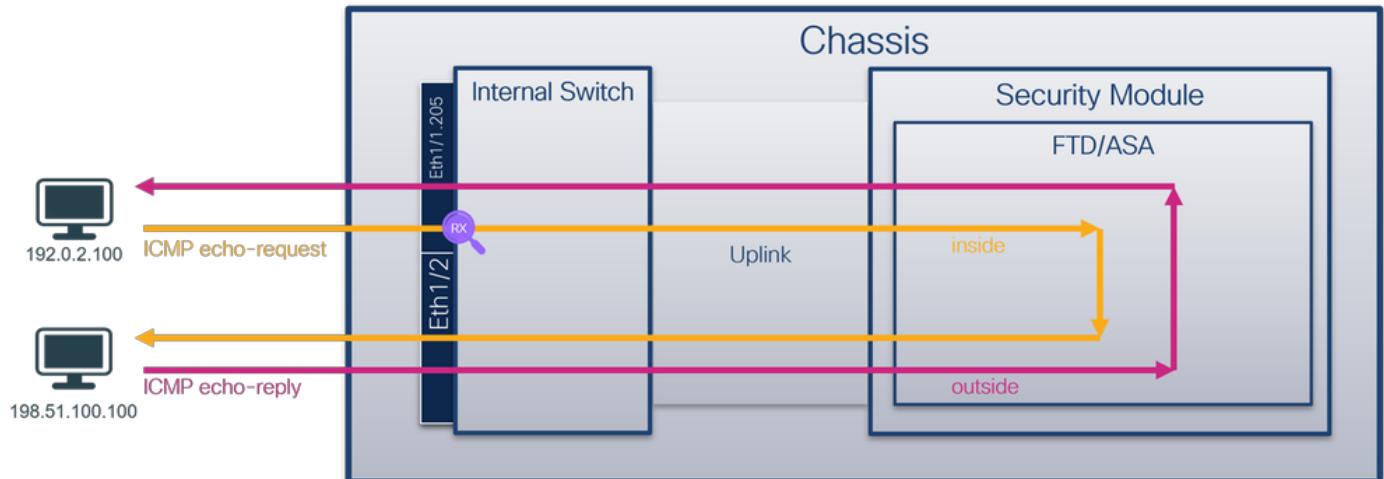
* Diferentemente do 3100, o Secure Firewall 1200/4200 suporta capturas bidirecionais (entrada e saída).

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

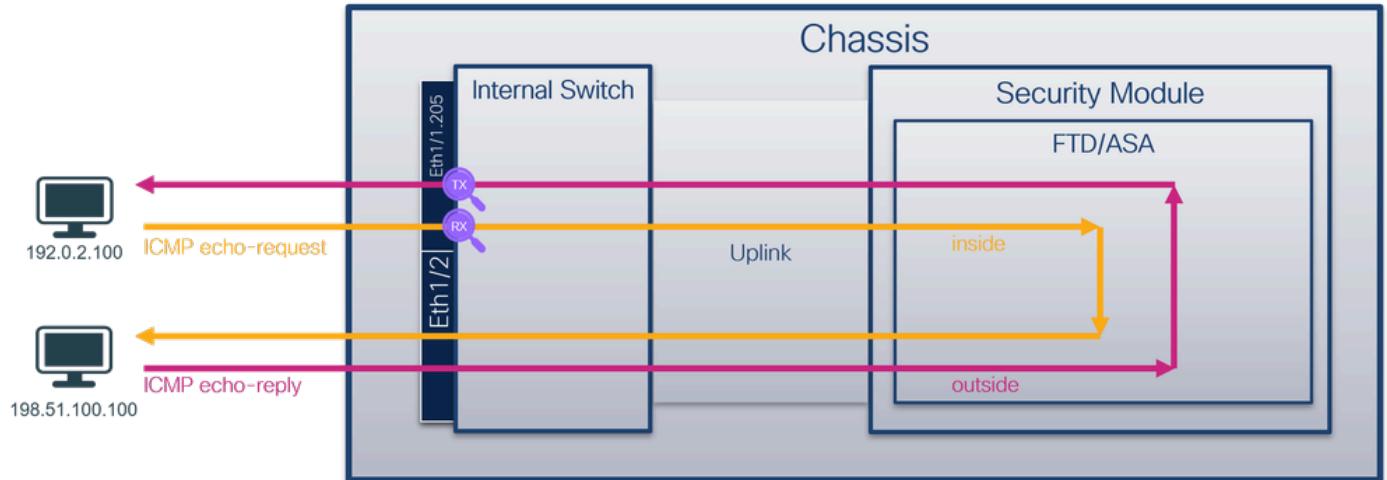
Use o FTD ou o ASA CLI para configurar e verificar uma captura de pacote nas subinterfaces Ethernet1/1.205 ou Portchannel1.205. Ambas as subinterfaces têm o nome inside.

Topologia, fluxo de pacotes e pontos de captura

Firewall seguro 3100:



Firewall seguro 1200/4200:



Configuração

Execute 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:

```
<#root>
```

```
>
```

```
show nameif
```

Interface	Name	Security
Ethernet1/1.205	inside	0
Ethernet1/2	outside	0
Management1/1	diagnostic	0

```
<#root>
```

```
>
```

```
show nameif
```

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

2. Criar uma sessão de captura:

```
<#root>

>

capture capsw switch interface inside
```

O Secure Firewall 1200/4200 suporta direcionalidade de captura:

```
<#root>

> capture capsw switch interface inside direction ?

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

> capture capsw switch interface inside direction both
```

3. Ative a sessão de captura:

```
<#root>

> 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:

```
<#root>

>

show capture capsw detail
```

Packet Capture info

Name:	capsw
Session:	1
Admin State:	enabled
Oper State:	up

Oper State Reason: Active

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

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1

Port Id: 1

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

Pcapsize: 6360

Filter: capsw-1-1

Packet Capture Filter Info

Name: capsw-1-1

Protocol: 0

Ivlan: 0

Ovlan: 205

Src Ip: 0.0.0.0

Dest Ip: 0.0.0.0

Src Ipv6: ::

Dest Ipv6: ::

Src MAC: 00:00:00:00:00:00

Dest MAC: 00:00:00:00:00:00

Src Port: 0

Dest Port: 0

Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

46 packets captured on disk using switch capture

Reading of capture file from disk is not supported

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:

```
<#root>  
>  
show capture caps w detail
```

Packet Capture info

```
Name: caps w  
  
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-caps w-ether net-1-4-0.pcap  
Pcapsize: 23442  
  
Filter: caps w-1-4
```

```
Packet Capture Filter Info  
Name: caps w-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:           caps-w-1-3
```

Packet Capture Filter Info

```
Name:             caps-w-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:

```
<#root>
```

```
>
```

```
connect fxos
```

```

...
firewall#
connect local-mgmt

firewall(local-mgmt)#
show portchannel summary

Flags: D - Down      P - Up in port-channel (members)
I - Individual H - Hot-standby (LACP only)
S - Suspended r - Module-removed
S - Switched R - Routed
U - Up (port-channel)
M - Not in use. Min-links not met
-----
Group Port-      Type     Protocol Member Ports
  Channel
-----
1    Po1(U)      Eth      LACP      Eth1/3(P)   Eth1/4(P)

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

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

```

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

Execute as etapas na seção Coletar arquivos de captura do switch interno do firewall seguro.

Capturar análise de arquivo

Use um aplicativo leitor de arquivo de captura de pacote para abrir os arquivos de captura para Ethernet1/1.205. Neste exemplo, a captura de pacotes no Secure Firewall 3100 é analisada. 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	1 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

00. = 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	1 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

00. = 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	Ethernet1/1	VLAN	Somente	Solicitações de eco ICMP do

captura de pacote na subinterface Ethernet1/1.205		Externa 205	entrada*	host 192.0.2.100 para o host 198.51.100.100
Configurar e verificar uma captura de pacote na subinterface Portchannel1.205 com as interfaces de membro Ethernet1/3 e Ethernet1/4	Ethernet1/3 Ethernet1/4	VLAN Externa 205	Somente entrada*	Solicitações de eco ICMP do host 192.0.2.100 para o host 198.51.100.100

* Diferentemente do 3100, o Secure Firewall 1200/4200 suporta capturas bidirecionais (entrada e saída).

Captura de pacotes em interfaces internas

O Secure Firewall 3100 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.

O Secure Firewall 1200 tem até 3 interfaces internas:

- in_data_uplink1 - específico para 1210 e 1250, essas interfaces conectam o aplicativo ao switch interno.
- in_data_uplink1, in_data_uplink2, in_data_uplink3 e in_mgmt_uplink2 - específicas para 1220, 1230, 1240, essas interfaces conectam o aplicativo ao switch interno.

 Note: Como a interface de gerenciamento no Secure Firewall 1200 está fora de banda, não há interfaces in_mgmt_uplink disponíveis neste modelo.

O Secure Firewall 4200 tem até 4 interfaces internas:

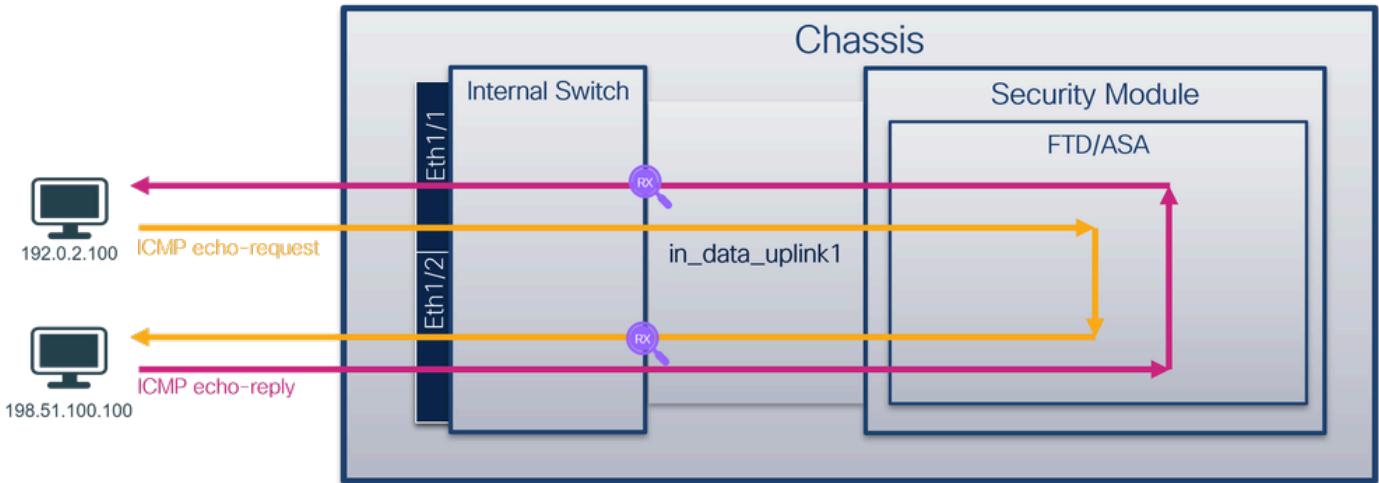
- in_data_uplink1 e in_data_uplink2 (somente 4245) - essas interfaces conectam o aplicativo ao switch interno. No caso do 4245, os pacotes têm平衡amento de carga nas duas interfaces de uplink.
 - in_mgmt_uplink1 e in_mgmt_uplink2 - essas interfaces fornecem um caminho de pacote dedicado para conexões de gerenciamento, como SSH para a interface de gerenciamento, ou a conexão de gerenciamento, também conhecida como sftunnel, entre o FMC e o FTD.
- O Secure Firewall 4200 suporta 2 interfaces de gerenciamento.

Tarefa 1

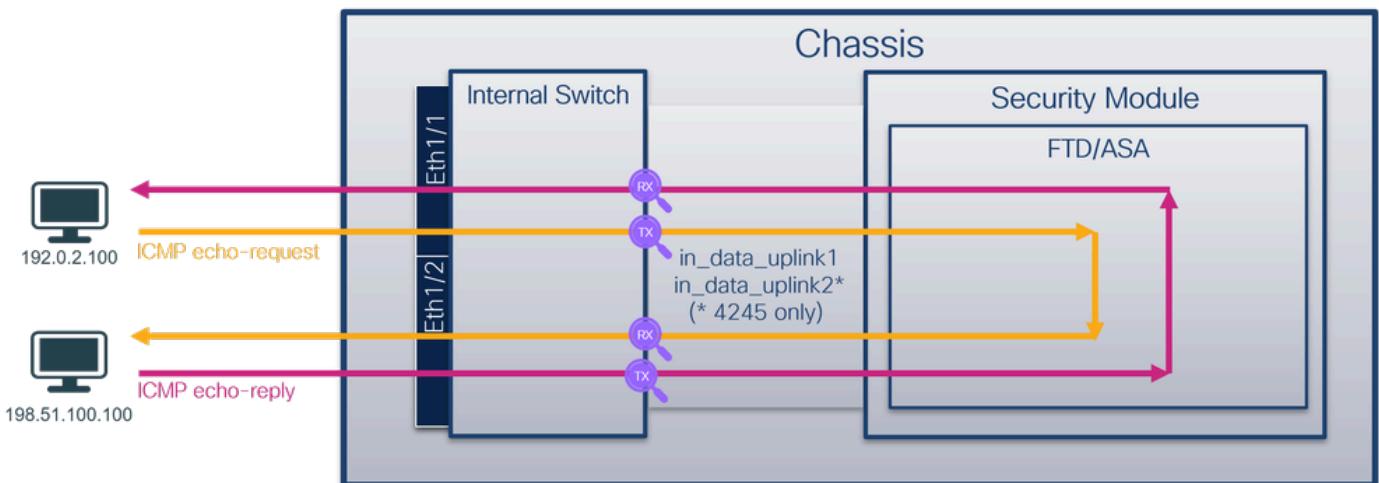
Use o FTD ou o ASA CLI para configurar e verificar uma captura de pacotes nas interfaces de uplink de dados.

Topologia, fluxo de pacotes e pontos de captura

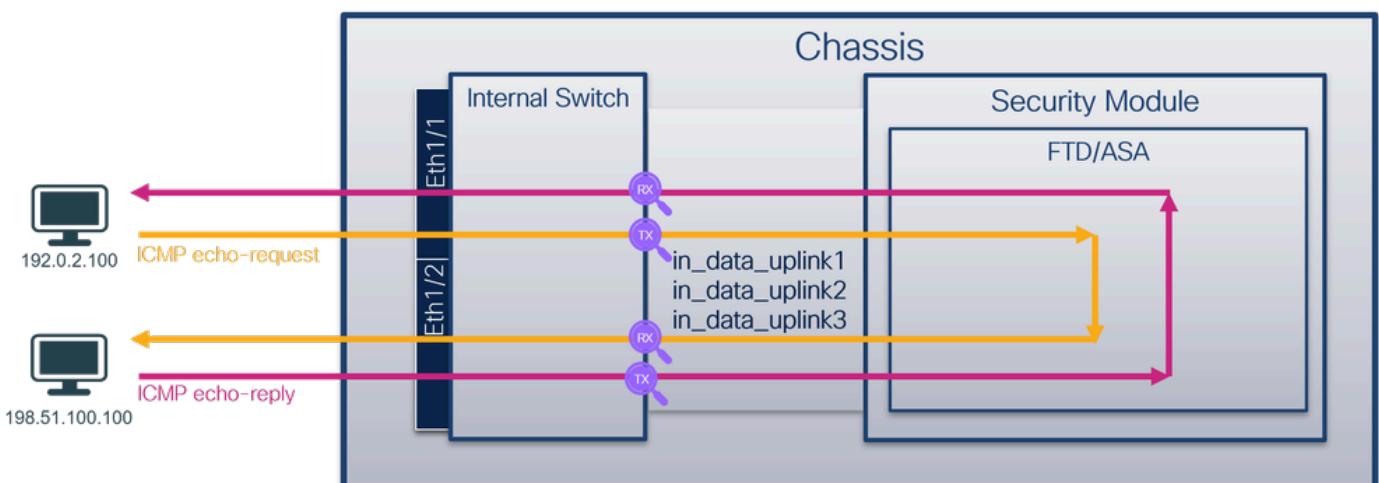
Firewall seguro 3100:



Firewall seguro 4200:



Firewall seguro 1200:



Configuração

Execute estas etapas no ASA ou no FTD CLI para configurar uma captura de pacote nas interfaces de uplink de dados.

Observe que o Secure Firewall 1210, 1250, 3100 e 4200 (exceto 4245) e tem apenas 1 interface de uplink ativa in_data_uplink1.

O Secure Firewall 1200 (exceto 1210 e 1250) e o 4245 têm várias interfaces de uplink in_data_uplink1, in_data_uplink2 e assim por diante. Sempre certifique-se de incluir todas as interfaces de uplink de dados.

Esta é uma saída do Secure Firewall 1220:

```
<#root>
>
cap capsw switch interface ?
```

Available interfaces to listen:

```
in_data_uplink1
Capture packets on internal data uplink1 interface

in_data_uplink2
Capture packets on internal data uplink2 interface

in_data_uplink3
Capture packets on internal data uplink3 interface
...
```

1. Criar uma sessão de captura:

```
<#root>
>
capture capsw switch interface in_data_uplink1
```

O Secure Firewall 1200/4200 suporta direcionalidade de captura:

```
<#root>
> capture capsw switch interface in_data_uplink1 direction ?
```

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

```
> capture capsw switch interface in_data_uplink1 direction both
```

2. Ative a sessão de captura:

```
<#root>
```

```
> 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:

```
<#root>
```

```
>
```

```
show capture capsw detail
```

Packet Capture info

```
Name: capsw
```

```
Session: 1
```

```
Admin State: enabled
```

```
Oper State: up
```

```
Oper State Reason: Active
```

```
Config Success: yes
```

```
Config Fail Reason:
```

```
Append Flag: overwrite
```

```
Session Mem Usage: 256
```

```
Session Pcap Snap Len: 1518
```

```
Error Code: 0
```

```
Drop Count: 0
```

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

Physical port:

```
Slot Id: 1
```

```

Port Id: 18
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-data-uplink1.pcap
Pcapsize: 7704

Filter: caps-w-1-18

Packet Capture Filter Info
Name: caps-w-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:

```

<#root>
>
connect fxos

...
firewall#
connect local-mgmt

firewall(local-mgmt)#
show portmanager switch status

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

```

0/2	SGMII	Up	1G	Full	None	Link-Up
0/3	SGMII	Up	1G	Full	None	Link-Up
0/4	SGMII	Up	1G	Full	None	Link-Up
0/5	SGMII	Down	1G	Half	None	Mac-Link-Down
0/6	SGMII	Down	1G	Half	None	Mac-Link-Down
0/7	SGMII	Down	1G	Half	None	Mac-Link-Down
0/8	SGMII	Down	1G	Half	None	Mac-Link-Down
0/9	1000_BaseX	Down	1G	Full	None	Link-Down
0/10	1000_BaseX	Down	1G	Full	None	Link-Down
0/11	1000_BaseX	Down	1G	Full	None	Link-Down
0/12	1000_BaseX	Down	1G	Full	None	Link-Down
0/13	1000_BaseX	Down	1G	Full	None	Link-Down
0/14	1000_BaseX	Down	1G	Full	None	Link-Down
0/15	1000_BaseX	Down	1G	Full	None	Link-Down
0/16	1000_BaseX	Down	1G	Full	None	Link-Down
0/17	1000_BaseX	Up	1G	Full	None	Link-Up
0/18	KR2	Up	50G	Full	None	Link-Up
0/19	KR	Up	25G	Full	None	Link-Up
0/20	KR	Up	25G	Full	None	Link-Up
0/21	KR4	Down	40G	Full	None	Link-Down
0/22	n/a	Down	n/a	Full	N/A	Reset
0/23	n/a	Down	n/a	Full	N/A	Reset
0/24	n/a	Down	n/a	Full	N/A	Reset
0/25	1000_BaseX	Down	1G	Full	None	Link-Down
0/26	n/a	Down	n/a	Full	N/A	Reset
0/27	n/a	Down	n/a	Full	N/A	Reset
0/28	n/a	Down	n/a	Full	N/A	Reset
0/29	1000_BaseX	Down	1G	Full	None	Link-Down
0/30	n/a	Down	n/a	Full	N/A	Reset
0/31	n/a	Down	n/a	Full	N/A	Reset
0/32	n/a	Down	n/a	Full	N/A	Reset
0/33	1000_BaseX	Down	1G	Full	None	Link-Down
0/34	n/a	Down	n/a	Full	N/A	Reset
0/35	n/a	Down	n/a	Full	N/A	Reset
0/36	n/a	Down	n/a	Full	N/A	Reset

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

Execute as etapas na seção Coletar arquivos de captura do switch interno do firewall seguro.

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. Neste exemplo, a captura de pacotes no Secure Firewall 3100 é analisada.

Verifique o ponto-chave - nesse caso, os pacotes ICMP echo request e echo reply 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	0x4dd93 (19859)	64	Echo (ping) request id=0x003a, seq=33/8448, ttl=64 (rep)
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 (req)
3	2022-08-07 22:40:07.684219	192.0.2.100	198.51.100.100	ICMP	102	0x4de8 (19944)	64	Echo (ping) request id=0x003a, seq=34/8704, ttl=64 (rep)
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 (req)
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 (rep)
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 (req)
7	2022-08-07 22:40:09.6909737	192.0.2.100	198.51.100.100	ICMP	102	0x4f2d (20269)	64	Echo (ping) request id=0x003a, seq=36/9216, ttl=64 (rep)
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 (req)
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 (rep)
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 (req)
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 (rep)
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 (req)
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 (rep)
14	2022-08-07 22:40:12.697209	198.51.100.100	192.0.2.100	ICMP	102	0x6fd7 (28631)	64	Echo (ping) reply id=0x003a, seq=39/9984, ttl=64 (req)
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 (rep)
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 (req)
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 (rep)
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 (req)

```

> Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
> Ethernet II, Src: Cisco_34:9a:15 (bc:7:12:34:9a: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

```

```

0000  00 50 56 9d e7 b0 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···:·!97-b··
0030  00 00 8b 1a 05 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 55 55 55 55 55 55 55 55  67UUUU

```

Explicação

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

Esta tabela resume a tarefa:

Tarefa	Ponto de captura	Filtro interno	Direção	Tráfego capturado
Configurar e verificar uma captura de pacote na interface de uplink in_data_uplink1	in_data_uplink1	Nenhum	Somente entrada*	Solicitações de eco ICMP do 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

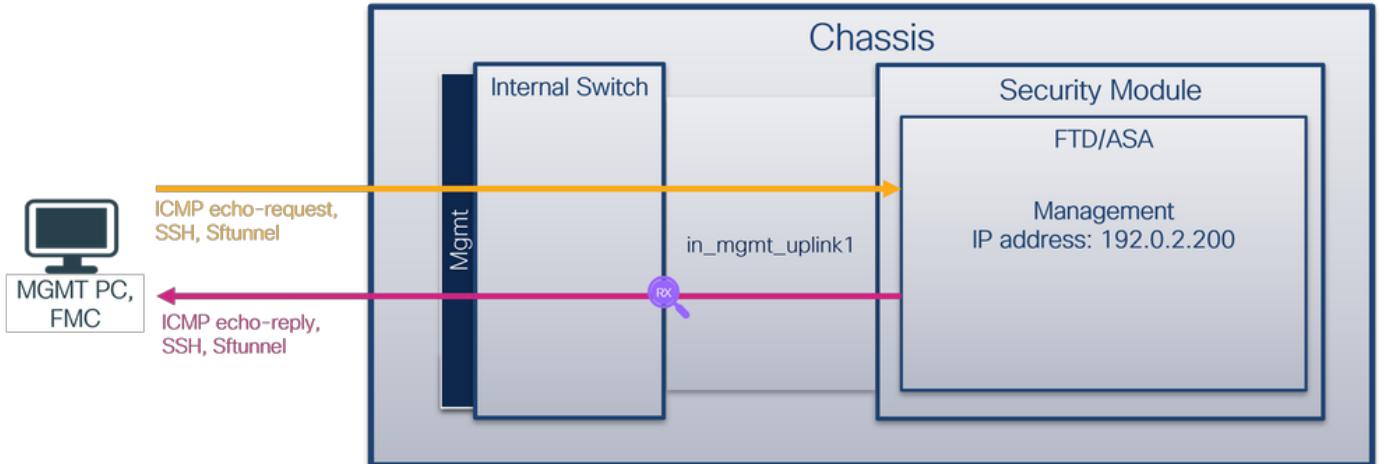
* Diferentemente do 3100, o Secure Firewall 1200/4200 suporta capturas bidirecionais (entrada e saída).

Tarefa 2

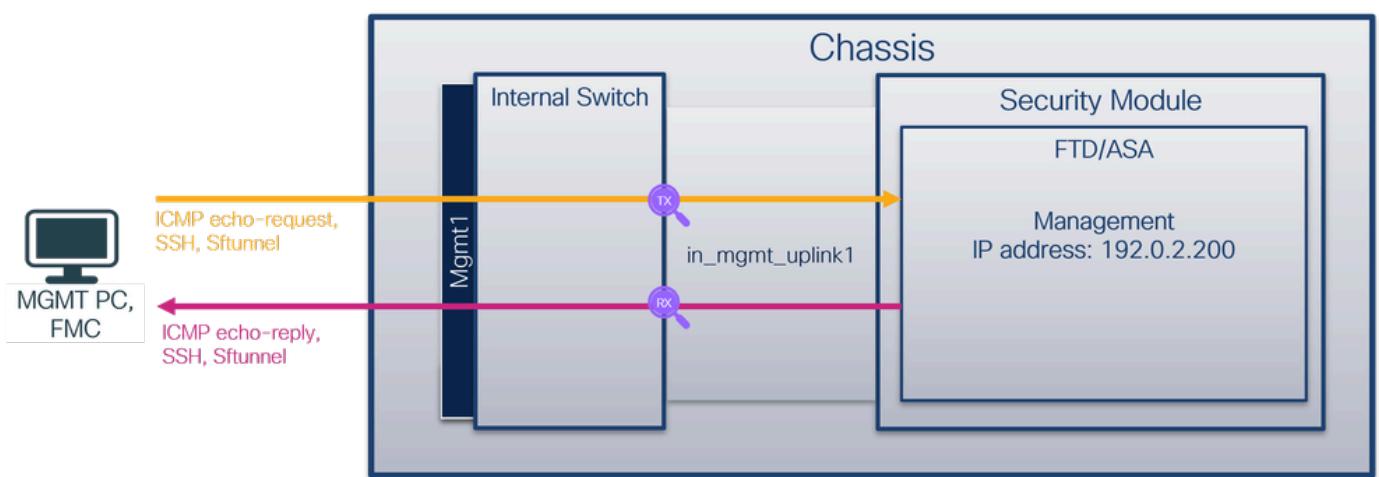
Use o FTD ou o ASA CLI para configurar e verificar uma captura de pacote na interface de uplink in_mgmt_uplink1. Somente os pacotes de conexões do plano de gerenciamento são capturados.

Topologia, fluxo de pacotes e pontos de captura

Firewall seguro 3100:



Firewall seguro 4200:



Configuração

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

1. Criar uma sessão de captura:

```
<#root>
>
capture capsw switch interface in_mgmt_uplink1
```

O Secure Firewall 4200 suporta direcionalidade de captura:

```
<#root>
> capture capsw switch interface in_mgmt_uplink1 direction ?
both To capture switch bi-directional traffic
```

```
egress To capture switch egressing traffic  
ingress To capture switch ingressing traffic
```

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

2. Ative a sessão de captura:

```
<#root>  
> 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:

```
<#root>  
> show capture capsw detail  
  
Packet Capture info  
  
Name: capsw  
  
Session: 1  
  
Admin State: enabled  
  
Oper State: up  
  
Oper State Reason: Active  
  
Config Success: yes  
Config Fail Reason:  
Append Flag: overwrite  
Session Mem Usage: 256  
Session Pcap Snap Len: 1518  
Error Code: 0  
Drop Count: 0  
  
Total Physical ports involved in Packet Capture: 1  
  
Physical port:  
Slot Id: 1
```

```

Port Id:          19

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

Pcapsize:        137248

Filter:          caps-w-1-19

Packet Capture Filter Info
Name:            caps-w-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:

```

<#root>
>
connect fxos

...
firewall#
connect local-mgmt

firewall(local-mgmt)#
show portmanager switch status

```

Dev/Port	Mode	Link	Speed	Duplex	Loopback Mode	Port Manager
----------	------	------	-------	--------	---------------	--------------

0/1	SGMII	Up	1G	Full	None	Link-Up
0/2	SGMII	Up	1G	Full	None	Link-Up
0/3	SGMII	Up	1G	Full	None	Link-Up
0/4	SGMII	Up	1G	Full	None	Link-Up
0/5	SGMII	Down	1G	Half	None	Mac-Link-Down
0/6	SGMII	Down	1G	Half	None	Mac-Link-Down
0/7	SGMII	Down	1G	Half	None	Mac-Link-Down
0/8	SGMII	Down	1G	Half	None	Mac-Link-Down
0/9	1000_BaseX	Down	1G	Full	None	Link-Down
0/10	1000_BaseX	Down	1G	Full	None	Link-Down
0/11	1000_BaseX	Down	1G	Full	None	Link-Down
0/12	1000_BaseX	Down	1G	Full	None	Link-Down
0/13	1000_BaseX	Down	1G	Full	None	Link-Down
0/14	1000_BaseX	Down	1G	Full	None	Link-Down
0/15	1000_BaseX	Down	1G	Full	None	Link-Down
0/16	1000_BaseX	Down	1G	Full	None	Link-Down
0/17	1000_BaseX	Up	1G	Full	None	Link-Up
0/18	KR2	Up	50G	Full	None	Link-Up
0/19	KR	Up	25G	Full	None	Link-Up
0/20	KR	Up	25G	Full	None	Link-Up
0/21	KR4	Down	40G	Full	None	Link-Down
0/22	n/a	Down	n/a	Full	N/A	Reset
0/23	n/a	Down	n/a	Full	N/A	Reset
0/24	n/a	Down	n/a	Full	N/A	Reset
0/25	1000_BaseX	Down	1G	Full	None	Link-Down
0/26	n/a	Down	n/a	Full	N/A	Reset
0/27	n/a	Down	n/a	Full	N/A	Reset
0/28	n/a	Down	n/a	Full	N/A	Reset
0/29	1000_BaseX	Down	1G	Full	None	Link-Down
0/30	n/a	Down	n/a	Full	N/A	Reset
0/31	n/a	Down	n/a	Full	N/A	Reset
0/32	n/a	Down	n/a	Full	N/A	Reset
0/33	1000_BaseX	Down	1G	Full	None	Link-Down
0/34	n/a	Down	n/a	Full	N/A	Reset
0/35	n/a	Down	n/a	Full	N/A	Reset
0/36	n/a	Down	n/a	Full	N/A	Reset

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

Execute as etapas na seção Coletar arquivos de captura do switch interno do firewall seguro.

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. Neste exemplo, a captura de pacotes no Secure Firewall 3100 é analisada.

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	192.0.2.2.200	192.0.2.1.101	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	192.0.2.2.200	192.0.2.1.101	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	192.0.2.2.200	192.0.2.1.101	TLSv1.2	990	0xb7d2 (47058)	64	Application Data
199	2022-08-07 23:21:45.928772	192.0.2.2.200	192.0.2.1.100	ICMP	78	0xbdd8 (48456)	64	Echo (ping) reply id=0x0001, seq=4539/47889, ttl=64
200	2022-08-07 23:21:45.949924	192.0.2.2.200	192.0.2.1.101	TLSv1.2	128	0xa497 (19095)	64	Application Data
201	2022-08-07 23:21:45.949927	192.0.2.2.200	192.0.2.1.101	TCP	70	0xa498 (19096)	64	8305 → 58885 [ACK] Seq=21997 Ack=26244 Win=4116 Len=0 TSv
202	2022-08-07 23:21:46.019895	192.0.2.2.200	192.0.2.1.101	TLSv1.2	100	0xa499 (19097)	64	Application Data
203	2022-08-07 23:21:46.019899	192.0.2.2.200	192.0.2.1.101	TLSv1.2	96	0xa49a (19098)	64	Application Data
204	2022-08-07 23:21:46.019903	192.0.2.2.200	192.0.2.1.101	TCP	70	0xa49b (19099)	64	8305 → 58885 [ACK] Seq=22053 Ack=26274 Win=4116 Len=0 TSv
205	2022-08-07 23:21:46.019906	192.0.2.2.200	192.0.2.1.101	TCP	70	0xa49c (19100)	64	8305 → 58885 [ACK] Seq=22053 Ack=26300 Win=4116 Len=0 TSv
206	2022-08-07 23:21:46.136415	192.0.2.2.200	192.0.2.1.101	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	192.0.2.2.200	192.0.2.1.100	ICMP	78	0xbdb9e (48542)	64	Echo (ping) reply id=0x0001, seq=4540/48145, ttl=64
208	2022-08-07 23:21:47.980409	192.0.2.2.200	192.0.2.1.100	ICMP	78	0xbdbf2 (48626)	64	Echo (ping) reply id=0x0001, seq=4541/48401, ttl=64
209	2022-08-07 23:21:48.406312	192.0.2.2.200	192.0.2.1.101	TCP	70	0xa49d (19101)	64	8305 → 58885 [ACK] Seq=22053 Ack=26366 Win=4116 Len=0 TSv
210	2022-08-07 23:21:48.983236	192.0.2.2.200	192.0.2.1.101	TLSv1.2	747	0xa49e (19102)	64	Application Data
211	2022-08-07 23:21:48.994386	192.0.2.2.200	192.0.2.1.100	ICMP	78	0xbe48 (48712)	64	Echo (ping) reply id=0x0001, seq=4542/48657, ttl=64
212	2022-08-07 23:21:50.008576	192.0.2.2.200	192.0.2.1.100	ICMP	78	0xbea6 (48806)	64	Echo (ping) reply id=0x0001, seq=4543/48913, ttl=64
213	2022-08-07 23:21:50.140167	192.0.2.2.200	192.0.2.1.101	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	192.0.2.2.200	192.0.2.1.101	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	192.0.2.2.200	192.0.2.1.101	TLSv1.2	990	0xb7d6 (47062)	64	Application Data
216	2022-08-07 23:21:51.015884	192.0.2.2.200	192.0.2.1.100	ICMP	78	0xbec1 (48833)	64	Echo (ping) reply id=0x0001, seq=4544/49169, ttl=64
217	2022-08-07 23:21:51.142842	192.0.2.2.200	192.0.2.1.101	TCP	70	0xb7d7 (47063)	64	39181 → 8305 [ACK] Seq=69004 Ack=967 Win=1384 Len=0 TSval
218	2022-08-07 23:21:52.030118	192.0.2.2.200	192.0.2.1.100	ICMP	78	0xbff02 (48898)	64	Echo (ping) reply id=0x0001, seq=4545/49425, ttl=64
219	2022-08-07 23:21:53.042744	192.0.2.2.200	192.0.2.1.100	ICMP	78	0xbff59 (48985)	64	Echo (ping) reply id=0x0001, seq=4546/49681, ttl=64
220	2022-08-07 23:21:53.073144	192.0.2.2.200	192.0.2.1.100	SSH	170	0xad34 (44340)	64	Server: Encrypted packet (len=112)
221	2022-08-07 23:21:53.194906	192.0.2.2.200	192.0.2.1.100	TCP	64	0xad35 (44341)	64	22 → 53249 [ACK] Seq=1025 Ack=881 Win=946 Len=0
222	2022-08-07 23:21:53.985480	192.0.2.2.200	192.0.2.1.101	TLSv1.2	747	0xa49f (19103)	64	Application Data
223	2022-08-07 23:21:54.102899	192.0.2.2.200	192.0.2.1.100	ICMP	78	0xbff63 (48995)	64	Echo (ping) reply id=0x0001, seq=4547/49937, ttl=64
224	2022-08-07 23:21:54.903675	192.0.2.2.200	192.0.2.1.101	TCP	70	0xa4a0 (19104)	64	8305 → 58885 [ACK] Seq=23407 Ack=26424 Win=4116 Len=0 TSv
225	2022-08-07 23:21:55.136700	192.0.2.2.200	192.0.2.1.100	TCPMD	70	authfert (anon)	64	Echo (ping) reply id=0x0001, seq=4540/49102, 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 do FTD 192.0.2.200 para o endereço IP do FMC 192.0.2.101 SSH do endereço IP de gerenciamento FTD

				192.0.2.200 para o host 192.0.2.100
--	--	--	--	--

* Diferentemente do 3100, o Secure Firewall 1200/4200 suporta capturas bidirecionais (entrada e saída).

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

Execute 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:

```
<#root>
>
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:

```
<#root>
>
capture capsw switch interface inside ethernet-type arp

<#root>
> 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:

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

Packet Capture info

```
Name: capsw

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

Total Physical ports involved in Packet Capture: 1

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

```
Filter: capsw-1-1
```

Packet Capture Filter Info

```
Name: capsw-1-1

Protocol: 0
Ivlan: 0
Ovlan: 0
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
```

```
EtherType: 2054
```

```
Total Physical breakout ports involved in Packet Capture: 0
```

```
0 packet captured on disk using switch capture
```

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

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

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

```
Packet Capture info
```

```
Name: capsw
```

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

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

```
Physical port:
```

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

```
Filter: capsw-1-1
```

```
Packet Capture Filter Info
```

```
Name: capsw-1-1
```

```
Protocol: 1
```

```
Ivlan:      0  
Ovlan:      0
```

```
src Ip:     198.51.100.100
```

```
Dest Ip:    0.0.0.0  
Src Ipv6:   ::  
Dest Ipv6:  ::  
Src MAC:    00:00:00:00:00:00  
Dest MAC:   00:00:00:00:00:00  
Src Port:   0  
Dest Port:  0  
Ethertype:  0
```

Total Physical breakout ports involved in Packet Capture: 0

0 packets captured on disk using switch capture

Reading of capture file from disk is not supported

Captura de pacotes nas interfaces da porta do switch L2

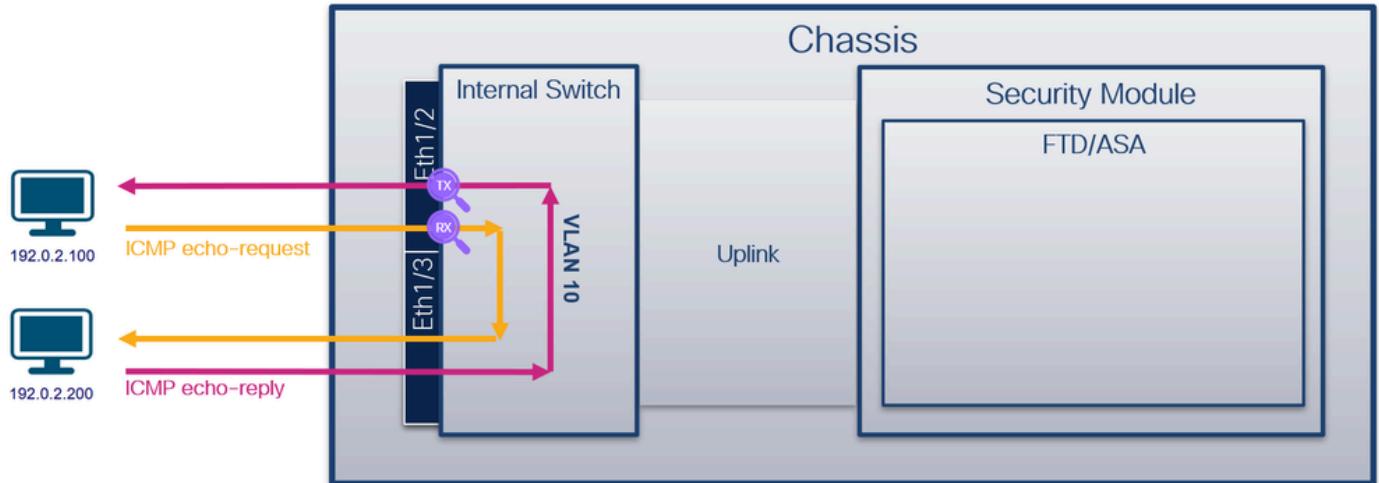
As portas do switch encaminham o tráfego na Camada 2, usando a função de switching no hardware. As portas de switch na mesma VLAN podem se comunicar entre si usando switching de hardware, e o tráfego não está sujeito à política de segurança de defesa contra ameaças. As portas de acesso aceitam apenas tráfego não marcado e você pode atribuí-las a uma única VLAN. As portas de tronco aceitam tráfego não marcado e marcado e podem pertencer a mais de uma VLAN. Por padrão, Ethernet 1/2 a 1/8 (1210) ou Ethernet 1/2 a 1/10 (1220) são configuradas como portas de switch de acesso na VLAN 1. Não é possível configurar a interface de gerenciamento como uma porta de switch.

Tarefa 1

Use o FTD ou o ASA CLI para configurar e verificar uma captura de pacotes nas subinterfaces Ethernet1/1 ou Ethernet1/2. Ambas as interfaces são interfaces de switch atribuídas à VLAN 10.

Topologia, fluxo de pacotes e pontos de captura

Firewall seguro 1200:



Configuração

Execute estas etapas no ASA ou FTD CLI para configurar uma captura de pacote na interface Ethernet1/2 ou Ethernet1/3:

1. Verifique as portas dos switches L2:

```
<#root>
>
show switch vlan

VLAN Name          Status      Ports
--- ---           -----
1     -            down       E1/4, E1/5, E1/6, E1/7
                           E1/8
10    VLAN-10       up        E1/2, E1/3
```

2. Crie uma sessão de capturas, o 1200 suporta direcionalidade de captura:

```
<#root>
>
capture caps w switch interface switchport 2 direction ?

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

>
capture caps w switch interface switchport 2 direction both
```

 Note: Embora a porta esteja rotulada como Ethernet1/2, ao executar uma captura de switch de Camada 2, você não pode especificá-la no formato Ethernet1/2. Em vez disso, use switchport 2.

3. Ativar a sessão de captura

```
<#root>  
>  
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:

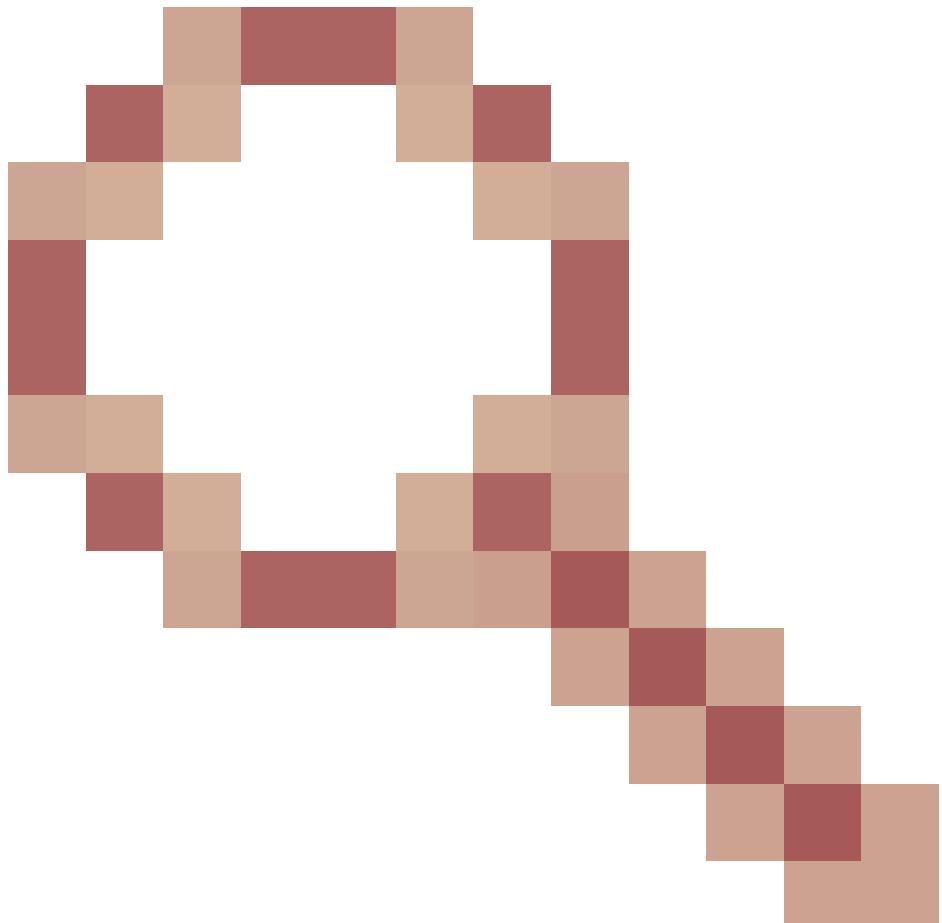
```
<#root>  
>  
show capture capsw detail  
  
Packet Capture info  
Name:  
capsw  
  
Session: 2  
Admin State: enabled  
Oper State: up  
Oper State Reason:  
  
Active  
  
Config Success: yes  
Config Fail Reason:  
Append Flag: overwrite  
Session Mem Usage: 256  
Session Pcap Snap Len: 1518  
Error Code: 0  
Drop Count: 0  
  
Total Physical ports involved in Packet Capture: 1  
  
Physical port:  
Slot Id: 1  
Port Id: 2  
Pcapfile: /mnt/disk0/packet-capture/sess-2-capsw-ethernet-1-2-0.pcap  
Pcapsize: 24  
Direction: both
```

Filter: caps-w-1-2

Packet Capture Filter Info
Name: caps-w-1-2
Protocol: 0
Ivlan: 0
Ovlan: 0
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

0 packet captured on disk using switch capture

Reading of capture file from disk is not supported



Devido ao defeito [CSCwq55508](#)

, o tamanho e a contagem de pacotes não são atualizados na saída dos comandos show capture para capturas de switch no Secure Firewall 1200. Como solução alternativa, isso pode ser verificado no shell de comando FXOS local-mgmt através do comando show portmanager switch pktcap-rules hardware:

```
<#root>

Firewall-1200(local-mgmt)#

show portmanager switch ptkcap-rules hardware

Hardware DB rule: 1 /

Direction: egress

HwIndex= 8196
RuleId= 6144
CounterIndex= 10

PacketCount= 38

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

Hardware DB rule: 2 /

Direction: ingress

HwIndex= 4104
RuleId= 5120
CounterIndex= 0

PacketCount= 37

Slot= 1
Interface= 2
Protocol= 0
EthertypeAtL2Offset= 0x0000
EtherTypeAtL3Offset= 0x0000
Ivlan= 0
Ovlan= 0
FlowId= 0
SrcEport= 0
TrgEport= 0
SrcId= 0
TcpUdpSrcPort= 0
TcpUdpDstPort= 0
SrcIpAddr= 0.0.0.0
```

```

DstIpAddr= 0.0.0.0
SrcIpv6Addr= ::

DestIpv6Addr= ::

SrcMacAddr= 00:00:00:00:00:00
DestMacAddr= 00:00:00:00:00:00

```

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

Execute as etapas na seção Coletar arquivos de captura do switch interno do firewall seguro.

Capturar análise de arquivo

Use um aplicativo leitor de arquivo de captura de pacote para abrir os arquivos de captura para a interface Ethernet 1/2 do switch L2. Neste exemplo, a captura de pacotes no Secure Firewall 1210 é analisada.

Verifique o ponto-chave - nesse caso, os pacotes ICMP echo request e echo reply são capturados.

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

Explicação

Esses pacotes nunca são encaminhados para o aplicativo (FTD/ASA) porque ambos os hosts estão conectados às portas do switch de Camada 2 dentro da mesma VLAN.

Esta tabela resume a tarefa:

Tarefa	Ponto de captura	Filtro interno	Direção	Tráfego capturado
Configurar e verificar uma captura de pacotes na interface Ethernet1/2 da porta do switch L2	Ethernet1/2	Nenhum	ambos	Solicitações de eco ICMP do host 192.0.2.200 para o host 192.0.2.100

				Respostas de eco ICMP do host 192.0.2.100 para o host 192.0.2.200
--	--	--	--	---

Captura de pacotes em chassis de várias instâncias

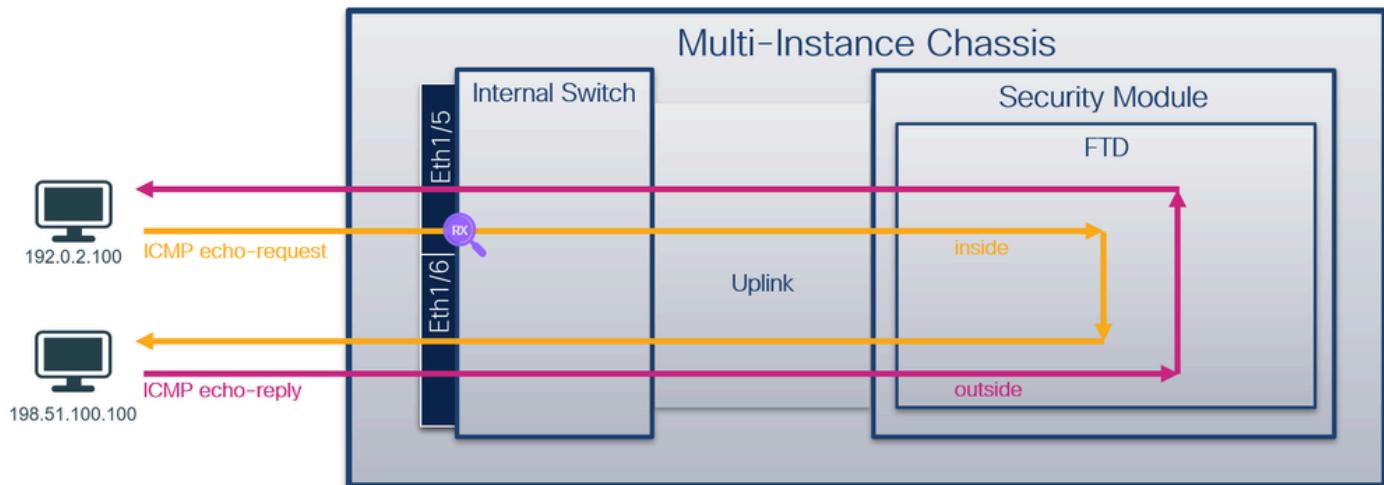
A captura de pacote de switch nas plataformas 3100/4200 no modo de implantação de várias instâncias difere das capturas de switch no modo nativo. No modo de várias instâncias, o comando `capture <name> switch` não está disponível nas instâncias de FTD. Em vez disso, as capturas de pacotes precisam ser configuradas usando a CLI FXOS no chassi, semelhante ao processo para as plataformas 4100/9300, usando o comando `scope packet-capture`.

Tarefa 1

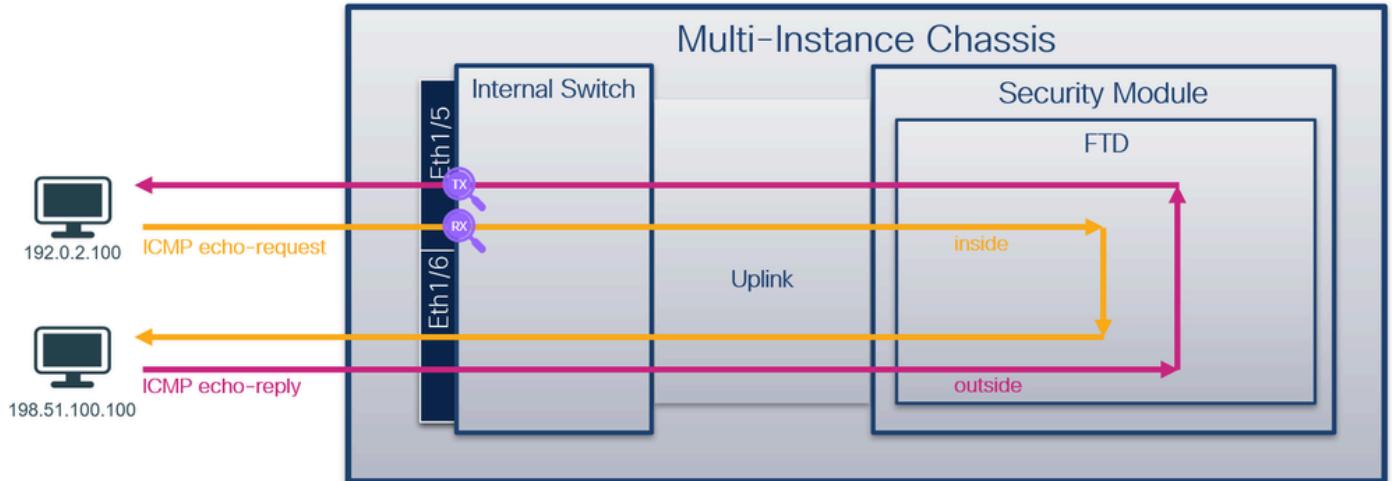
Use a CLI FXOS no chassi de várias instâncias para configurar e verificar uma captura de pacote de switch na interface Ethernet1/5.

Topologia, fluxo de pacotes e pontos de captura

Firewall seguro 3100:



Secure Firewall 4200 com capturas bidirecionais:



Configuração

CLI FXOS

Execute estas etapas na CLI FXOS do chassi para configurar uma captura de pacote na interface Ethernet1/5:

1. Identificar o tipo de aplicação e o identificador:

```
<#root>
firepower-3120 #
scope ssa

firepower-3120 /ssa #
show app-instance

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

Application Name	Identifier	Slot ID	Admin State	Operational State	Running Version
ftd					
ftd1	1	Enabled	Online	7.7.0.89	7.7.0.89
					Container

2. Crie uma sessão de captura:

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

```
firepower-3120 /packet-capture #

create session cap1

firepower-3120 /packet-capture/session* #

create phy-port Eth1/5

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

set app ftd

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

set app-instance ftd1

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

up

firepower-3120 /packet-capture/session* #

enable

firepower-3120 /packet-capture/session* #

commit-buffer

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

Firewall seguro 4200:

```
<#root>

firepower-4245#

scope packet-capture

firepower-4245 /packet-capture #

create session cap1

firepower-4245 /packet-capture/session* #

create phy-port Eth1/5

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

set app ftd

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

set app-instance ftd1
```

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

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

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

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

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

Verificação

CLI FXOS

Verifique os detalhes da captura na captura de pacote de escopo. Especificamente, verifique o nome da sessão de captura, o estado operacional e administrativo, o slot da interface e o identificador. Verifique se o valor de Pcapsize em bytes aumenta e se o número de pacotes capturados é diferente de zero:

```
<#root>

firepower-3120#
scope packet-capture

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

SSP Traffic Monitoring Session:
Name:

```
cap1

Session: 1
Admin State: Enabled
Oper State: Up
Oper State Reason:
```

Active

Config Success: Yes

```
Config Fail Reason:  
Append Flag: Overwrite  
Session Mem Usage: 256 MB  
Error Code: 0  
Drop Count: 0
```

```
Packet Count: 420
```

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

```
Pcapsize: 49128 bytes
```

```
Filter:  
Sub Interface: 0  
Application Instance:
```

```
ftd1
```

```
Application Name:
```

```
ftd
```

```
Direction: Ingress  
Drop: Disable
```

```
Firewall seguro 4200:
```

```
<#root>  
firepower-4245#  
scope packet-capture  
  
firepower-4245 /packet-capture #  
show session cap1
```

```
SSP Traffic Monitoring Session:  
Name:  
cap1
```

```
Session: 1  
Admin State: Enabled  
Oper State: Up  
Oper State Reason:  
  
Active
```

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

```
Packet Count: 95
```

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

```
Pcapsize: 11050 bytes
```

```
Filter:
Sub Interface: 0
Application Instance:
```

```
ftd1
```

```
Application Name:
```

```
ftd
```

```
Direction: Both
```

```
Drop: Disable
```

Coletar arquivos de captura

Execute as etapas de CLI FXOS 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 para Ethernet1/5. Neste exemplo, a captura de pacotes no Secure Firewall 3100 é analisada. 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	Delta	1	Source	Destination	Protocol	Length	ICMP Type	ICMP Code	TTL	Info
1	0.000000			192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request id=0x001d,
2	1.029095	1.029095	2	192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request id=0x001d,
3	2.047360	1.018265		192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request id=0x001d,
4	3.074748	1.027388		192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request id=0x001d,
5	4.093790	1.019042		192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request id=0x001d,
6	5.120831	1.027041		192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request id=0x001d,
7	6.149745	1.028914		192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request id=0x001d,
8	7.165826	1.016081		192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request id=0x001d,
9	8.193225	1.027399		192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request id=0x001d,
10	9.212156	1.018931		192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request id=0x001d,
11	10.242986	1.030830		192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request id=0x001d,
12	11.260600	1.017614		192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request id=0x001d,
13	12.289582	1.028982		192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request id=0x001d,
14	13.315929	1.026347		192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request id=0x001d,
15	14.332291	1.016362		192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request id=0x001d,
16	15.362416	1.030125		192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request id=0x001d,
17	16.388598	1.026182		192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request id=0x001d,
18	17.405060	1.016462		192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request id=0x001d,

> Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)	2
> Ethernet II, Src: VMware_88:3e:02 (00:50:56:88:3e:02), Dst: a2:11:04 (00:00:00:00:00:08) (a2:11:04:00:00:08)	
> Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100	
> Internet Control Message Protocol	

0000 a2 11 04 00 00 08 00 50 56 88 3e 02 08 0
0010 00 54 01 2c 40 00 40 01 4c 81 c0 00 02 0
0020 64 64 08 00 60 25 00 1d 07 a4 da 7e 8c 0
0030 00 00 5c 5f 0e 00 00 00 00 00 10 11 12 0
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 0
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 0
0060 36 37 55 55 55 55 55 55

Explicação

As capturas do switch são configuradas na interface Ethernet1/5.

Esta tabela resume a tarefa:

Tarefa	Ponto de captura	Filtro interno	Direção	Tráfego capturado
Configurar e verificar uma captura de pacote na interface Ethernet1/5	Ethernet1/5	Nenhum	Somente entrada*	Solicitações de eco ICMP do host 192.0.2.100 para o host 198.51.100.100

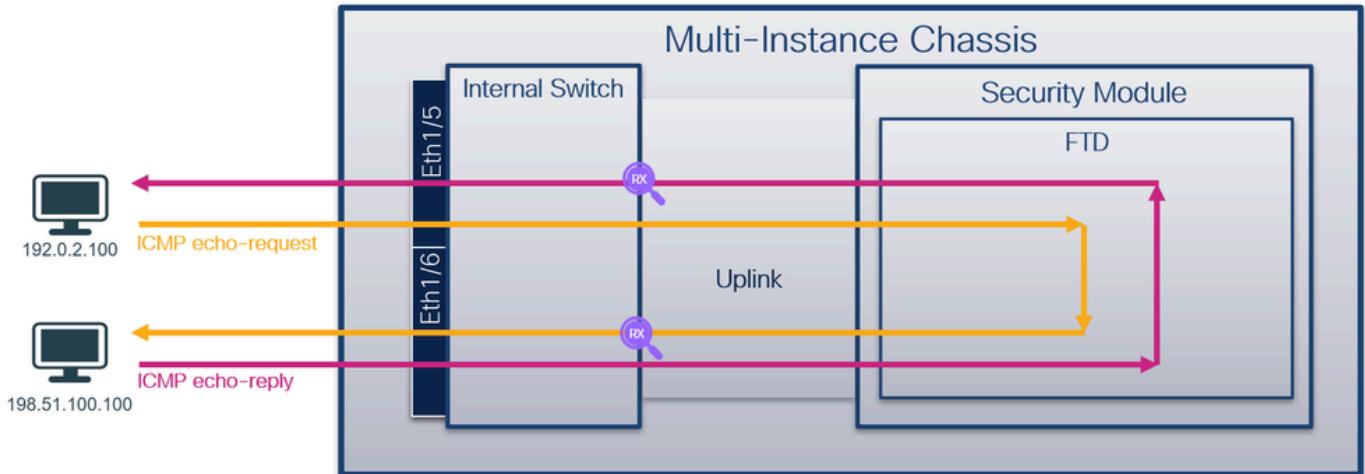
* Ao contrário do 3100, o Secure Firewall 4200 suporta capturas bidirecionais (entrada e saída).

Tarefa 2

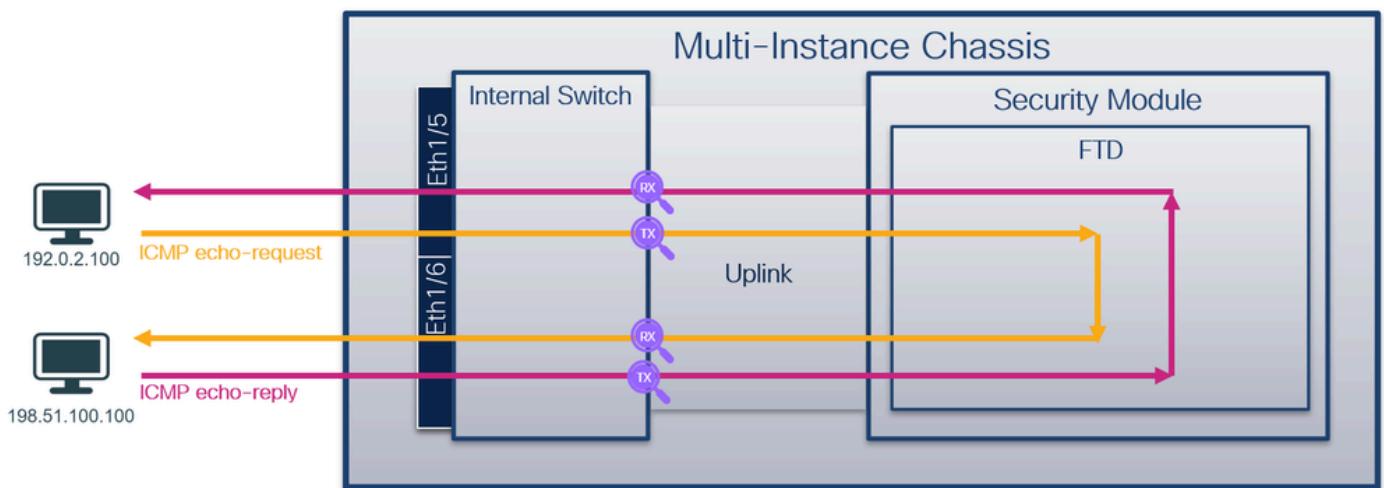
Use a CLI FXOS no chassis de várias instâncias para configurar e verificar uma captura de pacote de switch em interfaces de uplink de dados.

Topologia, fluxo de pacotes e pontos de captura

Firewall seguro 3100:



Firewall seguro 4200:



Configuração

CLI FXOS

Execute estas etapas na CLI FXOS do chassi para configurar uma captura de pacote nas interfaces de uplink de dados:

1. Identificar o tipo de aplicativo e o identificador:

```
<#root>
firepower-3120 /ssa #
show app-instance
```

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

```
ftd
```

```
ftd1
```

1	Enabled	Online	7.7.0.89	7.7.0.89	Contain
---	---------	--------	----------	----------	---------

2. Crie uma sessão de captura:

```
<#root>

firepower-3120#
scope packet-capture

firepower-3120 /packet-capture #
create session cap1

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

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

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

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

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

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

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

 Note: Diferentemente da implantação nativa, no modo de várias instâncias, use o número da porta em vez do nome da interface. Consulte a tabela na seção Visão Geral de Alto Nível da Arquitetura do Sistema para verificar o mapeamento da porta do switch interno.

Firewall seguro 4200:

```
<#root>

firepower-4245#
```

```
scope packet-capture

firepower-4245 /packet-capture #
create session cap1

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

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

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

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

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

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

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

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

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

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

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

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

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

Verificação

CLI FXOS

Verifique os detalhes da captura na captura de pacote de escopo. Especificamente, verifique o nome da sessão de captura, o estado operacional e administrativo, o slot da interface e o identificador. Verifique se o valor de Pcapsize em bytes aumenta e se o número de pacotes capturados é diferente de zero:

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

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

SSP Traffic Monitoring Session:

Name:

```
cap1

Session: 1
Admin State: Enabled
Oper State: Up
Oper State Reason:
```

Active

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

Packet Count: 171

Physical ports involved in Packet Capture:

```
Slot Id: 1
Port Id: 18
Pcapfile: /workspace/packet-capture/sess-1-cap1-data-uplink1.pcap
```

Pcapsize: 19932 bytes

```
Filter:
Sub Interface: 0
```

Application Instance:

ftd1

Application Name:

ftd

Direction:

Ingress

Drop: Disable

Firewall seguro 4200:

<#root>

firepower-4245#

scope packet-capture

firepower-4245 /packet-capture #

show session cap1

SSP Traffic Monitoring Session:

Name:

cap1

Session: 1

Admin State: Enabled

Oper State: Up

Oper State Reason:

Active

Config Success: Yes

Config Fail Reason:

Append Flag: Overwrite

Session Mem Usage: 256 MB

Error Code: 0

Drop Count: 0

Packet Count: 70

Physical ports involved in Packet Capture:

Slot Id:

```
Port Id:
```

```
11
```

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

```
Pcapsize: 8320 bytes
```

```
Filter:
```

```
Sub Interface: 0
```

```
Application Instance: ftd1
```

```
Application Name: ftd
```

```
D
```

```
irection: Both
```

```
Drop: Disable
```

```
Slot Id:
```

```
1
```

```
Port Id:
```

```
12
```

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

```
Pcapsize: 172 bytes
```

```
Filter:
```

```
Sub Interface: 0
```

```
Application Instance: ftd1
```

```
Application Name: ftd
```

```
Direction: Both
```

```
Drop: Disable
```

Coletar arquivos de captura

Execute as etapas FXOS CLI 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 da interface in_data_uplink1. Neste exemplo, a captura de pacotes no Secure Firewall 3100 é analisada.

Verifique o ponto-chave - nesse caso, os pacotes ICMP echo request e echo reply são capturados. Esses são os pacotes enviados do aplicativo para o switch interno.

No.	Time	Delta	Source	Destination	Protocol	Length	ICMP Type	ICMP Code	TTL	Info	
2	0.531209		0.531209 192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request	id=0x0021,
3	0.531212		0.000003 198.51.100.100	192.0.2.100	ICMP	102	8	0	64	Echo (ping) reply	id=0x0021,
4	1.554198		1.022986 192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request	id=0x0021,
5	1.554202		0.000004 198.51.100.100	192.0.2.100	ICMP	102	8	0	64	Echo (ping) reply	id=0x0021,
7	2.580952		0.881950 192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request	id=0x0021,
8	2.580962		0.000010 198.51.100.100	192.0.2.100	ICMP	102	8	0	64	Echo (ping) reply	id=0x0021,
11	3.603348		0.825013 192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request	id=0x0021,
12	3.603354		0.000006 198.51.100.100	192.0.2.100	ICMP	102	8	0	64	Echo (ping) reply	id=0x0021,
13	4.625531		1.022177 192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request	id=0x0021,
14	4.625536		0.000006 198.51.100.100	192.0.2.100	ICMP	102	8	0	64	Echo (ping) reply	id=0x0021,
15	5.653220		1.027684 192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request	id=0x0021,
16	5.653224		0.000001 198.51.100.100	192.0.2.100	ICMP	102	8	0	64	Echo (ping) reply	id=0x0021,
17	6.677315		1.024091 192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request	id=0x0021,
18	6.677319		0.000004 198.51.100.100	192.0.2.100	ICMP	102	8	0	64	Echo (ping) reply	id=0x0021,
20	7.698995		0.920534 192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request	id=0x0021,
21	7.699000		0.000005 198.51.100.100	192.0.2.100	ICMP	102	8	0	64	Echo (ping) reply	id=0x0021,
22	8.722879		1.023879 192.0.2.100	198.51.100.100	ICMP	102	8	0	64	Echo (ping) request	id=0x0021,
23	8.722886		0.000007 198.51.100.100	192.0.2.100	ICMP	102	8	0	64	Echo (ping) reply	id=0x0021,

```
> Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
> Ethernet II, Src: a2:8e:03:00:00:01 (a2:8e:03:00:00:01), Dst: VMware_88:71:44 (00:50:56:88:71:44)
> Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
> Internet Control Message Protocol
```

0000 00 50 56 88 71 44 a2 8e 03 00 00 01 08 0
0010 00 54 92 f9 40 00 40 01 ba b3 c0 00 02 6
0020 64 64 08 00 47 10 00 21 02 a4 78 8c 8c 6
0030 00 00 e7 62 03 00 00 00 00 00 10 11 12 1
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 2
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 3
0060 36 37 55 55 55 55

Explicação

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

Esta tabela resume a tarefa:

Tarefa	Ponto de captura	Filtro interno	Direção	Tráfego capturado
Configurar e verificar uma captura de pacote na interface de uplink in_data_uplink1	in_data_uplink1	Nenhum	Somente entrada*	Solicitações de eco ICMP do 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

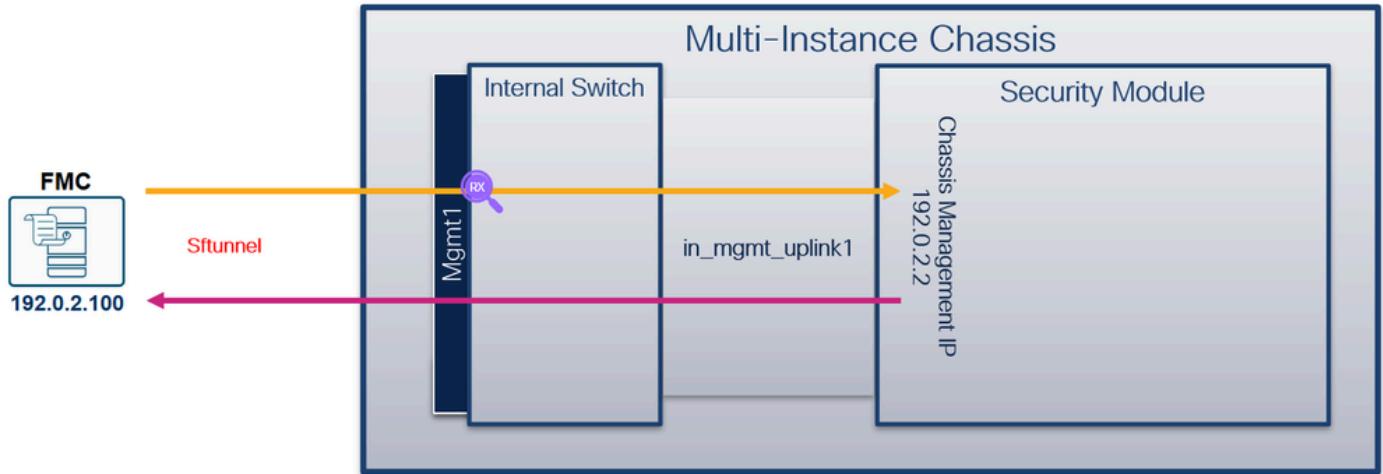
* Ao contrário do 3100, o Secure Firewall 4200 suporta capturas bidirecionais (entrada e saída).

Tarefa 3

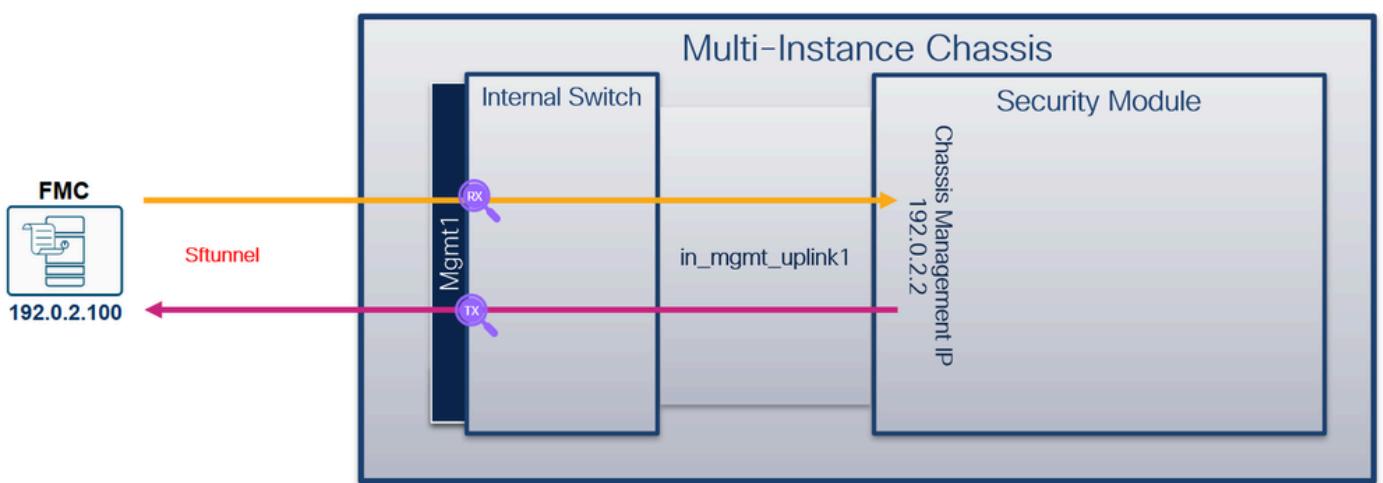
Use a CLI FXOS no chassis de várias instâncias para configurar e verificar uma captura de pacote de switch na interface de gerenciamento, capturando o tráfego sftunnel entre o chassis e o FMC.

Topologia, fluxo de pacotes e pontos de captura

Firewall seguro 3100:



Secure Firewall 4200 com capturas bidirecionais:



Configuração

CLI FXOS

Execute as seguintes etapas na CLI FXOS do chassi para configurar uma captura de pacote para o tráfego sftunnel na interface de gerenciamento.

1. Crie um filtro de captura de pacotes para capturar somente o tráfego TCP (número de protocolo 6).

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

firepower-4245 /packet-capture #
create filter filter1

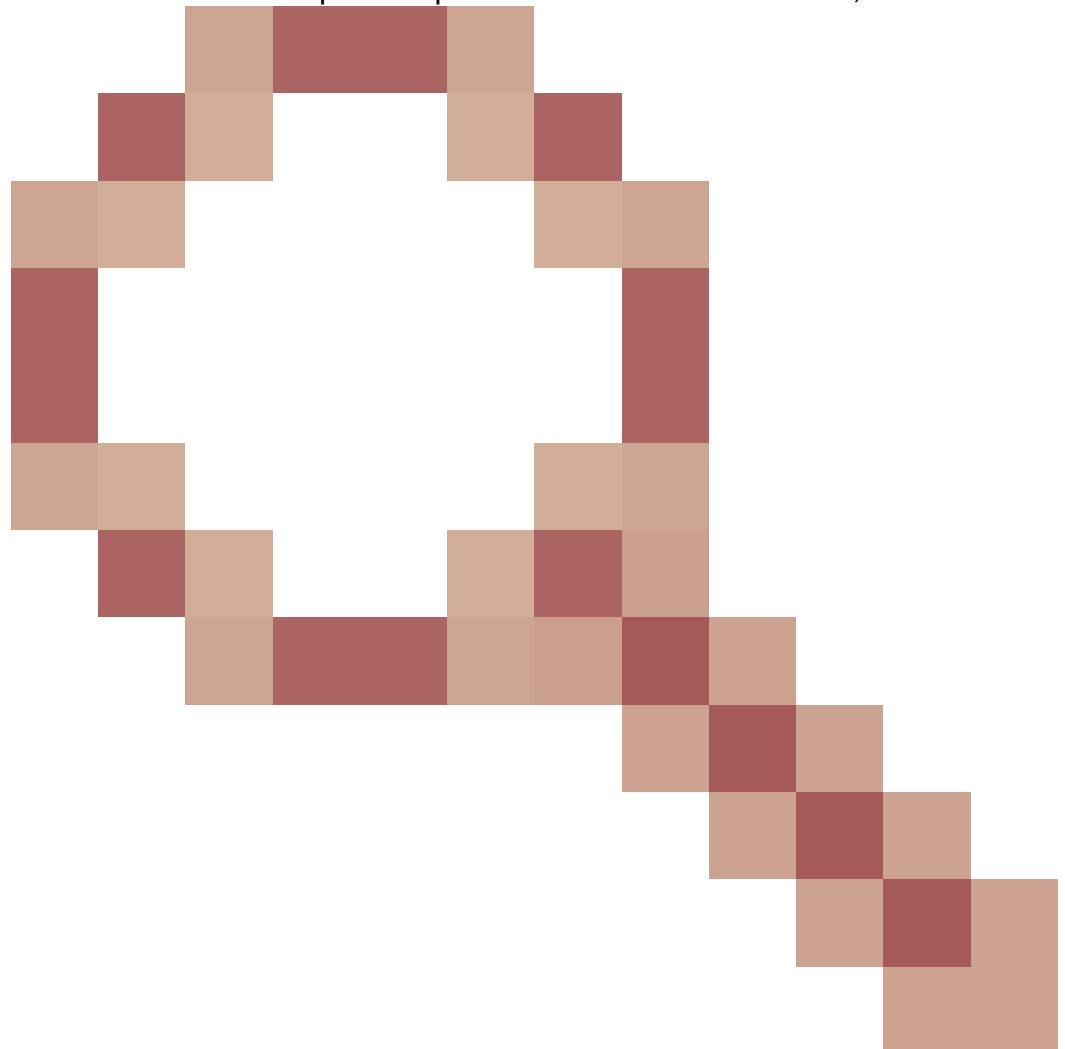
firepower-4245 /packet-capture/filter* #
set protocol 6
```

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

firepower-4245 /packet-capture/filter #
up

firepower-4245 /packet-capture #
```

 Note: Embora o Secure Firewall 4200 suporte capturas de switch bidirecionais, devido ao



bug [CSCwq64141](#)

, não é possível criar filtros de captura de switch específicos com condições de correspondência que capturam o tráfego em ambas as direções. Portanto, o filtro nessa tarefa é configurado para corresponder a todo o tráfego TCP, permitindo a captura do tráfego sftunnel em ambas as direções no Secure Firewall 4200.

2. Crie uma sessão de captura para a interface de gerenciamento. De acordo com a tabela na seção Visão Geral de Alto Nível da Arquitetura do Sistema, a porta de gerenciamento no Firewall Seguro 3100 é mapeada para a porta de switch interna Eth1/17:

```
<#root>

firepower-3120#
scope packet-capture

firepower-3120 /packet-capture #
create session cap1

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

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

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

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

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

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

firepower-3120 /packet-capture #
```

A porta de gerenciamento 1 no Secure Firewall 4200 é mapeada para a porta interna do switch Eth1/9:

```
<#root>

firepower-4245#
scope packet-capture

firepower-4245 /packet-capture #
create session cap1

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

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

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

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

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

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

Verificação

CLI FXOS

Verifique os detalhes da captura na captura de pacote de escopo. Especificamente, verifique o nome da sessão de captura, o estado administrativo e operacional, o slot da interface, o filtro e o identificador. Verifique se o valor de Pcapsize em bytes aumenta e se o número de pacotes capturados é diferente de zero:

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

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

SSP Traffic Monitoring Session:

Name:

cap1

Session: 1
Admin State: Enabled
Oper State: Up
Oper State Reason:

Active

Config Success: Yes

```
Config Fail Reason:  
Append Flag: Overwrite  
Session Mem Usage: 256 MB  
Error Code: 0  
Drop Count: 0  
Packet Count:
```

```
694
```

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

```
1
```

```
Port Id:  
17
```

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

```
Pcapsize:  
81093 bytes
```

```
Filter:  
filter1
```

```
Sub Interface: 0  
Application Instance:  
Application Name:  
Direction:
```

```
Ingress
```

```
Drop: Disable
```

```
Firewall seguro 4200:
```

```
<#root>  
firepower-4245#  
scope packet-capture  
  
firepower-4245 /packet-capture #  
show session cap1
```

```
SSP Traffic Monitoring Session:
```

Name:

cap1

Session: 1
Admin State: Enabled
Oper State: Up
Oper State Reason:

Active

Config Success: Yes
Config Fail Reason:
Append Flag: Overwrite
Session Mem Usage: 256 MB
Error Code: 0
Drop Count: 0
Packet Count:

222

Physical ports involved in Packet Capture:
Slot Id:

1

Port Id:

9

Pcapfile:

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

Pcapsize:

40180 bytes

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

Both

Drop: Disable

Coletar arquivos de captura

Execute as etapas de CLI FXOS 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 para a interface de gerenciamento. Neste exemplo, a captura de pacotes no Secure Firewall 4200 é analisada. Verifique os pontos principais:

1. É necessário um filtro para limpar a captura e exibir somente o tráfego sftunnel.
2. O tráfego sftunnel é capturado em ambas as direções.

No.	Time	Delta	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
11	3.763383	1.237589	192.0.2.2	192.0.2.100	TLSv1.2	112	8305	40401	Application Data
16	3.773452	0.000001	192.0.2.100	192.0.2.2	TLSv1.2	112	40401	8305	Application Data
17	3.773453	0.000001	192.0.2.2	192.0.2.100	TCP	70	8305	40401	8305 → 40401 [ACK] Seq=43 Ack=43 Win=2569 Len=0 TSval=3876531435 TSecr=3192301323
18	3.773454	0.000001	192.0.2.2	192.0.2.100	TLSv1.2	112	8305	40401	Application Data
19	3.803628	0.030174	192.0.2.100	192.0.2.2	TCP	70	40401	8305	40401 → 8305 [ACK] Seq=43 Ack=43 Win=6779 Len=0 TSval=3192301345 TSecr=3876531420
20	3.803630	0.000002	192.0.2.100	192.0.2.2	TLSv1.2	112	40401	8305	Application Data
24	3.853924	0.000002	192.0.2.100	192.0.2.2	TCP	70	40401	8305	40401 → 8305 [ACK] Seq=85 Ack=85 Win=6779 Len=0 TSval=3192301402 TSecr=3876531435
26	3.874044	0.000002	192.0.2.2	192.0.2.100	TCP	70	8305	40401	8305 → 40401 [ACK] Seq=85 Ack=85 Win=2569 Len=0 TSval=3876531527 TSecr=3192301345
27	4.035768	0.161724	192.0.2.2	192.0.2.100	TLSv1.2	1317	8305	40401	Application Data
28	4.076076	0.040308	192.0.2.100	192.0.2.2	TCP	70	40401	8305	40401 → 8305 [ACK] Seq=85 Ack=1332 Win=6779 Len=0 TSval=3192301620 TSecr=3876531694
29	4.076079	0.000003	192.0.2.100	192.0.2.2	TLSv1.2	104	40401	8305	Application Data
30	4.076081	0.000002	192.0.2.2	192.0.2.100	TCP	70	8305	40401	8305 → 40401 [ACK] Seq=1332 Ack=119 Win=2569 Len=0 TSval=3876531732 TSecr=3192301620
41	9.779092	0.226272	192.0.2.2	192.0.2.100	TLSv1.2	112	8305	55953	Application Data
42	9.779138	0.020116	192.0.2.100	192.0.2.2	TLSv1.2	112	55953	8305	Application Data
43	9.779140	0.000002	192.0.2.2	192.0.2.100	TCP	70	8305	55953	8305 → 55953 [ACK] Seq=43 Ack=449 Win=449 Len=0 TSval=3876537435 TSecr=3192307323
44	9.779141	0.000001	192.0.2.2	192.0.2.100	TLSv1.2	112	8305	55953	Application Data
45	9.799255	0.020114	192.0.2.100	192.0.2.2	TCP	70	55953	8305	55953 → 8305 [ACK] Seq=43 Ack=43 Win=501 Len=0 TSval=3192307342 TSecr=3876537417
46	9.799256	0.000001	192.0.2.100	192.0.2.2	TLSv1.2	112	55953	8305	Application Data
47	9.839497	0.040241	192.0.2.2	192.0.2.100	TCP	70	8305	55953	8305 → 55953 [ACK] Seq=85 Ack=85 Win=449 Len=0 TSval=3876537497 TSecr=3192307342
48	9.859627	0.020130	192.0.2.100	192.0.2.2	TCP	70	55953	8305	55953 → 8305 [ACK] Seq=85 Ack=85 Win=501 Len=0 TSval=3192307401 TSecr=3876537436
69	19.770764	0.010094	192.0.2.2	192.0.2.100	TLSv1.2	112	8305	40401	Application Data
70	19.770765	0.000001	192.0.2.100	192.0.2.2	TLSv1.2	112	40401	8305	Application Data
71	19.770766	0.000001	192.0.2.2	192.0.2.100	TCP	70	8305	40401	8305 → 40401 [ACK] Seq=1374 Ack=161 Win=2569 Len=0 TSval=3876547432 TSecr=3192317320
72	19.770767	0.000001	192.0.2.2	192.0.2.100	TLSv1.2	112	8305	40401	Application Data
88	19.811006	0.010059	192.0.2.100	192.0.2.2	TLSv1.2	112	40401	8305	Application Data
82	19.851277	0.010099	192.0.2.100	192.0.2.2	TCP	70	40401	8305	40401 → 8305 [ACK] Seq=203 Ack=1416 Win=6779 Len=0 TSval=3192317398 TSecr=3876547432
83	19.861343	0.010066	192.0.2.2	192.0.2.100	TCP	70	8305	40401	8305 → 40401 [ACK] Seq=1416 Ack=203 Win=2569 Len=0 TSval=3876547517 TSecr=3192317351
103	25.760447	0.895497	192.0.2.2	192.0.2.100	TLSv1.2	112	8305	55953	Application Data
104	25.780633	0.020186	192.0.2.100	192.0.2.2	TLSv1.2	112	55953	8305	Application Data
105	25.780636	0.000003	192.0.2.2	192.0.2.100	TCP	70	8305	55953	8305 → 55953 [ACK] Seq=127 Ack=127 Win=449 Len=0 TSval=3876553439 TSecr=3192323324
106	25.780637	0.000001	192.0.2.2	192.0.2.100	TLSv1.2	112	8305	55953	Application Data
107	25.800833	0.020196	192.0.2.100	192.0.2.2	TCP	70	55953	8305	55953 → 8305 [ACK] Seq=127 Ack=127 Win=501 Len=0 TSval=3192323345 TSecr=3876553420
108	25.800836	0.000003	192.0.2.100	192.0.2.2	TLSv1.2	112	55953	8305	Application Data
109	25.851155	0.050319	192.0.2.2	192.0.2.100	TCP	70	8305	55953	8305 → 55953 [ACK] Seq=169 Ack=169 Win=449 Len=0 TSval=3876553507 TSecr=3192323345

Explicação

As capturas do switch são configuradas na interface de gerenciamento.

Esta tabela resume a tarefa:

Tarefa	Ponto de captura	Filtro interno	Direção	Tráfego capturado
Configurar e verificar uma captura de pacote para o tráfego sftunnel na interface de gerenciamento	*Ethernet1/9	tráfego TCP	**ambos	Tráfego Sftunnel (porta TCP 8305) entre o host 192.0.2.100 e o host 192.0.2.2

* Consulte a tabela na seção Visão Geral de Alto Nível da Arquitetura do Sistema para verificar o mapeamento da porta do switch interno.

** Ao contrário do 3100, o Secure Firewall 4200 suporta capturas bidirecionais (entrada e saída).

Coletar Arquivos de Captura do Switch Interno com Firewall Seguro

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:

```
<#root>  
asa#  
capture capsw switch stop
```

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

```
<#root>  
asa#  
show capture capsw detail  
  
Packet Capture info  
  
Name: capsw  
  
Session: 1  
  
Admin State: disabled  
  
Oper State: down
```

Oper State Reason: Session_Admin_Shut

Config Success: yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518

```

Error Code:          0
Drop Count:         0

Total Physical ports involved in Packet Capture: 1

Physical port:
Slot Id:           1
Port Id:           1

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

```

```

Pcapsize:          139826
Filter:            capsw-1-1

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

```

```

Total Physical breakout ports involved in Packet Capture: 0

886 packets captured on disk using switch capture

Reading of capture file from disk is not supported

```

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

```

<#root>

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

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

```

```
asa#  
copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap tftp://198.51.100.10/  
  
Source filename [/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap]?  
Destination filename [sess-1-capsw-ethernet-1-1-0.pcap]?  
Copy in progress...C  
  
139826 bytes copied in 0.532 secs
```

FTD

Execute estas etapas para coletar arquivos de captura do switch interno na CLI do FTD e copiá-los para servidores acessíveis por meio de interfaces de dados ou diagnóstico:

1. Vá para o diagnóstico CLI:

```
<#root>  
>  
system support diagnostic-cli  
  
Attaching to Diagnostic CLI ... Click 'Ctrl+a then d' to detach.  
Type help or '?' for a list of available commands.  
  
firepower>  
enable  
  
Password:  
<-- Enter  
  
firepower#
```

2. Pare a captura:

```
<#root>  
firepower#  
capture capi switch stop
```

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

```
<#root>
```

```
firepower#  
show capture capsw detail  
  
Packet Capture info  
  
Name: capsw  
  
Session: 1  
  
Admin State: disabled  
  
Oper State: down  
  
Oper State Reason: Session_Admin_Shut  
  
Config Success: yes  
Config Fail Reason:  
Append Flag: overwrite  
Session Mem Usage: 256  
Session Pcap Snap Len: 1518  
Error Code: 0  
Drop Count: 0  
  
Total Physical ports involved in Packet Capture: 1  
Physical port:  
Slot Id: 1  
Port Id: 1  
  
Pcapfile:  
/mnt/disk0/packet-capture/  
sess-1-capsw-ethernet-1-1-0.pcap  
  
Pcapsize: 139826  
Filter: capsw-1-1  
  
Packet Capture Filter Info  
Name: capsw-1-1  
Protocol: 0  
Ivlan: 0  
Ovlan: 0  
Src Ip: 0.0.0.0  
Dest Ip: 0.0.0.0  
Src Ipv6: ::  
Dest Ipv6: ::  
Src MAC: 00:00:00:00:00:00  
Dest MAC: 00:00:00:00:00:00  
Src Port: 0  
Dest Port: 0  
Ethertype: 0  
  
Total Physical breakout ports involved in Packet Capture: 0  
886 packets captured on disk using switch capture
```

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

4. Use o comando CLI copy para exportar o arquivo para destinos remotos.

```
<#root>

firepower#

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

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

firepower#

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

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

139826 bytes copied in 0.532 secs
```

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

1. Pare a captura:

```
<#root>

>

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:

```
<#root>
```

```
>

show capture capsw detail

Packet Capture info

Name:          capsw

Session:        1

Admin State:    disabled

Oper State:     down

Oper State Reason: Session_Admin_Shut

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

Total Physical ports involved in Packet Capture: 1

Physical port:
Slot Id:        1
Port Id:        1

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

Pcapsize:       139826
Filter:         capsw-1-1

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

Total Physical breakout ports involved in Packet Capture: 0
886 packets captured on disk using switch capture
Reading of capture file from disk is not supported
```

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

```
<#root>
>
expert

admin@firepower:~$
sudo su

root@firepower:/home/admin
```

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

```
<#root>

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

root@KSEC-FPR3100-1:/home/admin
ls -l /ngfw/var/common/sess*
-rwxr-xr-x 1 root admin 139826 Aug  7 20:14
/ngfw/var/common/sess-1-capsw-ethernet-1-1-0.pcap

-rwxr-xr-x 1 root admin      24 Aug  6 21:58 /ngfw/var/common/sess-1-capsw-ethernet-1-3-0.pcap
```

5. No FMC, escolha Devices > File Download:

The screenshot shows the Firewall Management Center interface. The top navigation bar includes tabs for Overview, Analysis, Policies, Devices (which is highlighted), Objects, Integration, Deploy, and reporting. A user is logged in as lab_domain \ admin. The main area displays several widgets: Unique Applications over Time (line chart), Top Web Applications Seen (No Data), Top Client Applications Seen (No Data), Traffic by Application Risk (Risk: Medium, Total Bytes: 52.83 KB), Top Server Applications Seen (No Data), and Top Operating Systems Seen (No Data). A context menu is open over the 'File Download' link in the Troubleshoot section, listing options like Site To Site, Remote Access, Dynamic Access Policy, Troubleshooting, and Site to Site Monitoring.

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

The screenshot shows the 'File Download' page under the 'Devices / Troubleshoot' section. It has fields for 'Device' (set to FPR3100-1) and 'File' (set to sess-1-capsw-ethernet-1-1-0.pcap). Below these are 'Back' and 'Download' buttons. The top navigation bar and right-hand sidebar are visible.

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.