

Interne Switch-opnamen van beveiligde firewall en firewall configureren en controleren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Overzicht op hoog niveau van de systeemarchitectuur](#)

[Overzicht op hoog niveau van de interne Switch](#)

[Packet Flow en Capture points](#)

[Configuratie en verificatie op FirePOWER-applicatie 4100/9300](#)

[PacketCapture op een fysieke of poortkanaal-interface](#)

[PacketCaptures op backplane interfaces](#)

[Packet Capture op toepassingen en toepassingspoorten](#)

[Packet Capture op een subinterface van een fysieke of poortkanaal-interface](#)

[PacketCapture filters](#)

[Opnamebestanden van FirePOWER 4100/9300 interne Switch verzamelen](#)

[Richtlijnen, beperkingen en beste praktijken voor pakketvastlegging in Switch](#)

[Configuratie en verificatie van beveiligde firewall 3100](#)

[PacketCapture op een fysieke of poortkanaal-interface](#)

[Packet Capture op een subinterface van een fysieke of poortkanaal-interface](#)

[Packet Capture op interne interfaces](#)

[PacketCapture filters](#)

[Opnamebestanden van beveiligde firewall 3100 interne Switch](#)

[Richtlijnen, beperkingen en beste praktijken voor pakketvastlegging in Switch](#)

[Gerelateerde informatie](#)

Inleiding

In dit document worden de configuratie en verificatie van de Firepower beschreven en wordt de Secure Firewall interne switch weergegeven.

Voorwaarden

Vereisten

Basisproductkennis, opnameanalyse.

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

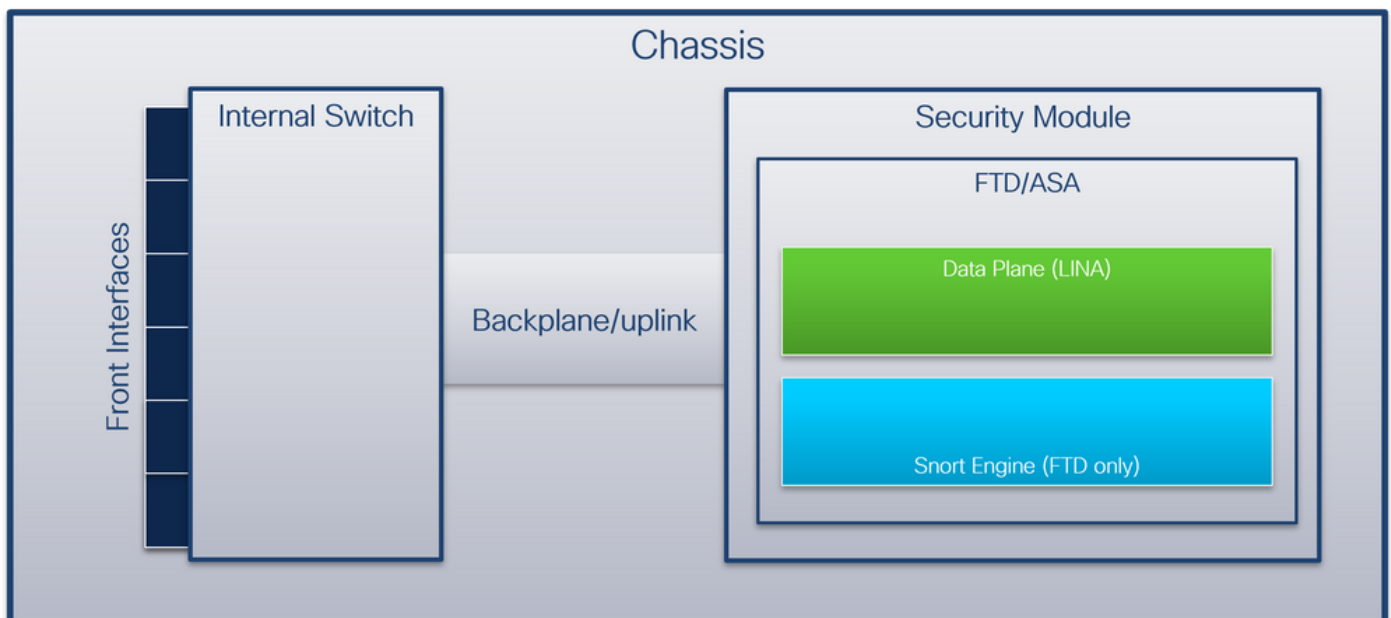
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Secure Firewall 31xx
- Firepower 41xx
- Firepower 93xx
- Cisco Secure Xersible Operating System (FXOS) 2.12.0.x
- Cisco Secure Firewall Threat Defence (FTD) 7.2.0.x
- Cisco Secure Firewall Management Center (FMC) 7.2.0.x
- Cisco Secure Firewall Device Manager (FDM) 7.2.0.x
- Adaptieve security applicatie (ASA) 9.18(1)x
- Adaptieve security applicatie Apparaatbeheer (ASDM) 7.18.1.x
- Wireshark 3.6.7 (<https://www.wireshark.org/download.html>)

Achtergrondinformatie

Overzicht op hoog niveau van de systeemarchitectuur

Vanuit het pakketstroomperspectief kan de architectuur van de Firepower 4100/9300 en Secure Firewall 3100 worden gevisualiseerd zoals in deze afbeelding:



Het chassis bevat deze onderdelen:

- **Interne switch** - doorstuurt pakket van het netwerk naar de applicatie en vice versa. De switch wordt aangesloten op de **voorinterfaces** die zich op de ingebouwde interfacemodule of de externe netwerkmodules bevinden en kan bijvoorbeeld worden aangesloten op switches. Voorbeelden van frontinterfaces zijn Ethernet 1/1, Ethernet 2/4, enzovoort. De "voorkant" is geen sterke technische definitie. In dit document wordt het gebruikt om interfaces die zijn aangesloten op externe apparaten te onderscheiden van de backplane of uplink-interfaces.

- **Backplane of uplink** - een interfaceinterface die de beveiligingsmodule (SM) verbindt met de switch. Deze tabel toont backplane interfaces op Firepower 4100/9300 en uplink-interface op Secure Firewall 3100:

Platform	Aantal ondersteunde beveiligingsmodules	Backplane/uplink-interfaces	In kaart gebrachte toepassingsinterfa
FirePOWER 4100 (behalve FirePOWER 4110/4112)	1	SM1: Ethernet1/9 Ethernet1/10	Interne gegevens0/0 Interne gegevens0/1
FirePOWER-applicatie 4110/4112	1	Ethernet1/9	Interne gegevens0/0
FirePOWER-applicatie 9300	3	SM1: Ethernet1/9 Ethernet1/10 SM2: Ethernet T1/E1 Ethernet T1/E1 SM3: Ethernet T1/E1 Ethernet T1/E1	Interne gegevens0/0 Interne gegevens0/0 Interne gegevens0/0 Interne gegevens0/0 Interne gegevens0/0
Secure-firewall 3100	1	SM1: in_data_uplink1	Interne gegevens0/1

In het geval van 2 backplane interfaces per module, de interne switch en de toepassingen op de modules voeren verkeer load-balancing over de 2 interfaces uit.

- **Security module, security engine of blade** - de module waarin applicaties zoals FTD of ASA zijn geïnstalleerd. Firepower 9300 ondersteunt maximaal 3 beveiligingsmodules.
- **Toegewezen applicatie interface** - applicaties, zoals FTD of ASA, brengen de backplane of uplink interfaces in kaart naar interne interfaces. Met andere woorden, de backplane of uplink interfaces zijn zichtbaar als interne interfaces in toepassingen.

Gebruik de opdracht **show interface detail** om interne interfaces te verifiëren:

```
> show interface detail | grep Interface
Interface Internal-Contro0/0 "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
```

Overzicht op hoog niveau van de interne Switch

FirePOWER-applicatie 4100/9300

Om een doorsturen besluit te nemen gebruikt de switch een **interface-VLAN-tag**, of **poort-VLAN-tag**, en een **Virtual Network-tag (VN-tag)**.

De port VLAN-tag wordt gebruikt door de interne switch om een interface te identificeren. De switch voegt de poort VLAN-tag in op elk toegangspakket dat op de voorinterfaces kwam. De VLAN-tag wordt automatisch geconfigureerd door het systeem en kan niet handmatig worden gewijzigd. De waarde van de tag kan worden gecontroleerd in de **fxos** opdrachtshell:

```
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
  uddl disable
  no shutdown
```

De VN-tag wordt ook door de inwendige switch ingevoegd en gebruikt om de pakketten door te sturen naar de applicatie. Het wordt automatisch ingesteld door het systeem en kan niet handmatig worden gewijzigd.

De port VLAN-tag en de VN-tag worden gedeeld met de applicatie. De applicatie voegt de respectievelijke uitgaande interface VLAN-tags en de VN-tags in elk pakket in. Wanneer een pakketje van de applicatie wordt ontvangen door de switch op de backplane interfaces, leest de switch de VLAN-tag voor de uitgaande interface en de VN-tag, identificeert de toepassing en de uitgangsinterface, stript de VLAN-tag voor poorten en de VN-tag en stuurt het pakketbestand door

naar het netwerk.

Secure-firewall 3100

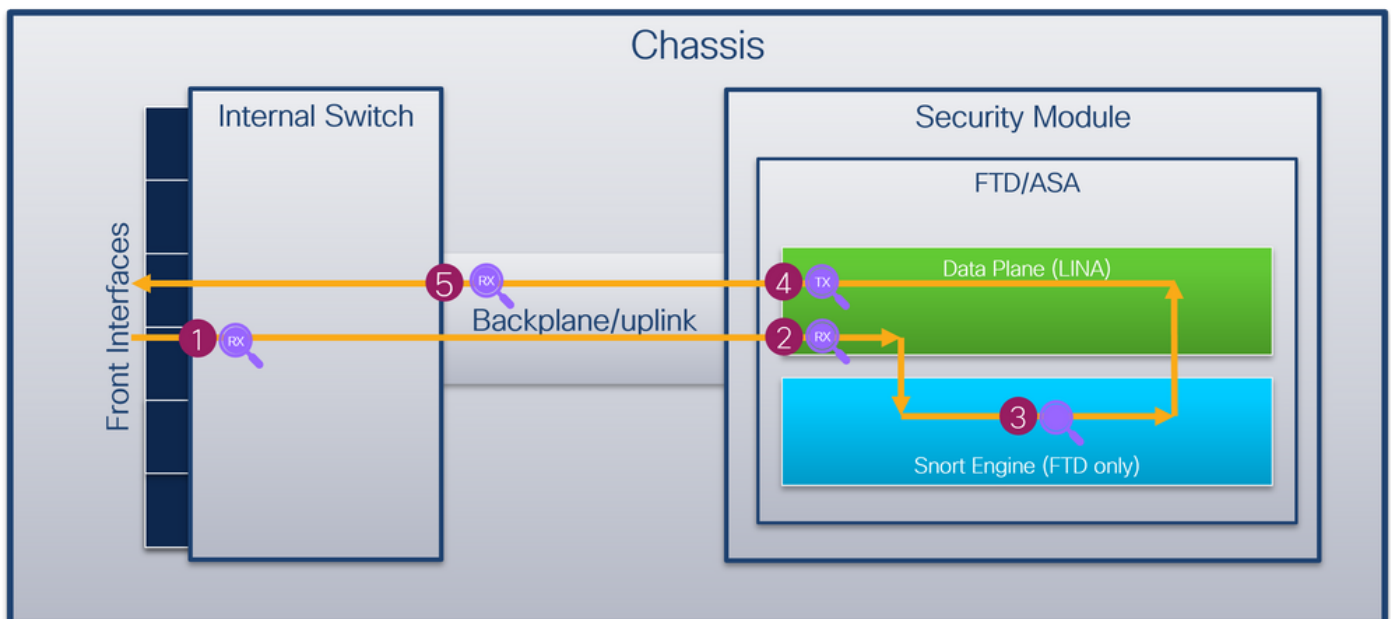
Net zoals in Firepower 4100/9300, wordt de poort VLAN tag gebruikt door de switch om een interface te identificeren.

De poort VLAN-tag wordt gedeeld met de toepassing. De toepassing voegt de respectievelijke uitgaande interface VLAN-tags in elk pakket in. Wanneer een pakketje uit de applicatie wordt ontvangen door de switch op de uplink-interface, leest de switch de VLAN-tag van de uitgaande interface, identificeert hij de uitgangsinterface, stript hij de VLAN-tag van de poort en stuurt hij het pakketje door naar het netwerk.

Packet Flow en Capture points

Firepower 4100/9300 en Secure Firewall 3100 ondersteunen pakketvastlegging op de interfaces van de switch.

Dit getal toont de pakketopnamepunten langs het pakketpad in het chassis en de toepassing:



De opnamepunten zijn:

1. Inwendig switch-frontinterface-ingangspunt. Een voorinterface is elke interface die is aangesloten op de peer devices zoals switches.
2. Opnamepunt voor interface-ingang van gegevensvlak
3. Snelopnamepunt
4. Uitgangspunt van de gegevensvlak-interface
5. Interne switch-backplane of uplink-ingangspunt. Een backplane of uplink-interface verbindt de interne switch met de toepassing.

De interne switch ondersteunt alleen invoerinterfaceopnamen. Dat zijn alleen de pakketten die van het netwerk of van de ASA/FTD-toepassing worden ontvangen. **Uitgangspakket-opnamen worden niet ondersteund.**

Configuratie en verificatie op FirePOWER-applicatie 4100/9300

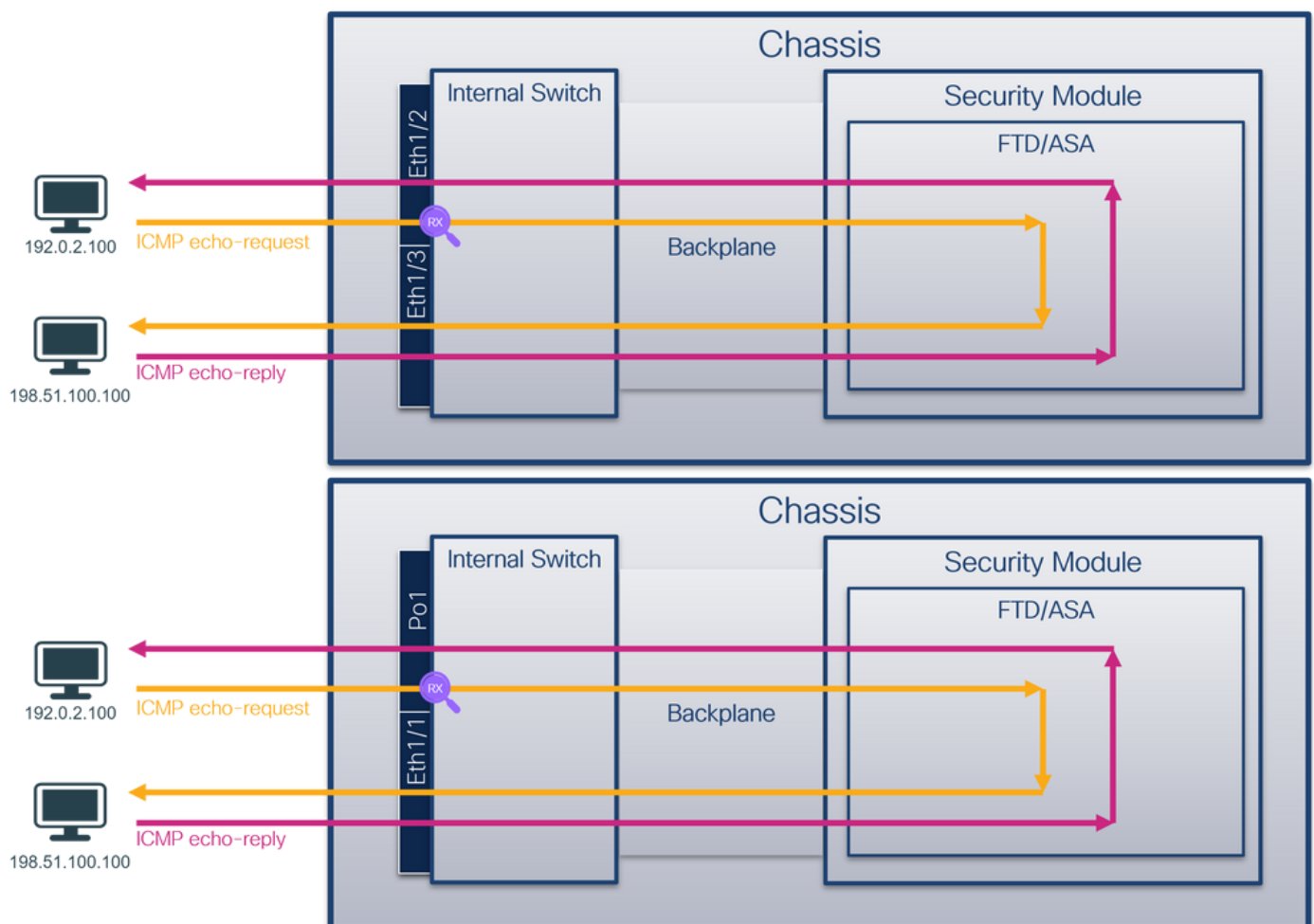
De interne switch Firepower 4100/9300 kan worden geconfigureerd in **Tools > Packet Capture** op FCM of in **scope packet-capture** in FXOS CLI. Raadpleeg voor de beschrijving van de pakketopnameopties de *configuratiehandleiding voor Cisco Firepower 4100/9300 FXOS Chassis Manager* of de *configuratiehandleiding voor Cisco Firepower 4100/9300 FXOS CLI*, hoofdstuk **Problemen oplossen**, sectie **Packet Capture**.

Deze scenario's behandelen de gemeenschappelijke gevallen van het gebruik van Firepower 4100/9300 interne switch vangt.

PacketCapture op een fysieke of poortkanaal-interface

Gebruik de FCM en CLI om een pakketopname op interface Ethernet1/2 of Portchannel1 interface te configureren en te verifiëren. Zorg er in het geval van een poort-kanaal interface voor dat u alle fysieke lidinterfaces selecteert.

Topologie, pakketstroom en de opnamepunten

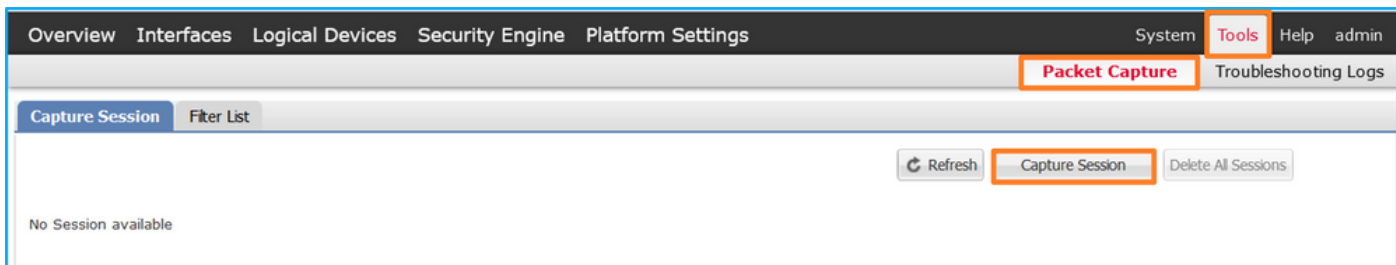


Configuratie

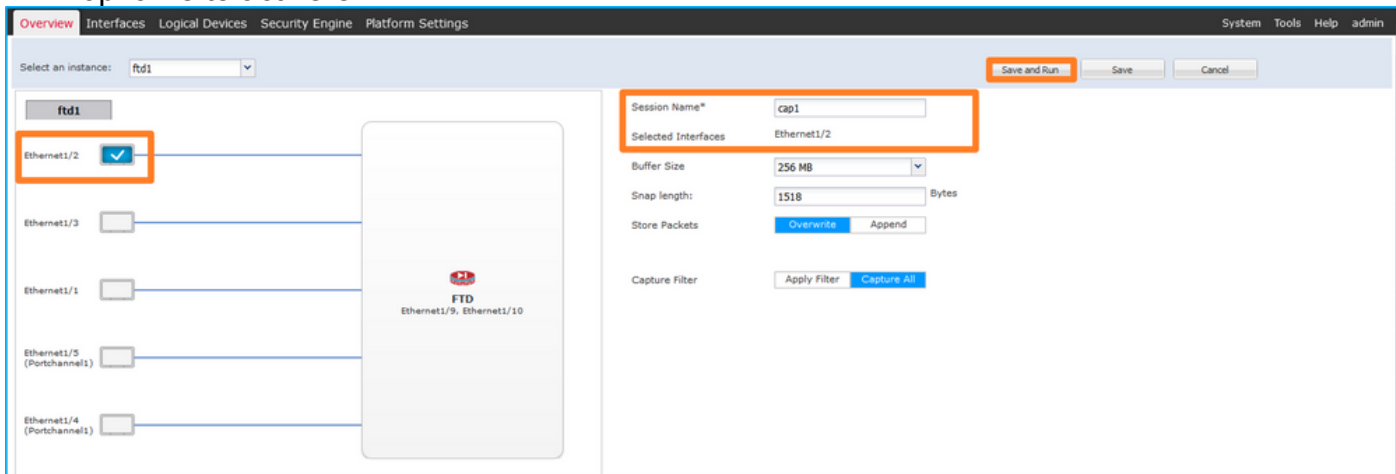
FCM

Volg deze stappen op FCM om een pakketopname op interfaces Ethernet1/2 of Portchannel1 te configureren:

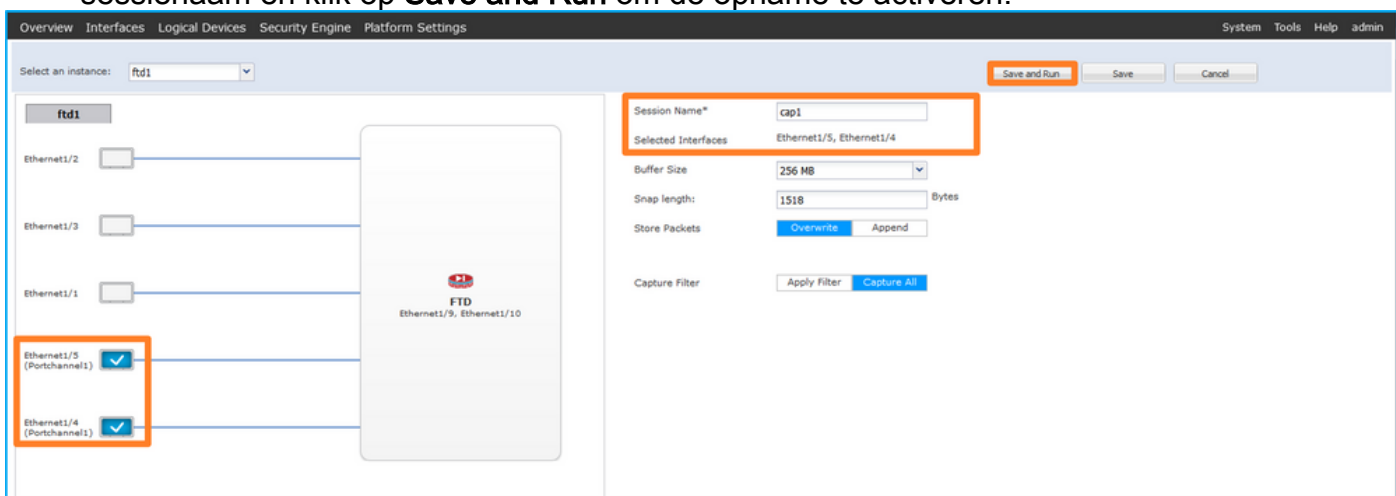
1. Gebruik **Gereedschappen > Packet Capture > Capture Session** om een nieuwe opnamesessie te maken:



2. Selecteer de interface **Ethernet1/2**, geef de sessienaam op en klik op **Save and Run** om de opname te activeren:



3. In het geval van een poort-kanaal interface, selecteer alle fysieke lidinterfaces, geef de sessienaam en klik op **Save and Run** om de opname te activeren:



FXOS CLI

Volg deze stappen op FXOS CLI om een pakketopname op interfaces Ethernet1/2 of Portchannel1 te configureren:

1. Identificeer het toepassingstype en de identificatiecode:

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

Native No Not Applicable None

2. In het geval van een poort-kanaal-interface, identificeer zijn lidinterfaces:

```
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. Een opnamesessie maken:

```
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 #
```

Voor poort-kanaal interfaces wordt een afzonderlijke opname voor elke lidinterface geconfigureerd:

```
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 #
```

Verificatie

FCM

Controleer de **interfacenaam**, zorg ervoor dat de **operationele status** omhoog is en dat de **bestandsgrootte (in bytes)** toeneemt:

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

Portchannel1 met lid interfaces Ethernet1/4 en Ethernet1/5:

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

FXOS CLI

Controleer de opnamedetails in scope-pakketopname:

```
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
```

Poortkanaal 1 met lidinterfaces Ethernet1/4 en Ethernet1/5:

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

Traffic Monitoring Session:

```
Packet Capture Session Name: cap1
Session: 1
Admin State: Enabled
Oper State: Up
Oper State Reason: Active
Config Success: Yes
```

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

Physical ports involved in Packet Capture:

Slot Id: 1
Port Id: 4
Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-4-0.pcap
Pcapsize: 310276 bytes

Filter:

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

Slot Id: 1
Port Id: 5
Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-5-0.pcap
Pcapsize: 160 bytes

Filter:

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

Opnamebestanden verzamelen

Volg de stappen in het gedeelte **Verzamel Firepower 4100/9300 Internal Switch Capture Files**.

Capture file analyse

Gebruik een applicatie voor pakketopname om het opnamebestand voor Ethernet1/2 te openen. Selecteer het eerste pakket en controleer de belangrijkste punten:

1. Alleen ICMP-pakketten voor echoverzoek worden opgenomen. Elk pakket wordt 2 keer opgenomen en getoond.
2. De oorspronkelijke pakketheader is zonder de VLAN-tag.
3. De switch voegt extra poort VLAN-tag **102** in die de toegangsinterface Ethernet1/2 identificeert.
4. Op de switch staat een extra VN-tag.

The image shows a Wireshark capture of ICMP Echo (ping) requests. The packet list pane shows 29 packets of type ICMP Echo (ping) request, all with length 108 bytes. The first packet is selected, and its details are shown in the packet details pane. The details pane is divided into four sections, each with a red box and a number:

- 4**: Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)
- 2**: Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
- 3**: Internet Control Message Protocol
- 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102**

Selecteer het tweede pakket en controleer de belangrijkste punten:

1. Alleen ICMP-pakketten voor echoverzoek worden opgenomen. Elk pakket wordt 2 keer opgenomen en getoond.
2. De oorspronkelijke pakketheader is zonder de VLAN-tag.
3. De switch voegt extra poort VLAN-tag 102 in die de toegangsinterface Ethernet1/2 identificeert.

The image shows a Wireshark capture of ICMP Echo (ping) requests. The second packet is selected, and its details are shown in the packet details pane. The details pane is divided into three sections, each with a red box and a number:

- 3**: 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
- 2**: Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
- Internet Control Message Protocol**

Open de opnamebestanden voor Portchannel1-lidinterfaces. Selecteer het eerste pakket en controleer de belangrijkste punten:

1. Alleen ICMP-pakketten voor echoverzoek worden opgenomen. Elk pakket wordt 2 keer opgenomen en getoond.

- De oorspronkelijke pakketheader is zonder de VLAN-tag.
- De switch voegt een extra poort VLAN-tag 1001 in die de toegangsinterface Portchannel1 identificeert.
- Op de switch staat een extra VN-tag.

Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_3, in Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: a2:76:f2:00:00:25 (a2:76:f2:00:00:25)

1 VN-Tag

- 1... .. = Direction: From Bridge
- .0.. .. = Pointer: vif_id
- .00 0000 0101 0100 .. = Destination: 84
-0..... = Looped: No
-0..... = Reserved: 0
-000..... = Version: 0
- Type: 802.1Q Virtual LAN (0x8100)

3 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1001

- 000. = Priority: Best Effort (default) (0)
- ...0 .. = DEI: Ineligible
- ... 0011 1110 1001 = ID: 1001
- Type: IPv4 (0x0800)

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

Internet Control Message Protocol

Selecteer het tweede pakket en controleer de belangrijkste punten:

- Alleen ICMP-pakketten voor echoverzoek worden opgenomen. Elk pakket wordt 2 keer opgenomen en getoond.
- De oorspronkelijke pakketheader is zonder de VLAN-tag.
- De switch voegt een extra poort VLAN-tag 1001 in die de toegangsinterface Portchannel1 identificeert.

Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture_u0_3, in Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: a2:76:f2:00:00:25 (a2:76:f2:00:00:25)

3 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1001

- 000. = Priority: Best Effort (default) (0)
- ...0 .. = DEI: Ineligible
- ... 0011 1110 1001 = ID: 1001
- Type: IPv4 (0x0800)

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

Internet Control Message Protocol

Uitleg

Wanneer een pakketopname op een frontinterface is geconfigureerd, neemt de switch elk pakket tweemaal tegelijk op:

- Na de invoeging van de poort VLAN-tag.
- Na het inbrengen van de VN-tag.

In de volgorde van bewerkingen wordt de VN-tag in een later stadium ingevoegd dan de invoeging van de VLAN-tag in de poort. In het opnamebestand wordt het pakket met de VN-tag echter eerder weergegeven dan het pakket met de poort VLAN-tag.

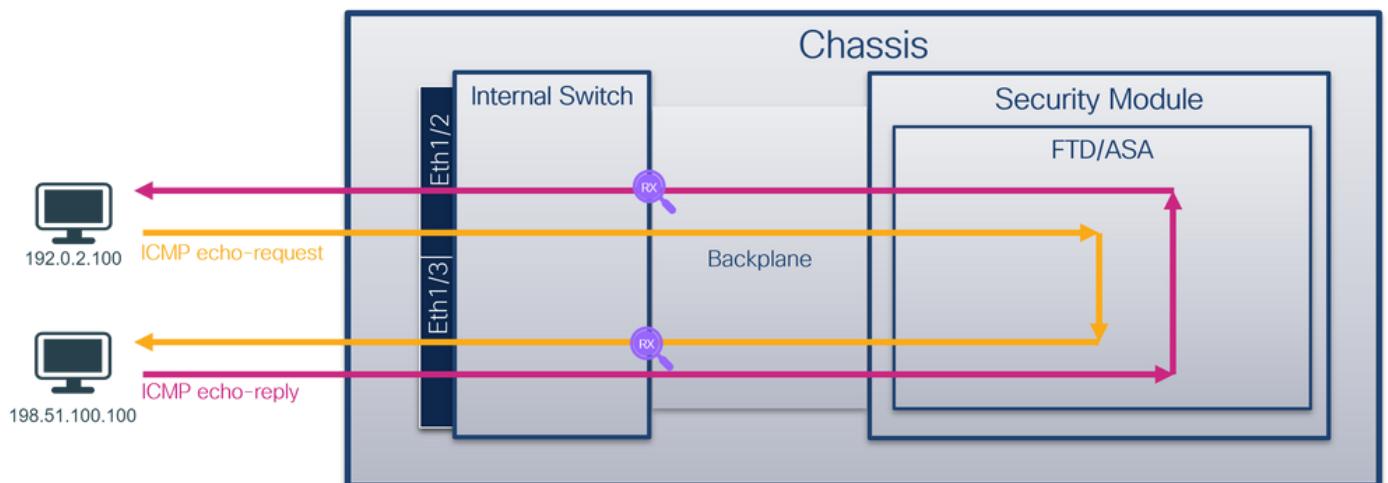
In deze tabel wordt de taak samengevat:

Taak	Opnamepunt	Interne poort VLAN in opgenomen pakketten	Richting	Opgenomen verkeer
Configureer en controleer een pakketopname op interface Ethernet1/2	Ethernet1/2	102	Alleen inspringen	ICMP-echoverzoeken van host 192.0.2.10 naar host 198.51.100.
Configureer en controleer een pakketopname op interface Portchannel1 met lidinterfaces Ethernet1/4 en Ethernet1/5	Ethernet1/4 Ethernet1/5	1001	Alleen inspringen	ICMP-echoverzoeken van host 192.0.2.10 naar host 198.51.100.

PacketCaptures op backplane interfaces

Gebruik FCM en CLI om een pakketopname op backplane interfaces te configureren en te verifiëren.

Topologie, pakketstroom en de opnamepunten

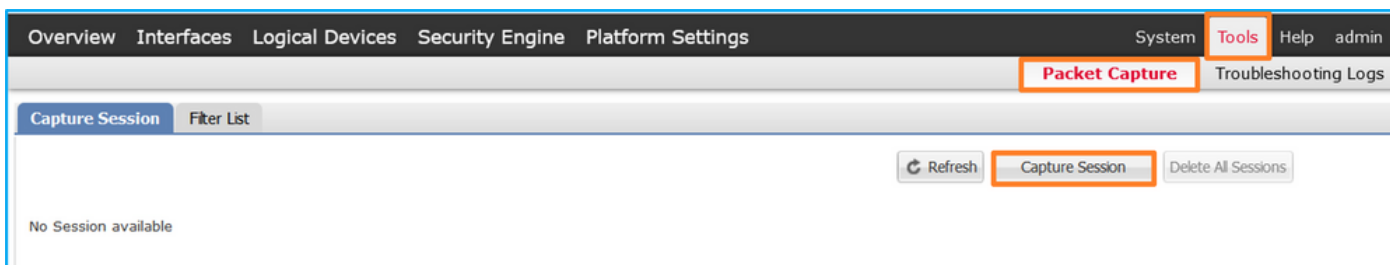


Configuratie

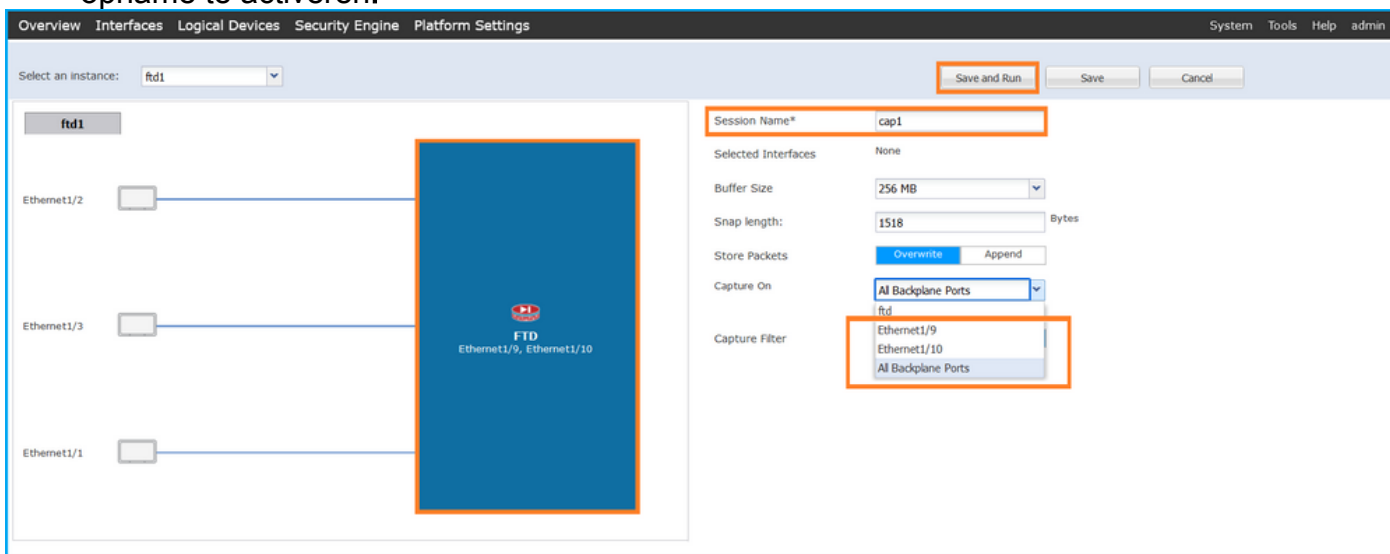
FCM

Volg deze stappen op FCM om pakketopnamen op backplane interfaces te configureren:

1. Gebruik **Gereedschappen > Packet Capture > Capture Session** om een nieuwe opnamesessie te maken:



2. Als u pakketten op alle backplane interfaces wilt opnemen, selecteert u de toepassing en vervolgens **Alle backplane poorten** uit de **vervolgkeuzelijst Capture On**. U kunt ook de specifieke backplane interface kiezen. In dit geval zijn backplane interfaces Ethernet1/9 en Ethernet1/10 beschikbaar. Geef de **sessienaam** op en klik op **Opslaan en Uitvoeren** om de opname te activeren:



FXOS CLI

Volg deze stappen op FXOS CLI om pakketopnamen op backplane interfaces te configureren:

1. Identificeer het toepassingstype en de identificatiecode:

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

2. Een opnamesessie maken:

```
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 #
```

Verificatie

FCM

Controleer de **interfacenaam**, zorg ervoor dat de **operationele status** omhoog is en dat de **bestandsgrootte (in bytes)** toeneemt:

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

FXOS CLI

Controleer de opnamedetails in **scope-pakketopname**:

```
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
```

Opnamebestanden verzamelen

Volg de stappen in het gedeelte **Verzamel Firepower 4100/9300 Internal Switch Capture Files.**

Capture file analyse

Gebruik een applicatie voor pakketvastlegging om de opnamebestanden te openen. Zorg er bij meer dan 1 backplane interface voor dat alle opnamebestanden voor elke backplane interface worden geopend. In dit geval worden de pakketten opgenomen op de backplane interface Ethernet1/9.

Selecteer het eerste en het tweede pakket en controleer de belangrijkste punten:

1. Elk pakket met ICMP-echoverzoek wordt opgenomen en 2 keer weergegeven.
2. De oorspronkelijke pakketheader is zonder de VLAN-tag.
3. De switch voegt extra poort VLAN-tag **103** in die de uitgaande interface Ethernet1/3 identificeert.
4. Op de switch staat een extra VN-tag.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-07-14 20:20:36.513854256	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (no response found!)
2	2022-07-14 20:20:36.513857289	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	0xc2c2 (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	0xc2c2 (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 (reply in 7)
7	2022-07-14 20:20:37.538046165	198.51.100.100	192.0.2.100	ICMP	108	0xc9b (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	0xc9b (52379)	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 (reply in 11)
11	2022-07-14 20:20:38.562048288	198.51.100.100	192.0.2.100	ICMP	108	0xc44 (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	0xc44 (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 10)
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 (request in 14)
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 20:20:40.610179685	198.51.100.100	192.0.2.100	ICMP	108	0xcdbf (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	0xcdbf (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 (reply in 23)
23	2022-07-14 20:20:41.634084102	198.51.100.100	192.0.2.100	ICMP	108	0xc36 (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	0xc36 (52790)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64 (request in 22)
25	2022-07-14 20:20:42.657799898	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 20:20:42.657799898	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 20:20:42.657980675	198.51.100.100	192.0.2.100	ICMP	108	0xc49 (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	0xc49 (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 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0

> Ethernet II, Src: Cisco b9:77:2d (58:97:bd:b9:77:2d), Dst: VMware 9d:e7:50 (00:50:56:9d:e7:50)

```

0000 00 50 56 9d e7 50 58 97 bd b9 77 2d 09 26 00 00  PV..PX: ..w-&..
0010 00 0a 21 00 00 67 08 45 00 00 54 59 90 40 00  ....B:  E..TV@
0020 40 01 f4 1c c0 09 02 64 c6 33 64 64 08 00 22 68  @.....d 3dd- "h
0030 00 01 00 0f 89 7a d0 62 00 00 00 b3 d7 89 00  ....2:b .....
0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b  ....  !"e $%&'()*+
0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b  ....  !"e $%&'()*+
0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37  .... /0123 4567
  
```

4 VNI-Tag

```

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

3 802.1Q 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)
  
```

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

Internet Control Message Protocol

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-07-14 20:20:36.513854256	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (no response found!)
2	2022-07-14 20:20:36.513857289	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	0x5990 (22928)	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	0x5990 (22928)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 3)


```

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

Selecteer het derde en vierde pakket en controleer de belangrijkste punten:

1. Elk ICMP-echoantwoord wordt opgenomen en 2 keer weergegeven.
2. De oorspronkelijke pakketheader is zonder de VLAN-tag.
3. De switch voegt extra poort VLAN-tag 102 in die de uitgangsinterface Ethernet1/2 identificeert.
4. Op de switch staat een extra VN-tag.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-07-14 20:20:36.513854256	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (no response found!)
2	2022-07-14 20:20:36.513857289	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	0x5268 (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	0x5268 (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 3)


```

Frame 3: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VMware 9d:e8:be (00:50:56:9d:e8:be)
  VN-Tag
  0... .. = Direction: To Bridge
  .0... .. = Pointer: vif_id
  ..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
  
```

Uitleg

Wanneer een pakketopname op een backplane interface is geconfigureerd, neemt de switch elk pakket twee keer op. In dit geval ontvangt de switch binnen de poort pakketten die al door de toepassing op de beveiligingsmodule zijn gelabeld met de port VLAN-tag en de VN-tag. De VLAN-tag identificeert de uitgangsinterface die het interne chassis gebruikt om de pakketten naar het netwerk te doorsturen. De VLAN-tag 103 in ICMP-echoverdrachtpakketten identificeert Ethernet1/3 als de uitgangsinterface, terwijl VLAN-tag 102 in ICMP-echoantwoordpakketten Ethernet1/2 als de uitgangsinterface identificeert. De switch verwijdert de VN-tag en de interne VLAN-tag voordat de pakketten naar het netwerk worden doorgestuurd.

In deze tabel wordt de taak samengevat:

Taak	Opname punt	Interne poort opgenomen pakketten	VLAN in g	Richtin g	Opgenomen verkeer
Configureer en controleer pakketopnamen op backplane interfaces	Backplane interface s	102 103		Alleen insprin gen	ICMP-echoverzoeken van host 192.0.2.10 naar host 198.51.100.100 ICMP-echoantwoorden van host 198.51.100.100 op host 192.0.2.10

Packet Capture op toepassingen en toepassingspoorten

Het pakket van de toepassing of van de toepassingspoort wordt altijd gevormd op backplane interfaces en bovendien op de voorinterfaces als de gebruiker de richting van de toepassingsopname specificeert.

Er zijn voornamelijk 2 gevallen van gebruik:

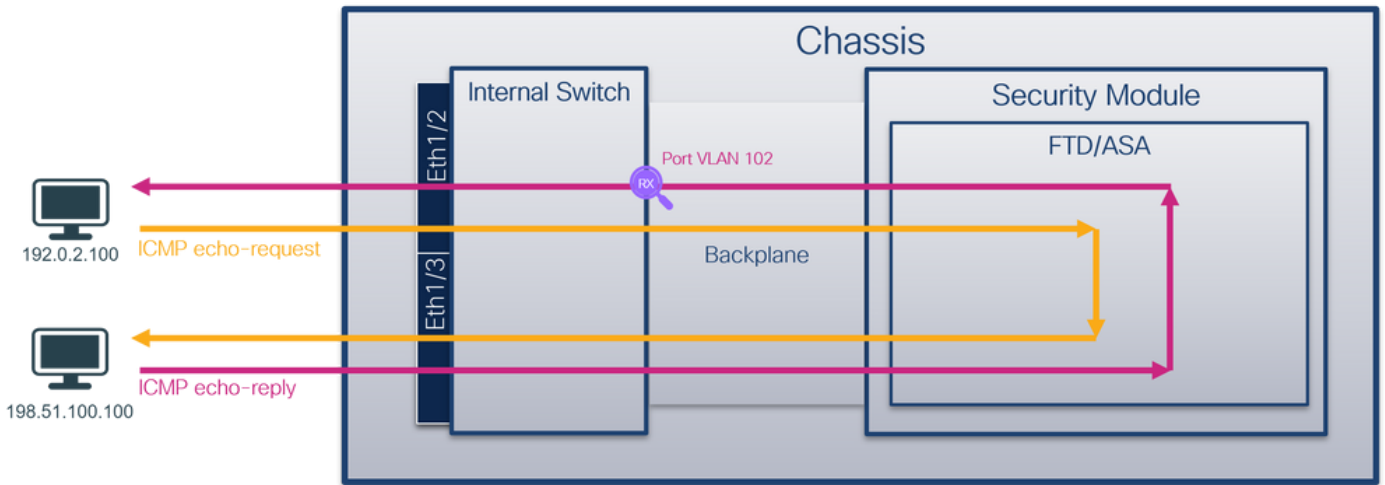
- Configureer pakketopnamen op backplane interfaces voor pakketten die een specifieke frontinterface verlaten. Configureer bijvoorbeeld pakketopnamen op de backplane interface Ethernet1/9 voor pakketten die interface Ethernet1/2 verlaten.
- Configureer de gelijktijdige pakketopname op een specifieke voorinterface en de backplane interfaces. Configureer bijvoorbeeld gelijktijdige pakketopname op interface Ethernet1/2 en op de backplane interface Ethernet1/9 voor pakketten die interface Ethernet1/2 verlaten.

Deze paragraaf behandelt beide gebruikgevallen.

Taak 1

Gebruik de FCM en CLI om een pakketopname op de backplane interface te configureren en te verifiëren. Pakketten waarvoor de toepassingspoort Ethernet1/2 is geïdentificeerd als de uitgangsinterface worden opgenomen. In dit geval worden ICMP-antwoorden opgenomen.

Topologie, pakketstroom en de opnamepunten

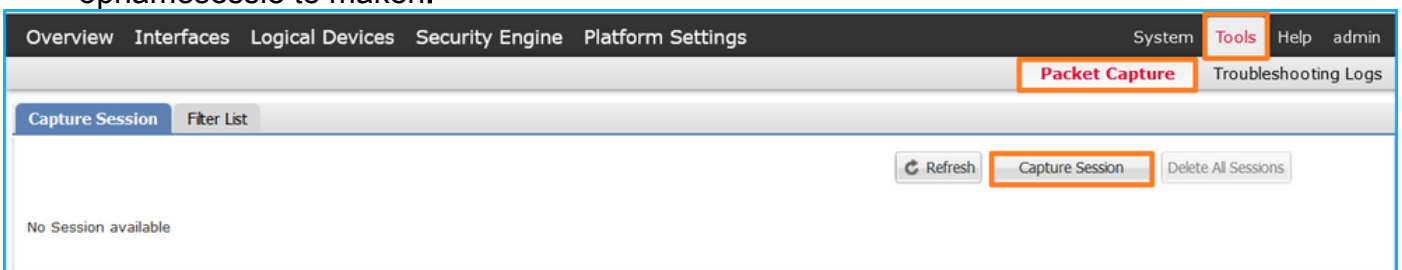


Configuratie

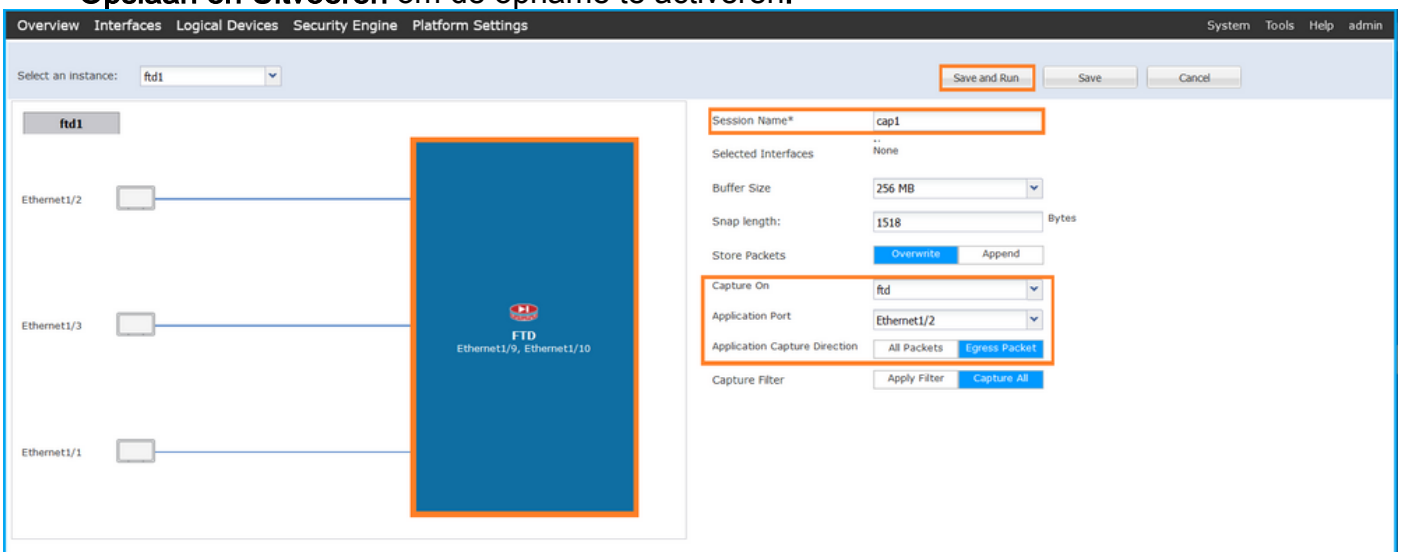
FCM

Volg deze stappen op FCM om een pakketopname te configureren op de FTD-toepassing en de toepassingspoort Ethernet1/2:

1. Gebruik **Gereedschappen > Packet Capture > Capture Session** om een nieuwe opnamesessie te maken:



2. Selecteer de toepassing, **Ethernet1/2** in de vervolgkeuzelijst **Toepassingspoort** en selecteer **Uitgangspakket** in de richting **Toepassingsopname**. Geef de **sessienaam** op en klik op **Opslaan en Uitvoeren** om de opname te activeren:



FXOS CLI

Volg deze stappen op FXOS CLI om pakketopnamen op backplane interfaces te configureren:

1. Identificeer het toepassingstype en de identificatiecode:

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

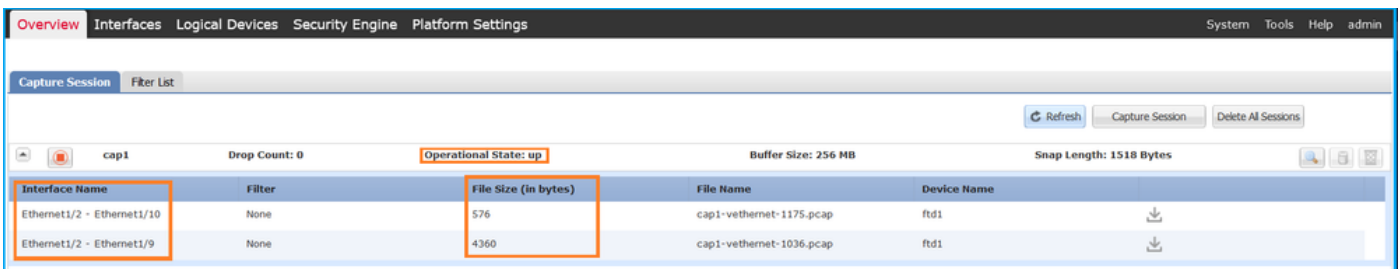
2. Een opnamesessie maken:

```
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 #
```

Verificatie

FCM

Controleer de **interfacenaam**, zorg ervoor dat de **operationele status** omhoog is en dat de **bestandsgrootte (in bytes)** toeneemt:



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

FXOS CLI

Controleer de opnamedetails in **scope-pakketopname**:

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

Traffic Monitoring Session:

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

Application ports involved in Packet Capture:

Slot Id: 1
Link Name: 112
Port Name: Ethernet1/2

App Name: ftd

Sub Interface: 0

Application Instance Identifier: ftd1

Application ports resolved to:

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

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

Opnamebestanden verzamelen

Volg de stappen in het gedeelte **Verzamel Firepower 4100/9300 Internal Switch Capture Files**.

Capture file analyse

Gebruik een applicatie voor pakketvastlegging om de opnamebestanden te openen. In het geval van meerdere backplane interfaces, zorg ervoor dat alle opnamebestanden voor elke backplane interface worden geopend. In dit geval worden de pakketten opgenomen op de backplane interface Ethernet1/9.

Selecteer het eerste en het tweede pakket en controleer de belangrijkste punten:

1. Elk ICMP-echoantwoord wordt opgenomen en 2 keer weergegeven.
2. De oorspronkelijke pakketheader is zonder de VLAN-tag.
3. De switch voegt extra poort VLAN-tag **102** in die de uitgangsinterface Ethernet1/2 identificeert.
4. Op de switch staat een extra VN-tag.

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
2	2022-08-01 10:03:22.231239747	198.51.100.100	192.0.2.100	ICMP	108	0x42f8 (17144)	64	Echo (ping) reply
3	2022-08-01 10:03:23.232244769	198.51.100.100	192.0.2.100	ICMP	108	0x4303 (17331)	64	Echo (ping) reply
4	2022-08-01 10:03:23.232247753	198.51.100.100	192.0.2.100	ICMP	108	0x43b3 (17331)	64	Echo (ping) reply
5	2022-08-01 10:03:24.234703981	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64	Echo (ping) reply
6	2022-08-01 10:03:24.234706751	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64	Echo (ping) reply
7	2022-08-01 10:03:25.258672449	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64	Echo (ping) reply
8	2022-08-01 10:03:25.258674861	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64	Echo (ping) reply
9	2022-08-01 10:03:26.282663169	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64	Echo (ping) reply
10	2022-08-01 10:03:26.282666183	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64	Echo (ping) reply
11	2022-08-01 10:03:27.306671694	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64	Echo (ping) reply
12	2022-08-01 10:03:27.306674378	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64	Echo (ping) reply
13	2022-08-01 10:03:28.330664677	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64	Echo (ping) reply
14	2022-08-01 10:03:28.330667153	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64	Echo (ping) reply
15	2022-08-01 10:03:29.354795931	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply
16	2022-08-01 10:03:29.354936706	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply
17	2022-08-01 10:03:30.378795204	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64	Echo (ping) reply
18	2022-08-01 10:03:30.378798172	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64	Echo (ping) reply
19	2022-08-01 10:03:31.402772217	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64	Echo (ping) reply
20	2022-08-01 10:03:31.402774775	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64	Echo (ping) reply
21	2022-08-01 10:03:32.426693254	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64	Echo (ping) reply
22	2022-08-01 10:03:32.426695691	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64	Echo (ping) reply

```

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

```

```

> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
0000 .... = 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

```

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
2	2022-08-01 10:03:22.231239747	198.51.100.100	192.0.2.100	ICMP	108	0x42f8 (17144)	64	Echo (ping) reply
3	2022-08-01 10:03:23.232244769	198.51.100.100	192.0.2.100	ICMP	108	0x4303 (17331)	64	Echo (ping) reply
4	2022-08-01 10:03:23.232247753	198.51.100.100	192.0.2.100	ICMP	108	0x43b3 (17331)	64	Echo (ping) reply
5	2022-08-01 10:03:24.234703981	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64	Echo (ping) reply
6	2022-08-01 10:03:24.234706751	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64	Echo (ping) reply
7	2022-08-01 10:03:25.258672449	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64	Echo (ping) reply
8	2022-08-01 10:03:25.258674861	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64	Echo (ping) reply
9	2022-08-01 10:03:26.282663169	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64	Echo (ping) reply
10	2022-08-01 10:03:26.282666183	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64	Echo (ping) reply
11	2022-08-01 10:03:27.306671694	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64	Echo (ping) reply
12	2022-08-01 10:03:27.306674378	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64	Echo (ping) reply
13	2022-08-01 10:03:28.330664677	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64	Echo (ping) reply
14	2022-08-01 10:03:28.330667153	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64	Echo (ping) reply
15	2022-08-01 10:03:29.354795931	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply
16	2022-08-01 10:03:29.354936706	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply
17	2022-08-01 10:03:30.378795204	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64	Echo (ping) reply
18	2022-08-01 10:03:30.378798172	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64	Echo (ping) reply
19	2022-08-01 10:03:31.402772217	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64	Echo (ping) reply
20	2022-08-01 10:03:31.402774775	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64	Echo (ping) reply
21	2022-08-01 10:03:32.426693254	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64	Echo (ping) reply
22	2022-08-01 10:03:32.426695691	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64	Echo (ping) reply

```

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

```

```

> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
0000 .... = 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

```

Uitleg

In dit geval is Ethernet1/2 met poort VLAN-tag 102 de uitgangside interface voor de ICMP-echoantwoordpakketten.

Wanneer de richting van de toepassingsopname is ingesteld op **Uitgang** in de opnameopties, worden pakketten met de poort VLAN-tag 102 in de Ethernet-header opgenomen op de backplane interfaces in de toegangsrichting.

In deze tabel wordt de taak samengevat:

Taak	Opnamepunt	Interne poort VLAN in opgenomen pakketten	Richting	Opgenomen verkeer
Configureren en verifiëren van opnamen op applicatie- en toepassingspoort Ethernet1/2	Backplane interfaces	102	Alleen insprong en	ICMP-echoantwoorden van host 198.51.100.100 op host en 192.0.2.100

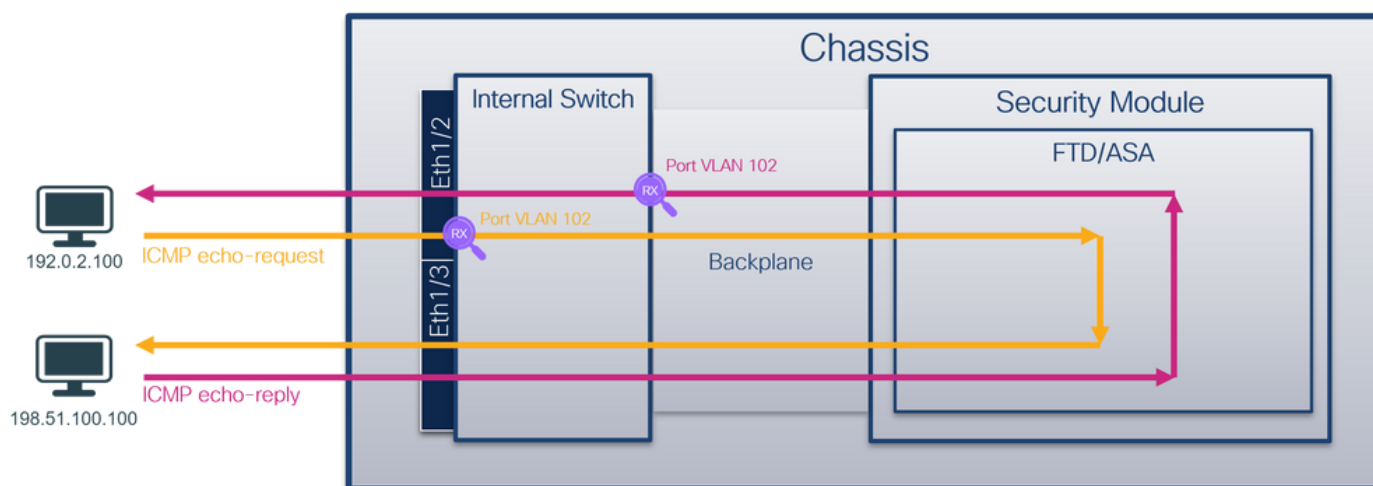
Taak 2

Gebruik de FCM en CLI om een pakketopname op de backplane interface en de voorinterface Ethernet1/2 te configureren en te verifiëren.

Gelijktijdige pakketopnamen worden geconfigureerd op:

- Voorinterface - de pakketten met de poort VLAN 102 op de interface Ethernet1/2 worden opgenomen. Opgenomen pakketten zijn ICMP-echoverzoeken.
- Backplane interfaces - pakketten waarvoor Ethernet1/2 is geïdentificeerd als de uitgaande interface, of de pakketten met de poort VLAN 102, worden opgenomen. Opgenomen pakketten zijn ICMP-echoantwoorden.

Topologie, pakketstroom en de opnamepunten

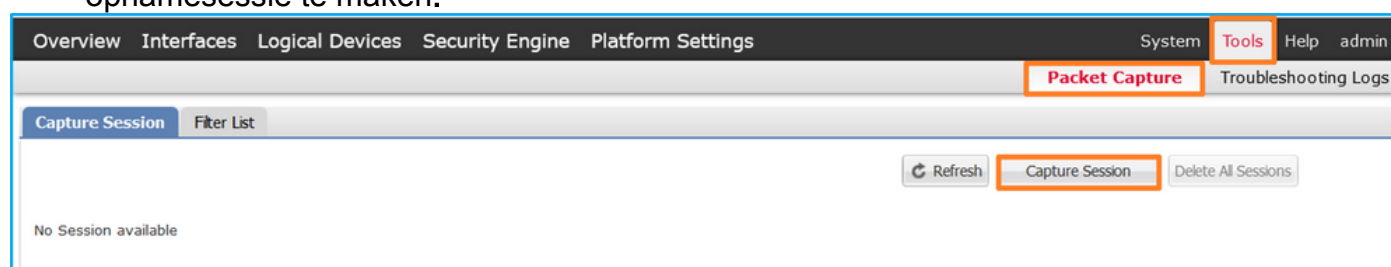


Configuratie

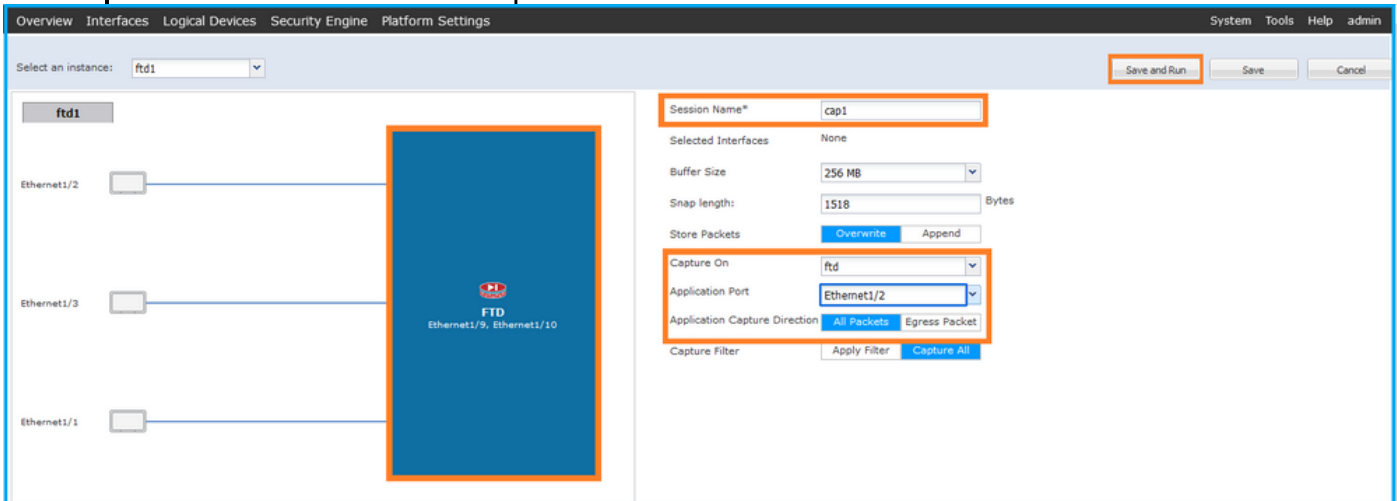
FCM

Volg deze stappen op FCM om een pakketopname te configureren op de FTD-toepassing en de toepassingspoort Ethernet1/2:

1. Gebruik **Gereedschappen > Packet Capture > Capture Session** om een nieuwe opnamesessie te maken:



- Selecteer de FTD-toepassing, **Ethernet1/2** in de vervolgkeuzelijst **Toepassingspoorten** en selecteer **Alle pakketten** in de **toepassingsopnamerichtlijn**. Geef de **sessienaam** op en klik op **Opslaan en Uitvoeren** om de opname te activeren:



FXOS CLI

Volg deze stappen op FXOS CLI om pakketopnamen op backplane interfaces te configureren:

- Identificeer het toepassingstype en de identificatiecode:

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

- Een opnamesessie maken:

```
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
```

Verificatie

FCM

Controleer de **interfacenaam**, zorg ervoor dat de **operationele status** omhoog is en dat de **bestandsgrootte** (in bytes) toeneemt:

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/2	None	95040	cap1-ethernet-1-2-0-0.pcap	ftd1
Ethernet1/2 - Ethernet1/10	None	368	cap1-vethernet-1175.pcap	ftd1
Ethernet1/2 - Ethernet1/9	None	13040	cap1-vethernet-1036.pcap	ftd1

FXOS CLI

Controleer de opnamedetails in scope-pakketopname:

```
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:

Opnamebestanden verzamelen

Volg de stappen in het gedeelte **Verzamel Firepower 4100/9300 Internal Switch Capture Files.**

Capture file analyse

Gebruik een applicatie voor pakketvastlegging om de opnamebestanden te openen. In het geval van meerdere backplane interfaces, zorg ervoor dat alle opnamebestanden voor elke backplane interface worden geopend. In dit geval worden de pakketten opgenomen op de backplane interface Ethernet1/9.

Open het opnamebestand voor de interface Ethernet1/2, selecteer het eerste pakket en controleer de belangrijkste punten:

1. Alleen ICMP-echoverdrachtpakketten worden opgenomen. Elk pakket wordt 2 keer opgenomen en getoond.
2. De oorspronkelijke pakketheader is zonder de VLAN-tag.
3. De switch voegt extra poort VLAN-tag 102 in die de toegangsinterface Ethernet1/2 identificeert.
4. Op de switch staat een extra VN-tag.

The screenshot displays a network capture analysis tool interface. The top section shows a list of captured packets, with the first packet selected. The packet details are shown in a tree view on the left, and the raw packet data is shown in hexadecimal and ASCII on the right.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info
1	2022-08-01 11:33:19.070693081	192.0.2.100	198.51.100.100	ICMP	108	0xc009 (49161)	64 Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found!)
2	2022-08-01 11:33:19.070695347	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found!)
3	2022-08-01 11:33:19.071217121	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found!)
4	2022-08-01 11:33:19.071218458	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found!)
5	2022-08-01 11:33:20.072036625	192.0.2.100	198.51.100.100	ICMP	108	0xc00a (49326)	64 Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found!)
6	2022-08-01 11:33:20.072038399	192.0.2.100	198.51.100.100	ICMP	102	0xc167 (49511)	64 Echo (ping) request id=0x0013, seq=3/768, ttl=64 (no response found!)
7	2022-08-01 11:33:22.074576640	192.0.2.100	198.51.100.100	ICMP	108	0xc175 (49525)	64 Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found!)
8	2022-08-01 11:33:22.074578010	192.0.2.100	198.51.100.100	ICMP	102	0xc208 (49672)	64 Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found!)
9	2022-08-01 11:33:23.075779089	192.0.2.100	198.51.100.100	ICMP	108	0xc211 (49681)	64 Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found!)
10	2022-08-01 11:33:23.075781513	192.0.2.100	198.51.100.100	ICMP	102	0xc211 (49681)	64 Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found!)
11	2022-08-01 11:33:24.081839490	192.0.2.100	198.51.100.100	ICMP	108	0xc2e2 (49890)	64 Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found!)
12	2022-08-01 11:33:25.105807895	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100)	64 Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found!)
13	2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294)	64 Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found!)
14	2022-08-01 11:33:27.153830201	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (50454)	64 Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found!)
15	2022-08-01 11:33:28.177847175	192.0.2.100	198.51.100.100	ICMP	102	0xc578 (50552)	64 Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found!)
16	2022-08-01 11:33:29.201804760	192.0.2.100	198.51.100.100	ICMP	108	0xc578 (50552)	64 Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found!)
17	2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (50565)	64 Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found!)
18	2022-08-01 11:33:30.225834765	192.0.2.100	198.51.100.100	ICMP	108	0xc585 (50565)	64 Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found!)
19	2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc618 (50712)	64 Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found!)
20	2022-08-01 11:33:31.249828955	192.0.2.100	198.51.100.100	ICMP	108	0xc618 (50712)	64 Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found!)
21	2022-08-01 11:33:31.249831121	192.0.2.100	198.51.100.100	ICMP	102	0xc64f (50767)	64 Echo (ping) request id=0x0013, seq=14/3584, ttl=64 (no response found!)
22	2022-08-01 11:33:32.273867960	192.0.2.100	198.51.100.100	ICMP	108	0xc64f (50767)	64 Echo (ping) request id=0x0013, seq=14/3584, ttl=64 (no response found!)

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

VN-Tag

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

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102

- 000... = Priority: Best Effort (default) (0)
- ...0 ... = DEI: Ineligible
- ... 0000 0110 0110 = ID: 102
- Type: IPv4 (0x0800)

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

Internet Control Message Protocol

Selecteer het tweede pakket en controleer de belangrijkste punten:

1. Alleen ICMP-echoverdrachtpakketten worden opgenomen. Elk pakket wordt 2 keer opgenomen en getoond.
2. De oorspronkelijke pakketheader is zonder de VLAN-tag.
3. De switch voegt extra poort VLAN-tag 102 in die de toegangsinterface Ethernet1/2 identificeert.

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	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	0x4ff0 (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	0x4ffb (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	0x53a6 (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	0x53a6 (21414)	64	Echo (ping) reply id=0x0013, seq=8/2048, ttl=64
17	2022-08-01 11:33:27.154398212	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 11:33:27.154400198	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 (21740)	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 (21740)	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 11:33:31.250387808	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 11:33:31.250389971	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	0x56e7 (22247)	64	Echo (ping) reply id=0x0013, seq=15/3840, ttl=64

> Frame 2: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0 > Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VMware 9d:e8:be (00:50:56:9d:e8:be)		<pre> 0000 00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00 -PV...X...M...&... 0010 00 0a 81 00 00 66 08 00 45 00 00 54 4f 27 00 00 -.....F...E...TO... 0020 40 01 3e 86 c6 33 64 64 c0 00 02 64 00 00 95 7c -@->...3dd...d... 0030 00 13 00 01 f2 b9 e7 62 c0 00 00 00 cb 7f 06 00 -.....b..... 0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b -..... 0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b -.....l"m \$%&'()*+ 0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 -,-./0123 4567 </pre>
> VN-Tag 0... .. = Direction: To Bridge .0... .. = Pointer: vif_id ..00 0000 0000 0000 .. = Destination: 0 .. = Looped: No ..0... .. = 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 (0x0000)		
> Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100 > Internet Control Message Protocol		

Uitleg

Als de optie **All Packets** in de **Application Capture Direction** is geselecteerd, worden er 2 simultane pakketopnamen geconfigureerd met betrekking tot de geselecteerde toepassingspoort Ethernet1/2: een opname op de voorinterface Ethernet1/2 en een opname op geselecteerde backplane interfaces.

Wanneer een pakketopname op een frontinterface is geconfigureerd, neemt de switch elk pakket tweemaal tegelijk op:

- Na de invoeging van de poort VLAN-tag.
- Na het inbrengen van de VN-tag.

In de volgorde van bewerkingen wordt de VN-tag in een later stadium ingevoegd dan de invoeging van de VLAN-tag in de poort. Maar in het opnamebestand wordt het pakket met de VN-tag eerder weergegeven dan het pakket met de poort VLAN-tag. In dit voorbeeld identificeert de VLAN-tag 102 in ICMP-echoverdrachtpakketten Ethernet1/2 als de toegangsinterface.

Wanneer een pakketopname op een backplane interface is geconfigureerd, neemt de switch elk pakket twee keer op. De interne switch ontvangt pakketten die al zijn getagd door de applicatie op de security module met de port VLAN tag en de VN tag. De port VLAN-tag identificeert de uitgangsinterface die het interne chassis gebruikt om de pakketten door te sturen naar het netwerk. In dit voorbeeld identificeert de VLAN-tag 102 in ICMP-echoantwoordpakketten Ethernet1/2 als de uitgangsinterface.

De switch verwijdert de VN-tag en de interne VLAN-tag voordat de pakketten naar het netwerk worden doorgestuurd.

In deze tabel wordt de taak samengevat:

Taak	Opnamepunt	Interne poort VLAN in opgenomen	Richting	Opgenomen verkeer
------	------------	---------------------------------	----------	-------------------

pakketten

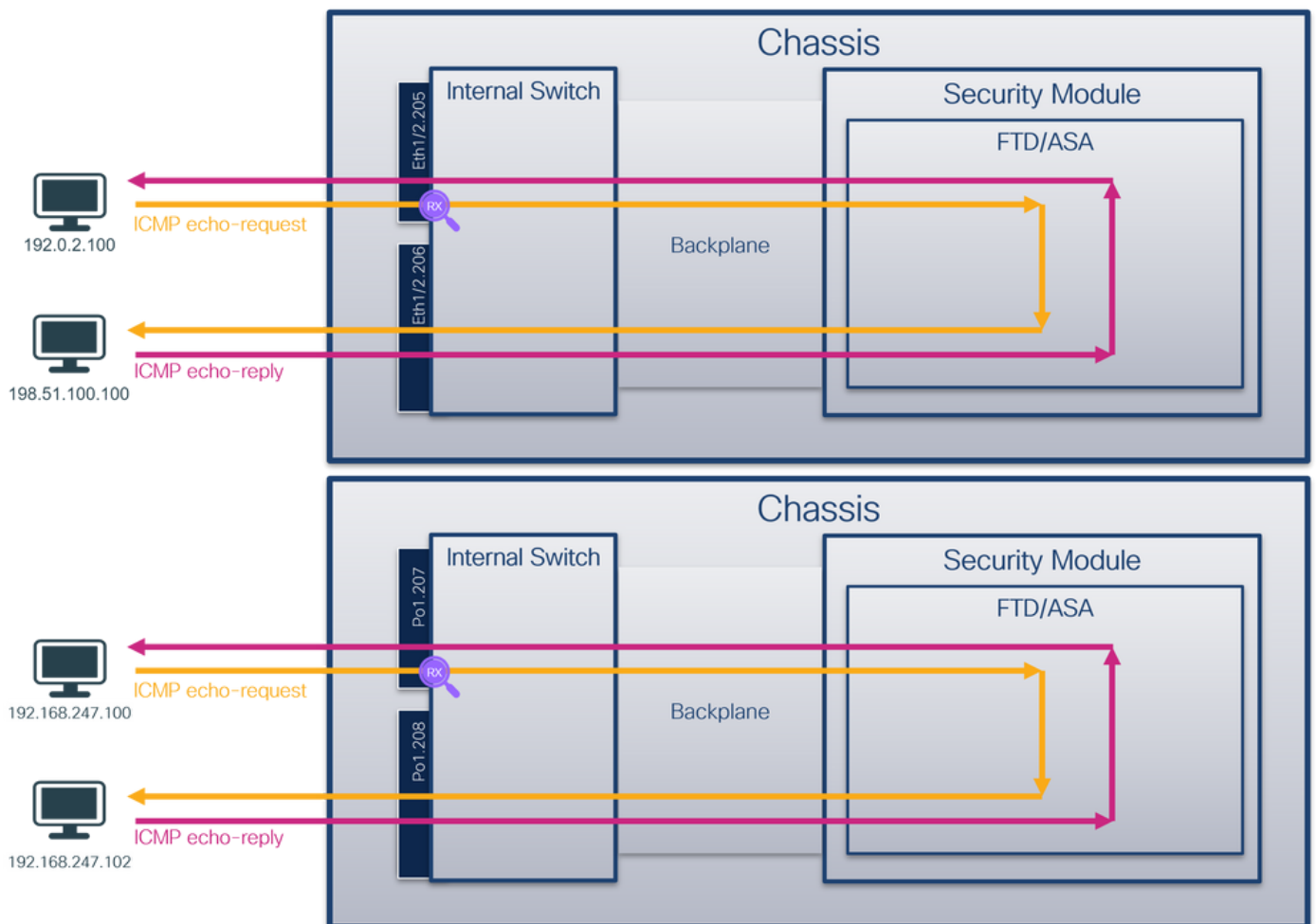
Configureren en verifiëren van opnamen op applicatie- en toepassingspoort Ethernet1/2	Backplane interfaces	102	Alleen inspringe n	Alleen inspringe n
	Interface Ethernet1/2	102	Alleen inspringe n	Alleen inspringe n

Alleen ICMP-echoantwoorden van host 198.51.100.100 op host n 192.0.2.100
Alleen ICMP-echoverzoeken van host 192.0.2.10 naar host n 198.51.100.100

Packet Capture op een subinterface van een fysieke of poortkanaal-interface

Gebruik FCM en CLI om een pakketopname op subinterface Ethernet1/2.205 of poortkanaal-subinterface Portchannel1.207 te configureren en te verifiëren. Subinterfaces en opnamen op subinterfaces worden alleen ondersteund voor de FTD-toepassing in containermodus. In dit geval wordt een pakketopname op Ethernet1/2.205 en Portchannel1.207 geconfigureerd.

Topologie, pakketstroom en de opnamepunten

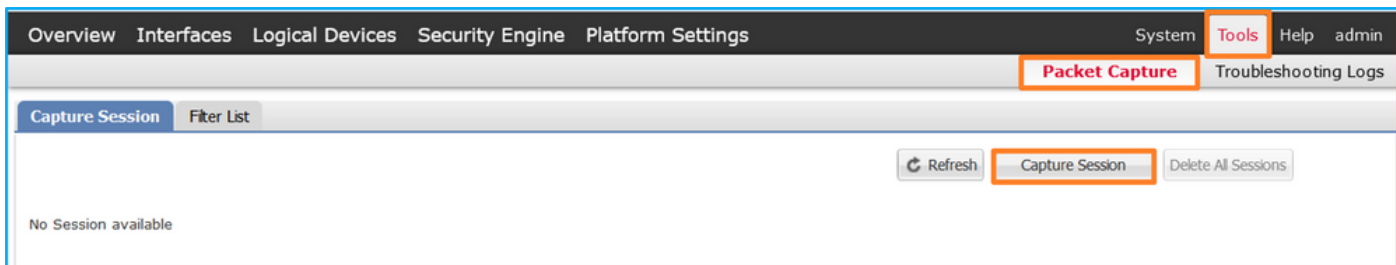


Configuratie

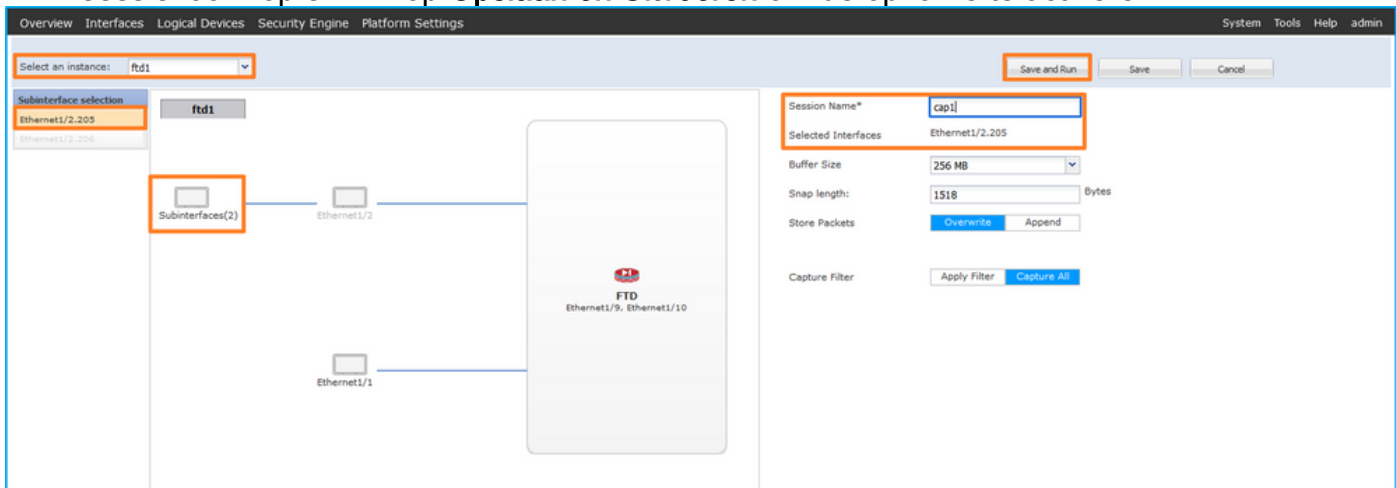
FCM

Volg deze stappen op FCM om een pakketopname te configureren op de FTD-toepassing en de toepassingspoort Ethernet1/2:

1. Gebruik **Gereedschappen > Packet Capture > Capture Session** om een nieuwe opnamesessie te maken:



2. Selecteer de specifieke toepassingsinstantie ftd1, de subinterface Ethernet1/2.205, geef de sessienaam op en klik op **Opslaan en Uitvoeren** om de opname te activeren:



3. In het geval van een poortkanaal-subinterface zijn vanwege de Cisco bug-ID [CSC33119](https://www.cisco.com/cisco/webbugtool/bugdetails.do?bugID=CSC33119) subinterfaces niet zichtbaar in de FCM. Gebruik de FXOS CLI om opnamen te configureren op poortkanaal-subinterfaces.

FXOS CLI

Volg deze stappen op FXOS CLI om een pakketopname te configureren op subinterfaces Ethernet1/2.205 en Portchannel1.207:

1. Identificeer het toepassingstype en de identificatiecode:

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

2. In het geval van een poort-kanaal-interface, identificeer zijn lidinterfaces:

```
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-Channel	Type	Protocol	Member	Ports
1	Po1(SU)	Eth	LACP	Eth1/3(P)	Eth1/3(P)

3. Een opnamesessie maken:

```
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 #
```

Voor poort-kanaal subinterfaces, maak een pakketopname voor elke poort-kanaal lidinterface:

```
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 #
```

Verificatie

FCM

Controleer de **interfacenaam**, zorg ervoor dat de **operationele status** omhoog is en dat de **bestandsgrootte (in bytes)** toeneemt:

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/2.205	None	233992	cap1-ethernet-1-2-0.pcap	fd1

Poortkanaal subinterface-opnamen die op FXOS CLI zijn geconfigureerd, zijn ook zichtbaar op FCM; ze kunnen echter niet worden bewerkt:

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

FXOS CLI

Controleer de opnamedetails in scope-pakketopname:

```
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
```

Poortkanaal 1 met lidinterfaces Ethernet1/3 en Ethernet1/4:

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

Traffic Monitoring Session:

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

Physical ports involved in Packet Capture:

```
Slot Id: 1
```


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

Opnamebestanden verzamelen

Volg de stappen in het gedeelte Verzamel Firepower 4100/9300 Internal Switch Capture Files.

Capture file analyse

Gebruik een applicatie voor pakketvastlegging om het opnamebestand te openen. Selecteer het eerste pakket en controleer de belangrijkste punten:

1. Alleen ICMP-echoverdrachtpakketten worden opgenomen. Elk pakket wordt 2 keer opgenomen en getoond.
2. De oorspronkelijke pakketheader heeft de VLAN-tag 2005.
3. De switch voegt extra poort VLAN-tag 102 in die de toegangsinterface Ethernet1/2 identificeert.
4. Op de switch staat een extra VN-tag.

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


```

> Frame 1: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface capture_u0.1, id 0
> Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: a2:76:f2:00:00:1b (a2:76:f2:00:00:1b)
  VN-Tag
  1... .. = Direction: From Bridge
  .0... .. = Pointer: vif_id
  ..00 0000 0101 0100 ... = Destination: 84
  ... .. = Looped: No
  ... .. = Reserved: 0
  ... .. = Version: 0
  ... .. = Source: 0
  Type: 802.1Q Virtual LAN (0x8100)
  802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
  000... .. = Priority: Best Effort (default) (0)
  ...0 ... .. = DEI: Ineligible
  ... 0000 0110 0110 = ID: 102
  Type: 802.1Q Virtual LAN (0x8100)
  802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 205
  000... .. = Priority: Best Effort (default) (0)
  ...0 ... .. = DEI: Ineligible
  ... 0000 1100 1101 = ID: 205
  Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
  Internet Control Message Protocol
  
```

Selecteer het tweede pakket en controleer de belangrijkste punten:

Selecteer het tweede pakket en controleer de belangrijkste punten:

1. Alleen ICMP-echoverdrachtpakketten worden opgenomen. Elk pakket wordt 2 keer opgenomen en getoond.
2. De oorspronkelijke pakketheader heeft de VLAN-tag 207.

The screenshot shows a list of 27 ICMP Echo (ping) requests. Packet 2 is selected. The details pane for packet 2 shows the following structure:

- Frame 2: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface capture_u0_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: 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

Uitleg

Wanneer een pakketopname op een frontinterface is geconfigureerd, neemt de switch elk pakket tweemaal tegelijk op:

- Na de invoeging van de poort VLAN-tag.
- Na het inbrengen van de VN-tag.

In de volgorde van bewerkingen wordt de VN-tag in een later stadium ingevoegd dan de invoeging van de VLAN-tag in de poort. Maar in het opnamebestand wordt het pakket met de VN-tag eerder weergegeven dan het pakket met de poort VLAN-tag. Bovendien, in het geval van subinterfaces, in de opnamebestanden, bevat elk tweede pakket niet de poort VLAN-tag.

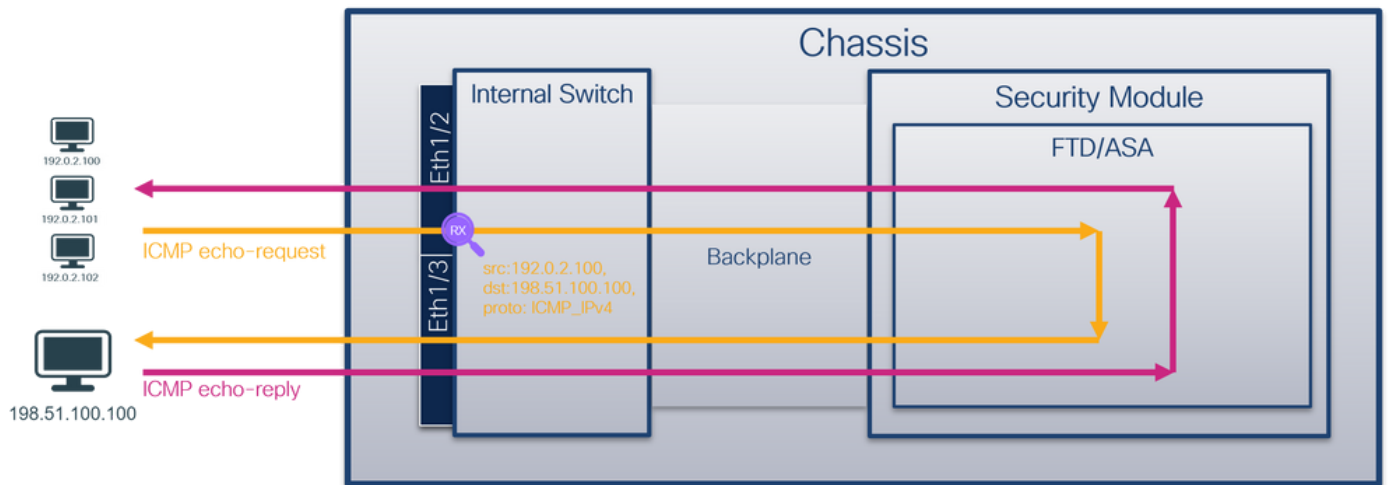
In deze tabel wordt de taak samengevat:

Taak	Opnamepunt	Interne poort opgenomen pakketten	Richting	Opgenomen verkeer
Configureer en controleer een pakketopname op subinterface Ethernet1/2.205	Ethernet1/2.205	102	Alleen inspringen	ICMP-echoverzoeken van host 192.0.2.10 naar host 198.51.100
Configureer en controleer een pakketopname op Portchannel1 subinterface met lidinterfaces Ethernet1/3 en Ethernet1/4	Ethernet1/3G Ethernet1/4	1001	Alleen inspringen	ICMP-echoverzoeken van 192.168.207.100 voor host 192.168.207.102

PacketCapture filters

Gebruik FCM en CLI om een pakketopname op interface Ethernet1/2 met een filter te configureren en te verifiëren.

Topologie, pakketstroom en de opnamepunten

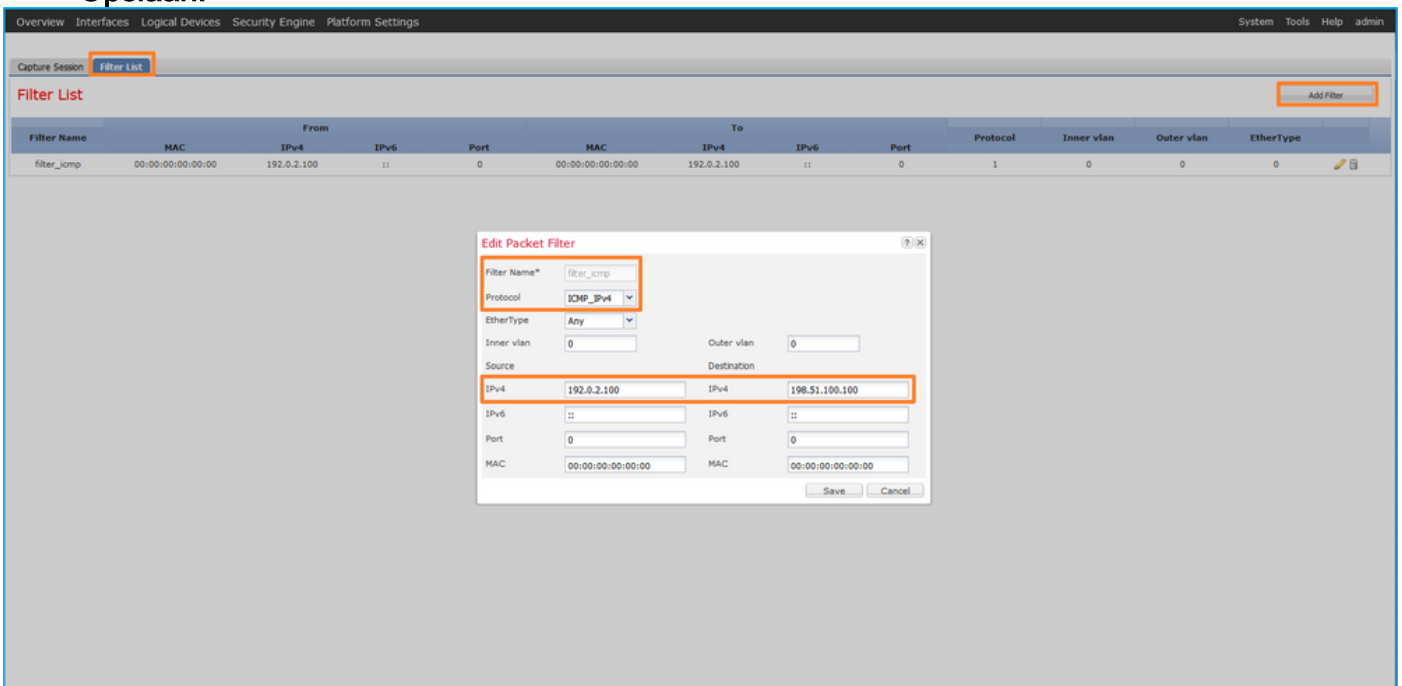


Configuratie

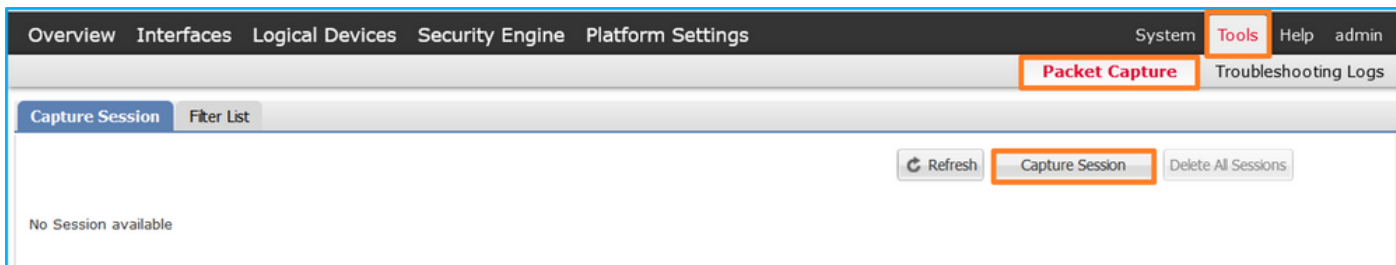
FCM

Volg deze stappen op FCM om een opnamefilter te configureren voor ICMP-echoverdrachtpakketten van host 192.0.2.100 naar host 198.51.100.100 en pas deze toe op pakketopname op interface Ethernet1/2:

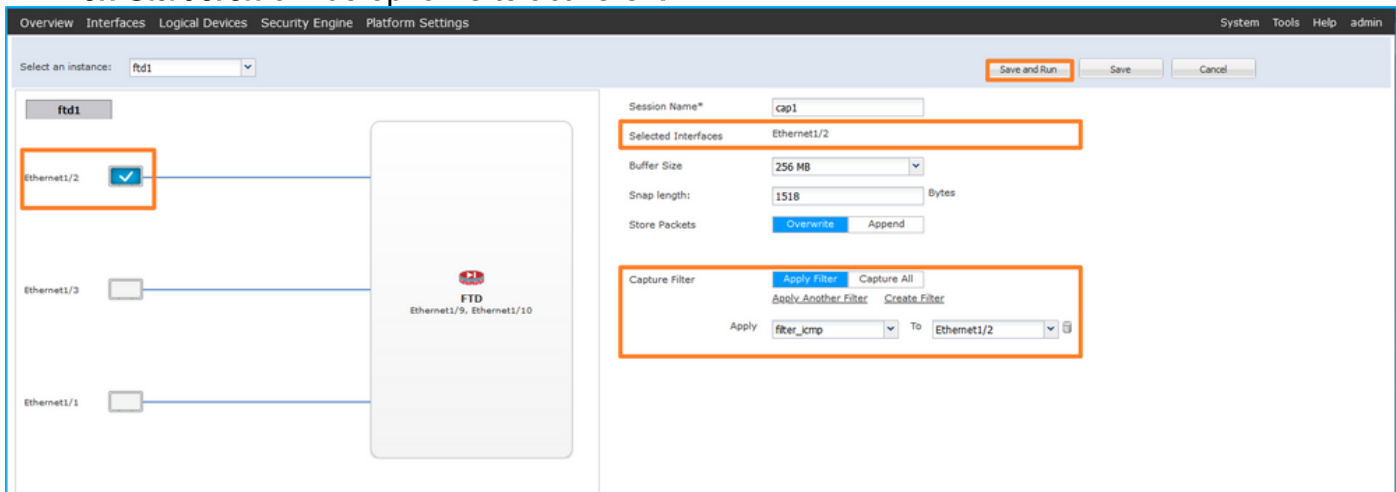
1. Gebruik **Gereedschappen > Packet Capture > Filterlijst > Filter toevoegen** om een opnamefilter te maken.
2. Specificeer de **filternaam**, het **protocol**, de **bron van IPv4**, de **bestemming van IPv4** en klik op **Opslaan**:



3. Gebruik **Gereedschappen > Packet Capture > Capture Session** om een nieuwe opnamesessie te maken:



4. Selecteer Ethernet1/2, geef de sessienaam op, pas het opnamefilter toe en klik op Opslaan en Uitvoeren om de opname te activeren:



FXOS CLI

Volg deze stappen op FXOS CLI om pakketopnamen op backplane interfaces te configureren:

1. Identificeer het toepassingstype en de identificatiecode:

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

2. Identificeer het IP-protocolnummer in <https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>. In dit geval is het ICMP-protocolnummer 1.

3. Een opnamesessie maken:

2.

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

```

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

```

Verificatie

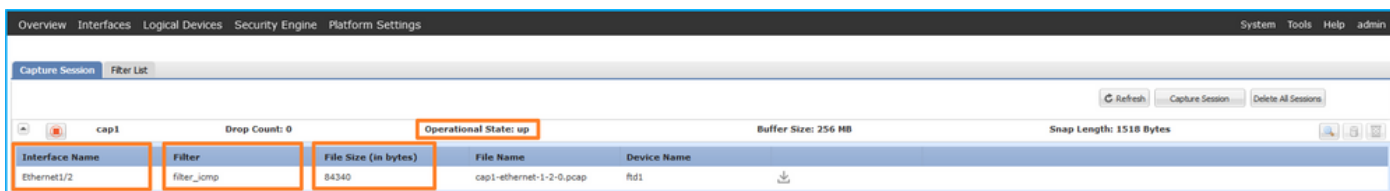
FCM

Controleer de **interfacenaam**, zorg ervoor dat de **operationele status** omhoog is en dat de **bestandsgrootte (in bytes)** toeneemt:



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

Controleer de interfacenaam, het **filter**, controleer of de **operationele status** is ingesteld en of de **bestandsgrootte (in bytes)** toeneemt in **Gereedschappen > Packet Capture > Capture Session**:



Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/2	filter_icmp	84340	cap1-ethernet-1-2-0.pcap	fd1

FXOS CLI

Controleer de opnamedetails in **scope-pakketopname**:

```

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

Opnamebestanden verzamelen

Volg de stappen in het gedeelte Verzamel Firepower 4100/9300 Internal Switch Capture Files.

Capture file analyse

Gebruik een applicatie voor pakketvastlegging om het opnamebestand te openen. Selecteer het eerste pakket en controleer de belangrijkste punten

1. Alleen ICMP-echoverdrachtpakketten worden opgenomen. Elk pakket wordt 2 keer opgenomen en getoond.
2. De oorspronkelijke pakketheader is zonder de VLAN-tag.
3. De switch voegt extra poort VLAN-tag 102 in die de toegangsinterface Ethernet1/2 identificeert.
4. Op de switch staat een extra VN-tag.

The screenshot shows a packet capture in Wireshark. The top pane displays a list of 20 ICMP Echo (ping) request packets. The first packet is highlighted with a red box and a '1' next to it. The second pane shows the details of the selected packet, with several fields highlighted by red boxes and numbered 2, 3, and 4:

- 2: Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
- 3: 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
- 4: VN-Tag

The bottom pane shows the raw packet bytes in hexadecimal and ASCII.

Selecteer het tweede pakket en controleer de belangrijkste punten:

1. Alleen ICMP-echoverdrachtpakketten worden opgenomen. Elk pakket wordt 2 keer

opgenomen en getoond.

2. De oorspronkelijke pakketheader is zonder de VLAN-tag.
3. De switch voegt extra poort VLAN-tag 102 in die de toegangsinterface Ethernet1/2 identificeert.

The image shows a Wireshark capture of ICMP Echo (ping) requests. The packet list pane shows 20 packets, with the first two highlighted in blue. The packet details pane for the selected packet shows the following structure:

- Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture_u0_1, in Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)
- 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
 - 000. = Priority: Best Effort (default) (0)
 - ...0 = DEI: Ineligible
 - ...0000 0110 0110 = ID: 102
 - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
- Internet Control Message Protocol

Uitleg

Wanneer een pakketopname op een frontinterface is geconfigureerd, neemt de switch elk pakket tweemaal tegelijk op:

- Na de invoering van de poort VLAN-tag.
- Na het inbrengen van de VN-tag.

In de volgorde van bewerkingen wordt de VN-tag in een later stadium ingevoegd dan de invoering van de VLAN-tag in de poort. Maar in het opnamebestand wordt het pakket met de VN-tag eerder weergegeven dan het pakket met de poort VLAN-tag.

Wanneer een opnamefilter wordt toegepast, worden alleen de pakketten opgenomen die overeenkomen met het filter in de invoerrichting.

In deze tabel wordt de taak samengevat:

Taak	Opnamepunt	Interne poort VLAN in opgenomen pakketten	Richting	Eigen filter	Opgenomen verkeer
Configureer en controleer een pakketopname met een filter op de voorinterface Ethernet1/2	Ethernet1/2	102	Alleen inspringen	Protocol: ICMP Bron: 192.0.2.1 Bestemming: 198.51.100.100	ICMP-echoverzoeken van 192.0.2.10 naar host 198.51.100.100

Opnamebestanden van FirePOWER 4100/9300 interne Switch verzamelen

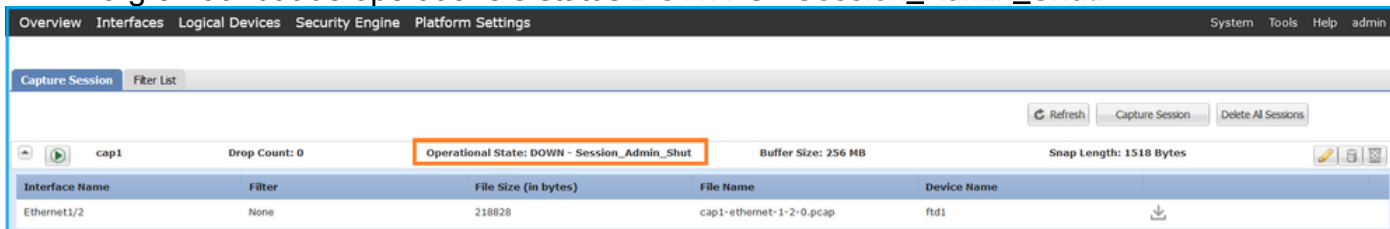
FCM

Volg deze stappen op FCM om interne switch-opnamebestanden te verzamelen:

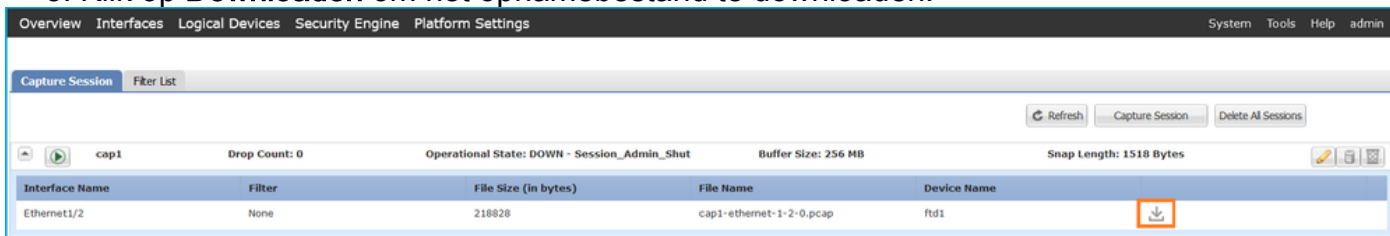
1. Klik op de knop **Sessie uitschakelen** om de actieve opname te stoppen:



2. Zorg ervoor dat de operationele status **DOWN** is - **Session_Admin_Shut**:



3. Klik op **Downloaden** om het opnamebestand te downloaden:



In het geval van poort-kanaal interfaces, herhaal deze stap voor elke lidinterface.

FXOS CLI

Volg deze stappen op de FXOS CLI om opnamebestanden te verzamelen:

1. Stop de actieve opname:

```
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. Upload het opnamebestand vanuit het bereik van de opdracht local-mgmt:

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

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

In het geval van poort-kanaal interfaces, kopieer het opnamebestand voor elke lidinterface.

Richtlijnen, beperkingen en beste praktijken voor Interne Switch PacketCapture

Raadpleeg voor de richtlijnen en beperkingen met betrekking tot Firepower 4100/9300 interne switch-opname de *configuratiehandleiding voor Cisco Firepower 4100/9300 FXOS Chassis Manager* of de *configuratiehandleiding voor Cisco Firepower 4100/9300 FXOS CLI*, hoofdstuk **Problemen oplossen**, paragraaf **Packet Capture**.

Dit is de lijst met best practices op basis van het gebruik van pakketvastlegging in TAC-gevallen:

- Let op richtlijnen en beperkingen.
- Leg pakketten vast op alle poortkanaallidinterfaces en analyseer alle opnamebestanden.
- Gebruik opnamefilters.
- Overweeg de impact van NAT op IP-adressen van pakketten wanneer een opnamefilter is geconfigureerd.
- Vergroot of verlaag de **Magnetische Lens** die de framegrootte aangeeft voor het geval dat deze verschilt van de standaardwaarde van 1518 bytes. Een kortere grootte resulteert in een hoger aantal opgenomen pakketten en vice versa.
- Pas de **buffergrootte** naar wens aan.
- Let op de **Drop Count** op FCM of FXOS CLI. Zodra de grens van de buffergrootte wordt bereikt, stijgt de teller van de dalingstelling.
- Gebruik het filter **!vntag** op Wireshark om alleen pakketten weer te geven zonder de VN-tag. Dit is handig om VN-getagde pakketten te verbergen in de voorste pakketopnamebestanden.
- Gebruik het filter **frame.number&1** op Wireshark om alleen oneven frames weer te geven. Dit is handig om dubbele pakketten te verbergen in de pakketopnamebestanden van de backplane interface.
- In het geval van protocollen zoals TCP, past Wireshark door gebrek kleuringsregels toe die pakketten met specifieke voorwaarden in verschillende kleuren tonen. In het geval van een interne switch wordt het pakket op basis van dubbele pakketten in opnamebestanden

opgenomen, zodat het pakket op een fout-positieve manier kan worden gekleurd en gemarkeerd. Als u pakketopnamebestanden analyseert en een filter toepast, exporteert u de weergegeven pakketten naar een nieuw bestand en opent u het nieuwe bestand.

Configuratie en verificatie op Secure-firewall 3100

In tegenstelling tot Firepower 4100/9300, legt de switch in de Secure Firewall 3100 vast op de opdrachtregelinterface van de toepassing via de opdracht **Capture <name> switch**, waarin de **switch** Option aangeeft dat de opnamen op de switch zijn geconfigureerd.

Dit is de opnameopdracht met de **switch** optie:

```
> capture cap_sw switch ?
buffer          Configure size of capture buffer, default is 256MB
ethernet-type  Capture Ethernet packets of a particular type, default is IP
interface       Capture packets on a specific interface
ivlan          Inner Vlan
match          Capture packets based on match criteria
ovlan          Outer Vlan
packet-length  Configure maximum length to save from each packet, default is
               64 bytes
real-time      Display captured packets in real-time. Warning: using this
               option with a slow console connection may result in an
               excessive amount of non-displayed packets due to performance
               limitations.
stop           Stop packet capture
trace          Trace the captured packets
type           Capture packets based on a particular type
<cr>
```

De algemene stappen voor de configuratie van de pakketopname zijn als volgt:

1. Specificeer een toegangsinterface:

Switch Capture Configuration accepteert de **ingangsisinterface nameif**. De gebruiker kan namen van gegevensinterfaces, interne uplink, of de beheersinterfaces specificeren:

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

management      Name of interface Management1/1
```

2. Specificeer het Ethernet kader EtherType. Het standaard EtherType is IP. De optiewaarden van het **Ethernet-type** specificeren EtherType:

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

```
sgt
vlan
```

3. Specificeer de overeenkomende voorwaarden. De optie **Capture match** specificeert de matchcriteria:

```
> 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
pftp
sctp
snp
spi      SPI value
tcp
udp
<cr>
```

4. Specificeer andere optionele parameters zoals de buffergrootte, de pakketlengte, enzovoort.
5. Schakel de opname in. Het commando **no Capture <name> switch stop** activeert de opname:

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

6. Controleer de opnamegegevens:

- De beheerstatus is **ingeschakeld**, en de operationele status is **ingesteld** en actief.
- De grootte van het pakketopnamebestand wordt **verhoogd**.
- Het aantal opgenomen pakketten in de uitvoer van de **show Capture <cap_name>** is niet nul.
- Opname pad **pcapfile**. De opgenomen pakketten worden automatisch opgeslagen in de map **/mnt/disk0/packet-capture/**.
- Opnameomstandigheden. De software maakt automatisch opnamefilters op basis van de opnameomstandigheden.

```
> show capture capsw
27 packet captured on disk using switch capture
Reading of capture file from disk is not supported
```

```
>show capture capsw detail
Packet Capture info
  Name:          capsw
  Session:      1
  Admin State:  enabled
  Oper State:   up
```

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

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1
Port Id: 1
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize: 18838
Filter: capsw-1-1

Packet Capture Filter Info

Name: capsw-1-1
Protocol: 0
Ivlan: 0
Ovlan: 205
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

0 packet captured on disk using switch capture

Reading of capture file from disk is not supported

7. Stop de opnamen indien nodig:

```
> capture capsw switch stop
```

```
>show capture capsw detail
```

Packet Capture info

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

Total Physical ports involved in Packet Capture: 1

Physical port:

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

Packet Capture Filter Info

```
Name:                capsw-1-1
Protocol:            0
Ivlan:              0
Ovlan:              205
Src Ip:              0.0.0.0
Dest Ip:             0.0.0.0
Src Ipv6:            ::
Dest Ipv6:           ::
Src MAC:             00:00:00:00:00:00
Dest MAC:            00:00:00:00:00:00
Src Port:            0
Dest Port:           0
Ethertype:          0
```

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

8. Verzamel de opnamebestanden. Volg de stappen in het gedeelte **Verzamel Secure Firewall 3100 Internal Switch Capture Files**.

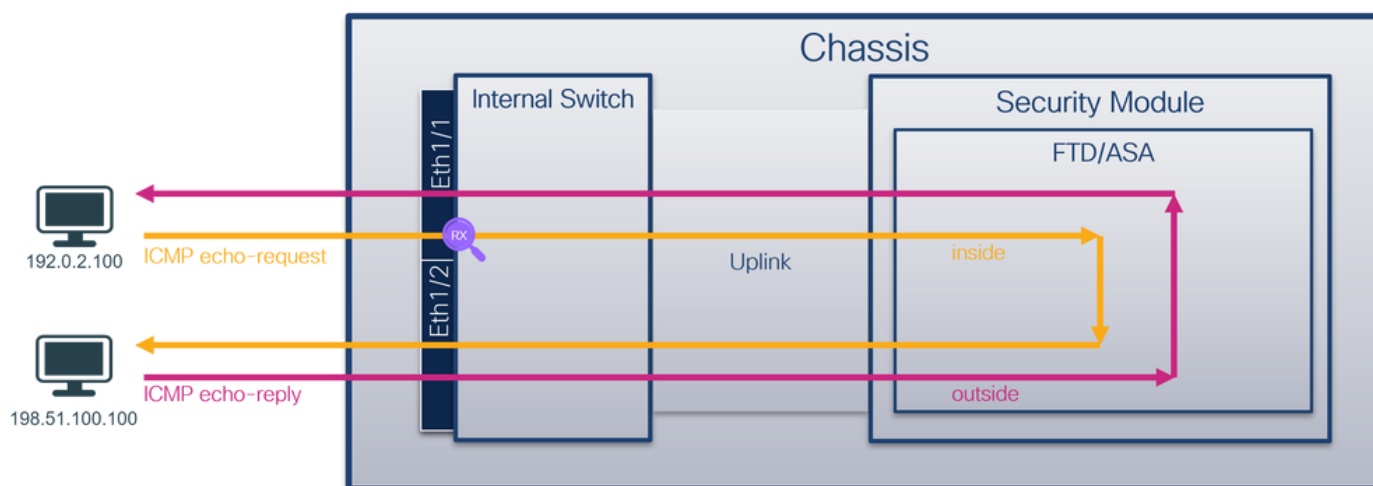
In versie 7.2 wordt de switch-opnameconfiguratie niet ondersteund door het VCC of de FDM. Switch In het geval van ASA-softwareversie 9.18(1) en hoger kunnen internethetefoonopnamen worden geconfigureerd in ASDM-versies 7.18.1.x en hoger.

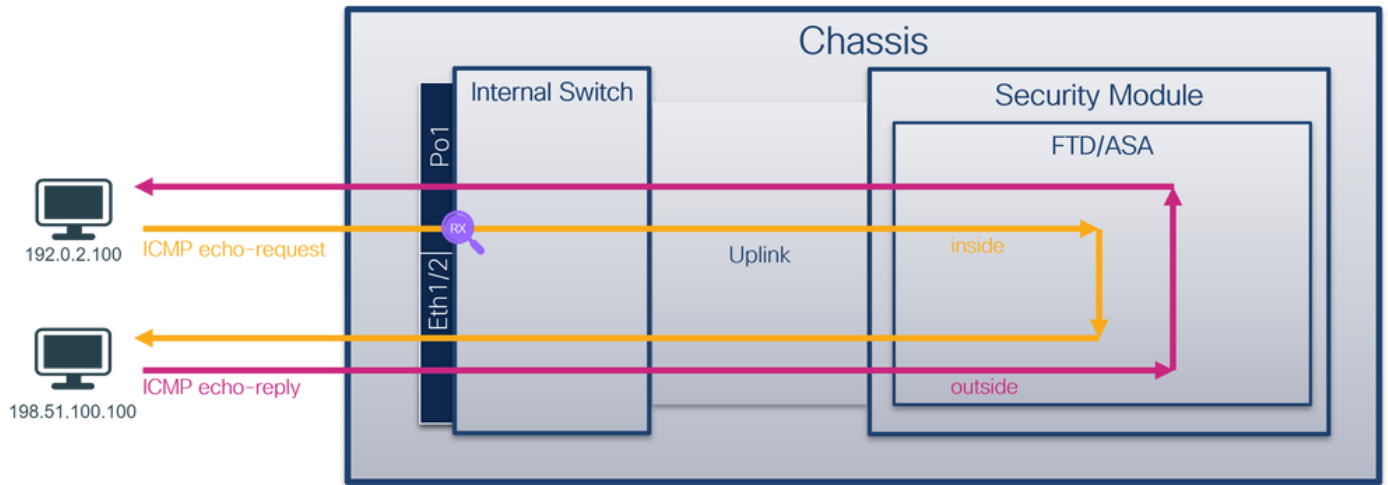
Deze scenario's zijn gebaseerd op veelgebruikte cases van Secure Firewall 3100 interne switch.

PacketCapture op een fysieke of poortkanaal-interface

Gebruik de FTD of ASA CLI om een pakketopname op interface Ethernet1/1 of Portchannel1 interface te configureren en te verifiëren. Beide interfaces hebben de naam **vanbinnen**.

Topologie, pakketstroom en de opnamepunten





Configuratie

Volg deze stappen op ASA of FTD CLI om een pakketopname te configureren op interface Ethernet1/1 of poortkanaal1:

1. Controleer de naam:

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

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

2. Een opnamesessie maken:

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

3. De opnamesessie inschakelen:

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

Verificatie

Controleer de naam van de opnamesessie, de administratieve en operationele status, de interfacekaart en de identificatie. Zorg ervoor dat de waarde **Capsize** in bytes toeneemt en dat het aantal opgenomen pakketten niet-nul is:

```
> 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

In het geval van Port-channel1 wordt de opname op alle lidinterfaces geconfigureerd:

> **show capture capsw detail**

Packet Capture info

Name: capsw
Session: 1
Admin State: enabled
Oper State: up
Oper State Reason: Active
Config Success: yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0

Total Physical ports involved in Packet Capture: 2

Physical port:

Slot Id: 1
Port Id: 4
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-4-0.pcap
Pcapsize: 28824
Filter: capsw-1-4

Packet Capture Filter Info

Name: caps-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-caps-ethernet-1-3-0.pcap
Pcapsize: 18399
Filter: caps-1-3

Packet Capture Filter Info

Name: caps-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

De poortkanaals lidinterfaces kunnen in de FXOS **local-mgmt** commando shell worden geverifieerd via de **show portchannel** summiere opdracht:

> **connect fxos**

...

KSEC-FPR3100-1 **connect local-mgmt**

KSEC-FPR3100-1(local-mgmt) **show portchannel summary**

Flags: D - Down P - Up in port-channel (members)

I - Individual H - Hot-standby (LACP only)

s - Suspended r - Module-removed

S - Switched R - Routed

U - Up (port-channel)

M - Not in use. Min-links not met

```
-----  
Group Port-      Type      Protocol  Member Ports  
Channel  
-----  
1      Po1(U)      Eth      LACP      Eth1/3(P)  Eth1/4(P)
```

LACP KeepAlive Timer:

Channel PeerKeepAliveTimerFast

1 Po1(U) False

Cluster LACP Status:

Channel ClusterSpanned ClusterDetach ClusterUnitID ClusterSysID

1 Po1(U) False False 0 clust

Om toegang te krijgen tot de FXOS op ASA, voert u de opdracht **connect fxos admin uit**. In het geval van multi-context, stel het bevel in de admincontext in werking.

Opnamebestanden verzamelen

Volg de stappen in het gedeelte **Verzamel Secure Firewall 3100 Internal Switch Capture Files**.

Capture file analyse

Gebruik een applicatie voor pakketopname om de opnamebestanden voor Ethernet1/1 te openen. Selecteer het eerste pakket en controleer de belangrijkste punten:

1. Alleen ICMP-echoverdrachtpakketten worden opgenomen.
2. De oorspronkelijke pakketheader is zonder de VLAN-tag.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-07 19:50:06.925768	192.0.2.100	198.51.100.100	ICMP	102	0x9a10 (39440)	64	Echo (ping) request id=0x0034, seq=1/256, ttl=64 (no res
2	2022-08-07 19:50:07.921684	192.0.2.100	198.51.100.100	ICMP	102	0x9a3a (39482)	64	Echo (ping) request id=0x0034, seq=2/512, ttl=64 (no res
3	2022-08-07 19:50:08.924468	192.0.2.100	198.51.100.100	ICMP	102	0x9aa6 (39590)	64	Echo (ping) request id=0x0034, seq=3/768, ttl=64 (no res
4	2022-08-07 19:50:09.928484	192.0.2.100	198.51.100.100	ICMP	102	0x9afe (39678)	64	Echo (ping) request id=0x0034, seq=4/1024, ttl=64 (no re
5	2022-08-07 19:50:10.928245	192.0.2.100	198.51.100.100	ICMP	102	0x9b10 (39696)	64	Echo (ping) request id=0x0034, seq=5/1280, ttl=64 (no re
6	2022-08-07 19:50:11.929144	192.0.2.100	198.51.100.100	ICMP	102	0x9b34 (39732)	64	Echo (ping) request id=0x0034, seq=6/1536, ttl=64 (no re
7	2022-08-07 19:50:12.932943	192.0.2.100	198.51.100.100	ICMP	102	0x9b83 (39811)	64	Echo (ping) request id=0x0034, seq=7/1792, ttl=64 (no re
8	2022-08-07 19:50:13.934155	192.0.2.100	198.51.100.100	ICMP	102	0x9b8b (39819)	64	Echo (ping) request id=0x0034, seq=8/2048, ttl=64 (no re
9	2022-08-07 19:50:14.932804	192.0.2.100	198.51.100.100	ICMP	102	0x9c07 (39943)	64	Echo (ping) request id=0x0034, seq=9/2304, ttl=64 (no re
10	2022-08-07 19:50:15.937143	192.0.2.100	198.51.100.100	ICMP	102	0x9cc6 (40134)	64	Echo (ping) request id=0x0034, seq=10/2560, ttl=64 (no r
11	2022-08-07 19:50:16.934848	192.0.2.100	198.51.100.100	ICMP	102	0x9d68 (40296)	64	Echo (ping) request id=0x0034, seq=11/2816, ttl=64 (no r
12	2022-08-07 19:50:17.936908	192.0.2.100	198.51.100.100	ICMP	102	0x9ded (40429)	64	Echo (ping) request id=0x0034, seq=12/3072, ttl=64 (no r
13	2022-08-07 19:50:18.939584	192.0.2.100	198.51.100.100	ICMP	102	0x9e5a (40538)	64	Echo (ping) request id=0x0034, seq=13/3328, ttl=64 (no r
14	2022-08-07 19:50:19.941262	192.0.2.100	198.51.100.100	ICMP	102	0x9efb (40699)	64	Echo (ping) request id=0x0034, seq=14/3584, ttl=64 (no r
15	2022-08-07 19:50:20.940716	192.0.2.100	198.51.100.100	ICMP	102	0x9f50 (40784)	64	Echo (ping) request id=0x0034, seq=15/3840, ttl=64 (no r
16	2022-08-07 19:50:21.940288	192.0.2.100	198.51.100.100	ICMP	102	0x9fe4 (40932)	64	Echo (ping) request id=0x0034, seq=16/4096, ttl=64 (no r
17	2022-08-07 19:50:22.943302	192.0.2.100	198.51.100.100	ICMP	102	0xa031 (41009)	64	Echo (ping) request id=0x0034, seq=17/4352, ttl=64 (no r
18	2022-08-07 19:50:23.944679	192.0.2.100	198.51.100.100	ICMP	102	0xa067 (41063)	64	Echo (ping) request id=0x0034, seq=18/4608, ttl=64 (no r

> Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)	0000 bc e7 12 34 9a 14 00 50 56 9d e8 be 08 00 45 00 ...4...P V....E-
> Ethernet II, Src: VMware_9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco_34:9a:14 (bc:e7:12:34:9a:14)	0010 00 54 9a 10 40 00 40 01 b3 9c c0 00 02 64 c6 33 ..T.@:.....d:3
> Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100	0020 64 64 08 00 c6 91 00 34 00 01 61 17 f0 62 00 00 dd....4..a..b..
> Internet Control Message Protocol	0030 00 00 18 ec 08 00 00 00 00 00 10 11 12 13 14 15!#\$%&'()*+,-./0123456789:;<=>?@A
	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
	0060 36 37 55 55 55 55

Open de opnamebestanden voor Portchannel1-lidinterfaces. Selecteer het eerste pakket en controleer de belangrijkste punten:

1. Alleen ICMP-echoverdrachtpakketten worden opgenomen.
2. De oorspronkelijke pakketheader is zonder de VLAN-tag.

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

Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface Ethernet1/1, Src: VMware_9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco_34:9a:2c (bc:e7:12:34:9a:2c)		0000 bc e7 12 34 9a 2c 00 50 56 9d e8 be 08 00 45 00P V.....E 0010 00 54 92 96 40 00 40 01 bb 16 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..MM.b.. 0030 00 00 0e c8 04 00 00 00 00 00 10 11 12 13 14 15 0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 !"#%& 0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,-./012345 0060 36 37 55 55 55 55 67UUUU
--	--	---

Uitleg

De switch Captures worden geconfigureerd op interfaces Ethernet1/1 of Portchannel1.

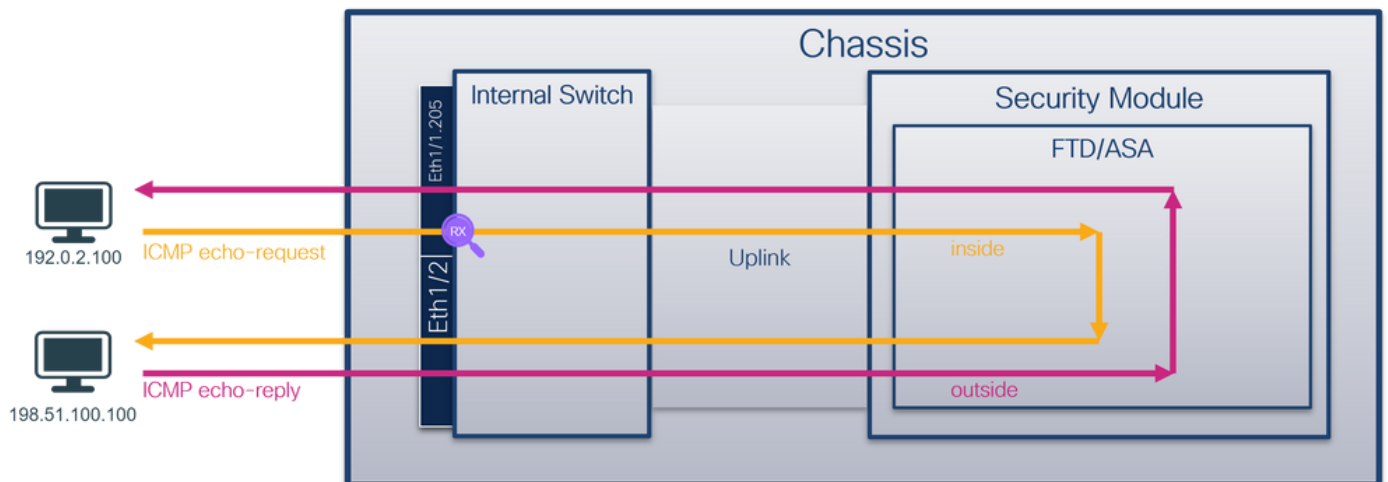
In deze tabel wordt de taak samengevat:

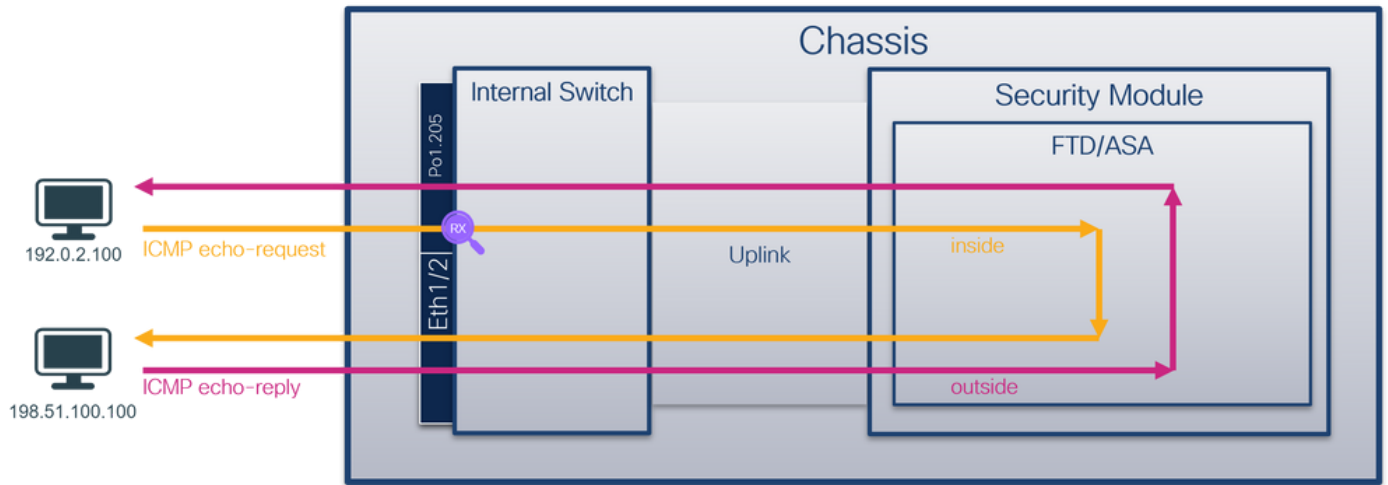
Taak	Opnamepunt	Intern filter	Richting	Opgenomen verkeer
Configureer en controleer een pakketopname op interface Ethernet1/1	Ethernet1/1	None	Alleen inspringen	ICMP-echoverzoeken van host 192.0.2.10 naar host 198.51.100.100
Configureer en controleer een pakketopname op interface Portchannel1 met lidinterfaces Ethernet1/3 en Ethernet1/4	Ethernet1/3 Ethernet1/4	None	Alleen inspringen	ICMP-echoverzoeken van host 192.0.2.10 naar host 198.51.100.100

Packet Capture op een subinterface van een fysieke of poortkanaal-interface

Gebruik de FTD of ASA CLI om een pakketopname op subinterfaces Ethernet1/1.205 of Portchannel1.205 te configureren en te verifiëren. Beide subinterfaces hebben de naam **erin**.

Topologie, pakketstroom en de opnamepunten





Configuratie

Volg deze stappen op ASA of FTD CLI om een pakketopname te configureren op interface Ethernet1/1 of poortkanaal1:

1. Controleer de naam:

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

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

2. Een opnamesessie maken:

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

3. De opnamesessie inschakelen:

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

Verificatie

Controleer de naam van de opnamesessie, de administratieve en operationele status, de interfacekaart en de identificatie. Zorg ervoor dat de waarde **Pcapsize** in bytes toeneemt en dat het aantal opgenomen pakketten niet-nul is:

```
> 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

In dit geval wordt een filter met router VLAN **Ovlan=205** gemaakt en op de interface toegepast.

In het geval van Port-channel1 wordt de opname met een filter **Ovlan=205** geconfigureerd op alle lidinterfaces:

> **show capture capsw detail**

Packet Capture info

Name: capsw
Session: 1
Admin State: enabled
Oper State: up
Oper State Reason: Active
Config Success: yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0

Total Physical ports involved in Packet Capture: 2

Physical port:

Slot Id: 1
Port Id: 4
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-4-0.pcap

Pcapsize: 23442
Filter: capsw-1-4

Packet Capture Filter Info

Name: capsw-1-4
Protocol: 0
Ivlan: 0
Ovlan: 205
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Physical port:

Slot Id: 1
Port Id: 3
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-3-0.pcap
Pcapsize: 5600
Filter: capsw-1-3

Packet Capture Filter Info

Name: capsw-1-3
Protocol: 0
Ivlan: 0
Ovlan: 205
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

49 packet captured on disk using switch capture

Reading of capture file from disk is not supported

De poortkanaals lidinterfaces kunnen in de FXOS **local-mgmt** commando shell worden geverifieerd via de **show portchannel** summiere opdracht:

> **connect fxos**

...

KSEC-FPR3100-1 **connect local-mgmt**
KSEC-FPR3100-1(local-mgmt) **show portchannel summary**
Flags: D - Down P - Up in port-channel (members)
I - Individual H - Hot-standby (LACP only)
s - Suspended r - Module-removed
S - Switched R - Routed
U - Up (port-channel)
M - Not in use. Min-links not met

Group Port- Type Protocol Member Ports
Channel

1 Po1(U) Eth LACP Eth1/3(P) Eth1/4(P)

LACP KeepAlive Timer:

Channel PeerKeepAliveTimerFast

1 Po1(U) False

Cluster LACP Status:

Channel ClusterSpanned ClusterDetach ClusterUnitID ClusterSysID

1 Po1(U) False False 0 clust

Om toegang te krijgen tot de FXOS op ASA, voert u de opdracht **connect fxos admin uit**. In het geval van multi-context, stel dit bevel in de admincontext in werking.

Opnamebestanden verzamelen

Volg de stappen in het gedeelte **Verzamel Secure Firewall 3100 Internal Switch Capture Files**.

Capture file analyse

Gebruik een applicatie voor pakketopname om de opnamebestanden voor Ethernet1/1.205 te openen. Selecteer het eerste pakket en controleer de belangrijkste punten:

1. Alleen ICMP-echoverdrachtpakketten worden opgenomen.
2. De oorspronkelijke pakketheader heeft VLAN-tag 205.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-07 21:21:01.607187	192.0.2.100	198.51.100.100	ICMP	106	0x411f (16671)	64	Echo (ping) request id=0x0037, seq=1/256, ttl=64 (no res
2	2022-08-07 21:21:02.609418	192.0.2.100	198.51.100.100	ICMP	106	0x413a (16698)	64	Echo (ping) request id=0x0037, seq=2/512, ttl=64 (no res
3	2022-08-07 21:21:03.610671	192.0.2.100	198.51.100.100	ICMP	106	0x421a (16922)	64	Echo (ping) request id=0x0037, seq=3/768, ttl=64 (no res
4	2022-08-07 21:21:04.609160	192.0.2.100	198.51.100.100	ICMP	106	0x426c (17004)	64	Echo (ping) request id=0x0037, seq=4/1024, ttl=64 (no re
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 re
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 re
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 re
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 re
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 re
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 r
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 r
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 r
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 r
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 r
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 r
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 r
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 r
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 r

> Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)	
> Ethernet II, Src: VMware_9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco_34:9a:14 (bc:e7:12:34:9a:14)	
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 205	
000. = Priority: Best Effort (default) (0)	
...0 = DEI: Ineligible	
... 0000 1100 1101 = ID: 205	
Type: IPv4 (0x0800)	
Trailer: 55555555	
> Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100	
> Internet Control Message Protocol	

Open de opnamebestanden voor Portchannel1-lidinterfaces. Selecteer het eerste pakket en controleer de belangrijkste punten:

1. Alleen ICMP-echoverdrachtpakketten worden opgenomen.
2. De oorspronkelijke pakketheader heeft VLAN-tag 205.

The screenshot displays a network traffic capture. The top part is a list of 18 ICMP Echo (ping) requests. Each entry includes a sequence number, time, source IP (192.0.2.100), destination IP (198.51.100.100), protocol (ICMP), length (106), IP ID, and TTL (64). The bottom part shows a detailed view of the first frame (Frame 1), which is 106 bytes on wire and 106 bytes captured. The frame structure is as follows:

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

Uitleg

De switch neemt op worden geconfigureerd op subinterfaces Ethernet1/1.205 of Portchannel1.205 met een filter dat overeenkomt met router VLAN 205.

In deze tabel wordt de taak samengevat:

Taak	Opname punt	Intern filter	Richting	Opgenomen verkeer
Configureer en controleer een pakketopname op subinterface Ethernet1/1.205	Ethernet 1/E1	Buiten VLAN 2015	Alleen inspringen	ICMP-echoverzoeken van host 192.0.2.10 naar host 198.51.100.1
Configureer en controleer een pakketopname op subinterface Portchannel1.205 met lidinterfaces Ethernet1/3 en Ethernet1/4	Ethernet 1/3G Ethernet 1/4	Buiten VLAN 2015	Alleen inspringen	ICMP-echoverzoeken van host 192.0.2.10 naar host 198.51.100.1

Packet Capture op interne interfaces

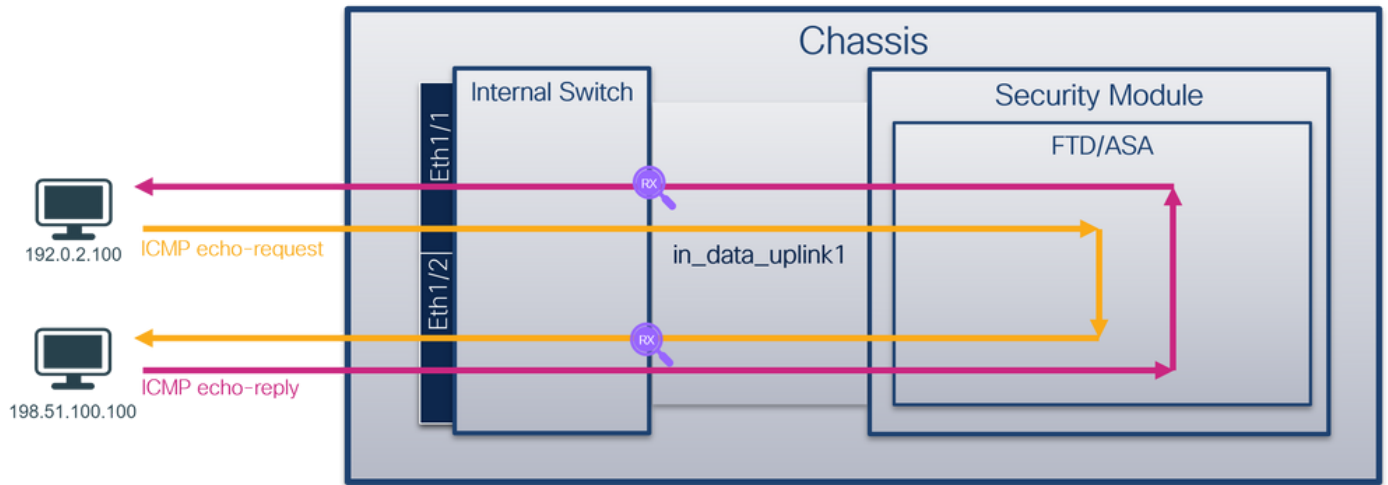
De Secure Firewall heeft 2 interne interfaces:

- **in_data_uplink1** - sluit de applicatie aan op de switch.
- **in_mgmt_uplink1** - biedt een speciaal pakketpad voor beheerverbindingen, zoals SSH naar de beheerinterface of de beheerverbinding, ook bekend als de sftunnel, tussen het FMC en het FTD.

Taak 1

Gebruik de FTD of ASA CLI om een pakketopname te configureren en te verifiëren op de uplink-interface **in_data_uplink1**.

Topologie, pakketstroom en de opnamepunten



Configuratie

Volg deze stappen op ASA of FTD CLI om een pakketopname te configureren op interface `in_data_uplink1`:

1. Een opnamesessie maken:

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

2. De opnamesessie inschakelen:

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

Verificatie

Controleer de naam van de opnamesessie, de administratieve en operationele status, de interfacekaart en de identificatie. Zorg ervoor dat de waarde **Pcapsize** in bytes toeneemt en dat het aantal opgenomen pakketten niet-nul is:

```
> show capture capsw detail
```

Packet Capture info

```

Name:          capsw
Session:          1
Admin State:   enabled
Oper State:    up
Oper State Reason: Active
Config Success:   yes
Config Fail Reason:
Append Flag:      overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code:       0
Drop Count:       0

```

Total Physical ports involved in Packet Capture: 1

Physical port:

```

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

```

Packet Capture Filter Info

Name: caps-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

In dit geval wordt er een opname gemaakt op de interface met een interne ID 18 die de in_data_uplink1 interface op de Secure Firewall 3130 is. De opdracht switch status van show portmanager in de opdrachtshell van FXOS local-mgmt toont de interface-ID's:

> connect fxos

...

KSEC-FPR3100-1 connect local-mgmt

KSEC-FPR3100-1(local-mgmt) show portmanager switch status

Table with 7 columns: Dev/Port, Mode, Link, Speed, Duplex, Loopback Mode, Port Manager. It lists various network ports and their status, with port 0/18 highlighted in bold as KR2, Up, 50G, Full, None, Link-Up.

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

Om toegang te krijgen tot de FXOS op ASA, voert u de opdracht **connect fxos admin uit**. In het geval van multi-context, stel dit bevel in de admincontext in werking.

Opnamebestanden verzamelen

Volg de stappen in het gedeelte **Verzamel Secure Firewall 3100 Internal Switch Capture Files**.

Capture file analyse

Gebruik een applicatie voor pakketopnamebestanden om de opnamebestanden voor interface `in_data_uplink1` te openen. Controleer het belangrijkste punt - in dit geval worden ICMP-echoverzoek en echoantwoordpakketten opgenomen. Dit zijn de pakketten die van de applicatie naar de interne switch worden gestuurd.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-07 22:40:06.685606	192.0.2.100	198.51.100.100	ICMP	102	0x4d93 (19859)	64	Echo (ping) request id=0x003a, seq=33/8448, ttl=64 (repl
2	2022-08-07 22:40:06.685615	198.51.100.100	192.0.2.100	ICMP	102	0x6cdc (27868)	64	Echo (ping) reply id=0x003a, seq=33/8448, ttl=64 (requ
3	2022-08-07 22:40:07.684219	192.0.2.100	198.51.100.100	ICMP	102	0x40e8 (19944)	64	Echo (ping) request id=0x003a, seq=34/8704, ttl=64 (repl
4	2022-08-07 22:40:07.689300	198.51.100.100	192.0.2.100	ICMP	102	0x6db2 (28082)	64	Echo (ping) reply id=0x003a, seq=34/8704, ttl=64 (requ
5	2022-08-07 22:40:08.685736	192.0.2.100	198.51.100.100	ICMP	102	0x4edc (20188)	64	Echo (ping) request id=0x003a, seq=35/8960, ttl=64 (repl
6	2022-08-07 22:40:08.690806	198.51.100.100	192.0.2.100	ICMP	102	0x6dbf (28095)	64	Echo (ping) reply id=0x003a, seq=35/8960, ttl=64 (requ
7	2022-08-07 22:40:09.690737	192.0.2.100	198.51.100.100	ICMP	102	0x4f2d (28269)	64	Echo (ping) request id=0x003a, seq=36/9216, ttl=64 (repl
8	2022-08-07 22:40:09.690744	198.51.100.100	192.0.2.100	ICMP	102	0x6e80 (28288)	64	Echo (ping) reply id=0x003a, seq=36/9216, ttl=64 (requ
9	2022-08-07 22:40:10.692266	192.0.2.100	198.51.100.100	ICMP	102	0x4fb1 (28401)	64	Echo (ping) request id=0x003a, seq=37/9472, ttl=64 (repl
10	2022-08-07 22:40:10.692272	198.51.100.100	192.0.2.100	ICMP	102	0x6ed5 (28373)	64	Echo (ping) reply id=0x003a, seq=37/9472, ttl=64 (requ
11	2022-08-07 22:40:11.691159	192.0.2.100	198.51.100.100	ICMP	102	0x5008 (28488)	64	Echo (ping) request id=0x003a, seq=38/9728, ttl=64 (repl
12	2022-08-07 22:40:11.691166	198.51.100.100	192.0.2.100	ICMP	102	0x6f3b (28475)	64	Echo (ping) reply id=0x003a, seq=38/9728, ttl=64 (requ
13	2022-08-07 22:40:12.692135	192.0.2.100	198.51.100.100	ICMP	102	0x50b8 (28664)	64	Echo (ping) request id=0x003a, seq=39/9984, ttl=64 (repl
14	2022-08-07 22:40:12.692209	198.51.100.100	192.0.2.100	ICMP	102	0x6fd7 (28631)	64	Echo (ping) reply id=0x003a, seq=39/9984, ttl=64 (requ
15	2022-08-07 22:40:13.697320	192.0.2.100	198.51.100.100	ICMP	102	0x5184 (28868)	64	Echo (ping) request id=0x003a, seq=40/10240, ttl=64 (reg
16	2022-08-07 22:40:13.697327	198.51.100.100	192.0.2.100	ICMP	102	0x703e (28734)	64	Echo (ping) reply id=0x003a, seq=40/10240, ttl=64 (rec
17	2022-08-07 22:40:14.698512	192.0.2.100	198.51.100.100	ICMP	102	0x51d8 (28952)	64	Echo (ping) request id=0x003a, seq=41/10496, ttl=64 (reg
18	2022-08-07 22:40:14.698518	198.51.100.100	192.0.2.100	ICMP	102	0x70dd (28893)	64	Echo (ping) reply id=0x003a, seq=41/10496, ttl=64 (rec

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

Uitleg

Wanneer een switch op de uplink-interface is geconfigureerd, worden alleen pakketten die van de toepassing naar de interne switch zijn verzonden opgenomen. Pakketten die naar de toepassing worden verzonden, worden niet opgenomen.

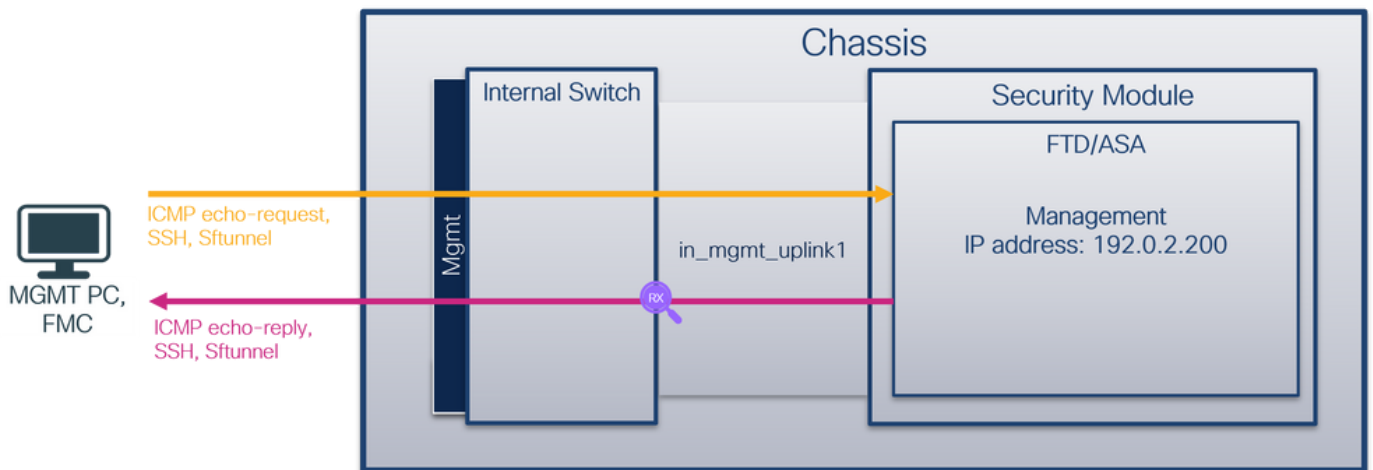
In deze tabel wordt de taak samengevat:

Taak	Opnamepunt	Intern filter	Richting	Opgenomen verkeer
Configureer en controleer een pakketopname op de uplink-interface <code>in_data_uplink1</code>	<code>in_data_uplink1</code>	None	Alleen inspringen	ICMP-echoverzoeken van host 192.0.2.10 naar host 198.51.100.100 ICMP-echoantwoorden van host 198.51.100.100 op host 192.0.2.10

Taak 2

Gebruik de FTD of ASA CLI om een pakketopname op de uplink-interface `in_mgmt_uplink1` te configureren en te verifiëren. Alleen de pakketten met beheervliegtuigverbindingen worden opgenomen.

Topologie, pakketstroom en de opnamepunten



Configuratie

Volg deze stappen op ASA of FTD CLI om een pakketopname te configureren op interface `in_mgmt_uplink1`:

1. Een opnamesessie maken:

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

2. De opnamesessie inschakelen:

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

Verificatie

Controleer de naam van de opnamesessie, de administratieve en operationele status, de interfacekaart en de identificatie. Zorg ervoor dat de waarde **Pcapsize** in bytes toeneemt en dat het aantal opgenomen pakketten niet-nul is:

```
> 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-1-19

Packet Capture Filter Info

Name: caps-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

In dit geval wordt er een opname gemaakt op de interface met een interne ID 19 die de **in_mgmt_uplink1** interface is op de Secure Firewall 3130. De opdracht **switch status** van **show portmanager** in de opdrachtshell van **FXOS local-mgmt** toont de interface-ID's:

> connect fxos

...

KSEC-FPR3100-1 connect local-mgmt

KSEC-FPR3100-1(local-mgmt) show portmanager switch status

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

0/31	n/a	Down	n/a	Full	N/A	Reset
0/32	n/a	Down	n/a	Full	N/A	Reset
0/33	1000_BaseX	Down	1G	Full	None	Link-Down
0/34	n/a	Down	n/a	Full	N/A	Reset
0/35	n/a	Down	n/a	Full	N/A	Reset
0/36	n/a	Down	n/a	Full	N/A	Reset

Om toegang te krijgen tot de FXOS op ASA, voert u de opdracht **connect fxos admin uit**. In het geval van multi-context, stel dit bevel in de admincontext in werking.

Opnamebestanden verzamelen

Volg de stappen in het gedeelte **Verzamel Secure Firewall 3100 Internal Switch Capture Files**.

Capture file analyse

Gebruik een applicatie voor pakketopname om de opnamebestanden voor interface **in_mgmt_uplink1** te openen. Controleer het belangrijkste punt - in dit geval worden alleen de pakketten vanaf het IP-adres voor beheer 192.0.2.200 weergegeven. De voorbeelden zijn SSH, Sftunnel of ICMP echo antwoordpakketten. Dit zijn de pakketten die door de switch van de applicatie naar het netwerk worden verzonden.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
196	2022-08-07 23:21:45.133362	192.0.2.200	192.0.2.101	TCP	1518	0xb7d0 (47056)	64	39181 → 8305 [ACK] Seq=61372 Ack=875 Win=1384 Len=1448 TS
197	2022-08-07 23:21:45.133385	192.0.2.200	192.0.2.101	TCP	1518	0xb7d1 (47057)	64	39181 → 8305 [ACK] Seq=62820 Ack=875 Win=1384 Len=1448 TS
198	2022-08-07 23:21:45.133388	192.0.2.200	192.0.2.101	TLSv1.2	990	0xb7d2 (47058)	64	Application Data
199	2022-08-07 23:21:45.928772	192.0.2.200	192.0.2.100	ICMP	78	0xbd48 (48456)	64	Echo (ping) reply id=0x0001, seq=4539/47889, ttl=64
200	2022-08-07 23:21:45.949024	192.0.2.200	192.0.2.101	TLSv1.2	128	0x4a97 (19095)	64	Application Data
201	2022-08-07 23:21:45.949027	192.0.2.200	192.0.2.101	TCP	70	0x4a98 (19096)	64	8305 → 58885 [ACK] Seq=21997 Ack=26244 Win=4116 Len=0 TSv
202	2022-08-07 23:21:46.019895	192.0.2.200	192.0.2.101	TLSv1.2	100	0x4a99 (19097)	64	Application Data
203	2022-08-07 23:21:46.019899	192.0.2.200	192.0.2.101	TLSv1.2	96	0x4a9a (19098)	64	Application Data
204	2022-08-07 23:21:46.019903	192.0.2.200	192.0.2.101	TCP	70	0x4a9b (19099)	64	8305 → 58885 [ACK] Seq=22053 Ack=26274 Win=4116 Len=0 TSv
205	2022-08-07 23:21:46.019906	192.0.2.200	192.0.2.101	TCP	70	0x4a9c (19100)	64	8305 → 58885 [ACK] Seq=22053 Ack=26300 Win=4116 Len=0 TSv
206	2022-08-07 23:21:46.136415	192.0.2.200	192.0.2.101	TCP	70	0xb7d3 (47059)	64	39181 → 8305 [ACK] Seq=65188 Ack=921 Win=1384 Len=0 TSval
207	2022-08-07 23:21:46.958148	192.0.2.200	192.0.2.100	ICMP	78	0xbd9e (48542)	64	Echo (ping) reply id=0x0001, seq=4540/48145, ttl=64
208	2022-08-07 23:21:47.980409	192.0.2.200	192.0.2.100	ICMP	78	0xbdf2 (48626)	64	Echo (ping) reply id=0x0001, seq=4541/48401, ttl=64
209	2022-08-07 23:21:48.406312	192.0.2.200	192.0.2.101	TCP	70	0x4a9d (19101)	64	8305 → 58885 [ACK] Seq=22053 Ack=26366 Win=4116 Len=0 TSv
210	2022-08-07 23:21:48.903236	192.0.2.200	192.0.2.101	TLSv1.2	747	0x4a9e (19102)	64	Application Data
211	2022-08-07 23:21:48.994386	192.0.2.200	192.0.2.100	ICMP	78	0xbe48 (48712)	64	Echo (ping) reply id=0x0001, seq=4542/48657, ttl=64
212	2022-08-07 23:21:50.000576	192.0.2.200	192.0.2.100	ICMP	78	0xbe4e (48806)	64	Echo (ping) reply id=0x0001, seq=4543/48913, ttl=64
213	2022-08-07 23:21:50.140167	192.0.2.200	192.0.2.101	TCP	1518	0xb7d4 (47060)	64	39181 → 8305 [ACK] Seq=65188 Ack=921 Win=1384 Len=1448 TS
214	2022-08-07 23:21:50.140171	192.0.2.200	192.0.2.101	TCP	1518	0xb7d5 (47061)	64	39181 → 8305 [ACK] Seq=66636 Ack=921 Win=1384 Len=1448 TS
215	2022-08-07 23:21:50.140175	192.0.2.200	192.0.2.101	TLSv1.2	990	0xb7d6 (47062)	64	Application Data
216	2022-08-07 23:21:51.015884	192.0.2.200	192.0.2.100	ICMP	78	0xbec1 (48833)	64	Echo (ping) reply id=0x0001, seq=4544/49169, ttl=64
217	2022-08-07 23:21:51.142842	192.0.2.200	192.0.2.101	TCP	70	0xb7d7 (47063)	64	39181 → 8305 [ACK] Seq=69004 Ack=967 Win=1384 Len=0 TSval
218	2022-08-07 23:21:52.030118	192.0.2.200	192.0.2.100	ICMP	78	0xbf02 (48898)	64	Echo (ping) reply id=0x0001, seq=4545/49425, ttl=64
219	2022-08-07 23:21:53.042744	192.0.2.200	192.0.2.100	ICMP	78	0xbf59 (48985)	64	Echo (ping) reply id=0x0001, seq=4546/49681, ttl=64
220	2022-08-07 23:21:53.073144	192.0.2.200	192.0.2.100	SSH	170	0xad34 (44340)	64	Server: Encrypted packet (len=112)
221	2022-08-07 23:21:53.194906	192.0.2.200	192.0.2.100	TCP	64	0xad35 (44341)	64	22 → 53249 [ACK] Seq=1025 Ack=881 Win=946 Len=0
222	2022-08-07 23:21:53.905480	192.0.2.200	192.0.2.101	TLSv1.2	747	0x4a9f (19103)	64	Application Data
223	2022-08-07 23:21:54.102899	192.0.2.200	192.0.2.100	ICMP	78	0xbf63 (48995)	64	Echo (ping) reply id=0x0001, seq=4547/49937, ttl=64
224	2022-08-07 23:21:54.903675	192.0.2.200	192.0.2.101	TCP	70	0x4aa0 (19104)	64	8305 → 58885 [ACK] Seq=23407 Ack=26424 Win=4116 Len=0 TSv
225	2022-08-07 23:21:55.136700	192.0.2.200	192.0.2.100	TCP	70	0xbf64 (48996)	64	Echo (ping) reply id=0x0001, seq=4548/50103, ttl=64


```

> Frame 1: 747 bytes on wire (5976 bits), 747 bytes captured (5976 bits)
> Ethernet II, Src: Cisco_34:9a:00 (bc:e7:12:34:9a:00), Dst: Cisco_11:38:2a (a4:53:0e:11:38:2a)
> Internet Protocol Version 4, Src: 192.0.2.200, Dst: 192.0.2.101
> Transmission Control Protocol, Src Port: 8305, Dst Port: 58885, Seq: 1, Ack: 1, Len: 677
> Transport Layer Security
0000 a4 53 0e 11 38 2a bc e7 12 34 9a 00 08 00 45 00 58 88 5
0010 02 d9 4a 3d 40 00 40 06 68 b4 c0 00 02 c8 c0 00 00 00 00
0020 02 65 20 71 e6 05 67 1b 2a c5 db e3 6b d4 80 18 00 00 00
0030 10 14 27 cc 00 00 01 01 08 0a 08 76 95 7f 91 02 00 00 00
0040 3d 41 17 03 02 a0 22 64 01 e0 ff cc 98 f9 af 00 00 00 00
0050 07 40 75 19 a4 d5 df 6a d8 fe 66 8e 9b cc 8d 2f 00 00 00
0060 92 b2 1a 64 e7 20 36 03 8e 48 02 5a 7c 85 30 d4 00 00 00
0070 fa c0 a8 56 b8 ad a7 7e 19 3a c1 9c 4b 57 0e e0 00 00 00
0080 be ef 95 22 84 c1 c1 9d 9f 24 78 b4 15 1c 44 0e 00 00 00
0090 ea cb 43 9e 1f fd a7 70 75 e5 6b a4 f8 2b ee 47 00 00 00
00a0 2f 86 73 8f b1 e1 b5 c6 57 e3 a8 46 0e cb 26 b7 00 00 00
00b0 5b c7 e3 09 54 f3 c1 ff 26 d9 87 ea 51 3d 20 08 00 00 00
00c0 16 fd cb f5 4f 91 98 5e 86 15 17 55 68 6f 5d 04 00 00 00

```

Uitleg

Wanneer een switch op de uplink-interface voor beheer is geconfigureerd, worden alleen toegangspakketten die vanuit de toepassingsbeheerinterface zijn verzonden, opgenomen. Pakketten die bestemd zijn voor de interface voor toepassingsbeheer worden niet opgenomen.

In deze tabel wordt de taak samengevat:

Taak	Opnamepunt	Intern filter	Richting	Opgenomen verkeer
Configureer en	in_mgmt_	None	Alleen inspringen	ICMP-echoantwoorden van IP-adres voor

controleer een
pakketopname op
de beheeruplink-
interface uplink1

(van de
beheerinterface naar
het netwerk via de
interne switch)

FTD-beheer 192.0.2.200 op host 192.0.2.10
Sftunnel van FTD management IP-adres
192.0.2.200 naar FMC IP-adres 192.0.2.10
SSH van FTD management IP-adres
192.0.2.200 naar host 192.0.2.10

PacketCapture filters

De interne pakketopnamefilters van de switch worden geconfigureerd op dezelfde manier als het gegevensvlak opneemt. Gebruik de opties **ethernet-type** en **overeenkomende** om filters te configureren.

Configuratie

Volg deze stappen op ASA of FTD CLI om een pakketopname te configureren met een filter die ARP-frames of ICMP-pakketten aanpast vanaf host 198.51.100.100 op interface Ethernet1/1:

1. Controleer de naam:

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

2. Een opnamesessie voor ARP of ICMP maken:

```
> capture capsw switch interface inside ethernet-type arp
> capture capsw switch interface inside match icmp 198.51.100.100
```

Verificatie

Controleer de naam van de opnamesessie en het filter. De waarde van Ethertype is **2054** in decimaal en **0x0806** in hexadecimaal:

```
> 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: caps-1-1

Packet Capture Filter Info

Name: caps-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

Dit is de verificatie van het filter voor ICMP. IP-protocol 1 is de ICMP:

> **show capture caps-1-1 detail**

Packet Capture info

Name: caps-1-1
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: caps-1-1

Packet Capture Filter Info

Name: caps-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

Opnamebestanden van beveiligde firewall 3100 interne Switch

Gebruik ASA of FTD CLI om switch-opnamebestanden te verzamelen. Op FTD kan het opnamebestand ook via de CLI-kopieeropdracht worden geëxporteerd naar bestemmingen die via de gegevens- of diagnostische interfaces kunnen worden bereikt.

U kunt het bestand ook kopiëren naar `/ngfw/var/common` in de expert-modus en downloaden van FMC via de optie **File Download**.

In het geval van poort-kanaal interfaces zorg ervoor dat pakketopnamebestanden van alle lidinterfaces worden verzameld.

ASA

Volg deze stappen op om switch-opnamebestanden op ASA CLI te verzamelen:

1. Stop de vastlegging:

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

2. Controleer of de opnamesessie is gestopt en noteer de naam van het opnamebestand.

```
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. Gebruik de CLI-kopieeropdracht om het bestand naar externe bestemmingen te exporteren:

```
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

Volg deze stappen om switch-opnamebestanden op FTD CLI te verzamelen en deze naar servers te kopiëren die bereikbaar zijn via gegevens- of diagnostische interfaces:

1. Ga naar diagnostische CLI:

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

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

2. Stop de vastlegging:

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

3. Controleer of de opnamesessie is gestopt en noteer de naam van het opnamebestand:

```
firepower# show capture capsw detail
```

Packet Capture info

Name: capsu
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-capsu-ethernet-1-1-0.pcap**
Pcapsize: 139826
Filter: capsu-1-1

Packet Capture Filter Info

Name: capsu-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. Gebruik de CLI-kopieeropdracht om het bestand naar externe bestemmingen te exporteren.

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

Volg deze stappen om opnamebestanden te verzamelen bij FMC via de optie **Bestand downloaden**:

1. Stop de vastlegging:

```
> capture capsw switch stop
```

2. Controleer of de opnamesessie is gestopt en noteer de bestandsnaam en het pad voor het volledige opnamebestand:

```
> 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. Ga naar expertmodus en switch naar wortelmodus:

```
> expert
```

```
admin@firepower:~$ sudo su
```

```
root@firepower:/home/admin
```

4. Kopieert het opnamebestand naar `/ngfw/var/common/`:

```

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

```

5. Kies in FMC Apparaten > Bestand downloaden:

The screenshot shows the Fire Management Center (FMC) interface. The 'Devices' menu is open, and 'File Download' is highlighted. The interface includes a 'Summary Dashboard' with various charts and a navigation bar with tabs for Overview, Analysis, Policies, Devices, Objects, Integration, Deploy, and Reporting.

6. Kies de FTD, geef de naam van het opnamebestand op en klik op Downloaden:

The screenshot shows the 'File Download' dialog box in the FMC interface. The 'Device' dropdown is set to 'FPR3100-1' and the 'File' text box contains 'sess-1-capsw-ethernet-1-1-0.pcap'. There are 'Back' and 'Download' buttons at the bottom of the dialog.

Richtlijnen, beperkingen en beste praktijken voor pakketvastlegging in Switch

Richtsnoeren en beperkingen:

- Meervoudige switch-opnamesessies worden ondersteund, maar er kan slechts 1 switch-opnamesessie tegelijkertijd actief zijn. Een poging om 2 of meer opnamesessies in te schakelen, resulteert in een fout "**ERROR: Inschakelen sessie mislukt, als limiet van maximaal 1 actieve pakketopnamesessies bereikt**".
- Een actieve switch Capture kan niet worden verwijderd.
- Switch Captures kunnen niet gelezen worden op de applicatie. De gebruiker moet de bestanden exporteren.
- Bepaalde opties voor gegevensvlak vastleggen, zoals **dump**, **decoderen**, **pakketnummer**,

overtrekken en andere opties worden niet ondersteund voor switch-opnamen.

- In het geval van multi-context ASA, wordt de switch op gegevensinterfaces geconfigureerd in gebruikerscontexten. De switch legt op interfaces in_data_uplink1 vast en in_mgmt_uplink1 worden alleen ondersteund in de admin context.

Dit is de lijst met best practices op basis van het gebruik van pakketvastlegging in TAC-gevallen:

- Let op richtlijnen en beperkingen.
- Gebruik opnamefilters.
- Overweeg de impact van NAT op IP-adressen van pakketten wanneer een opnamefilter is geconfigureerd.
- Vergroot of verlaag de **pakketlengte** die de framegrootte aangeeft, voor het geval dat deze verschilt van de standaardwaarde van 1518 bytes. Een kortere grootte resulteert in een hoger aantal opgenomen pakketten en vice versa.
- Pas indien nodig de **buffergrootte** aan.
- Let op de **Drop Count** in de output van de opdracht **show cap <cap_name> detail**. Zodra de grens van de buffergrootte wordt bereikt, stijgt de teller van de dalingstelling.

Gerelateerde informatie

- [Firepower 4100/9300 Chassis Manager en FXOS CLI-configuratiehandleidingen](#)
- [Cisco Secure Firewall 3100 Introductiegids](#)
- [Cisco Firepower 4100/9300 FXOS opdrachtreferentie](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.