

# Sichere Firewall- und FirePOWER-interne Switch-Erfassung konfigurieren und überprüfen

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Allgemeiner Überblick über die Systemarchitektur](#)

[Allgemeiner Überblick über den internen Switch-Betrieb](#)

[Paketfluss und Erfassungspunkte](#)

[Konfiguration und Verifizierung für Firepower 4100/9300](#)

[Paketerfassung an einer physischen oder Port-Channel-Schnittstelle](#)

[Paketerfassung an Backplane-Schnittstellen](#)

[Paketerfassung auf Anwendungs- und Anwendungs-Ports](#)

[Paketerfassung auf einer Subschnittstelle einer physischen oder Port-Channel-Schnittstelle](#)

[Paketerfassungsfilter](#)

[Sammeln von FirePOWER 4100/9300-internen Switch-Erfassungsdateien](#)

[Richtlinien, Einschränkungen und Best Practices für die interne Switch-Paketerfassung](#)

[Konfiguration und Verifizierung auf einer sicheren Firewall 3100](#)

[Paketerfassung an einer physischen oder Port-Channel-Schnittstelle](#)

[Paketerfassung auf einer Subschnittstelle einer physischen oder Port-Channel-Schnittstelle](#)

[Paketerfassung an internen Schnittstellen](#)

[Paketerfassungsfilter](#)

[Erfassen von Dateien für den internen Secure Firewall 3100-Switch](#)

[Richtlinien, Einschränkungen und Best Practices für die interne Switch-Paketerfassung](#)

[Zugehörige Informationen](#)

## Einleitung

In diesem Dokument werden die Konfiguration und Verifizierung der FirePOWER und der interne Switch für die sichere Firewall beschrieben.

## Voraussetzungen

### Anforderungen

Grundlegendes Produktwissen, Erfassungsanalyse

### Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

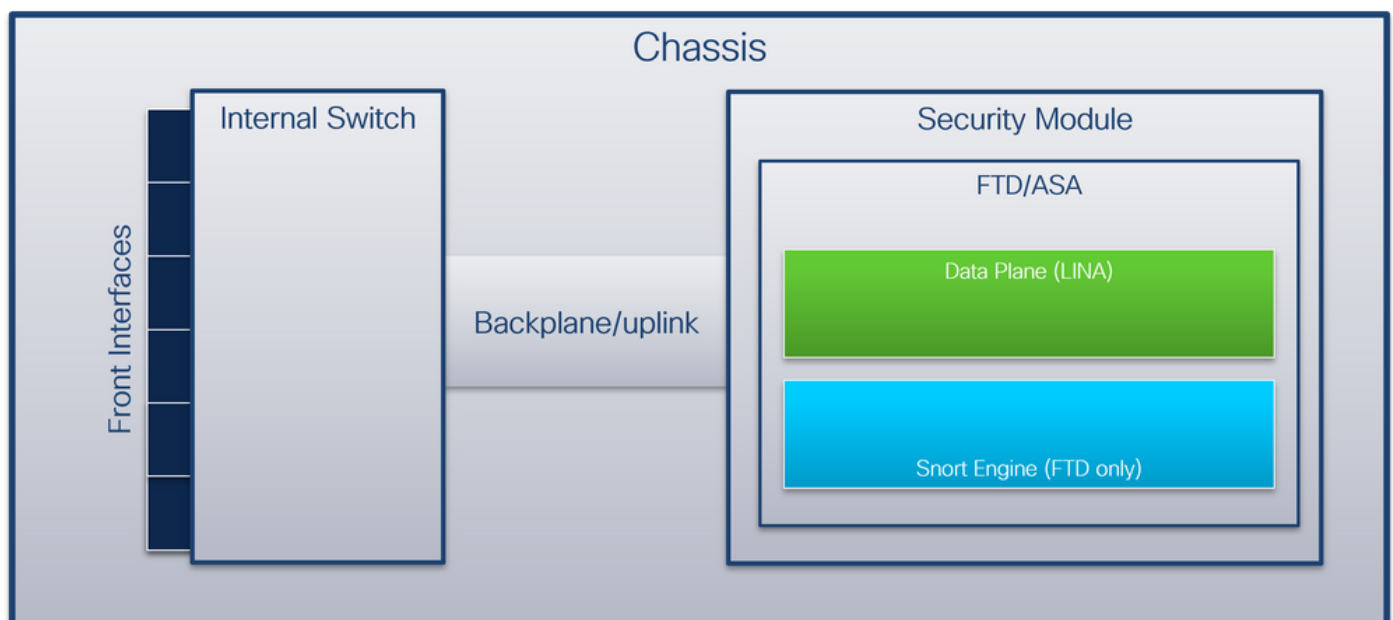
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

## Hintergrundinformationen

### Allgemeiner Überblick über die Systemarchitektur

Aus Sicht des Paketflusses kann die Architektur der Firepower 4100/9300 und der Secure Firewall 3100 wie in der folgenden Abbildung dargestellt dargestellt werden:



Das Gehäuse umfasst folgende Komponenten:

- **Interner Switch** - Leitet Pakete vom Netzwerk an die Anwendung weiter und umgekehrt. Der interne Switch wird mit den **Frontschnittstellen** verbunden, die sich auf dem integrierten Schnittstellenmodul oder externen Netzwerkmodulen befinden und mit externen Geräten, z. B. Switches, verbunden werden. Beispiele für Schnittstellen an der Vorderseite sind Ethernet 1/1, Ethernet 2/4 usw. "Front" ist keine starke technische Definition. In diesem Dokument

werden Schnittstellen, die mit externen Geräten verbunden sind, von den Backplane- oder Uplink-Schnittstellen unterschieden.

- **Backplane oder Uplink** - eine interne Schnittstelle, die das Sicherheitsmodul (SM) mit dem internen Switch verbindet. Diese Tabelle zeigt die Backplane-Schnittstellen für Firepower 4100/9300 und die Uplink-Schnittstelle für Secure Firewall 3100:

Plattform	Anzahl unterstützter Sicherheitsmodule	Backplane/Uplink-Schnittstellen	Zugeordnete Anwendungsschnittstellen
Firepower 4100 (außer Firepower 4110/4112)	1	SM1: Ethernet1/9 Ethernet 1/10	Interne Daten0/0 Interne Daten0/1
FirePOWER 4110/4112	1	Ethernet1/9	Interne Daten0/0
FirePOWER 9300	3	SM1: Ethernet1/9 Ethernet 1/10	Interne Daten0/0 Interne Daten0/1
		SM2: Ethernet 1/11 Ethernet 1/12	Interne Daten0/0 Interne Daten0/1
		SM3: Ethernet 1/13 Ethernet 1/14	Interne Daten0/0 Interne Daten0/1
Sichere Firewall 3100	1	SM1: in_data_uplink1	Interne Daten0/1

Bei zwei Backplane-Schnittstellen pro Modul führen der interne Switch und die Anwendungen auf den Modulen Datenverkehr-Load-Balancing über die beiden Schnittstellen durch.

- **Sicherheitsmodul, Security Engine oder Blade** - das Modul, in dem Anwendungen wie FTD oder ASA installiert sind. Firepower 9300 unterstützt bis zu drei Sicherheitsmodule.
- **Zugeordnete Anwendungsschnittstelle** - Anwendungen wie FTD oder ASA ordnen die Backplane- oder Uplink-Schnittstellen internen Schnittstellen zu. Mit anderen Worten: Die Backplane- oder Uplink-Schnittstellen sind in Anwendungen als interne Schnittstellen sichtbar.

Verwenden Sie den Befehl **show interface detail**, um interne Schnittstellen zu überprüfen:

```
> show interface detail | grep Interface
Interface Internal-Control0/0 "ha_ctl_nlp_int_tap", is up, line protocol is up
Control Point Interface States:
  Interface number is 6
  Interface config status is active
  Interface state is active
Interface Internal-Data0/0 "", is up, line protocol is up
Control Point Interface States:
  Interface number is 2
  Interface config status is active
  Interface state is active
Interface Internal-Data0/1 "", is up, line protocol is up
Control Point Interface States:
  Interface number is 3
  Interface config status is active
  Interface state is active
```

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

## Allgemeiner Überblick über den internen Switch-Betrieb

### FirePOWER 4100/9300

Zur Weiterleitungsentscheidung verwendet der interne Switch einen **Schnittstellen-VLAN-Tag** oder **Port-VLAN-Tag** und einen **virtuellen Netzwerk-Tag (VN-Tag)**.

Das Port-VLAN-Tag wird vom internen Switch verwendet, um eine Schnittstelle zu identifizieren. Der Switch fügt den Port-VLAN-Tag in jedes Eingangspaket ein, das an den Frontschnittstellen empfangen wurde. Der VLAN-Tag wird automatisch vom System konfiguriert und kann nicht manuell geändert werden. Der Tag-Wert kann in der **fxos**-Befehlsshell überprüft werden:

```
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
```

Der VN-Tag wird ebenfalls vom internen Switch eingefügt und für die Weiterleitung der Pakete an die Anwendung verwendet. Es wird automatisch vom System konfiguriert und kann nicht manuell geändert werden.

Das Port-VLAN-Tag und das VN-Tag werden gemeinsam mit der Anwendung genutzt. Die Anwendung fügt die jeweiligen VLAN-Tags für die Ausgangsschnittstelle und die VN-Tags in jedes



Paket ein. Wenn ein Paket von der Anwendung vom internen Switch an den Backplane-Schnittstellen empfangen wird, liest der Switch den VLAN-Tag der Ausgangsschnittstelle und den VN-Tag, identifiziert die Anwendung und die Ausgangsschnittstelle, entfernt den VLAN-Tag des Ports und den VN-Tag und leitet das Paket an das Netzwerk weiter.

## Sichere Firewall 3100

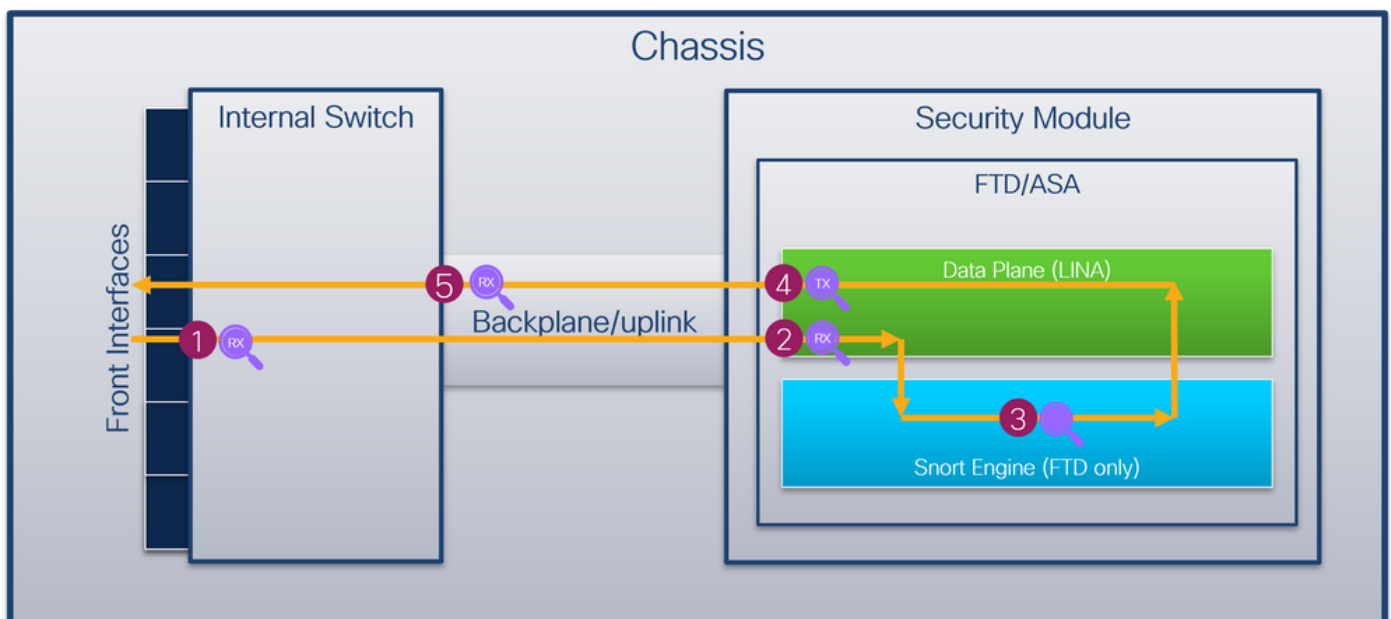
Wie bei Firepower 4100/9300 wird das Port-VLAN-Tag vom internen Switch verwendet, um eine Schnittstelle zu identifizieren.

Das Port-VLAN-Tag wird mit der Anwendung gemeinsam genutzt. Die Anwendung fügt die entsprechenden VLAN-Tags für die Ausgangsschnittstelle in jedes Paket ein. Wenn ein Paket von der Anwendung vom internen Switch der Uplink-Schnittstelle empfangen wird, liest der Switch den VLAN-Tag der Ausgangsschnittstelle, identifiziert die Ausgangsschnittstelle, entfernt den VLAN-Tag des Ports und leitet das Paket an das Netzwerk weiter.

## Paketfluss und Erfassungspunkte

Die Firepower 4100/9300 und die Secure Firewall 3100 unterstützen die Paketerfassung an den Schnittstellen des internen Switches.

Diese Abbildung zeigt die Paketerfassungspunkte entlang des Paketpfads innerhalb des Chassis und der Anwendung:



Die wichtigsten Punkte sind:

1. Eingangserfassungspunkt an der Vorderseite des internen Switches. Eine Front-Schnittstelle ist jede Schnittstelle, die mit den Peer-Geräten wie Switches verbunden ist.
2. Eingangserfassungspunkt der Datenebenenschnittstelle
3. Snort Capture Point
4. Ausgangspunkt der Datenebenenschnittstelle
5. Interner Eingangserfassungspunkt an der Backplane oder dem Uplink des Switches. Eine Backplane- oder Uplink-Schnittstelle verbindet den internen Switch mit der Anwendung.

Der interne Switch unterstützt nur Eingangsschnittstellenerfassungen. Das heißt, dass nur die

Pakete erfasst werden können, die vom Netzwerk oder von der ASA-/FTD-Anwendung empfangen wurden. **Egress-Paketerfassungen werden nicht unterstützt.**

## Konfiguration und Verifizierung auf FirePOWER 4100/9300

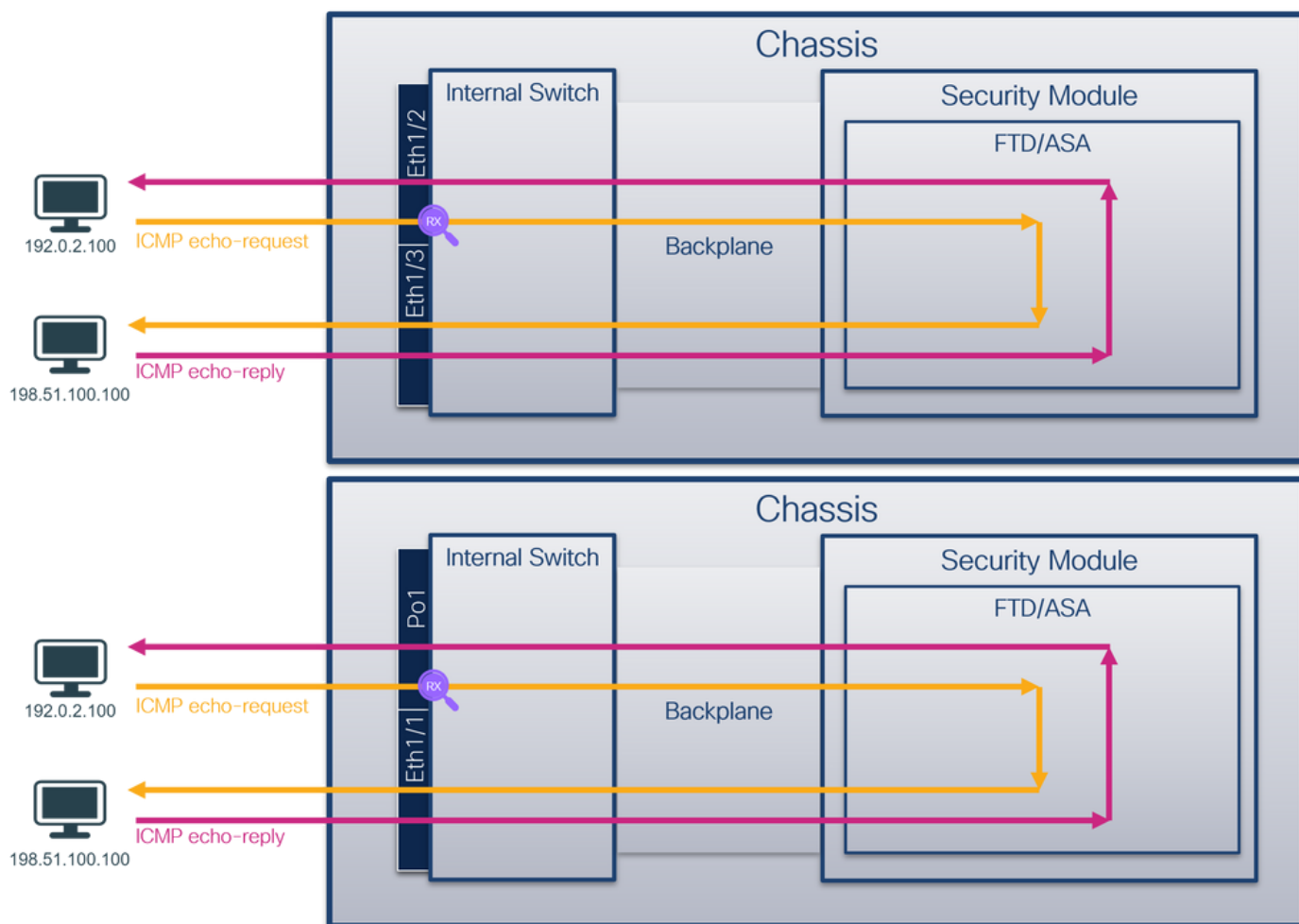
Die FirePOWER 4100/9300-internen Switch-Erfassungen können unter **Tools > Packet Capture** auf FCM oder im **Bereich Packet-Capture** in FXOS CLI konfiguriert werden. Eine Beschreibung der Optionen zur Paketerfassung finden Sie im *Konfigurationsleitfaden für Cisco Firepower 4100/9300 FXOS Chassis Manager* oder im *Konfigurationsleitfaden für Cisco Firepower 4100/9300 FXOS CLI*, Kapitel **Fehlerbehebung**, Abschnitt **Paketerfassung**.

Diese Szenarien beziehen sich auf häufige Anwendungsfälle von FirePOWER 4100/9300-internen Switch-Erfassungen.

### Paketerfassung an einer physischen oder Port-Channel-Schnittstelle

Verwenden Sie den FCM und die CLI, um eine Paketerfassung an der Schnittstelle Ethernet1/2 oder Port-Channel1 zu konfigurieren und zu überprüfen. Bei einer Port-Channel-Schnittstelle müssen Sie alle physischen Mitglieds-Schnittstellen auswählen.

#### Topologie, Paketfluss und Erfassungspunkte

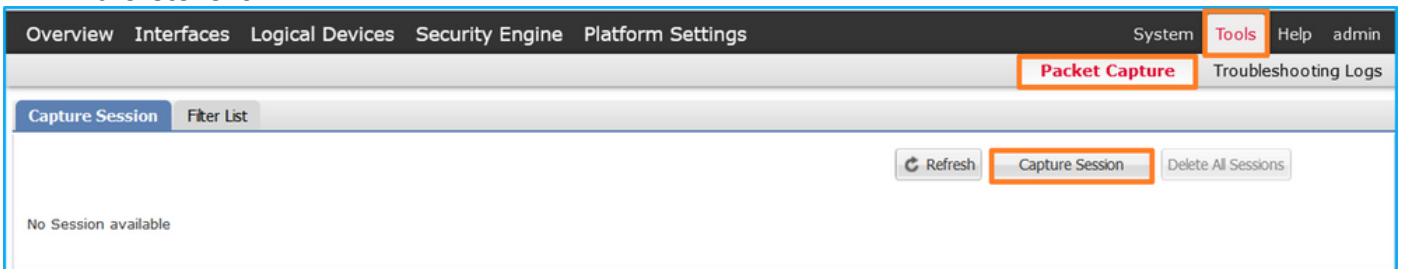


#### Konfiguration

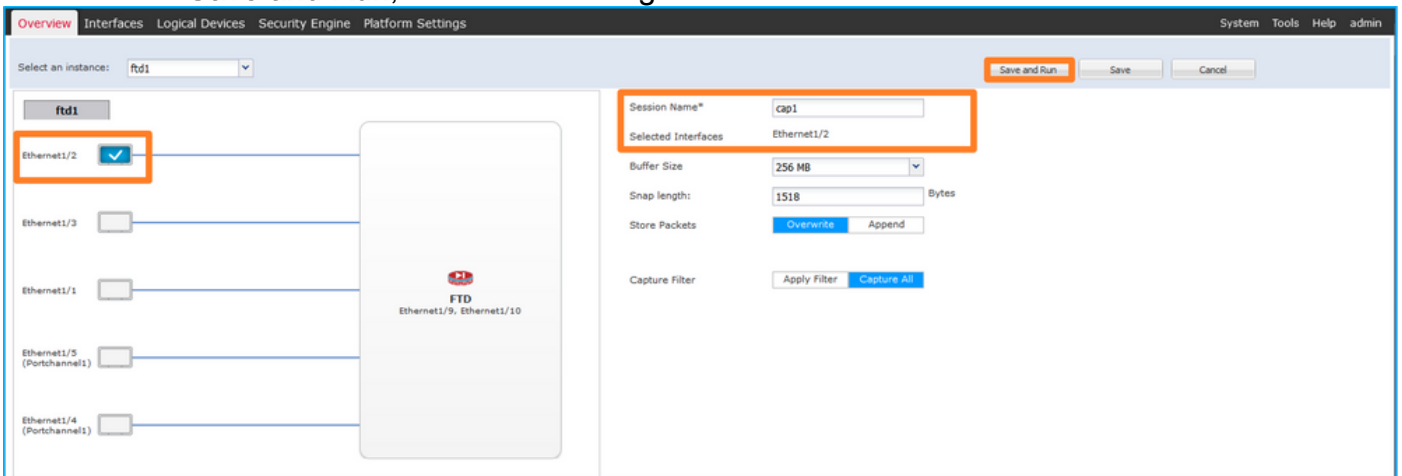
##### FCM

Befolgen Sie die folgenden Schritte auf FCM, um eine Paketerfassung an den Schnittstellen Ethernet1/2 oder Port-Channel1 zu konfigurieren:

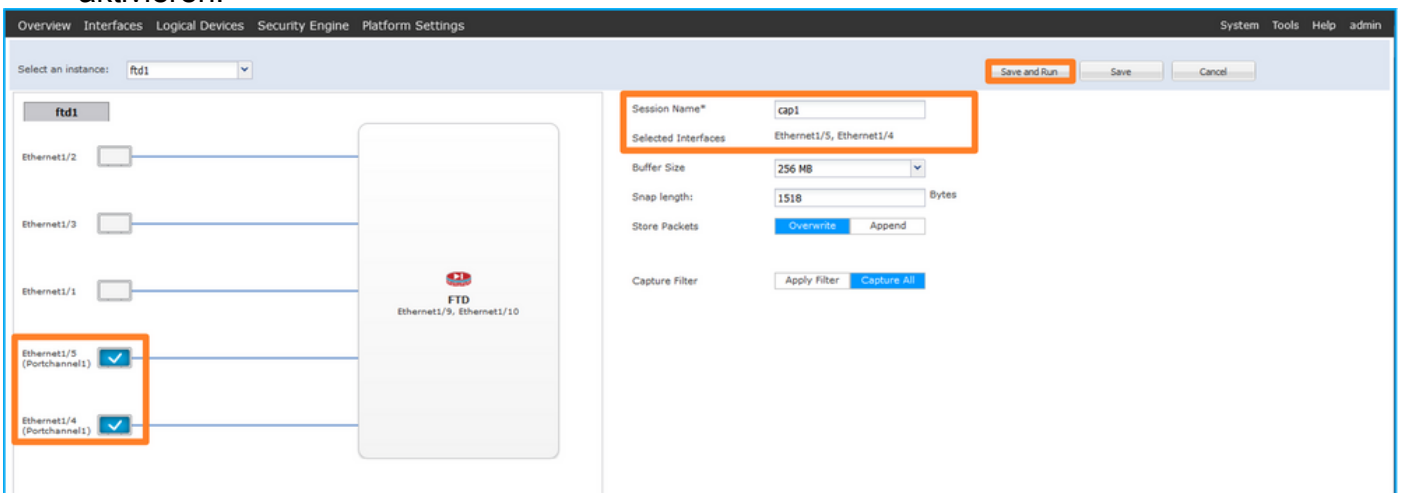
1. Verwenden Sie **Tools > Packet Capture > Capture Session**, um eine neue Erfassungssitzung zu erstellen:



2. Wählen Sie die Schnittstelle **Ethernet1/2** aus, geben Sie den Sitzungsnamen an, und klicken Sie auf **Save and Run**, um die Erfassung zu aktivieren:



3. Wählen Sie bei einer Port-Channel-Schnittstelle alle physischen Member-Schnittstellen aus, geben Sie den Sitzungsnamen an, und klicken Sie auf **Save and Run**, um die Erfassung zu aktivieren:



## FXOS-CLI

Führen Sie die folgenden Schritte auf der FXOS-CLI aus, um eine Paketerfassung an den Schnittstellen Ethernet1/2 oder Port-Channel1 zu konfigurieren:

1. Identifizieren Sie den Anwendungstyp und die Kennung:

```

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. Geben Sie bei einer Port-Channel-Schnittstelle deren Mitgliedsschnittstellen an:

```

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. Eine Aufzeichnungssitzung erstellen:

```

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 #

```

Für Port-Channel-Schnittstellen wird eine separate Erfassung für jede Member-Schnittstelle konfiguriert:

```

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 #

```

## Verifizierung

### FCM

Überprüfen Sie den **Schnittstellennamen**, stellen Sie sicher, dass der **Betriebsstatus** aktiv ist und

dass die Dateigröße (in Byte) ansteigt:

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

Port-Channel1 mit Mitgliedsschnittstellen Ethernet1/4 und 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

Überprüfen Sie die Erfassungsdetails in der Paketerfassung:

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

Traffic Monitoring Session:

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

Physical ports involved in Packet Capture:

```
Slot Id: 1
Port Id: 2
Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap
Pcapsize: 75136 bytes
Filter:
Sub Interface: 0
Application Instance Identifier: ftd1
Application Name: ftd
```

Port-Channel 1 mit den Mitgliedsschnittstellen Ethernet1/4 und 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**

## Erfassungsdateien erfassen

Befolgen Sie die Schritte im Abschnitt **Sammeln von FirePOWER 4100/9300-internen Switch-Erfassungsdateien**.

## Analyse der Erfassungsdatei

Öffnen Sie die Erfassungsdatei für Ethernet1/2 mit einer Anwendung zum Lesen der Paketerfassungsdatei. Wählen Sie das erste Paket aus, und überprüfen Sie die Schlüsselpunkte:

1. Es werden nur ICMP-Echoanforderungspakete erfasst. Jedes Paket wird erfasst und zweimal angezeigt.
2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.
3. Der interne Switch fügt den zusätzlichen Port-VLAN-Tag **102 ein**, der die Eingangsschnittstelle Ethernet1/2 identifiziert.
4. Der interne Switch fügt einen zusätzlichen VN-Tag ein.



Packet capture analysis showing a series of ICMP Echo (ping) requests from source IP 192.0.2.100 to destination IP 198.51.100.100. The requests are numbered 1 through 29, all showing a TTL of 64 and a response of "no response found".

Frame 1 details (Frame 108 bytes on wire):

- VLAN-Tag (4):** Direction: From Bridge, Pointer: vif\_id, Destination: 10, Looped: No, Reserved: 0, Version: 0, Source: 0.
- 802.1Q Virtual LAN (3):** Priority: Best Effort (default) (0), DEI: Ineligible, ID: 102.
- Internet Protocol Version 4 (2):** Src: 192.0.2.100, Dst: 198.51.100.100.
- Internet Control Message Protocol**

Wählen Sie das zweite Paket aus, und überprüfen Sie die wichtigsten Punkte:

1. Es werden nur ICMP-Echoanforderungspakete erfasst. Jedes Paket wird erfasst und zweimal angezeigt.
2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.
3. Der interne Switch fügt den zusätzlichen Port-VLAN-Tag 102 ein, der die Eingangsschnittstelle Ethernet1/2 identifiziert.

Packet capture analysis showing the same series of ICMP Echo (ping) requests. Frame 2 details (Frame 102 bytes on wire) are highlighted:

- VLAN-Tag (3):** Priority: Best Effort (default) (0), DEI: Ineligible, ID: 102.
- Internet Protocol Version 4 (2):** Src: 192.0.2.100, Dst: 198.51.100.100.
- Internet Control Message Protocol**

Öffnen Sie die Erfassungsdateien für Portchannel1-Mitgliedsschnittstellen. Wählen Sie das erste Paket aus, und überprüfen Sie die wichtigsten Punkte:

1. Es werden nur ICMP-Echoanforderungspakete erfasst. Jedes Paket wird erfasst und zweimal angezeigt.



- Der ursprüngliche Paket-Header enthält kein VLAN-Tag.
- Der interne Switch fügt ein zusätzliches Port-VLAN-Tag 1001 ein, das die Eingangsschnittstelle Port-Channel1 identifiziert.
- Der interne Switch fügt einen zusätzlichen VN-Tag ein.

Wireshark packet capture showing ICMP Echo requests. The first packet (No. 1) is highlighted with a red box. The packet details pane shows a 'VN-Tag' (802.1Q Virtual LAN) with 'ID: 1001' and 'Priority: Best Effort (default) (0)'. The 'Internet Protocol Version 4' and 'Internet Control Message Protocol' sections are also highlighted with red boxes.

Wählen Sie das zweite Paket aus, und überprüfen Sie die wichtigsten Punkte:

- Es werden nur ICMP-Echoanforderungspakete erfasst. Jedes Paket wird erfasst und zweimal angezeigt.
- Der ursprüngliche Paket-Header enthält kein VLAN-Tag.
- Der interne Switch fügt ein zusätzliches Port-VLAN-Tag 1001 ein, das die Eingangsschnittstelle Port-Channel1 identifiziert.

Wireshark packet capture showing ICMP Echo requests. The second packet (No. 2) is highlighted with a red box. The packet details pane shows a '802.1Q Virtual LAN' with 'ID: 1001' and 'Priority: Best Effort (default) (0)'. The 'Internet Protocol Version 4' and 'Internet Control Message Protocol' sections are also highlighted with red boxes.

## Erklärung

Wenn eine Paketerfassung an einer vorderen Schnittstelle konfiguriert ist, erfasst der Switch gleichzeitig jedes Paket zweimal:



- Nach dem Einfügen des Port-VLAN-Tags.
- Nach dem Einfügen des VN-Tags.

In der Reihenfolge der Vorgänge wird das VN-Tag zu einem späteren Zeitpunkt eingefügt als das Port-VLAN-Tag. In der Erfassungsdatei wird das Paket mit dem VN-Tag jedoch vor dem Paket mit dem Port-VLAN-Tag angezeigt.

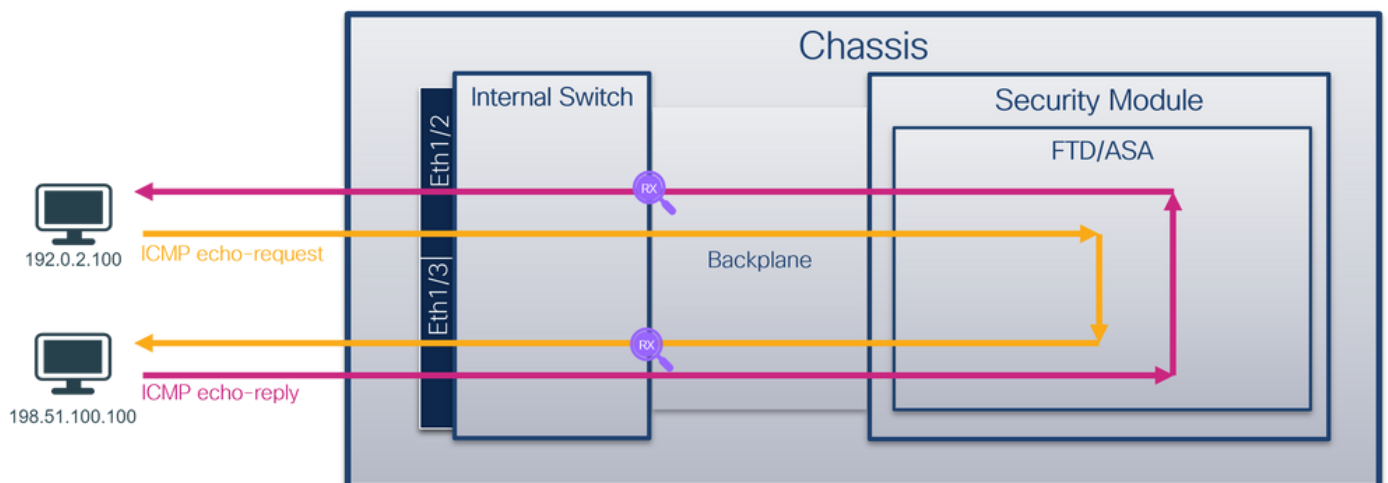
In dieser Tabelle ist die Aufgabe zusammengefasst:

Aufgabe	Erfassungspunkt	Internes Port-VLAN in erfassten Paketen	Richtung	Erfasster Datenverkehr
Konfigurieren und Überprüfen der Paketerfassung an der Schnittstelle Ethernet1/2	Ethernet1/2	102	Nur Eingang	ICMP-Echo-Anfragen von Host 192.0.2.100 an Host 198.51.100.
Konfiguration und Verifizierung der Paketerfassung an der Schnittstelle Port-Channel1 mit den Mitgliedsschnittstellen Ethernet1/4 und Ethernet1/5	Ethernet1/4 Ethernet1/5	1001	Nur Eingang	ICMP-Echo-Anfragen von Host 192.0.2.100 an Host 198.51.100.

## Paketerfassung an Backplane-Schnittstellen

Verwenden Sie den FCM und die CLI, um eine Paketerfassung an Backplane-Schnittstellen zu konfigurieren und zu überprüfen.

### Topologie, Paketfluss und Erfassungspunkte

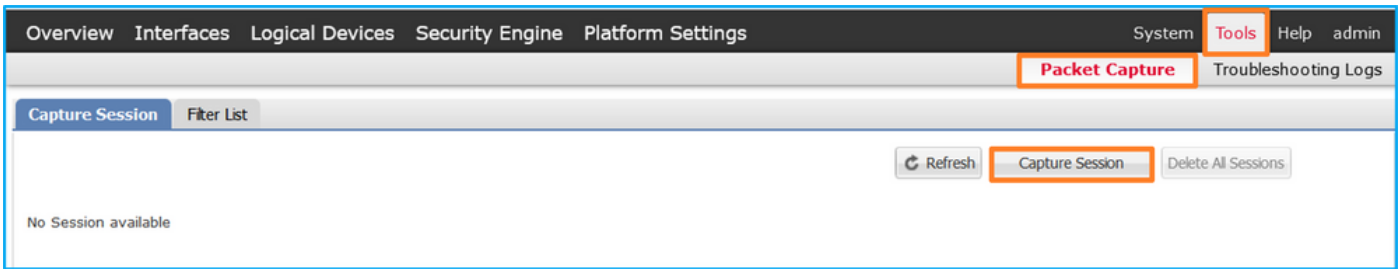


## Konfiguration

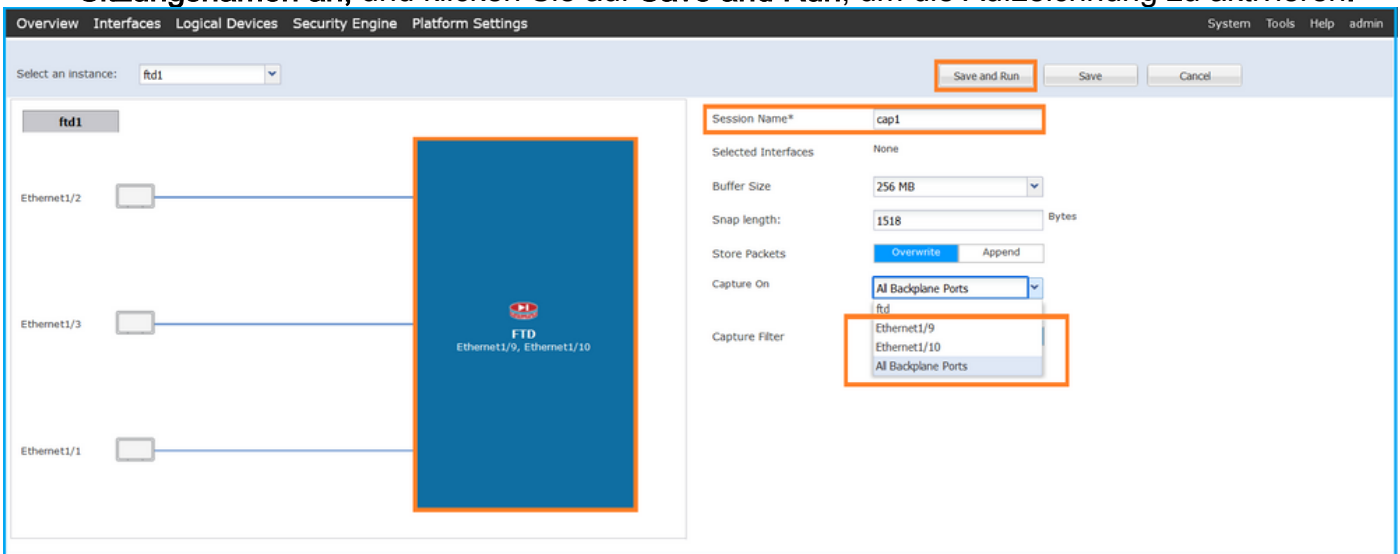
### FCM

Führen Sie die folgenden Schritte auf FCM aus, um die Paketerfassung an Backplane-Schnittstellen zu konfigurieren:

1. Verwenden Sie **Tools > Packet Capture > Capture Session**, um eine neue Erfassungssitzung zu erstellen:



2. Um Pakete auf allen Backplane-Schnittstellen zu erfassen, wählen Sie die Anwendung und anschließend **Alle Backplane-Ports** aus der **Dropdown-Liste Capture On (Erfassung auf)** aus. Sie können auch die spezifische Backplane-Schnittstelle auswählen. In diesem Fall sind die Backplane-Schnittstellen Ethernet1/9 und Ethernet1/10 verfügbar. Geben Sie den **Sitzungsnamen an**, und klicken Sie auf **Save and Run**, um die Aufzeichnung zu aktivieren:



## FXOS-CLI

Führen Sie die folgenden Schritte auf der FXOS-CLI aus, um die Paketerfassung an Backplane-Schnittstellen zu konfigurieren:

1. Identifizieren Sie den Anwendungstyp und die Kennung:

```
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. Eine Aufzeichnungssitzung erstellen:

```
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 #

```

## Verifizierung

## FCM

Überprüfen Sie den **Schnittstellennamen**, stellen Sie sicher, dass der **Betriebsstatus** aktiv ist und dass die **Dateigröße (in Byte)** ansteigt:

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

Überprüfen Sie die Erfassungsdetails in der **Paketerfassung**:

```

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

## Erfassungsdateien erfassen

Befolgen Sie die Schritte im Abschnitt **Sammeln von FirePOWER 4100/9300-internen Switch-Erfassungsdateien**.

## Analyse der Erfassungsdatei

Öffnen Sie die Erfassungsdateien mit einer Anwendung zum Lesen von Paketerfassungsdateien. Bei mehr als einer Backplane-Schnittstelle müssen alle Erfassungsdateien für jede Backplane-Schnittstelle geöffnet werden. In diesem Fall werden die Pakete an der Backplane-Schnittstelle Ethernet1/9 erfasst.

Wählen Sie das erste und das zweite Paket aus, und überprüfen Sie die Schlüsselpunkte:

1. Jedes ICMP-Echo-Anforderungspaket wird erfasst und zweimal angezeigt.
2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.
3. Der interne Switch fügt den zusätzlichen Port-VLAN-Tag **103** ein, der die Ausgangsschnittstelle Ethernet1/3 identifiziert.
4. Der interne Switch fügt einen zusätzlichen VN-Tag ein.

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	0xcc2c (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 2)
4	2022-07-14 20:20:36.514119312	198.51.100.100	192.0.2.100	ICMP	108	0xcc2c (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64
5	2022-07-14 20:20:37.537723822	192.0.2.100	198.51.100.100	ICMP	108	0x5a80 (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	0x5a80 (23040)	64	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (reply in 7)
7	2022-07-14 20:20:37.538046165	198.51.100.100	192.0.2.100	ICMP	108	0xcc9b (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 6)
8	2022-07-14 20:20:37.538048311	198.51.100.100	192.0.2.100	ICMP	108	0xcc9b (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64
9	2022-07-14 20:20:38.561776064	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (no response found!)
10	2022-07-14 20:20:38.561778310	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (reply in 11)
11	2022-07-14 20:20:38.562048288	198.51.100.100	192.0.2.100	ICMP	108	0xccca (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	0xccca (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64
13	2022-07-14 20:20:39.585677043	192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366)	64	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (no response found!)
14	2022-07-14 20:20:39.585678455	192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366)	64	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (reply in 15)
15	2022-07-14 20:20:39.585936554	198.51.100.100	192.0.2.100	ICMP	108	0xcd8d (52621)	64	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64 (request in 14)
16	2022-07-14 20:20:39.585937900	198.51.100.100	192.0.2.100	ICMP	108	0xcd8d (52621)	64	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64
17	2022-07-14 20:20:40.609804804	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (23419)	64	Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (no response found!)
18	2022-07-14 20:20:40.609807618	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (23419)	64	Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (reply in 19)
19	2022-07-14 20:20:40.610179685	198.51.100.100	192.0.2.100	ICMP	108	0xcd8f (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64 (request in 18)
20	2022-07-14 20:20:40.610181944	198.51.100.100	192.0.2.100	ICMP	108	0xcd8f (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64
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	0xccc6 (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	0xccc6 (52790)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64
25	2022-07-14 20:20:42.657709898	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (no response found!)
26	2022-07-14 20:20:42.657711660	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (reply in 27)
27	2022-07-14 20:20:42.657980675	198.51.100.100	192.0.2.100	ICMP	108	0xccc9 (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	0xccc9 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64
29	2022-07-14 20:20:43.681736697	192.0.2.100	198.51.100.100	ICMP	108	0x5c52 (23634)	64	Echo (ping) request id=0x0001, seq=22/5632, ttl=64 (no response found!)

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

```
0000 00 50 56 9d e7 50 58 97 bd b9 77 2d 89 26 00 00 ..PV.PX. .-.-&..
0010 00 0a 81 00 00 67 08 00 45 00 00 54 59 90 40 00 .....g. E..TY:@
0020 40 01 f4 1c c0 00 02 64 c6 33 64 04 00 00 22 68 @.....d :3dd..h
0030 00 01 00 0f 89 7a d0 62 00 00 00 00 b3 d7 09 00 .....z-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 .... I* $$(')*+
0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ..-./0123 4567
```



No.	Time	Source	Destination	Protocol	Length	IP ID	TTL	Info
1	2022-07-14 20:20:36.513854256	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (no response found!)
2	2022-07-14 20:20:36.513857289	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	0xccc2c (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	0xccc2c (52268)	64	Echo (ping) reply id=0x0001, 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 b9:77:2d (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
  
```

Wählen Sie das dritte und das vierte Paket aus, und überprüfen Sie die Hauptpunkte:

1. Jede ICMP-Echoantwort wird erfasst und zweimal angezeigt.
2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.
3. Der interne Switch fügt den zusätzlichen Port-VLAN-Tag 102 ein, der die Ausgangsschnittstelle Ethernet1/2 identifiziert.
4. Der interne Switch fügt einen zusätzlichen VN-Tag ein.

No.	Time	Source	Destination	Protocol	Length	IP ID	TTL	Info
1	2022-07-14 20:20:36.513854256	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (no response found!)
2	2022-07-14 20:20:36.513857289	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	0xccc2c (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	0xccc2c (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64

```

> 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
  
```

## Erklärung

Wenn eine Paketerfassung auf einer Backplane-Schnittstelle konfiguriert ist, erfasst der Switch gleichzeitig jedes Paket zweimal. In diesem Fall empfängt der interne Switch Pakete, die bereits von der Anwendung auf dem Sicherheitsmodul mit dem Port-VLAN-Tag und dem VN-Tag markiert wurden. Der VLAN-Tag identifiziert die Ausgangsschnittstelle, über die das interne Chassis die Pakete an das Netzwerk weiterleitet. Der VLAN-Tag 103 in den ICMP-Echoanforderungspaketen identifiziert Ethernet1/3 als Ausgangsschnittstelle, während der VLAN-Tag 102 in den ICMP-Echoantwortpaketen Ethernet1/2 als Ausgangsschnittstelle identifiziert. Der interne Switch entfernt den VN-Tag und den VLAN-Tag der internen Schnittstelle, bevor die Pakete an das Netzwerk weitergeleitet werden.

In dieser Tabelle ist die Aufgabe zusammengefasst:

Aufgabe	Erfassungspunkt	Internes Port-VLAN in erfassten Paketen	Richtung	Erfasster Datenverkehr
Konfiguration und Überprüfung der Paketerfassung an Backplane-Schnittstellen	Backplane-Schnittstellen	102 103	Nur Eingang	ICMP-Echo-Anfragen von Host 192.0.2.100 an Host 198.51.100.100 ICMP-Echo-Antworten von Host 198.51.100.100 zu Host 192.0.2.100

## Paketerfassung auf Anwendungs- und Anwendungs-Ports

Die Paketerfassung für Anwendungs- oder Anwendungsports wird immer an Backplane-Schnittstellen und zusätzlich an den vorderen Schnittstellen konfiguriert, wenn der Benutzer die Richtung der Anwendungserfassung angibt.

Es gibt hauptsächlich zwei Anwendungsfälle:

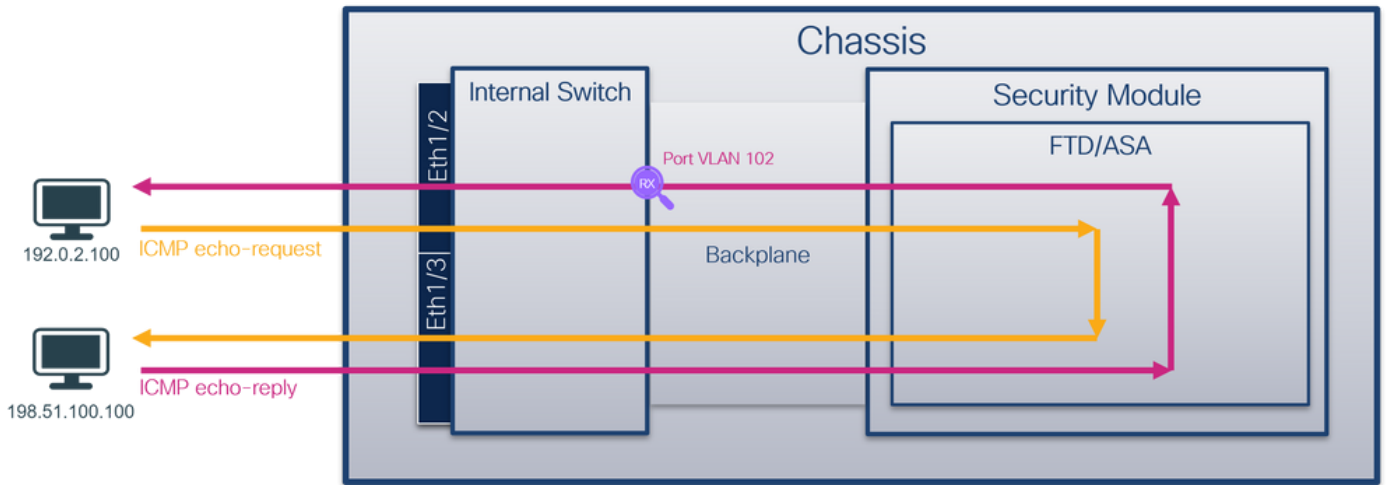
- Konfigurieren Sie die Paketerfassung an Backplane-Schnittstellen für Pakete, die eine bestimmte Front-Schnittstelle verlassen. Konfigurieren Sie beispielsweise die Paketerfassung auf der Backplane-Schnittstelle Ethernet1/9 für Pakete, die die Schnittstelle Ethernet1/2 verlassen.
- Konfigurieren Sie die gleichzeitige Paketerfassung an einer bestimmten Front- und Backplane-Schnittstelle. Konfigurieren Sie z. B. die gleichzeitige Paketerfassung an Schnittstelle Ethernet1/2 und an Rückwandschnittstelle Ethernet1/9 für Pakete, die Schnittstelle Ethernet1/2 verlassen.

Dieser Abschnitt behandelt beide Anwendungsfälle.

### Aufgabe 1

Verwenden Sie den FCM und die CLI, um eine Paketerfassung auf der Backplane-Schnittstelle zu konfigurieren und zu überprüfen. Es werden Pakete erfasst, für die der Anwendungsport Ethernet1/2 als Ausgangsschnittstelle identifiziert wird. In diesem Fall werden ICMP-Antworten erfasst.

### Topologie, Paketfluss und Erfassungspunkte

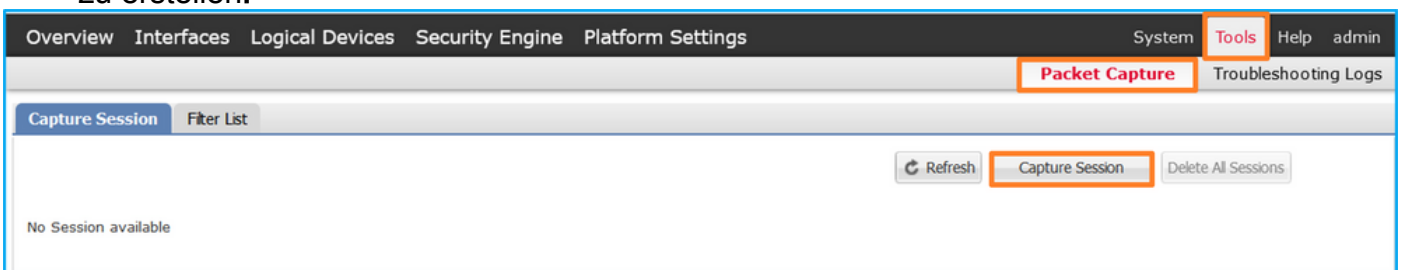


## Konfiguration

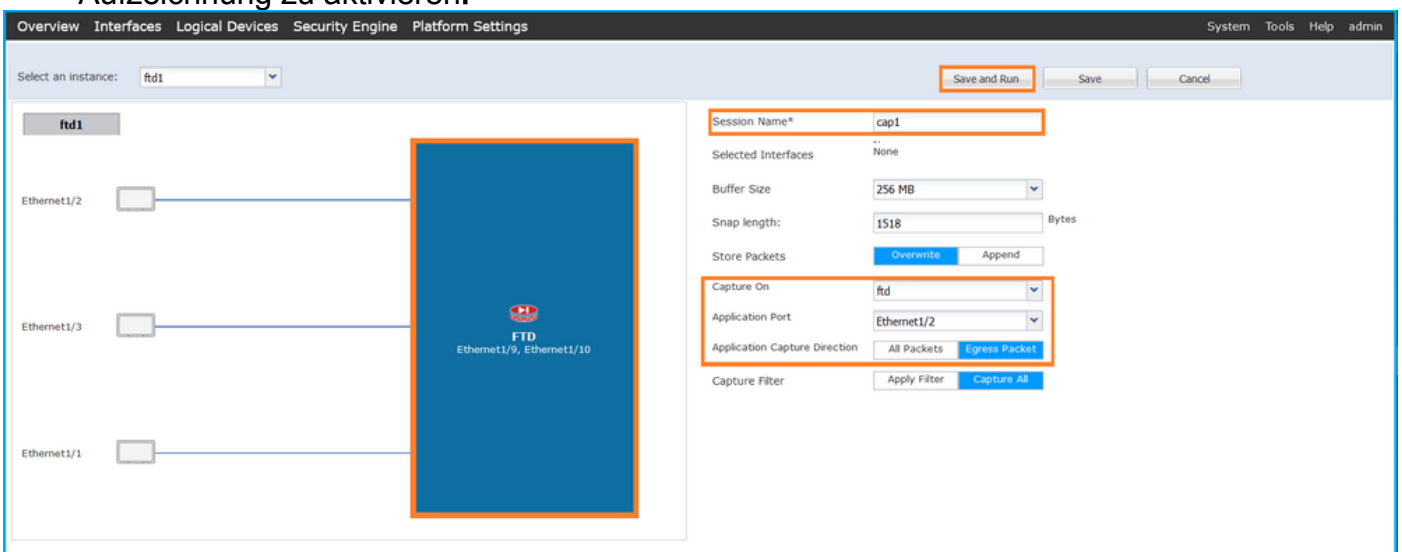
### FCM

Führen Sie die folgenden Schritte auf FCM aus, um eine Paketerfassung auf der FTD-Anwendung und dem Anwendungsport Ethernet1/2 zu konfigurieren:

1. Verwenden Sie **Tools > Packet Capture > Capture Session**, um eine neue Erfassungssitzung zu erstellen:



2. Wählen Sie die Anwendung **Ethernet1/2** in der **Anwendungsport-Dropdown-Liste** aus, und wählen Sie **Egress Packet** in **Application Capture Direction (Anwendungserfassungsrichtung)** aus. Geben Sie den **Sitzungsnamen** an, und klicken Sie auf **Save and Run**, um die Aufzeichnung zu aktivieren:



### FXOS-CLI

Führen Sie die folgenden Schritte auf der FXOS-CLI aus, um die Paketerfassung an Backplane-Schnittstellen zu konfigurieren:

1. Identifizieren Sie den Anwendungstyp und die Kennung:

```
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
```

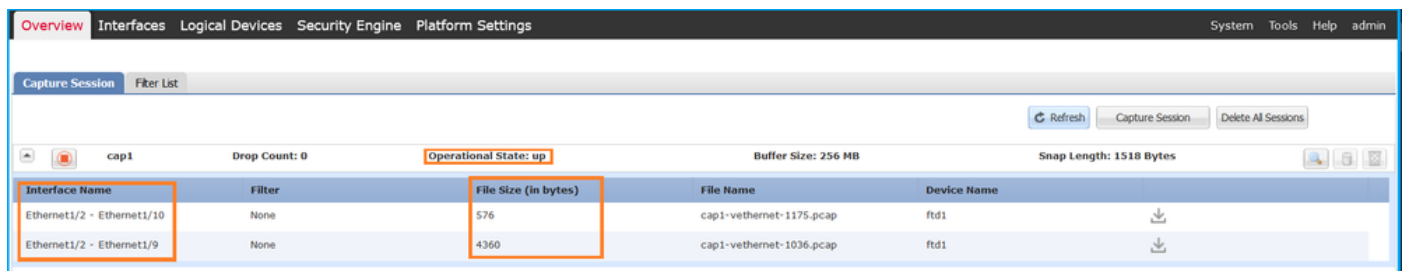
2. Eine Aufzeichnungssitzung erstellen:

```
firepower# scope packet-capture
firepower /packet-capture # create session cap1
firepower /packet-capture/session* # create app-port 1 l12 Ethernet1/2 ftd
firepower /packet-capture/session/app-port* # set app-identifier ftd1
firepower /packet-capture/session/app-port* # set filter ""
firepower /packet-capture/session/app-port* # set subinterface 0
firepower /packet-capture/session/app-port* # up
firepower /packet-capture/session* # commit
firepower /packet-capture/session #
```

## Verifizierung

## FCM

Überprüfen Sie den **Schnittstellennamen**, stellen Sie sicher, dass der **Betriebsstatus** aktiv ist und dass die **Dateigröße (in Byte)** ansteigt:



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

## FXOS-CLI

Überprüfen Sie die Erfassungsdetails in der Paketerfassung:

```
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:

## Erfassungsdateien erfassen

Befolgen Sie die Schritte im Abschnitt **Sammeln von FirePOWER 4100/9300-internen Switch-Erfassungsdateien**.

## Analyse der Erfassungsdatei

Öffnen Sie die Erfassungsdateien mit einer Anwendung zum Lesen von Paketerfassungsdateien. Bei mehreren Backplane-Schnittstellen müssen alle Erfassungsdateien für jede Backplane-Schnittstelle geöffnet werden. In diesem Fall werden die Pakete an der Backplane-Schnittstelle Ethernet1/9 erfasst.

Wählen Sie das erste und das zweite Paket aus, und überprüfen Sie die Schlüsselpunkte:

1. Jede ICMP-Echoantwort wird erfasst und zweimal angezeigt.
2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.
3. Der interne Switch fügt den zusätzlichen Port-VLAN-Tag **102 ein**, der die Ausgangsschnittstelle Ethernet1/2 identifiziert.
4. Der interne Switch fügt einen zusätzlichen VN-Tag ein.

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)

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

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

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

0000	00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00	PV...X...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 c0 c0 02 64 00 00 e3 0d 09 00	@J...3dd...d...
0030	00 12 00 01 dd a4 e7 62 00 00 00 e3 0d 09 00 00	...b...d...
0040	00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b	...e...d...
0050	1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b	...l...\$X\$()*+...
0060	2c 2d 2e 2f 30 31 32 33 34 35 36 37	.../0123 4567

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)

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

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

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

0000	00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00	PV...X...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 c0 c0 02 64 00 00 e3 0d 09 00	@J...3dd...d...
0030	00 12 00 01 dd a4 e7 62 00 00 00 e3 0d 09 00 00	...b...d...
0040	00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b	...e...d...
0050	1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b	...l...\$X\$()*+...
0060	2c 2d 2e 2f 30 31 32 33 34 35 36 37	.../0123 4567

### Erklärung

In diesem Fall ist Ethernet1/2 mit dem Port-VLAN-Tag 102 die Ausgangsschnittstelle für die ICMP-Echoantwortpakete.

Wenn die Erfassungsrichtung der Anwendung in den Erfassungsoptionen auf "Egress" (Ausgang) festgelegt ist, werden Pakete mit dem Port-VLAN-Tag 102 im Ethernet-Header an den Backplane-Schnittstellen in der Eingangsrichtung erfasst.

In dieser Tabelle ist die Aufgabe zusammengefasst:

Aufgabe	Erfassungspunkt	Internes Port-VLAN in erfassten Paketen	Richtung	Erfasster Datenverkehr
Konfiguration und Verifizierung von Erfassungen auf Anwendungs- und Anwendungsport Ethernet1/2	Backplane-Schnittstelle	102	Nur Eingang	ICMP-Echo-Antworten von Host 198.51.100.100 zu Host 192.0.2.100

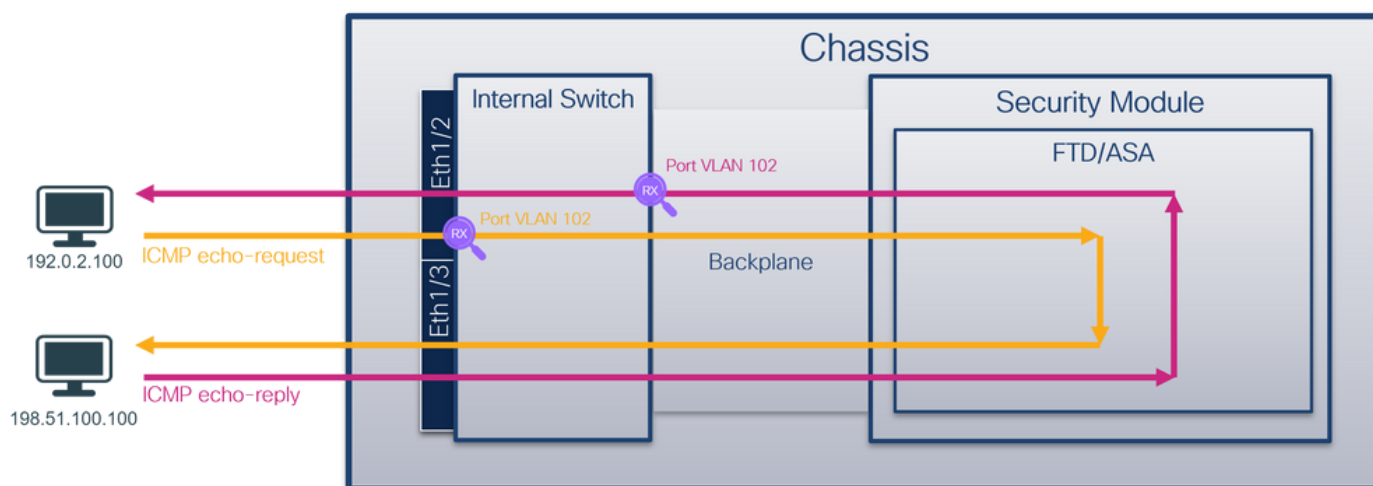
## Aufgabe 2

Verwenden Sie den FCM und die CLI, um eine Paketerfassung auf der Backplane-Schnittstelle und der Front-Schnittstelle Ethernet1/2 zu konfigurieren und zu überprüfen.

Die gleichzeitige Paketerfassung wird konfiguriert auf:

- Front-Schnittstelle - Die Pakete mit dem Port VLAN 102 an der Schnittstelle Ethernet1/2 werden erfasst. Die erfassten Pakete sind ICMP-Echo-Anfragen.
- Backplane-Schnittstellen - Pakete, bei denen Ethernet1/2 als Ausgangsschnittstelle identifiziert wird, oder Pakete mit dem Port-VLAN 102 werden erfasst. Die erfassten Pakete sind ICMP-Echoantworten.

## Topologie, Paketfluss und Erfassungspunkte

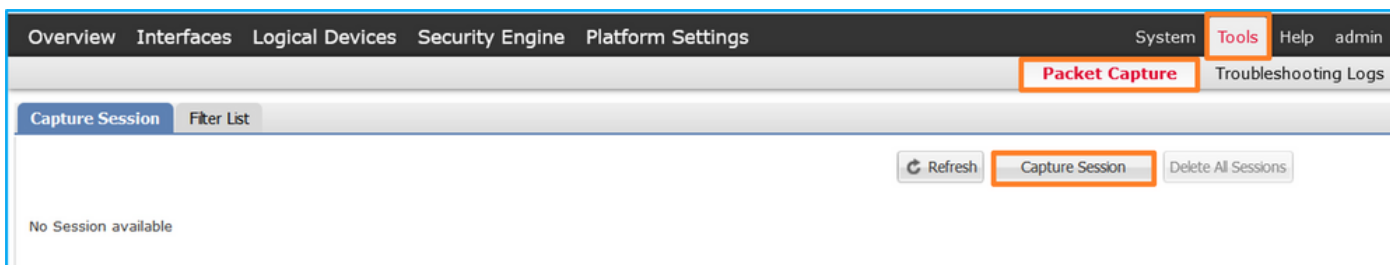


## Konfiguration

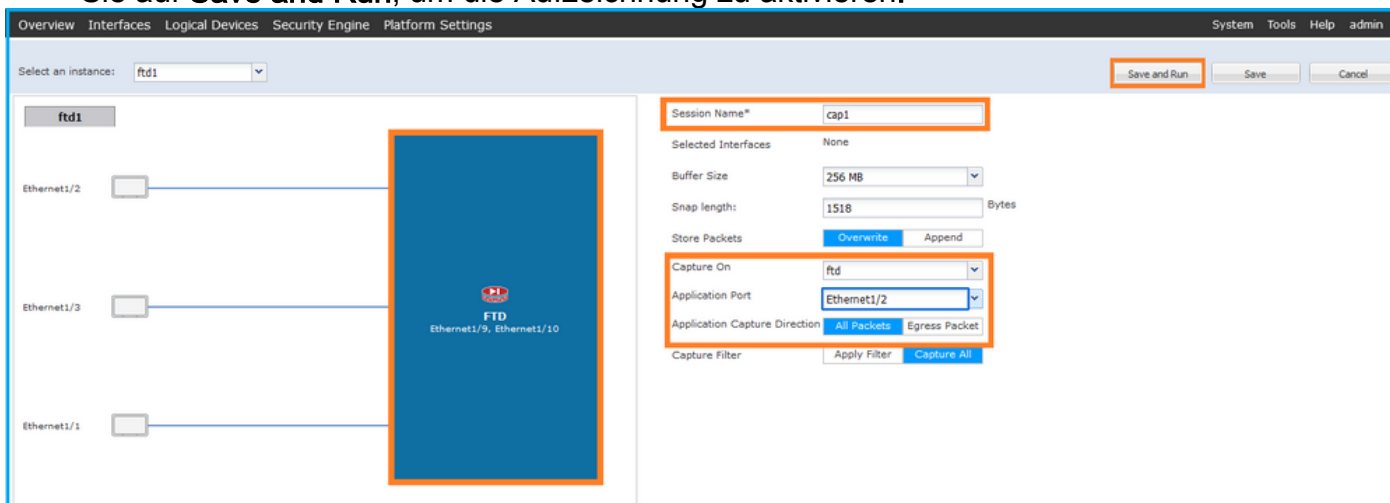
### FCM

Führen Sie die folgenden Schritte auf FCM aus, um eine Paketerfassung auf der FTD-Anwendung und dem Anwendungsport Ethernet1/2 zu konfigurieren:

1. Verwenden Sie **Tools > Packet Capture > Capture Session**, um eine neue Erfassungssitzung zu erstellen:



2. Wählen Sie die FTD-Anwendung **Ethernet1/2** in der Dropdown-Liste **Application Port (Anwendungspport)** aus, und wählen Sie **All Packets (Alle Pakete)** in **Application Capture Direction (Anwendungserfassungsrichtung)**. Geben Sie den **Sitzungsnamen** an, und klicken Sie auf **Save and Run**, um die Aufzeichnung zu aktivieren:



## FXOS-CLI

Führen Sie die folgenden Schritte auf der FXOS-CLI aus, um die Paketerfassung an Backplane-Schnittstellen zu konfigurieren:

1. Identifizieren Sie den Anwendungstyp und die Kennung:

```
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
```

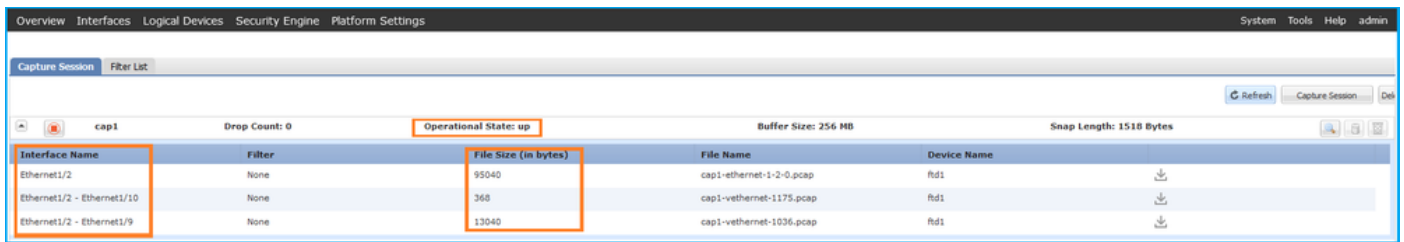
2. Eine Aufzeichnungssitzung erstellen:

```
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
```

## Verifizierung

### FCM

Überprüfen Sie den **Schnittstellennamen**, stellen Sie sicher, dass der **Betriebsstatus** aktiv ist und dass die **Dateigröße (in Byte)** ansteigt:



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

### FXOS-CLI

Überprüfen Sie die Erfassungsdetails in der **Paketerfassung**:

```
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:

### Erfassungsdateien erfassen

Befolgen Sie die Schritte im Abschnitt **Sammeln von FirePOWER 4100/9300-internen Switch-Erfassungsdateien**.

### Analyse der Erfassungsdatei

Öffnen Sie die Erfassungsdateien mit einer Anwendung zum Lesen von Paketerfassungsdateien. Bei mehreren Backplane-Schnittstellen müssen alle Erfassungsdateien für jede Backplane-Schnittstelle geöffnet werden. In diesem Fall werden die Pakete an der Backplane-Schnittstelle Ethernet1/9 erfasst.

Öffnen Sie die Erfassungsdatei für die Schnittstelle Ethernet1/2, wählen Sie das erste Paket aus, und überprüfen Sie die Schlüsselpunkte:

1. Nur ICMP-Echoanforderungspakete werden erfasst. Jedes Paket wird erfasst und zweimal angezeigt.
2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.
3. Der interne Switch fügt den zusätzlichen Port-VLAN-Tag 102 ein, der die Eingangsschnittstelle Ethernet1/2 identifiziert.
4. Der interne Switch fügt einen zusätzlichen VN-Tag ein.

No.	Time	Source	Destination	Protocol	Length	P ID	P 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	0xc00a (49326)	64	Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found)
7	2022-08-01 11:33:21.073266030	192.0.2.100	198.51.100.100	ICMP	108	0xc167 (49511)	64	Echo (ping) request id=0x0013, seq=3/768, ttl=64 (no response found)
8	2022-08-01 11:33:21.073268327	192.0.2.100	198.51.100.100	ICMP	102	0xc167 (49511)	64	Echo (ping) request id=0x0013, seq=3/768, ttl=64 (no response found)
9	2022-08-01 11:33:22.074576640	192.0.2.100	198.51.100.100	ICMP	108	0xc175 (49525)	64	Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found)
10	2022-08-01 11:33:22.074578010	192.0.2.100	198.51.100.100	ICMP	102	0xc175 (49525)	64	Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found)
11	2022-08-01 11:33:23.075779889	192.0.2.100	198.51.100.100	ICMP	108	0xc208 (49672)	64	Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found)
12	2022-08-01 11:33:23.075781513	192.0.2.100	198.51.100.100	ICMP	102	0xc208 (49672)	64	Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found)
13	2022-08-01 11:33:24.081839490	192.0.2.100	198.51.100.100	ICMP	108	0xc211 (49681)	64	Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found)
14	2022-08-01 11:33:24.081841386	192.0.2.100	198.51.100.100	ICMP	102	0xc211 (49681)	64	Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found)
15	2022-08-01 11:33:25.105806249	192.0.2.100	198.51.100.100	ICMP	108	0xc2e2 (49890)	64	Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found)
16	2022-08-01 11:33:25.105807895	192.0.2.100	198.51.100.100	ICMP	102	0xc2e2 (49890)	64	Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found)
17	2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	ICMP	108	0xc3b4 (50100)	64	Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found)
18	2022-08-01 11:33:26.129838114	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100)	64	Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found)
19	2022-08-01 11:33:27.153828653	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found)
20	2022-08-01 11:33:27.153830201	192.0.2.100	198.51.100.100	ICMP	102	0xc476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found)
21	2022-08-01 11:33:28.177847175	192.0.2.100	198.51.100.100	ICMP	108	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found)
22	2022-08-01 11:33:28.177849075	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found)
23	2022-08-01 11:33:29.201804760	192.0.2.100	198.51.100.100	ICMP	108	0xc578 (50552)	64	Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found)
24	2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	102	0xc578 (50552)	64	Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found)
25	2022-08-01 11:33:30.225834765	192.0.2.100	198.51.100.100	ICMP	108	0xc585 (50565)	64	Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found)
26	2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (50565)	64	Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found)
27	2022-08-01 11:33:31.249828955	192.0.2.100	198.51.100.100	ICMP	108	0xc618 (50712)	64	Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found)
28	2022-08-01 11:33:31.249831121	192.0.2.100	198.51.100.100	ICMP	102	0xc618 (50712)	64	Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found)
29	2022-08-01 11:33:32.273867960	192.0.2.100	198.51.100.100	ICMP	108	0xc64f (50767)	64	Echo (ping) request id=0x0013, seq=14/3584, ttl=64 (no response found)

```

c Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_1, id 0
  Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)
    VN-Tag
      1. .... = Direction: From Bridge
      .0. .... = Pointer: vif_id
      ..00 0000 0000 1010 .... = Destination: 10
      .... = Looped: No
      .... = Reserved: 0
      .... = 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
  
```

Wählen Sie das zweite Paket aus, und überprüfen Sie die wichtigsten Punkte:

- Nur ICMP-Echoanforderungspakete werden erfasst. Jedes Paket wird erfasst und zweimal angezeigt.
- Der ursprüngliche Paket-Header enthält kein VLAN-Tag.
- Der interne Switch fügt den zusätzlichen Port-VLAN-Tag 102 ein, der die Eingangsschnittstelle Ethernet1/2 identifiziert.

Packet list table showing ICMP Echo (ping) requests from 192.0.2.100 to 198.51.100.100. The first packet (No. 1) is highlighted with a red '1' and a yellow box around its IP ID field (0xc009).

Packet details for Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture\_u0\_1, id 0 Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)

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

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

Öffnen Sie die Erfassungsdatei für die Schnittstelle Ethernet1/9, wählen Sie das erste und das zweite Paket aus, und überprüfen Sie die Schlüsselpunkte:

- Jede ICMP-Echoantwort wird erfasst und zweimal angezeigt.
- Der ursprüngliche Paket-Header enthält kein VLAN-Tag.
- Der interne Switch fügt den zusätzlichen Port-VLAN-Tag 102 ein, der die Ausgangsschnittstelle Ethernet1/2 identifiziert.
- Der interne Switch fügt einen zusätzlichen VN-Tag ein.

Packet list table showing ICMP Echo (ping) replies from 198.51.100.100 to 192.0.2.100. The first packet (No. 1) is highlighted with a red '1' and a yellow box around its IP ID field (0x4f27).

Packet details for 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)

VN-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)

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



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 11:33:19.07514882	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 11:33:30.226401817	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...&amp;- 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  -@-&gt;...3dd...d...  0030  00 13 00 01 f2 b9 e7 62 00 00 00 00 cb 7f 06 00  -.....b..... 0040  00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b  -..... 0050  1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b  -.....l'm \$58'()*+ 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 .....0..... = Looped: No .....0..... = Reserved: 0 .....00..... = Version: 0 .....0000 0000 1010..... = Source: 10 Type: 802.1Q Virtual LAN (0x8100)	4	
> 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: 1Pv4 (0x0000)	3	
> Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100 > Internet Control Message Protocol	2	

## Erklärung

Wenn die Option **All Packets in the Application Capture Direction (Alle Pakete in Anwendungserfassungsrichtung)** ausgewählt ist, werden zwei gleichzeitige Paketerfassungen für den ausgewählten Anwendungsport Ethernet1/2 konfiguriert: eine Erfassung an der vorderen Schnittstelle Ethernet1/2 und eine Erfassung an ausgewählten Backplane-Schnittstellen.

Wenn eine Paketerfassung an einer vorderen Schnittstelle konfiguriert ist, erfasst der Switch gleichzeitig jedes Paket zweimal:

- Nach dem Einfügen des Port-VLAN-Tags.
- Nach dem Einfügen des VN-Tags.

In der Reihenfolge der Vorgänge wird das VN-Tag zu einem späteren Zeitpunkt eingefügt als das Port-VLAN-Tag. In der Erfassungsdatei wird das Paket mit dem VN-Tag jedoch früher angezeigt als das Paket mit dem Port-VLAN-Tag. In diesem Beispiel identifiziert der VLAN-Tag 102 in den ICMP-Echoanforderungspaketen Ethernet1/2 als Eingangsschnittstelle.

Wenn eine Paketerfassung auf einer Backplane-Schnittstelle konfiguriert ist, erfasst der Switch gleichzeitig jedes Paket zweimal. Der interne Switch empfängt Pakete, die bereits von der Anwendung auf dem Sicherheitsmodul mit dem Port-VLAN-Tag und dem VN-Tag markiert wurden. Der Port-VLAN-Tag identifiziert die Ausgangsschnittstelle, über die das interne Chassis die Pakete an das Netzwerk weiterleitet. In diesem Beispiel identifiziert der VLAN-Tag 102 in ICMP-Echo-Antwort-Paketen Ethernet1/2 als Ausgangsschnittstelle.

Der interne Switch entfernt den VN-Tag und den VLAN-Tag der internen Schnittstelle, bevor die Pakete an das Netzwerk weitergeleitet werden.

In dieser Tabelle ist die Aufgabe zusammengefasst:

<b>Aufgabe</b>	<b>Erfassungspunkt</b>	<b>Internes Port-VLAN in erfassten Paketen</b>	<b>Richtung</b>	<b>Erfasster Datenverkehr</b>
----------------	------------------------	--	-----------------	-------------------------------

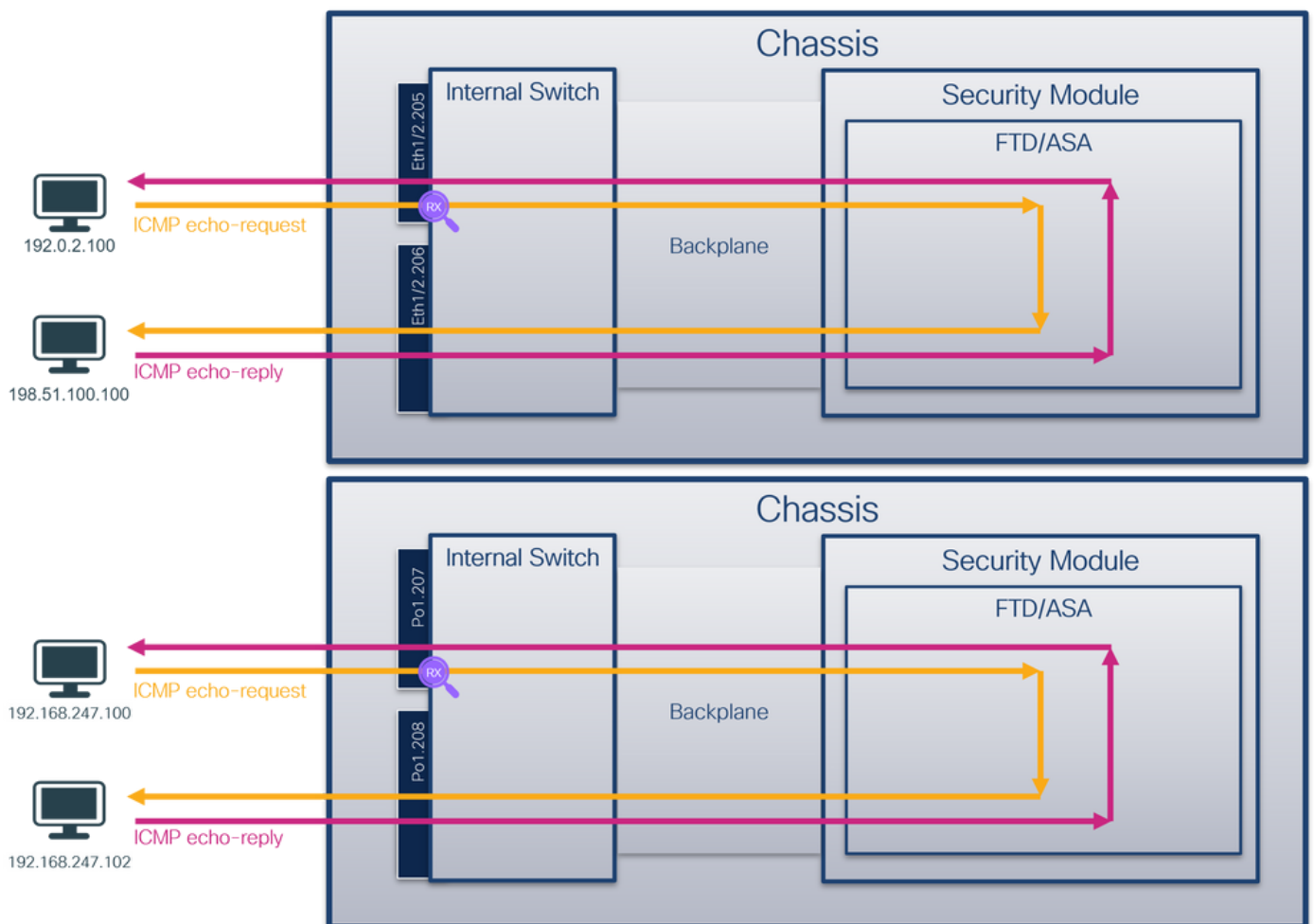


Konfiguration und Verifizierung von Erfassungen auf Anwendungs- und Anwendungspport Ethernet1/2	Backplane-Schnittstelle n Schnittstelle Ethernet1/2	102  102	Nur Eingang  Nur Eingang	ICMP-Echo-Antworten von Host 198.51.100.100 zu Host 192.0.2.100 ICMP-Echo-Anfragen von Host 192.0.2.100 an Host 198.51.100.100
---	---	----------------	--------------------------------	---

## Paketerfassung auf einer Subchnittstelle einer physischen oder Port-Channel-Schnittstelle

Verwenden Sie FCM und CLI, um eine Paketerfassung an der Subchnittstelle Ethernet1/2.205 oder der Port-Channel-Subchnittstelle Port-Channel1.207 zu konfigurieren und zu überprüfen. Subchnittstellen und Erfassungen an Subchnittstellen werden nur für die FTD-Anwendung im Containermodus unterstützt. In diesem Fall wird eine Paketerfassung auf Ethernet1/2.205 und Port-Channel1.207 konfiguriert.

### Topologie, Paketfluss und Erfassungspunkte



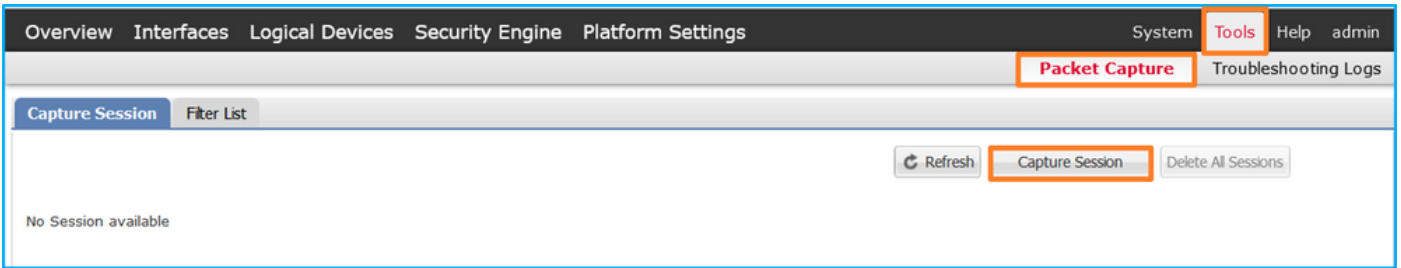
## Konfiguration

### FCM

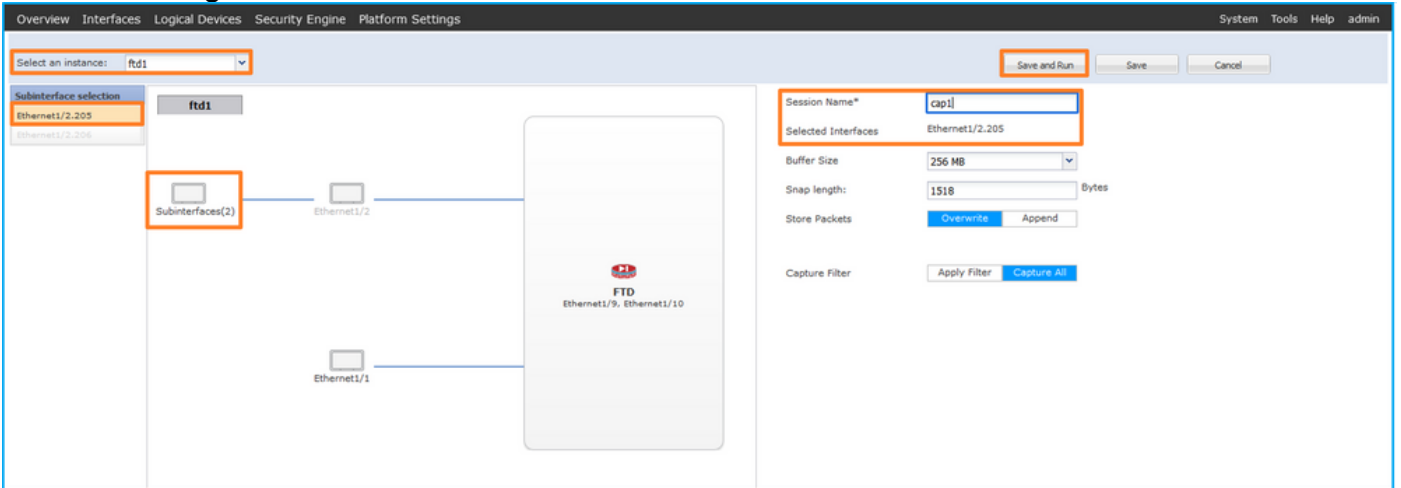
Führen Sie die folgenden Schritte auf FCM aus, um eine Paketerfassung auf der FTD-Anwendung und dem Anwendungspport Ethernet1/2 zu konfigurieren:

1. Verwenden Sie **Tools > Packet Capture > Capture Session**, um eine neue Erfassungssitzung

zu erstellen:



2. Wählen Sie die spezifische Anwendungsinstanz ftd1, die Subschnittstelle Ethernet1/2.205, geben Sie den Sitzungsnamen an, und klicken Sie auf **Speichern und Ausführen**, um die Erfassung zu aktivieren:



3. Im Fall einer Port-Channel-Subschnittstelle sind aufgrund der Cisco Bug-ID [CSCVq3119](https://www.cisco.com/cisco/web/bugtools/bugdetail.do?bugs=CSCVq3119)-Subschnittstellen im FCM nicht sichtbar. Verwenden Sie die FXOS-CLI, um Erfassungen auf Port-Channel-Subschnittstellen zu konfigurieren.

## FXOS-CLI

Befolgen Sie diese Schritte auf der FXOS-CLI, um eine Paketerfassung an den Subschnittstellen Ethernet1/2.205 und Port-Channel1.207 zu konfigurieren:

1. Identifizieren Sie den Anwendungstyp und die Kennung:

```
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. Geben Sie bei einer Port-Channel-Schnittstelle deren Mitgliedsschnittstellen an:

```
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. Eine Aufzeichnungssitzung erstellen:

```
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 #
```

Erstellen Sie für Port-Channel-Subschnittstellen eine Paketerfassung für jede Port-Channel-Member-Schnittstelle:

```
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 #
```

### Verifizierung

### FCM

Überprüfen Sie den **Schnittstellennamen**, stellen Sie sicher, dass der **Betriebsstatus** aktiv ist und dass die **Dateigröße (in Byte)** ansteigt:



Port-Channel-Subschnittstellenerfassungen, die auf FXOS CLI konfiguriert wurden, sind auch auf FCM sichtbar. Sie können jedoch nicht bearbeitet werden:

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

Überprüfen Sie die Erfassungsdetails in der Paketerfassung:

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

Traffic Monitoring Session:

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

Physical ports involved in Packet Capture:

```
Slot Id: 1
Port Id: 2
Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap
Pcapsize: 9324 bytes
Filter:
Sub Interface: 205
Application Instance Identifier: ftd1
Application Name: ftd
```

Port-Channel 1 mit den Mitgliedsschnittstellen Ethernet1/3 und 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

```

## Erfassungsdateien erfassen

Befolgen Sie die Schritte im Abschnitt **Sammeln von FirePOWER 4100/9300-internen Switch-Erfassungsdateien**.

## Analyse der Erfassungsdatei

Öffnen Sie die Erfassungsdatei mit einer Anwendung zum Lesen von Paketerfassungsdateien. Wählen Sie das erste Paket aus, und überprüfen Sie die wichtigsten Punkte:

1. Nur ICMP-Echoanforderungspakete werden erfasst. Jedes Paket wird erfasst und zweimal angezeigt.
2. Der ursprüngliche Paket-Header hat den VLAN-Tag **205**.
3. Der interne Switch fügt den zusätzlichen Port-VLAN-Tag **102** ein, der die Eingangsschnittstelle Ethernet1/2 identifiziert.
4. Der interne Switch fügt einen zusätzlichen VN-Tag ein.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-04 07:21:56.993302182	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 07:22:08.229940829	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 07:22:16.389975120	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	0xa1de (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)
  0000  a2 76 f2 00 00 1b 00 50 5d 9d e8 be 89 26 80 54  -v---IPV---&T
  0010  00 00 81 00 00 66 81 00 00 cd 08 00 45 00 00 54  -...f...E-T
  0020  95 74 40 00 40 01 b8 38 c0 00 02 64 c6 33 64 64  -t@-8--d3dd
  0030  00 00 eb 95 00 22 00 01 80 73 eb 62 00 00 00 00  -...-s-b...
  0040  d9 9d 00 00 00 00 00 10 11 12 13 14 15 16 17  -...-s-b...
  0050  18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27  -...-!*$%&'
  0060  28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37  -()*+,-./01234567

```

```

> VN-Tag
  1... .. = Direction: From Bridge
  .0... .. = Pointer: vif_id
  ..00 0000 0101 0100 .. = Destination: 84
  .. = Looped: No
  .. = Reserved: 0
  ..0... .. = Version: 0
  .... .. 0000 0000 0000 = Source: 0
  Type: 802.1Q Virtual LAN (0x8100)
  > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
  000... .. = Priority: Best Effort (default) (0)
  ...0 .. = DEI: Ineligible
  ... 0000 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

```



Wählen Sie das zweite Paket aus, und überprüfen Sie die wichtigsten Punkte:

1. Nur ICMP-Echoanforderungspakete werden erfasst. Jedes Paket wird erfasst und zweimal angezeigt.
2. Der ursprüngliche Paket-Header hat den VLAN-Tag 205.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-04 07:21:56.993302102	192.0.2.100	198.51.100.100	ICMP	112	0x9574 (38260)	64	Echo (ping) request id=0x0022, seq=1/256, ttl=64 (no response found!)
2	2022-08-04 07:21:56.993303597	192.0.2.100	198.51.100.100	ICMP	102	0x9574 (38260)	64	Echo (ping) request id=0x0022, seq=1/256, ttl=64 (no response found!)
3	2022-08-04 07:22:06.214264777	192.0.2.100	198.51.100.100	ICMP	112	0x9a81 (39553)	64	Echo (ping) request id=0x0022, seq=10/2560, ttl=64 (no response found!)
4	2022-08-04 07:22:06.214267373	192.0.2.100	198.51.100.100	ICMP	102	0x9a81 (39553)	64	Echo (ping) request id=0x0022, seq=10/2560, ttl=64 (no response found!)
5	2022-08-04 07:22:07.215113393	192.0.2.100	198.51.100.100	ICMP	112	0x9ac3 (39619)	64	Echo (ping) request id=0x0022, seq=11/2816, ttl=64 (no response found!)
6	2022-08-04 07:22:07.215115445	192.0.2.100	198.51.100.100	ICMP	102	0x9ac3 (39619)	64	Echo (ping) request id=0x0022, seq=11/2816, ttl=64 (no response found!)
7	2022-08-04 07:22:08.229938577	192.0.2.100	198.51.100.100	ICMP	112	0x9b33 (39731)	64	Echo (ping) request id=0x0022, seq=12/3072, ttl=64 (no response found!)
8	2022-08-04 07:22:08.229940829	192.0.2.100	198.51.100.100	ICMP	102	0x9b33 (39731)	64	Echo (ping) request id=0x0022, seq=12/3072, ttl=64 (no response found!)
9	2022-08-04 07:22:09.253944601	192.0.2.100	198.51.100.100	ICMP	112	0x9c0e (39950)	64	Echo (ping) request id=0x0022, seq=13/3328, ttl=64 (no response found!)
10	2022-08-04 07:22:09.253946899	192.0.2.100	198.51.100.100	ICMP	102	0x9c0e (39950)	64	Echo (ping) request id=0x0022, seq=13/3328, ttl=64 (no response found!)
11	2022-08-04 07:22:10.277953070	192.0.2.100	198.51.100.100	ICMP	112	0x9ccb (40139)	64	Echo (ping) request id=0x0022, seq=14/3584, ttl=64 (no response found!)
12	2022-08-04 07:22:10.277954736	192.0.2.100	198.51.100.100	ICMP	102	0x9ccb (40139)	64	Echo (ping) request id=0x0022, seq=14/3584, ttl=64 (no response found!)
13	2022-08-04 07:22:11.301931282	192.0.2.100	198.51.100.100	ICMP	112	0x9d84 (40324)	64	Echo (ping) request id=0x0022, seq=15/3840, ttl=64 (no response found!)
14	2022-08-04 07:22:11.301933600	192.0.2.100	198.51.100.100	ICMP	102	0x9d84 (40324)	64	Echo (ping) request id=0x0022, seq=15/3840, ttl=64 (no response found!)
15	2022-08-04 07:22:12.325936521	192.0.2.100	198.51.100.100	ICMP	112	0x9da2 (40354)	64	Echo (ping) request id=0x0022, seq=16/4096, ttl=64 (no response found!)
16	2022-08-04 07:22:12.325937895	192.0.2.100	198.51.100.100	ICMP	102	0x9da2 (40354)	64	Echo (ping) request id=0x0022, seq=16/4096, ttl=64 (no response found!)
17	2022-08-04 07:22:13.326988040	192.0.2.100	198.51.100.100	ICMP	112	0x9e07 (40455)	64	Echo (ping) request id=0x0022, seq=17/4352, ttl=64 (no response found!)
18	2022-08-04 07:22:13.326990258	192.0.2.100	198.51.100.100	ICMP	102	0x9e07 (40455)	64	Echo (ping) request id=0x0022, seq=17/4352, ttl=64 (no response found!)
19	2022-08-04 07:22:14.341944773	192.0.2.100	198.51.100.100	ICMP	112	0x9e6a (40554)	64	Echo (ping) request id=0x0022, seq=18/4608, ttl=64 (no response found!)
20	2022-08-04 07:22:14.341946249	192.0.2.100	198.51.100.100	ICMP	102	0x9e6a (40554)	64	Echo (ping) request id=0x0022, seq=18/4608, ttl=64 (no response found!)
21	2022-08-04 07:22:15.365941588	192.0.2.100	198.51.100.100	ICMP	112	0x9efb (40699)	64	Echo (ping) request id=0x0022, seq=19/4864, ttl=64 (no response found!)
22	2022-08-04 07:22:15.365942566	192.0.2.100	198.51.100.100	ICMP	102	0x9efb (40699)	64	Echo (ping) request id=0x0022, seq=19/4864, ttl=64 (no response found!)
23	2022-08-04 07:22:16.389973843	192.0.2.100	198.51.100.100	ICMP	112	0x9f68 (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	0x9f68 (40936)	64	Echo (ping) request id=0x0022, seq=20/5120, ttl=64 (no response found!)
25	2022-08-04 07:22:17.413936452	192.0.2.100	198.51.100.100	ICMP	112	0xa079 (41081)	64	Echo (ping) request id=0x0022, seq=21/5376, ttl=64 (no response found!)
26	2022-08-04 07:22:17.413938090	192.0.2.100	198.51.100.100	ICMP	102	0xa079 (41081)	64	Echo (ping) request id=0x0022, seq=21/5376, ttl=64 (no response found!)
27	2022-08-04 07:22:18.437954335	192.0.2.100	198.51.100.100	ICMP	112	0xa11e (41246)	64	Echo (ping) request id=0x0022, seq=22/5632, ttl=64 (no response found!)

```

> Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture_u0_1, id 0
  Ethernet II, Src: VMware 9d:1e:8b (00:50:56:9d:e8:8b), Dst: a2:76:f2:00:00:1b (a2:76:f2:00:00:1b)
  802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 205
  0000  ....  ....  = 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
  
```

Öffnen Sie nun die Capture-Dateien für Portchannel1.207. Wählen Sie das erste Paket und überprüfen Sie die Schlüsselpunkte

1. Nur ICMP-Echoanforderungspakete werden erfasst. Jedes Paket wird erfasst und zweimal angezeigt.
2. Der ursprüngliche Paket-Header hat den VLAN-Tag 207.
3. Der interne Switch fügt ein zusätzliches Port-VLAN-Tag 1001 ein, das die Eingangsschnittstelle Port-Channel1 identifiziert.
4. Der interne Switch fügt einen zusätzlichen VN-Tag ein.

Wireshark capture showing a series of ICMP Echo (ping) requests from 192.168.247.100 to 192.168.247.102. The packets are numbered 1 through 27. The first packet is selected.

Packet details for Frame 1:

- Ethernet II, Src: Cisco d8:ec:00 (00:17:df:d6:ec:00), Dst: a2:76:f2:00:00:1c (a2:76:f2:00:00:1c)
- VN-Tag
  - . . . . . = Direction: From Bridge
  - . 0. . . . . = Pointer: vif\_id
  - .. 00 0000 0011 1101 . . . . . = Destination: 61
  - . . . . . = Looped: No
  - . . . . . = Reserved: 0
  - . . . . . = Version: 0
  - . . . . . = Source: 0
  - Type: 802.1Q Virtual LAN (0x8100)
- 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1001
  - 000. . . . . = Priority: Best Effort (default) (0)
  - .. 0 . . . . . = DEI: Ineligible
  - ... 0011 1110 1001 = ID: 1001
  - Type: 802.1Q Virtual LAN (0x8100)
- 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 207
  - 000. . . . . = Priority: Best Effort (default) (0)
  - .. 0 . . . . . = DEI: Ineligible
  - ... 0000 1100 1111 = ID: 207
  - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.247.100, Dst: 192.168.247.102
- Internet Control Message Protocol

Wählen Sie das zweite Paket aus, und überprüfen Sie die wichtigsten Punkte:

- Nur ICMP-Echoanforderungspakete werden erfasst. Jedes Paket wird erfasst und zweimal angezeigt.
- Der ursprüngliche Paket-Header hat den VLAN-Tag 207.

Wireshark capture showing a series of ICMP Echo (ping) requests. The second packet is selected.

Packet details for Frame 2:

- Ethernet II, Src: Cisco d8: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

## Erklärung

Wenn eine Paketfassung an einer vorderen Schnittstelle konfiguriert ist, erfasst der Switch gleichzeitig jedes Paket zweimal:

- Nach dem Einfügen des Port-VLAN-Tags.
- Nach dem Einfügen des VN-Tags.

In der Reihenfolge der Vorgänge wird das VN-Tag zu einem späteren Zeitpunkt eingefügt als das Port-VLAN-Tag. In der Erfassungsdatei wird das Paket mit dem VN-Tag jedoch früher angezeigt als das Paket mit dem Port-VLAN-Tag. Außerdem enthält bei Subschnittstellen in den Erfassungsdateien jedes zweite Paket nicht den Port-VLAN-Tag.

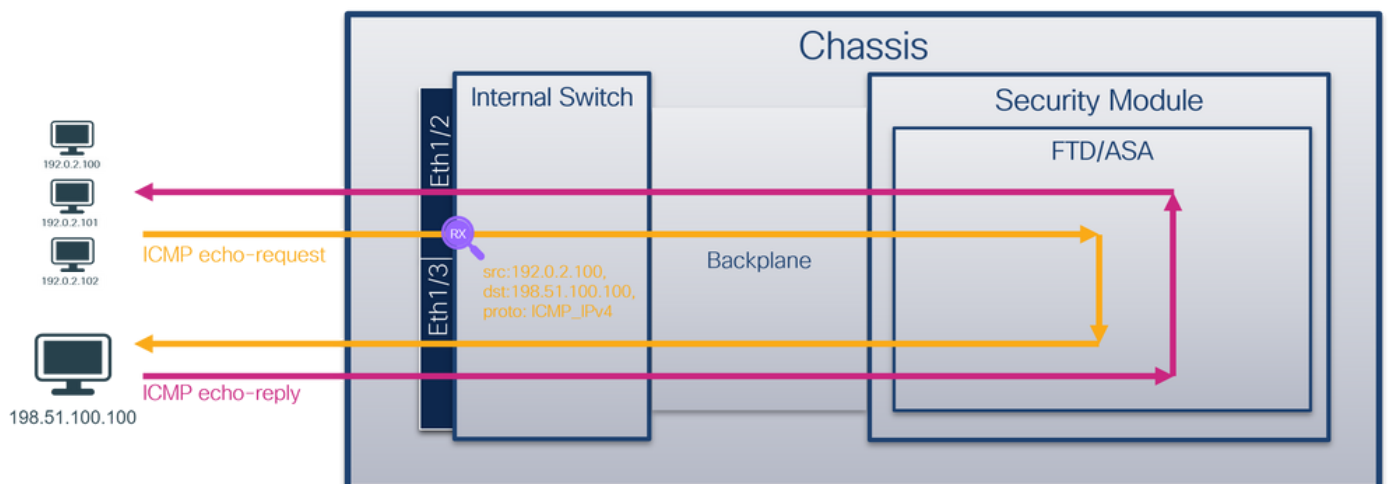
In dieser Tabelle ist die Aufgabe zusammengefasst:

Aufgabe	Erfassungspunkt	Internes Port-VLAN in erfassten Paketen	Richtung	Erfasster Datenverkehr
Konfiguration und Verifizierung einer Paketerfassung an der Subschnittstelle Ethernet1/2.205	Ethernet1/2.205	102	Nur Eingang	ICMP-Echo-Anfragen von Host 192.0.2.100 an Host 198.51.100
Konfiguration und Verifizierung der Paketerfassung an der Port-Channel-Subschnittstelle mit den Mitgliedsschnittstellen Ethernet1/3 und Ethernet1/4	Ethernet1/3 Ethernet1/4	1001	Nur Eingang	ICMP-Echo-Anfragen von 192.168.207.100 an Host 192.168.207.102

## Paketerfassungsfilter

Verwenden Sie den FCM und die CLI, um eine Paketerfassung an der Schnittstelle Ethernet1/2 mit einem Filter zu konfigurieren und zu überprüfen.

### Topologie, Paketfluss und Erfassungspunkte



## Konfiguration

### FCM

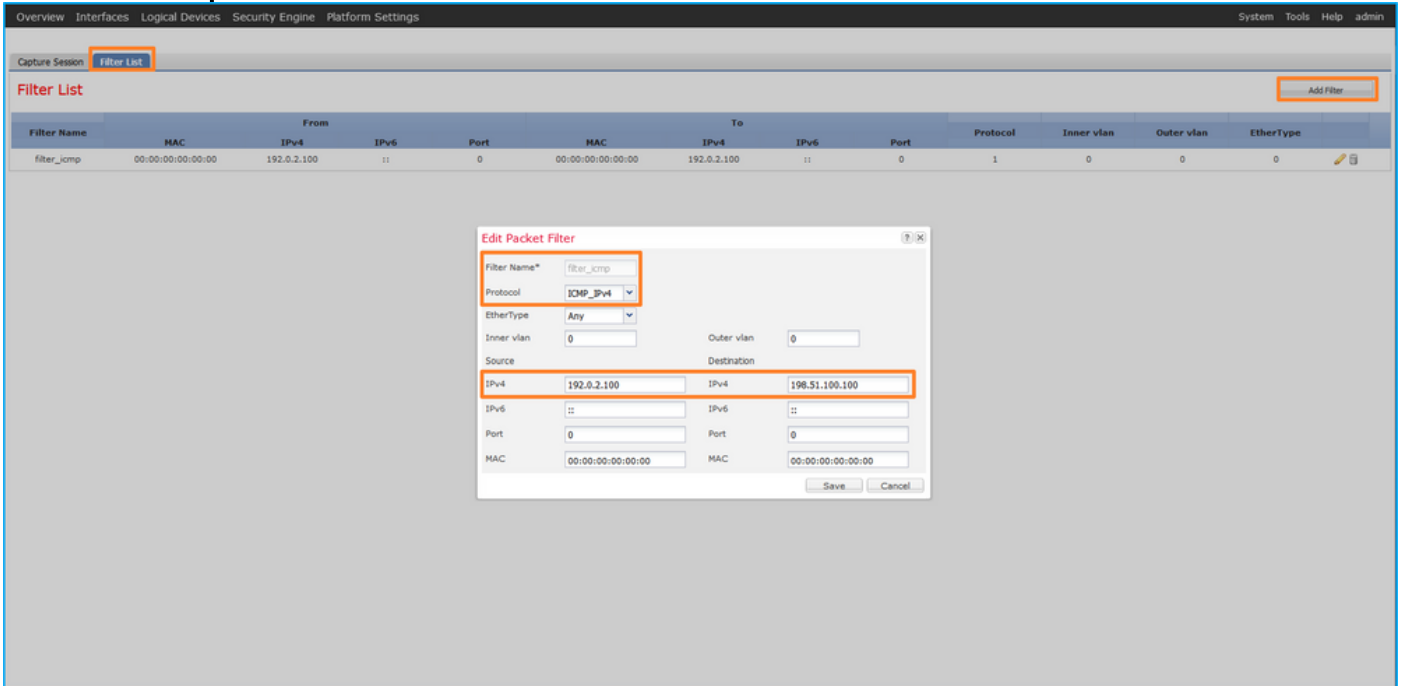
Führen Sie die folgenden Schritte auf FCM aus, um einen Erfassungsfilter für ICMP-Echo-Anforderungspakete vom Host 192.0.2.100 zum Host 198.51.100.100 zu konfigurieren und ihn auf die Paketerfassung an der Schnittstelle Ethernet1/2 anzuwenden:

1. Verwenden Sie **Extras > Paketerfassung > Filterliste > Filter hinzufügen**, um einen

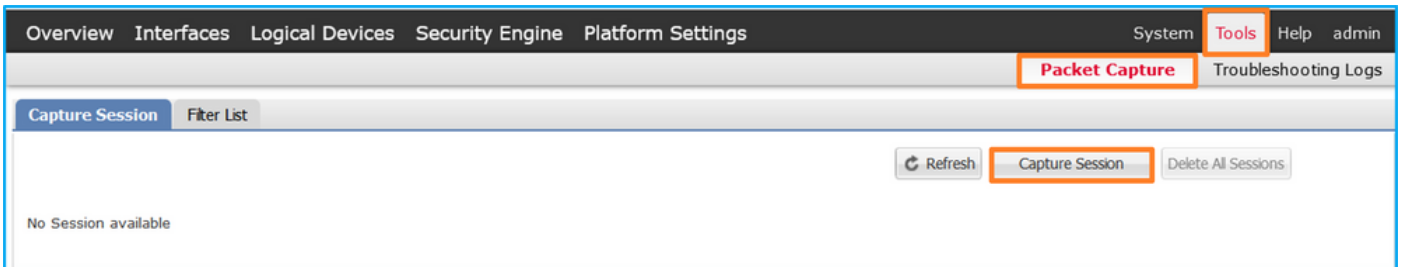


Erfassungsfiler zu erstellen.

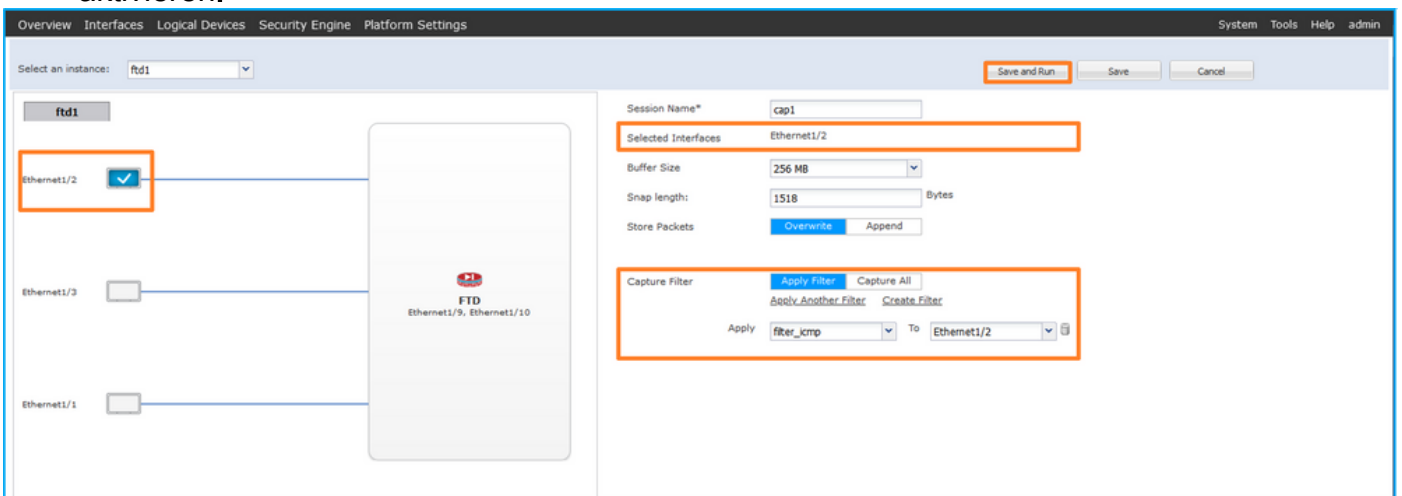
2. Geben Sie den **Filternamen**, das **Protokoll**, die **Quell-IPv4** und die **Ziel-IPv4** an, und klicken Sie auf **Speichern**:



3. Verwenden Sie **Tools > Packet Capture > Capture Session**, um eine neue Erfassungssitzung zu erstellen:



4. Wählen Sie **Ethernet1/2** aus, geben Sie den **Sitzungsnamen** an, wenden Sie den Erfassungsfiler an, und klicken Sie auf **Speichern und ausführen**, um die Erfassung zu aktivieren:



## FXOS-CLI

Führen Sie die folgenden Schritte auf der FXOS-CLI aus, um die Paketerfassung an Backplane-

Schnittstellen zu konfigurieren:

1. Identifizieren Sie den Anwendungstyp und die Kennung:

```
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. Geben Sie die IP-Protokollnummer in <https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>. In diesem Fall ist die ICMP-Protokollnummer 1.

3. Erstellen Sie eine Erfassungssitzung:

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 #
```

Verifizierung

FCM

Überprüfen Sie den **Schnittstellennamen**, stellen Sie sicher, dass der **Betriebsstatus** aktiv ist und dass die **Dateigröße (in Byte)** ansteigt:

Filter Name	MAC	From IPv4	IPv6	Port	MAC	To IPv4	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

Überprüfen Sie den Schnittstellennamen, den **Filter**, stellen Sie sicher, dass der **Betriebsstatus** aktiv ist, und erhöhen Sie die **Dateigröße (in Byte)** unter **Tools > 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	ftd1

## FXOS-CLI

Überprüfen Sie die Erfassungsdetails in der Paketerfassung:

```
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
```

## Erfassungsdateien erfassen

Befolgen Sie die Schritte im Abschnitt **Sammeln von FirePOWER 4100/9300-internen Switch-Erfassungsdateien**.

## Analyse der Erfassungsdatei

Öffnen Sie die Erfassungsdatei mit einer Anwendung zum Lesen von Paketerfassungsdateien. Erstes Paket auswählen und Schlüsselpunkte prüfen

1. Nur ICMP-Echoanforderungspakete werden erfasst. Jedes Paket wird erfasst und zweimal angezeigt.
2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.

3. Der interne Switch fügt den zusätzlichen Port-VLAN-Tag 102 ein, der die Eingangsschnittstelle Ethernet1/2 identifiziert.

4. Der interne Switch fügt einen zusätzlichen VN-Tag ein.

The image shows a Wireshark packet capture of ICMP Echo requests. The packet list pane shows 20 packets, with packet 2 selected. The packet details pane for packet 2 is expanded to show the following layers:

- VN-Tag** (802.1Q Virtual LAN):
  - Priority: Best Effort (default) (0)
  - DEI: Ineligible
  - ID: 102
- Internet Protocol Version 4**:
  - Src: 192.0.2.100
  - Dst: 198.51.100.100
- Internet Control Message Protocol**

Orange boxes highlight the following fields in the details pane:

- 2**: Internet Protocol Version 4 (Protocol)
- 3**: 802.1Q Virtual LAN, ID: 102
- 4**: VN-Tag, DEI: Ineligible

Wählen Sie das zweite Paket aus, und überprüfen Sie die wichtigsten Punkte:

1. Nur ICMP-Echoanforderungspakete werden erfasst. Jedes Paket wird erfasst und zweimal angezeigt.
2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.
3. Der interne Switch fügt den zusätzlichen Port-VLAN-Tag 102 ein, der die Eingangsschnittstelle Ethernet1/2 identifiziert.

The image shows a Wireshark packet capture of ICMP Echo requests. The packet list pane shows 20 packets, with packet 2 selected. The packet details pane for packet 2 is expanded to show the following layers:

- VN-Tag** (802.1Q Virtual LAN):
  - Priority: Best Effort (default) (0)
  - DEI: Ineligible
  - ID: 102
- Internet Protocol Version 4**:
  - Src: 192.0.2.100
  - Dst: 198.51.100.100
- Internet Control Message Protocol**

Orange boxes highlight the following fields in the details pane:

- 2**: Internet Control Message Protocol
- 3**: 802.1Q Virtual LAN, ID: 102
- 4**: Internet Protocol Version 4 (Protocol)

## Erklärung

Wenn eine Paketfassung an einer vorderen Schnittstelle konfiguriert ist, erfasst der Switch

gleichzeitig jedes Paket zweimal:

- Nach dem Einfügen des Port-VLAN-Tags.
- Nach dem Einfügen des VN-Tags.

In der Reihenfolge der Vorgänge wird das VN-Tag zu einem späteren Zeitpunkt eingefügt als das Port-VLAN-Tag. In der Erfassungsdatei wird das Paket mit dem VN-Tag jedoch früher angezeigt als das Paket mit dem Port-VLAN-Tag.

Wenn ein Erfassungsfiler angewendet wird, werden nur die Pakete erfasst, die mit dem Filter in Eingangsrichtung übereinstimmen.

In dieser Tabelle ist die Aufgabe zusammengefasst:

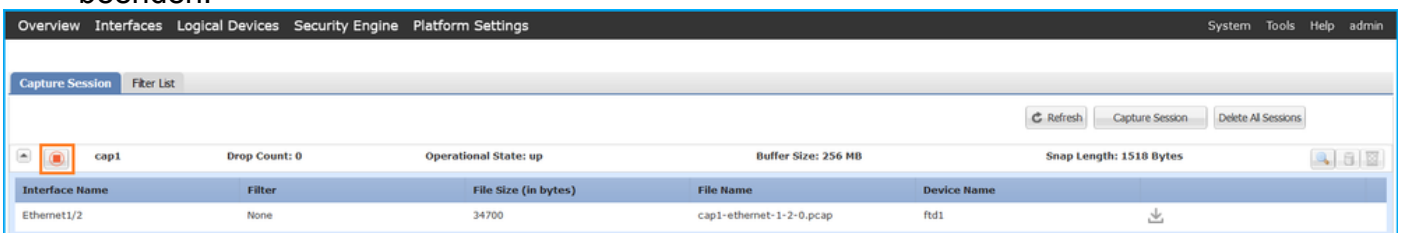
Aufgabe	Erfassungspunkt	Internes Port-VLAN in erfassten Paketen	Richtung	Benutzerfilter	Erfasster Datenverkehr
Konfigurieren und Überprüfen einer Paketerfassung mit einem Filter an der vorderen Schnittstelle "Ethernet1/2"	Ethernet1/2	102	Nur Eingang	Protokolle: ICMP Quelle: 192.0.2.100 Ziel: 198.51.100.100	ICMP-Echo-Anfragen von Host 192.0.2.100 an Host 198.51.100.100

## Sammeln von FirePOWER 4100/9300-internen Switch-Erfassungsdateien

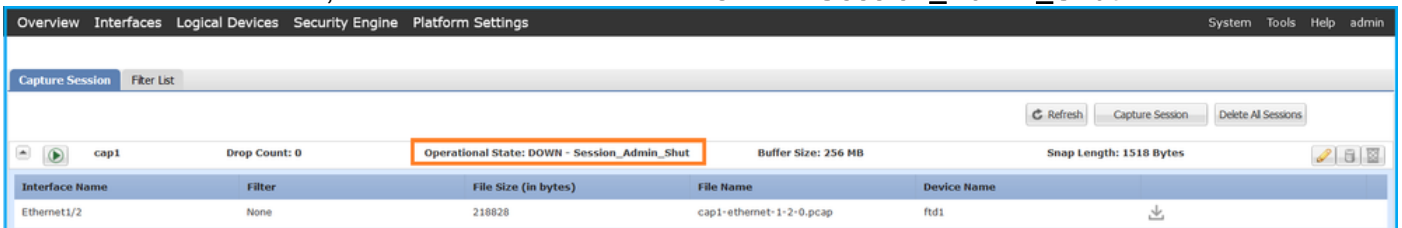
### FCM

Befolgen Sie diese Schritte auf FCM, um interne Switch-Erfassungsdateien zu sammeln:

1. Klicken Sie auf die Schaltfläche **Sitzung deaktivieren**, um die aktive Aufzeichnung zu beenden:

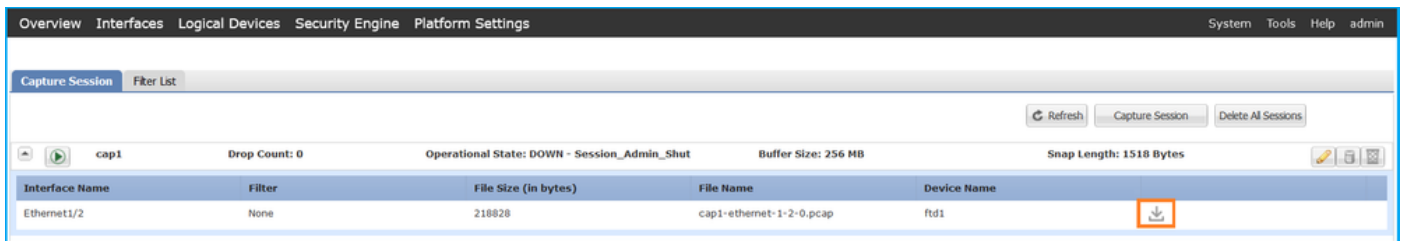


2. Stellen Sie sicher, dass der Betriebsstatus **DOWN - Session\_Admin\_Shut**:



3. Klicken Sie auf **Herunterladen**, um die Erfassungsdatei herunterzuladen:





Bei Port-Channel-Schnittstellen wiederholen Sie diesen Schritt für alle Teilnehmer-Schnittstellen.

## FXOS-CLI

Befolgen Sie diese Schritte auf der FXOS-CLI, um Erfassungsdateien zu erfassen:

### 1. Die aktive Erfassung beenden:

```
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. Laden Sie die Erfassungsdatei aus dem local-mgmt-Bereich hoch:

```
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:
```

Bei Port-Channel-Schnittstellen kopieren Sie die Erfassungsdatei für jede Member-Schnittstelle.

## Richtlinien, Einschränkungen und Best Practices für Interner Switch Paketerfassung

Die Richtlinien und Einschränkungen im Zusammenhang mit der internen Switch-Erfassung für Firepower 4100/9300 finden Sie im *Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide* oder im *Cisco Firepower 4100/9300 FXOS CLI Configuration Guide, Chapter Troubleshooting*, Abschnitt **Paketerfassung**.

Dies ist die Liste der Best Practices, die auf der Verwendung der Paketerfassung in TAC-Fällen basieren:

- Beachten Sie Richtlinien und Einschränkungen.
- Erfassen Sie Pakete an allen Port-Channel-Mitgliedsschnittstellen, und analysieren Sie alle Erfassungsdateien.
- Verwenden Sie Erfassungsfiler.
- Berücksichtigen Sie die Auswirkungen von NAT auf Paket-IP-Adressen, wenn ein Erfassungsfiler konfiguriert wird.
- Erhöhen oder verringern Sie die **Snap-Linse**, die die Frame-Größe angibt, falls sie vom Standardwert von 1518 Byte abweicht. Eine geringere Größe führt zu einer höheren Anzahl erfasster Pakete und umgekehrt.
- Passen Sie die **Puffergröße** nach Bedarf an.
- Beachten Sie die **Drop Count** für FCM oder FXOS CLI. Sobald die Puffergrößengrenze erreicht ist, erhöht sich der Zähler für die Verwerfung.
- Verwenden Sie `filter!vntag` in Wireshark, um nur Pakete ohne VN-Tag anzuzeigen. Dies ist nützlich, um VN-markierte Pakete in den Front-Interface-Paketerfassungsdateien auszublenden.
- Verwenden Sie den Filter `frame.number&1` in Wireshark, um nur ungerade Frames anzuzeigen. Dies ist nützlich, um doppelte Pakete in den Backplane-Schnittstellen-Paketerfassungsdateien auszublenden.
- Bei Protokollen wie TCP wendet Wireshark FarbregeIn an, die Pakete mit bestimmten Bedingungen in verschiedenen Farben anzeigen. Bei internen Switch-Erfassungen aufgrund doppelter Pakete in Erfassungsdateien kann das Paket farbig dargestellt und falsch-positiv markiert werden. Wenn Sie die Paketerfassungsdateien analysieren und einen beliebigen Filter anwenden, exportieren Sie die angezeigten Pakete in eine neue Datei und öffnen Sie stattdessen die neue Datei.

## Konfiguration und Verifizierung auf Sichere Firewall 3100

Im Gegensatz zu Firepower 4100/9300 werden die internen Switch-Erfassungen auf der Secure Firewall 3100 über den Befehl `capture <name> switch` auf der Befehlszeilenschnittstelle der Anwendung konfiguriert. Dabei gibt die **Switch**-Option an, dass die Erfassungen auf dem internen Switch konfiguriert werden.

Dies ist der Befehl `capture` mit der `switch`-Option:

> **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>
```

Allgemeine Schritte für die Konfiguration der Paketerfassung:

1. Geben Sie eine Eingangsschnittstelle an:

Die Switch-Erfassungskonfiguration akzeptiert den **Namen** der Eingangsschnittstelle. Der Benutzer kann die Namen der Datenschnittstellen, den internen Uplink oder die Verwaltungsschnittstellen angeben:

> **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. Geben Sie den Ethernet-Frame-EtherType an. Der Standard-EtherType ist IP. Die **Ethernet-**Optionswerte geben den EtherType an:

> **capture capsw switch interface inside ethernet-type ?**

```
802.1Q
<0-65535> Ethernet type
arp
ip
ip6
pppoed
pppoes
rarp
sgt
vlan
```

3. Geben Sie die Übereinstimmungsbedingungen an. Die Option **zum** Erfassen von Übereinstimmungen legt die Übereinstimmungskriterien fest:

> **capture capsw switch interface inside match ?**

```
<0-255> Enter protocol number (0 - 255)
ah
eigrp
esp
gre
icmp
icmp6
```

```
igmp
igrp
ip
ipinip
ipsec
mac      Mac-address filter
nos
ospf
pcp
pim
pptp
sctp
snp
spi      SPI value
tcp
udp
<cr>
```

4. Geben Sie andere optionale Parameter an, z. B. die Puffergröße, die Paketlänge usw.
5. Aktivieren Sie die Erfassung. Der Befehl `no capture <Name> switch stop` aktiviert die Erfassung:

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

6. Überprüfen Sie die Erfassungsdetails:

- Der Verwaltungsstatus ist **aktiviert**, und der Betriebsstatus ist **aktiv**.
- Größe der Paketerfassungsdatei **Pcapsize** erhöht sich.
- Die Anzahl der erfassten Pakete in der Ausgabe von `show capture <cap_name>` ist ungleich null.
- Capture-Pfad **PCAPFILE**. Die erfassten Pakete werden automatisch im Ordner `/mnt/disk0/packet-capture/` gespeichert.
- Erfassungsbedingungen. Die Software erstellt automatisch Erfassungsfilter, die auf Erfassungsbedingungen basieren.

```
> 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. Stoppen Sie die Erfassung bei Bedarf:

```
> 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. Sammeln Sie die Erfassungsdateien. Befolgen Sie die Schritte im Abschnitt **Sammeln von Dateien zur Erfassung interner Switches der Secure Firewall 3100**.

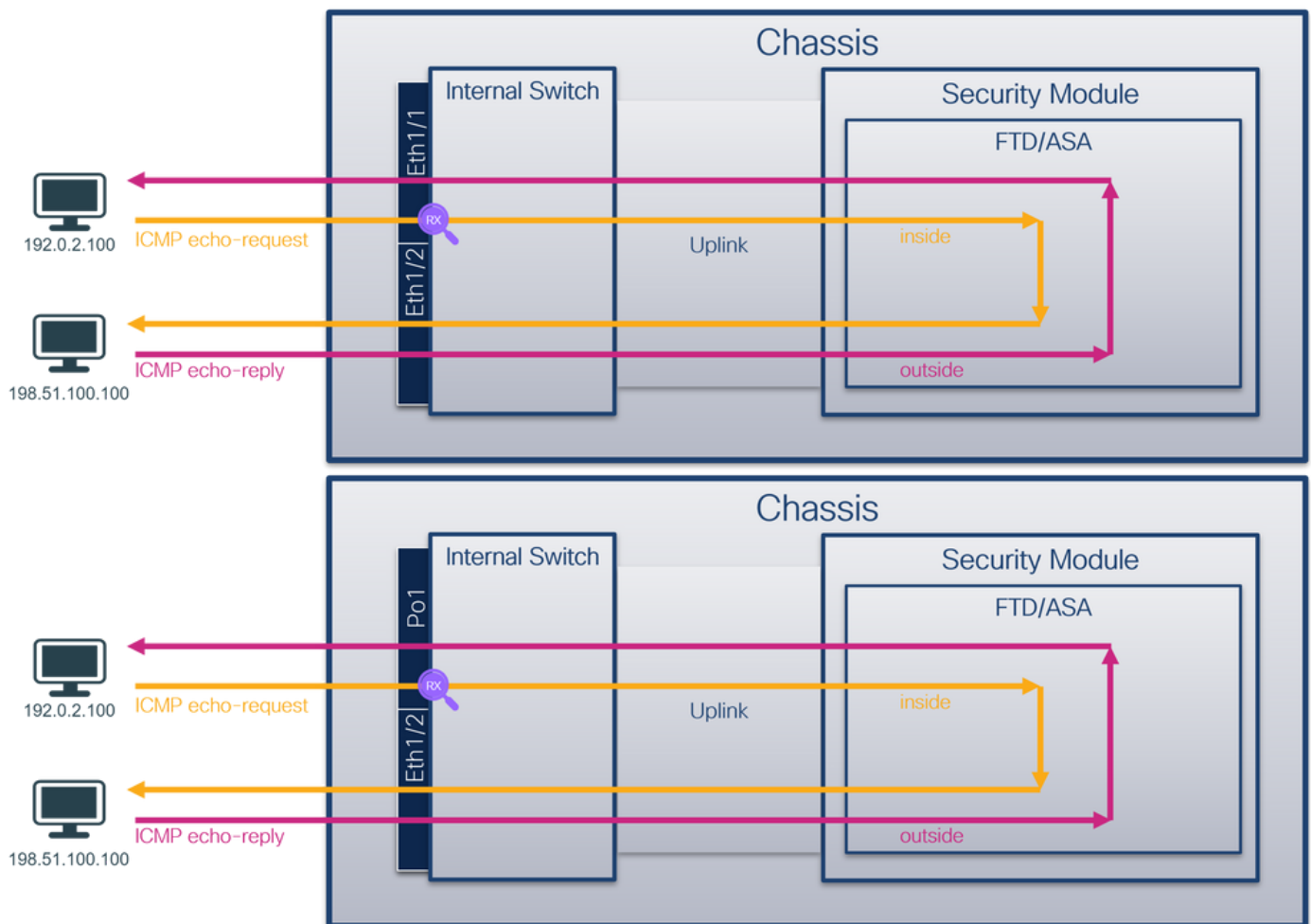
In Version 7.2 wird die interne Switch-Erfassungskonfiguration auf dem FMC oder FDM nicht unterstützt. Bei der ASA Software-Version 9.18(1) und höher können die internen Switch-Erfassungen in den ASDM-Versionen 7.18.1.x und höher konfiguriert werden.

Diese Szenarien beziehen sich auf häufige Anwendungsfälle der internen Switch-Erfassung für die sichere Firewall 3100.

### Paketerfassung an einer physischen oder Port-Channel-Schnittstelle

Verwenden Sie FTD oder ASA CLI, um eine Paketerfassung an der Schnittstelle Ethernet1/1 oder Port-Channel1 zu konfigurieren und zu überprüfen. Beide Schnittstellen enthalten den Namen `if`.

#### Topologie, Paketfluss und Erfassungspunkte



### Konfiguration

Befolgen Sie die folgenden Schritte auf der ASA- oder FTD-CLI, um eine Paketerfassung an der Schnittstelle Ethernet1/1 oder Port-channel1 zu konfigurieren:

## 1. Überprüfen Sie den Namen:

```
> 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. Eine Aufzeichnungssitzung erstellen:

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

## 3. Aufzeichnungssitzung aktivieren:

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

## Verifizierung

Überprüfen Sie den Namen der Erfassungssitzung, den Verwaltungs- und Betriebsstatus, den Schnittstellensteckplatz und die Kennung. Stellen Sie sicher, dass sich der **Pcapsize**-Wert in Byte erhöht und die Anzahl der erfassten Pakete ungleich null ist:

```
> 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

Im Fall von Port-channel1 wird die Erfassung an allen Mitgliedsschnittstellen konfiguriert:

> **show capture capsw detail**

Packet Capture info

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

Total Physical ports involved in Packet Capture: 2

Physical port:

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

Packet Capture Filter Info

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

Physical port:

**Slot Id:** 1  
**Port Id:** 3  
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-3-0.pcap  
**Pcapsize:** 18399  
Filter: capsw-1-3

#### Packet Capture Filter Info

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

Total Physical breakout ports involved in Packet Capture: 0

#### 56 packet captured on disk using switch capture

Reading of capture file from disk is not supported

Die Port-Channel-Member-Schnittstellen können in der FXOS-Befehlszeile **local-mgmt** mit dem Befehl **show port channel summary** überprüft werden:

```
> 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
```

Um auf FXOS auf ASA zuzugreifen, führen Sie den Befehl **connect fxos admin** aus. Bei Multi-Context führen Sie den Befehl im Admin-Kontext aus.

## Erfassungsdateien erfassen

Befolgen Sie die Schritte im Abschnitt **Sammeln von Dateien zur Erfassung interner Switches der Secure Firewall 3100**.

## Analyse der Erfassungsdatei

Öffnen Sie die Erfassungsdateien für Ethernet1/1 mit einer Anwendung zum Lesen der Paketerfassungsdatei. Wählen Sie das erste Paket aus, und überprüfen Sie die Schlüsselpunkte:

1. Nur ICMP-Echoanforderungspakete werden erfasst.
2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.

The screenshot shows a Wireshark capture of ICMP Echo (ping) requests. The packet list pane shows 18 packets, all ICMP Echo requests. The packet details pane shows Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol. The packet bytes pane shows the raw data.

Öffnen Sie die Erfassungsdateien für Portchannel1-Mitgliedsschnittstellen. Wählen Sie das erste Paket aus, und überprüfen Sie die wichtigsten Punkte:

1. Nur ICMP-Echoanforderungspakete werden erfasst.
2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.

The screenshot shows a Wireshark capture of ICMP Echo (ping) requests on Portchannel1. The packet list pane shows 18 packets, all ICMP Echo requests. The packet details pane shows Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol. The packet bytes pane shows the raw data.

## Erklärung

Die Switch-Erfassungen werden an den Schnittstellen Ethernet1/1 oder Port-Channel1 konfiguriert.

In dieser Tabelle ist die Aufgabe zusammengefasst:

Aufgabe	Erfassungspunkt	Interner Filter	Richtung	Erfasster Datenverkehr
Konfigurieren und Überprüfen der Paketerfassung an der Schnittstelle Ethernet1/1	Ethernet1/1	None	Nur Eingang	ICMP-Echo-Anfragen von Host 192.0.2.100 an Host 198.51.100.100
Konfiguration und Verifizierung der Paketerfassung an der Schnittstelle Ethernet1/3	Ethernet1/3	None	Nur Eingang	ICMP-Echo-Anfragen von Host 192.0.2.100 an Host 198.51.100.100

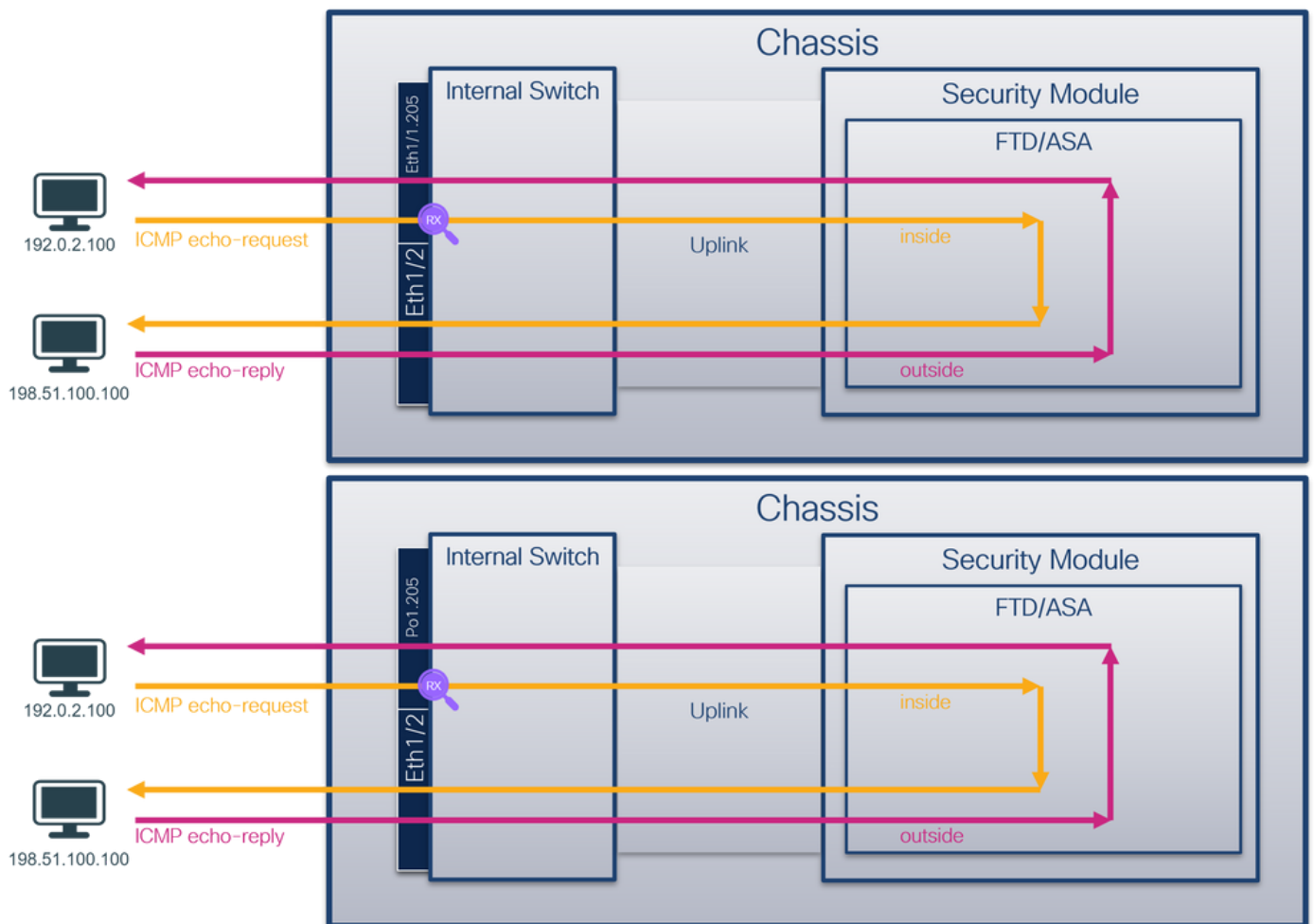


Port-Channel1 mit den  
Mitgliedsschnittstellen Ethernet1/3 und Ethernet1/4  
Ethernet1/4

## Paketerfassung auf einer Subchnittstelle einer physischen oder Port-Channel-Schnittstelle

Verwenden Sie die FTD- oder ASA-CLI, um eine Paketerfassung an den Subchnittstellen Ethernet1/1.205 oder Port-Channel1.205 zu konfigurieren und zu überprüfen. Beide Subchnittstellen haben den Namen **innen**.

### Topologie, Paketfluss und Erfassungspunkte



### Konfiguration

Befolgen Sie die folgenden Schritte auf der ASA- oder FTD-CLI, um eine Paketerfassung an der Schnittstelle Ethernet1/1 oder Port-channel1 zu konfigurieren:

1. Überprüfen Sie den Namen:

```
> 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. Eine Aufzeichnungssitzung erstellen:

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

## 3. Aufzeichnungssitzung aktivieren:

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

## Verifizierung

Überprüfen Sie den Namen der Erfassungssitzung, den Verwaltungs- und Betriebsstatus, den Schnittstellensteckplatz und die Kennung. Stellen Sie sicher, dass der **Pcapsize**-Wert in Byte erhöht wird und die Anzahl der erfassten Pakete ungleich null ist:

```
> 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 diesem Fall wird ein Filter mit dem äußeren VLAN **Ovlan=205** erstellt und auf die Schnittstelle angewendet.

Im Fall von Port-channel1 wird die Erfassung mit dem Filter **Ovlan=205** auf allen Member-Schnittstellen konfiguriert:

```
> 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

Die Port-Channel-Member-Schnittstellen können in der FXOS-Befehlszeile **local-mgmt** mit dem Befehl **show port channel summary** überprüft werden:

> **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
```

Um auf FXOS auf ASA zuzugreifen, führen Sie den Befehl **connect fxos admin** aus. Bei Multi-Context führen Sie diesen Befehl im Admin-Kontext aus.

## Erfassungsdateien erfassen

Befolgen Sie die Schritte im Abschnitt **Sammeln von Dateien zur Erfassung interner Switches der Secure Firewall 3100**.

## Analyse der Erfassungsdatei

Öffnen Sie die Erfassungsdateien für Ethernet1/1.205 mit einer Anwendung zum Lesen von Paketerfassungsdateien. Wählen Sie das erste Paket aus, und überprüfen Sie die Schlüsselpunkte:

1. Nur ICMP-Echoanforderungspakete werden erfasst.
2. Der ursprüngliche Paket-Header hat den VLAN-Tag 205.

The screenshot displays a network traffic capture in Wireshark. The top pane shows a list of 18 ICMP Echo (ping) requests. The first packet (No. 1) is highlighted with a red box. The packet details pane below shows the Ethernet II header with 'Virtual LAN, PRI: 0, DEI: 0, ID: 205' highlighted in yellow. The Internet Protocol Version 4 and Internet Control Message Protocol headers are also visible.

Öffnen Sie die Erfassungsdateien für Portchannel1-Mitgliedsschnittstellen. Wählen Sie das erste Paket aus, und überprüfen Sie die wichtigsten Punkte:

1. Nur ICMP-Echoanforderungspakete werden erfasst.
2. Der ursprüngliche Paket-Header hat den VLAN-Tag 205.

The screenshot displays a network traffic capture in Wireshark. The top pane shows a list of 18 ICMP Echo (ping) requests. The first packet (No. 1) is highlighted with a red box. The packet details pane below shows the Ethernet II header with 'Virtual LAN, PRI: 0, DEI: 0, ID: 205' highlighted in yellow. The Internet Protocol Version 4 and Internet Control Message Protocol headers are also visible.

## Erklärung

Die Switch-Erfassungen werden an den Subchnittstellen Ethernet1/1.205 oder Port-Channel1.205 mit einem Filter konfiguriert, der mit dem äußeren VLAN 205 übereinstimmt.

In dieser Tabelle ist die Aufgabe zusammengefasst:

Aufgabe	Erfassungspunkt	Interner Filter	Richtung	Erfasster Datenverkehr
Konfiguration und Verifizierung einer Paketerfassung an der Subchnittstelle Ethernet1/1.205	Ethernet 1/1	Äußeres VLAN 205	Nur Eingang	ICMP-Echo-Anfragen von Host 192.0.2.100 an Host 198.51.100.1
Konfiguration und Verifizierung einer Paketerfassung an der Subchnittstelle Ethernet 1/3	Ethernet 1/3	Äußeres VLAN 205	Nur Eingang	ICMP-Echo-Anfragen von Host 192.0.2.100 an Host 198.51.100.1



Port-Channel1.205 mit den  
Mitgliedsschnittstellen Ethernet1/3 und  
Ethernet1/4 Ethernet  
1/4 g

## Paketerfassung an internen Schnittstellen

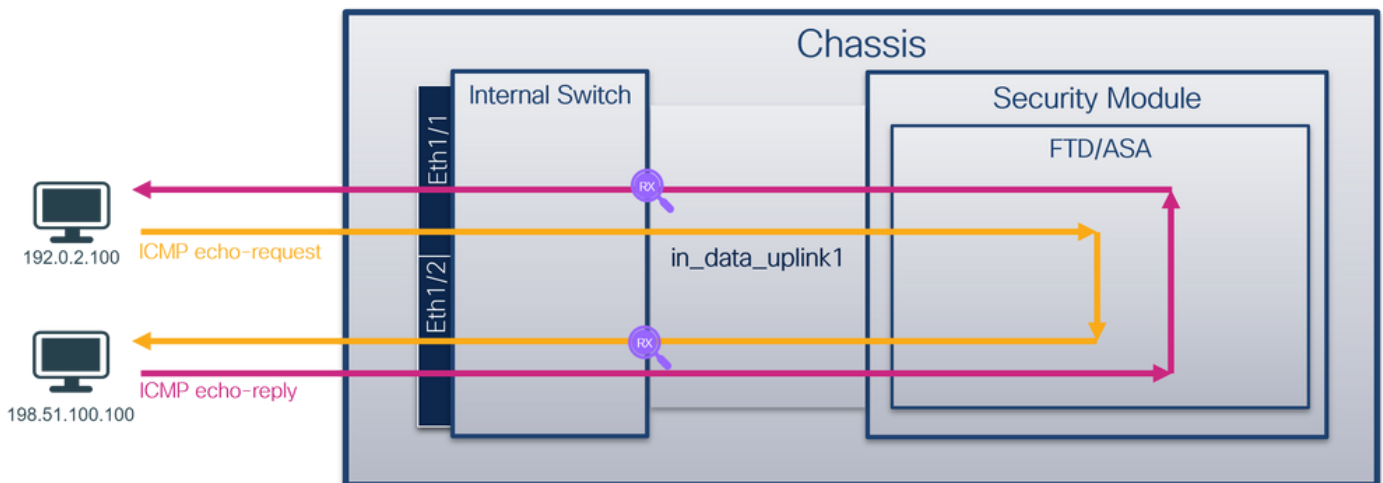
Die sichere Firewall verfügt über 2 interne Schnittstellen:

- **in\_data\_uplink1**: Verbindet die Anwendung mit dem internen Switch.
- **in\_mgmt\_uplink1** - Stellt einen dedizierten Paketpfad für Managementverbindungen wie SSH zur Verwaltungsschnittstelle oder die Verwaltungsverbindung (auch Sftunnel genannt) zwischen dem FMC und dem FTD bereit.

### Aufgabe 1

Verwenden Sie FTD oder ASA CLI, um eine Paketerfassung auf der Uplink-Schnittstelle **in\_data\_uplink1** zu konfigurieren und zu überprüfen.

### Topologie, Paketfluss und Erfassungspunkte



### Konfiguration

Führen Sie die folgenden Schritte auf ASA oder FTD CLI aus, um eine Paketerfassung auf der Schnittstelle **in\_data\_uplink1** zu konfigurieren:

1. Eine Aufzeichnungssitzung erstellen:

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

2. Aufzeichnungssitzung aktivieren:

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

### Verifizierung

Überprüfen Sie den Namen der Erfassungssitzung, den Verwaltungs- und Betriebsstatus, den Schnittstellensteckplatz und die Kennung. Stellen Sie sicher, dass der **Pcapsize**-Wert in Byte erhöht wird und die Anzahl der erfassten Pakete ungleich null ist:

> **show capture capsw detail**

Packet Capture info

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

Total Physical ports involved in Packet Capture: 1

Physical port:

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

Packet Capture Filter Info

Name: capsw-1-18  
Protocol: 0  
Ivlan: 0  
Ovlan: 0  
Src Ip: 0.0.0.0  
Dest Ip: 0.0.0.0  
Src Ipv6: ::  
Dest Ipv6: ::  
Src MAC: 00:00:00:00:00:00  
Dest MAC: 00:00:00:00:00:00  
Src Port: 0  
Dest Port: 0  
Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

**66 packets captured on disk using switch capture**

Reading of capture file from disk is not supported

In diesem Fall wird eine Erfassung auf der Schnittstelle mit der internen ID **18** erstellt, die die **in\_data\_uplink1**-Schnittstelle auf der sicheren Firewall 3130 ist. Der Befehl **show portManager switch status** in der FXOS-Befehlszeile **local-mgmt** gibt die Schnittstellen-IDs an:

> **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
<b>0/18</b>	<b>KR2</b>	<b>Up</b>	<b>50G</b>	<b>Full</b>	<b>None</b>	<b>Link-Up</b>
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

Um auf FXOS auf ASA zuzugreifen, führen Sie den Befehl **connect fxos admin** aus. Bei Multi-Context führen Sie diesen Befehl im Admin-Kontext aus.

## Erfassungsdateien erfassen

Befolgen Sie die Schritte im Abschnitt **Sammeln von Dateien zur Erfassung interner Switches der Secure Firewall 3100**.

## Analyse der Erfassungsdatei

Öffnen Sie die Erfassungsdateien für die Schnittstelle `in_data_uplink1` mit einer Anwendung zum Lesen von Paketerfassungsdateien. Überprüfen Sie den Schlüsselpunkt - in diesem Fall werden ICMP-Echoanforderungs- und Echoantwortpakete erfasst. Dies sind die Pakete, die von der Anwendung an den internen Switch gesendet werden.

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 (req
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 (repl
3	2022-08-07 22:40:07.684219	192.0.2.100	198.51.100.100	ICMP	102	0x4d08 (19944)	64	Echo (ping) request id=0x003a, seq=34/8704, ttl=64 (req
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 (repl
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 (req
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 (repl
7	2022-08-07 22:40:09.690737	192.0.2.100	198.51.100.100	ICMP	102	0x4f2d (20269)	64	Echo (ping) request id=0x003a, seq=36/9216, ttl=64 (req
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 (repl
9	2022-08-07 22:40:10.692266	192.0.2.100	198.51.100.100	ICMP	102	0x4fb1 (20401)	64	Echo (ping) request id=0x003a, seq=37/9472, ttl=64 (req
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 (repl
11	2022-08-07 22:40:11.691159	192.0.2.100	198.51.100.100	ICMP	102	0x5008 (20488)	64	Echo (ping) request id=0x003a, seq=38/9728, ttl=64 (req
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 (repl
13	2022-08-07 22:40:12.692135	192.0.2.100	198.51.100.100	ICMP	102	0x50b8 (20664)	64	Echo (ping) request id=0x003a, seq=39/9984, ttl=64 (req
14	2022-08-07 22:40:12.697209	198.51.100.100	192.0.2.100	ICMP	102	0x6fd7 (28631)	64	Echo (ping) reply id=0x003a, seq=39/9984, ttl=64 (repl
15	2022-08-07 22:40:13.697320	192.0.2.100	198.51.100.100	ICMP	102	0x5184 (20868)	64	Echo (ping) request id=0x003a, seq=40/10240, ttl=64 (req
16	2022-08-07 22:40:13.697327	198.51.100.100	192.0.2.100	ICMP	102	0x703e (28734)	64	Echo (ping) reply id=0x003a, seq=40/10240, ttl=64 (repl
17	2022-08-07 22:40:14.698512	192.0.2.100	198.51.100.100	ICMP	102	0x51d8 (20952)	64	Echo (ping) request id=0x003a, seq=41/10496, ttl=64 (req
18	2022-08-07 22:40:14.698518	198.51.100.100	192.0.2.100	ICMP	102	0x70dd (28893)	64	Echo (ping) reply id=0x003a, seq=41/10496, ttl=64 (repl

```

> 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
0000 00 50 56 9d e7 50 bc e7 12 34 9a 15 08 00 45 00  PV..P...d...E-
0010 00 54 4d 93 40 00 40 01 00 1a c0 00 02 64 c6 33  TM@.@...d3
0020 64 64 08 00 7f 15 00 20 21 39 3f f0 62 00 00  dd...197b...
0030 00 00 8b 1a 05 00 00 00 00 00 10 11 12 13 14 15  ....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  .... !"#%$
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
0060 36 37 55 55 55 55 55 55 67UUUU

```

## Erklärung

Wenn eine Switch-Erfassung an der Uplink-Schnittstelle konfiguriert ist, werden nur Pakete erfasst, die von der Anwendung an den internen Switch gesendet werden. An die Anwendung gesendete Pakete werden nicht erfasst.

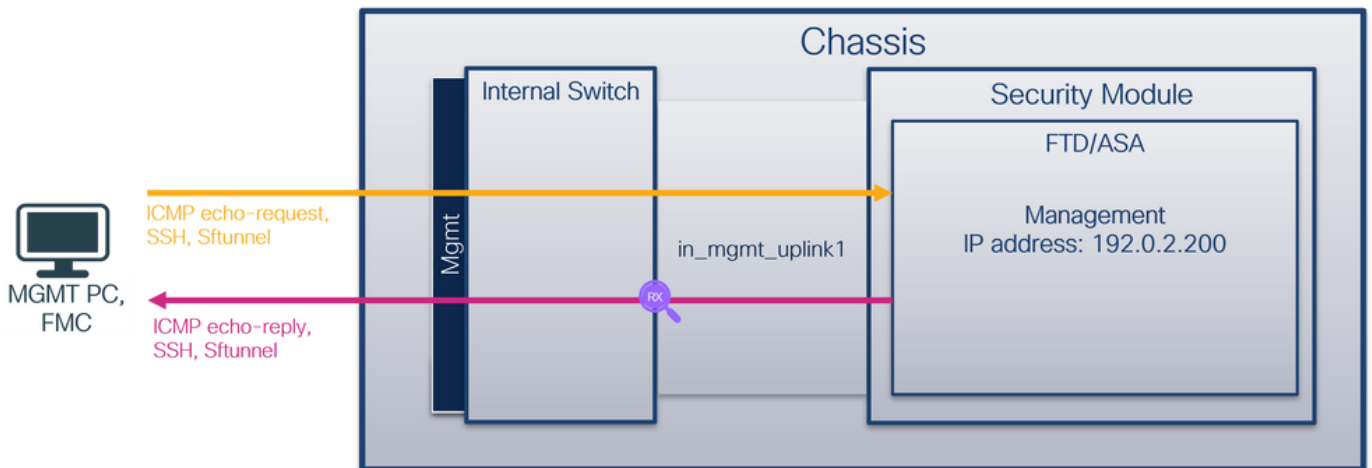
In dieser Tabelle ist die Aufgabe zusammengefasst:

Aufgabe	Erfassungspunkt	Interner Filter	Richtung	Erfasster Datenverkehr
Konfigurieren und Überprüfen einer Paketerfassung an der Uplink-Schnittstelle <code>in_data_uplink1</code>	<code>in_data_uplink1</code>	None	Nur Eingang	ICMP-Echo-Anfragen von Host 192.0.2.100 an Host 198.51.100.100 ICMP-Echo-Antworten von Host 198.51.100.100 zu Host 192.0.2.100

## Aufgabe 2

Verwenden Sie FTD oder ASA CLI, um eine Paketerfassung auf der Uplink-Schnittstelle `in_mgmt_uplink1` zu konfigurieren und zu überprüfen. Nur die Pakete der Verbindungen auf Verwaltungsebene werden erfasst.

## Topologie, Paketfluss und Erfassungspunkte



## Konfiguration

Führen Sie die folgenden Schritte auf ASA- oder FTD-CLI aus, um eine Paketerfassung auf der Schnittstelle `in_mgmt_uplink1` zu konfigurieren:

1. Eine Aufzeichnungssitzung erstellen:

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

2. Aufzeichnungssitzung aktivieren:

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

## Verifizierung

Überprüfen Sie den Namen der Erfassungssitzung, den Verwaltungs- und Betriebsstatus, den Schnittstellensteckplatz und die Kennung. Stellen Sie sicher, dass der **Pcapsize**-Wert in Byte

erhöht wird und die Anzahl der erfassten Pakete ungleich null ist:

```
> show capture capsw detail
```

Packet Capture info

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

Total Physical ports involved in Packet Capture: 1

Physical port:

```
Slot Id:       1
Port Id:       19
Pcapfile:      /mnt/disk0/packet-capture/sess-1-capsw-mgmt-uplink1.pcap
Pcapsize:     137248
Filter:        capsw-1-19
```

Packet Capture Filter Info

```
Name:          capsw-1-19
Protocol:      0
Ivlan:        0
Ovlan:        0
Src Ip:        0.0.0.0
Dest Ip:       0.0.0.0
Src Ipv6:      ::
Dest Ipv6:     ::
Src MAC:       00:00:00:00:00:00
Dest MAC:      00:00:00:00:00:00
Src Port:      0
Dest Port:     0
Ethertype:    0
```

Total Physical breakout ports involved in Packet Capture: 0

**281 packets captured on disk using switch capture**

Reading of capture file from disk is not supported

In diesem Fall wird eine Erfassung an der Schnittstelle mit einer internen ID 19 erstellt, die die **in\_mgmt\_uplink1**-Schnittstelle auf der sicheren Firewall 3130 ist. Der Befehl **show portManager switch status** in der FXOS-Befehlszeile **local-mgmt** gibt die Schnittstellen-IDs an:

```
> 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
<b>0/19</b>	<b>KR</b>	<b>Up</b>	<b>25G</b>	<b>Full</b>	<b>None</b>	<b>Link-Up</b>
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

Um auf FXOS auf ASA zuzugreifen, führen Sie den Befehl **connect fxos admin** aus. Bei Multi-Context führen Sie diesen Befehl im Admin-Kontext aus.

## Erfassungsdateien erfassen

Befolgen Sie die Schritte im Abschnitt **Sammeln von Dateien zur Erfassung interner Switches der Secure Firewall 3100**.

## Analyse der Erfassungsdatei

Öffnen Sie die Erfassungsdateien für die Schnittstelle **in\_mgmt\_uplink1** mit einer Anwendung zum Lesen der Paketerfassungsdatei. Überprüfen Sie den Schlüsselpunkt - in diesem Fall werden nur die Pakete der Management-IP-Adresse 192.0.2.200 angezeigt. Beispiele sind SSH-, Sftunnel- oder ICMP-Echo-Antwort-Pakete. Dies sind die Pakete, die von der Schnittstelle für das Anwendungsmanagement über den internen Switch an das Netzwerk gesendet werden.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
196	2022-08-07 23:21:45.133362	192.0.2.200	192.0.2.101	TCP	1518	0xb7d0 (47056)	64	39181 → 8305 [ACK] Seq=61372 Ack=875 Win=1384 Len=1448 TS
197	2022-08-07 23:21:45.133385	192.0.2.200	192.0.2.101	TCP	1518	0xb7d1 (47057)	64	39181 → 8305 [ACK] Seq=62820 Ack=875 Win=1384 Len=1448 TS
198	2022-08-07 23:21:45.133388	192.0.2.200	192.0.2.101	TLSv1.2	990	0xb7d2 (47058)	64	Application Data
199	2022-08-07 23:21:45.928772	192.0.2.200	192.0.2.100	ICMP	78	0xbd48 (48456)	64	Echo (ping) reply id=0x0001, seq=4539/47889, ttl=64
200	2022-08-07 23:21:45.949024	192.0.2.200	192.0.2.101	TLSv1.2	128	0x4a97 (19095)	64	Application Data
201	2022-08-07 23:21:45.949027	192.0.2.200	192.0.2.101	TCP	70	0x4a98 (19096)	64	8305 → 58885 [ACK] Seq=21997 Ack=26244 Win=4116 Len=0 TSv
202	2022-08-07 23:21:46.019895	192.0.2.200	192.0.2.101	TLSv1.2	100	0x4a99 (19097)	64	Application Data
203	2022-08-07 23:21:46.019899	192.0.2.200	192.0.2.101	TLSv1.2	96	0x4a9a (19098)	64	Application Data
204	2022-08-07 23:21:46.019903	192.0.2.200	192.0.2.101	TCP	70	0x4a9b (19099)	64	8305 → 58885 [ACK] Seq=22053 Ack=26274 Win=4116 Len=0 TSv
205	2022-08-07 23:21:46.019906	192.0.2.200	192.0.2.101	TCP	70	0x4a9c (19100)	64	8305 → 58885 [ACK] Seq=22053 Ack=26300 Win=4116 Len=0 TSv
206	2022-08-07 23:21:46.136415	192.0.2.200	192.0.2.101	TCP	70	0xb7d3 (47059)	64	39181 → 8305 [ACK] Seq=65188 Ack=921 Win=1384 Len=0 TSval
207	2022-08-07 23:21:46.958148	192.0.2.200	192.0.2.100	ICMP	78	0xbd9e (48542)	64	Echo (ping) reply id=0x0001, seq=4540/48145, ttl=64
208	2022-08-07 23:21:47.980409	192.0.2.200	192.0.2.100	ICMP	78	0xbd9f (48543)	64	Echo (ping) reply id=0x0001, seq=4541/48401, 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 23:21:50.008576	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	0xbfd7 (47063)	64	39181 → 8305 [ACK] Seq=69004 Ack=967 Win=1384 Len=0 TSval
218	2022-08-07 23:21:52.030118	192.0.2.200	192.0.2.100	ICMP	78	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

## Erklärung

Wenn eine Switch-Erfassung auf der Management-Uplink-Schnittstelle konfiguriert ist, werden nur von der Anwendungsmanagement-Schnittstelle gesendete Eingangspakete erfasst. Pakete, die für die Verwaltungsschnittstelle der Anwendung bestimmt sind, werden nicht erfasst.

In dieser Tabelle ist die Aufgabe zusammengefasst:

Aufgabe	Erfassungspunkt	Interner Filter	Richtung	Erfasster Datenverkehr
Konfigurieren und Überprüfen einer Paketerfassung auf der Management-Uplink-Schnittstelle	in_mgmt_uplink1	None	Nur Eingang (von der Managementschnittstelle zum Netzwerk über den internen Switch)	ICMP-Echoantworten von FTD-Verwaltung IP-Adresse 192.0.2.200 an Host 192.0.2.101 Sftunnel von FTD-Management-IP-Adresse 192.0.2.200 zu FMC-IP-Adresse 192.0.2.101 SSH von FTD-Management-IP-Adresse 192.0.2.200 an Host 192.0.2.100

## Paketerfassungsfiler

Die internen Switch-Paketerfassungsfiler werden auf die gleiche Weise konfiguriert wie die Paketerfassung auf Datenebene. Verwenden Sie **Ethernet-Typ** und **Match-Optionen**, um Filter zu konfigurieren.

## Konfiguration

Befolgen Sie die folgenden Schritte auf ASA oder FTD CLI, um eine Paketerfassung mit einem Filter zu konfigurieren, der ARP-Frames oder ICMP-Paketen von Host 198.51.100.100 auf Schnittstelle Ethernet1/1 entspricht:

## 1. Überprüfen Sie den Namen:

```
> show nameif
```

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

## 2. Erstellen einer Aufzeichnungssitzung für ARP oder ICMP:

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

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

## Verifizierung

Überprüfen Sie den Namen der Aufzeichnungssitzung und den Filter. Der Ethertype-Wert ist **2054** im Dezimalformat und **0x0806** im Hexadezimalformat:

```
> show capture capsw detail
```

Packet Capture info

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

Total Physical ports involved in Packet Capture: 1

Physical port:

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

### Packet Capture Filter Info

```
Name: capsw-1-1
Protocol: 0
Ivlan: 0
Ovlan: 0
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 2054
```

Total Physical breakout ports involved in Packet Capture: 0

0 packet captured on disk using switch capture

Reading of capture file from disk is not supported

Dies ist die Verifizierung des Filters für ICMP. IP-Protokoll 1 ist das ICMP:

```
> show capture capsw detail
```

Packet Capture info

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

Total Physical ports involved in Packet Capture: 1

Physical port:

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

Packet Capture Filter Info

```
Name:                capsw-1-1
Protocol:           1
Ivlan:                  0
Ovlan:                  0
Src Ip:              198.51.100.100
Dest Ip:                0.0.0.0
Src Ipv6:               ::
Dest Ipv6:              ::
Src MAC:                00:00:00:00:00:00
Dest MAC:               00:00:00:00:00:00
Src Port:               0
Dest Port:              0
Ethertype:              0
```

Total Physical breakout ports involved in Packet Capture: 0

0 packets captured on disk using switch capture

Reading of capture file from disk is not supported

## Erfassen von Dateien für den internen Secure Firewall 3100-Switch

Verwenden Sie die ASA- oder FTD-CLI, um interne Switch-Erfassungsdateien zu erfassen. Auf FTD kann die Erfassungsdatei auch über den CLI-Kopierbefehl an Ziele exportiert werden, die über die Daten- oder Diagnoseschnittstellen erreichbar sind.

Alternativ kann die Datei im Expertenmodus nach `/ngfw/var/common` kopiert und über die Option **File Download** vom FMC heruntergeladen werden.

Bei Port-Channel-Schnittstellen müssen Sie sicherstellen, dass die Paketerfassungsdateien von

allen Mitgliedsschnittstellen erfasst werden.

## ASA

Führen Sie die folgenden Schritte aus, um interne Switch-Erfassungsdateien in der ASA CLI zu erfassen:

### 1. Erfassung beenden:

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

### 2. Überprüfen Sie, ob die Aufzeichnungssitzung beendet wurde, und notieren Sie sich den Namen der Aufzeichnungsdatei.

```
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. Verwenden Sie den CLI-Befehl **copy**, um die Datei in Remote-Ziele zu exportieren:



```
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

Führen Sie die folgenden Schritte aus, um interne Switch-Erfassungsdateien auf der FTD-CLI zu erfassen und auf Server zu kopieren, die über Daten- oder Diagnoseschnittstellen erreichbar sind:

### 1. Rufen Sie die Diagnose-CLI auf:

```
> 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. Erfassung beenden:

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

### 3. Überprüfen Sie, ob die Aufzeichnungssitzung beendet wurde, und notieren Sie sich den Namen der Aufzeichnungsdatei:

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

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

Port Id: 1  
**Pcapfile:** /mnt/disk0/packet-capture/**sess-1-capsw-ethernet-1-1-0.pcap**  
Pcapsize: 139826  
Filter: capsw-1-1

#### Packet Capture Filter Info

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

Total Physical breakout ports involved in Packet Capture: 0

886 packets captured on disk using switch capture

Reading of capture file from disk is not supported

#### 4. Verwenden Sie den CLI-Befehl **copy**, um die Datei in Remote-Ziele zu exportieren.

```
firepower# copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap ?  
cluster: Copy to cluster: file system  
disk0: Copy to disk0: file system  
disk1: Copy to disk1: file system  
flash: Copy to flash: file system  
ftp: Copy to ftp: file system  
running-config Update (merge with) current system configuration  
scp: Copy to scp: file system  
smb: Copy to smb: file system  
startup-config Copy to startup configuration  
system: Copy to system: file system  
tftp: Copy to tftp: file system
```

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

Führen Sie die folgenden Schritte aus, um Erfassungsdateien von FMC über die Option **Dateidownload** zu sammeln:

#### 1. Erfassung beenden:

```
> capture capsw switch stop
```

#### 2. Überprüfen Sie, ob die Aufzeichnungssitzung beendet wurde, und notieren Sie den Dateinamen und den vollständigen Pfad der Erfassungsdatei:

```
> 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. Wechseln Sie in den Expertenmodus und in den Root-Modus:

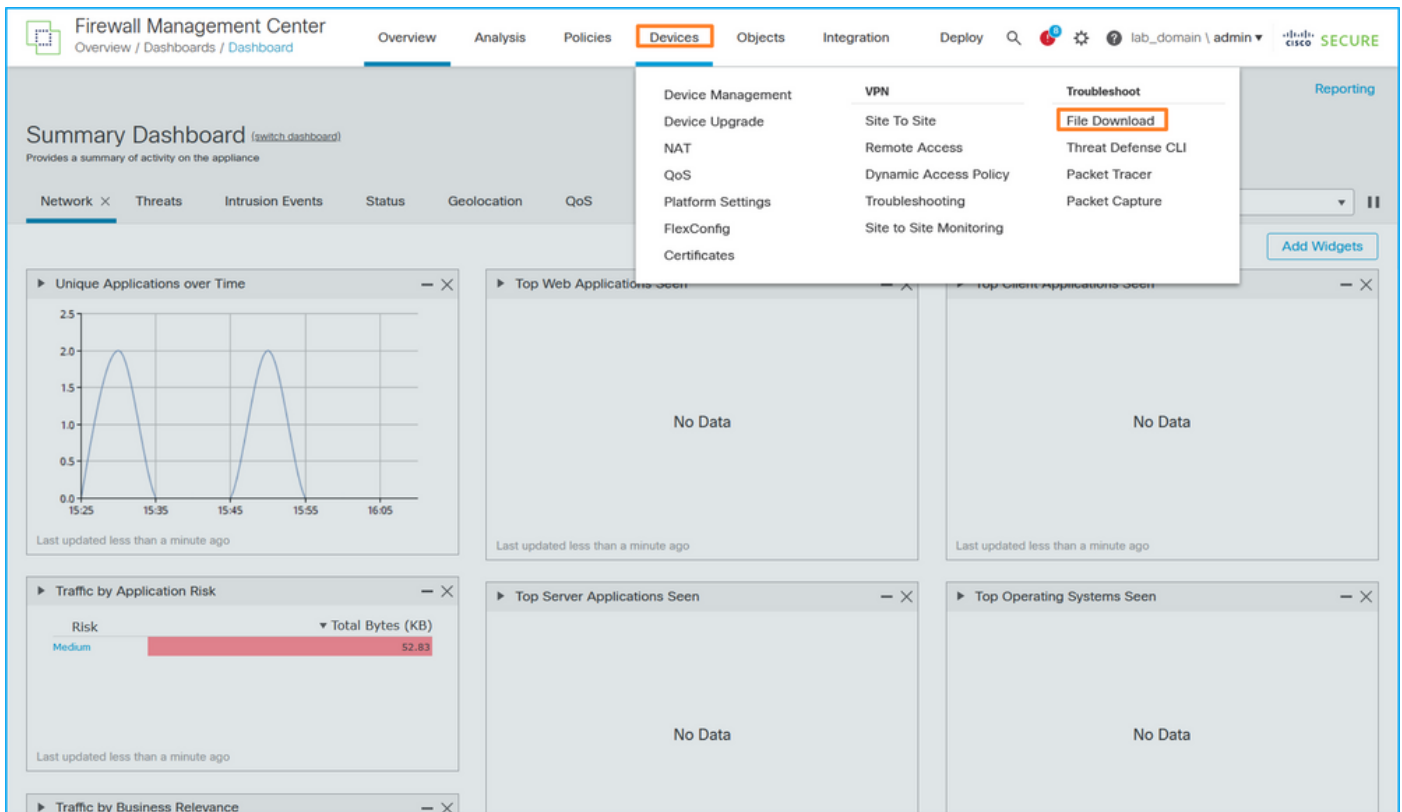
> **expert**

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

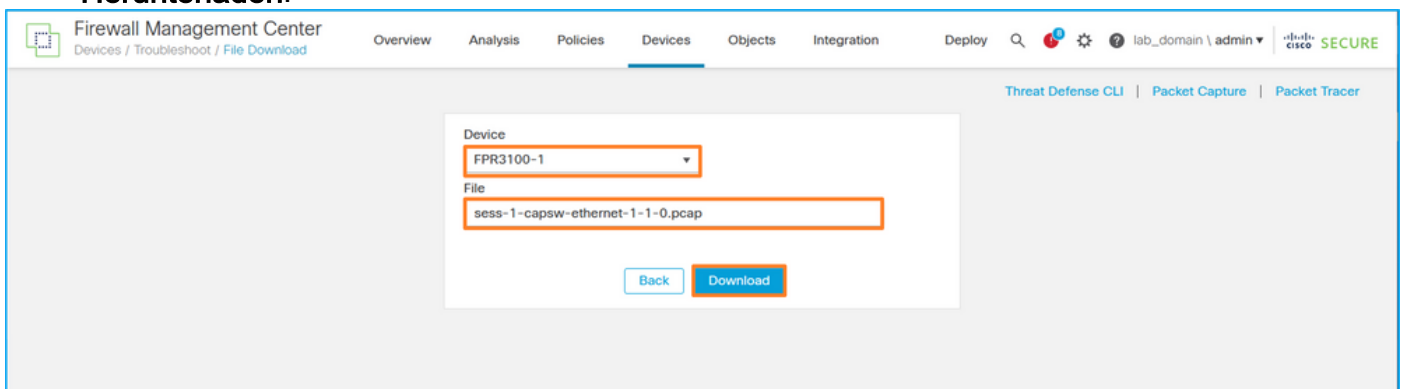
### 4. Kopieren Sie die Erfassungsdatei nach /ngfw/var/common/:

```
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. Wählen Sie auf FMC Devices > File Download:



6. Wählen Sie das FTD aus, geben Sie den Namen der Erfassungsdatei an, und klicken Sie auf **Herunterladen**:



## Richtlinien, Einschränkungen und Best Practices für die interne Switch-Paketerfassung

Richtlinien und Einschränkungen:

- Mehrere Sitzungen der Switch-Erfassungskonfiguration werden unterstützt, es kann jedoch nur jeweils eine Sitzung der Switch-Erfassung aktiv sein. Der Versuch, zwei oder mehr Aufzeichnungssitzungen zu aktivieren, führt zu dem Fehler **"FEHLER: Die Sitzung konnte nicht aktiviert werden, da maximal 1 aktive Paketerfassungssitzung erreicht wurde."**
- Die Erfassung eines aktiven Switches kann nicht gelöscht werden.
- Switch-Erfassungen können in der Anwendung nicht gelesen werden. Der Benutzer muss die Dateien exportieren.
- Bestimmte Erfassungsoptionen für die Datenebene wie **Dump**, **Decodierung**, **Paketnummer**, **Trace** und andere werden für Switch-Erfassungen nicht unterstützt.
- Bei Multi-Context-ASA werden die Switch-Erfassungen an Datenschnittstellen in Benutzerkontexten konfiguriert. Die Switch-Erfassungen an den Schnittstellen `in_data_uplink1` und `in_mgmt_uplink1` werden nur im Admin-Kontext unterstützt.

Dies ist die Liste der Best Practices, die auf der Verwendung der Paketerfassung in TAC-Fällen basieren:

- Beachten Sie Richtlinien und Einschränkungen.
- Verwenden Sie Erfassungsfiler.
- Berücksichtigen Sie die Auswirkungen von NAT auf Paket-IP-Adressen, wenn ein Erfassungsfiler konfiguriert wird.
- Erhöhen oder verringern Sie die **Paketlänge**, die die Frame-Größe angibt, falls sie sich vom Standardwert von 1518 Byte unterscheidet. Eine geringere Größe führt zu einer höheren Anzahl erfasster Pakete und umgekehrt.
- Passen Sie die **Puffergröße** nach Bedarf an.
- Beachten Sie den **Drop Count** in der Ausgabe des Befehls **show cap <cap\_name> detail**. Sobald die Puffergrößengrenze erreicht ist, erhöht sich der Zähler für die Verwerfung.

## Zugehörige Informationen

- [Firepower 4100/9300 Chassis Manager und FXOS CLI Konfigurationsanleitungen](#)
- [Cisco Secure Firewall 3100 - Erste Schritte](#)
- [Befehlsreferenz für Cisco Firepower 4100/9300 FXOS](#)



## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.