

# セキュアなファイアウォールとFirepower内部スイッチキャプチャの設定と確認

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[システムアーキテクチャの概要](#)

[内部スイッチの動作の概要](#)

[パケットフローとキャプチャポイント](#)

[Firepower 4100/9300の設定と確認](#)

[物理インターフェイスまたはポートチャンネルインターフェイスでのパケットキャプチャ](#)

[バックプレーンインターフェイスでのパケットキャプチャ](#)

[アプリケーションおよびアプリケーションポートでのパケットキャプチャ](#)

[物理インターフェイスまたはポートチャンネルインターフェイスのサブインターフェイスでのパケットキャプチャ](#)

[パケットキャプチャフィルタ](#)

[Firepower 4100/9300内部スイッチキャプチャファイルの収集](#)

[内部スイッチパケットキャプチャのガイドライン、制限事項、およびベストプラクティス](#)

[Secure Firewall 3100の設定と検証](#)

[物理インターフェイスまたはポートチャンネルインターフェイスでのパケットキャプチャ](#)

[物理インターフェイスまたはポートチャンネルインターフェイスのサブインターフェイスでのパケットキャプチャ](#)

[内部インターフェイスでのパケットキャプチャ](#)

[パケットキャプチャフィルタ](#)

[Secure Firewall 3100内部スイッチキャプチャファイルの収集](#)

[内部スイッチパケットキャプチャのガイドライン、制限事項、およびベストプラクティス](#)

[関連情報](#)

## 概要

このドキュメントでは、Firepowerの設定と検証、およびセキュアファイアウォールの内部スイッチキャプチャについて説明します。

## 前提条件

### 要件

製品に関する基本的な知識、キャプチャ分析。

## 使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

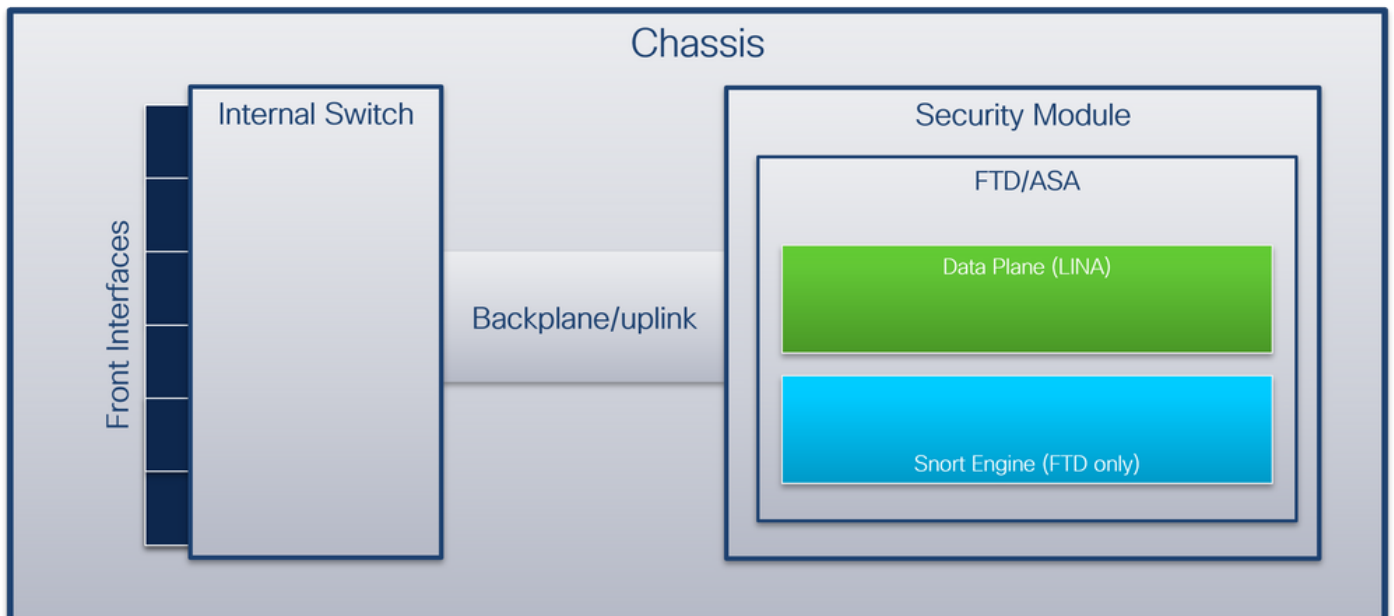
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Secure 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
- 適応型セキュリティアプライアンス(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>)

## 背景説明

### システムアーキテクチャの概要

パケットフローの観点から、Firepower 4100/9300およびSecure Firewall 3100のアーキテクチャを次の図のように視覚化できます。



シャーシには次のコンポーネントが含まれます。

- **内部スイッチ**：ネットワークからアプリケーションへ、またはその逆にパケットを転送します。内部スイッチは、組み込みインターフェイスモジュールまたは外部ネットワークモジュール上にある**前面インターフェイス**に接続され、スイッチなどの外部デバイスに接続されま

す。前面インターフェイスの例としては、Ethernet 1/1、Ethernet 2/4などがあります。「正面」は強い技術的定義ではありません。このドキュメントでは、外部デバイスに接続されているインターフェイスをバックプレーンまたはアップリンクインターフェイスと区別するために使用します。

- **バックプレーンまたはアップリンク**：セキュリティモジュール(SM)を内部スイッチに接続する内部インターフェイス。次の表に、Firepower 4100/9300のバックプレーンインターフェイスと、セキュアファイアウォール3100のアップリンクインターフェイスを示します。

Platform	サポートされるセキュリティモジュールの数	バックプレーン/アップリンクインターフェイス	マッピングされたリケーションインターフェイス
Firepower 4100 ( Firepower 4110/4112を除く )	1	SM1: Ethernet1/9 Ethernet1/10	Internal-Data0/0 Internal-Data0/1
Firepower 4110/4112	1	Ethernet1/9	Internal-Data0/0  Internal-Data0/0 Internal-Data0/1
FirePOWER 9300	3	SM1: Ethernet1/9 Ethernet1/10 SM2: Ethernet1/11 Ethernet1/12 SM3: Ethernet1/13 Ethernet1/14	Internal-Data0/0 Internal-Data0/1  Internal-Data0/0 Internal-Data0/1
Secure Firewall 3100	1	SM1:in_data_uplink1	Internal-Data0/1

モジュールごとに2つのバックプレーンインターフェイスがある場合、内部スイッチとモジュール上のアプリケーションが2つのインターフェイス上でトラフィックロードバランシングを実行します。

- セキュリティモジュール、セキュリティエンジン、またはブレード:FTDやASAなどのアプリケーションがインストールされているモジュール。Firepower 9300は最大3つのセキュリティモジュールをサポートします。
- **マッピングされたアプリケーションインターフェイス**:FTDやASAなどのアプリケーションは、バックプレーンまたはアップリンクインターフェイスを内部インターフェイスにマッピングします。つまり、バックプレーンまたはアップリンクインターフェイスは、アプリケーションの内部インターフェイスとして認識されます。

内部インターフェイスを確認するには、**show interface detail**コマンドを使用します。

```
> show interface detail | grep Interface
Interface Internal-Contro10/0 "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
```

## 内部スイッチの動作の概要

### Firepower 4100/9300

フォワーディング決定を行うために、内部スイッチではインターフェイスVLANタグ(ポートVLANタグ)と仮想ネットワークタグ(VN-tag)を使用します。

ポートVLANタグは、インターフェイスを識別するために内部スイッチによって使用されます。スイッチは、前面インターフェイスに到着した各入力パケットにポートVLANタグを挿入します。VLANタグはシステムによって自動的に設定され、手動で変更することはできません。タグの値は、**fxos**コマンドシェルで確認できます。

```
firepower# connect fxos
...
firepower(fxos)# show run int e1/2
!Command: show running-config interface Ethernet1/2
!Time: Tue Jul 12 22:32:11 2022

version 5.0(3)N2(4.120)

interface Ethernet1/2
description U: Uplink
no lldp transmit
no lldp receive
no cdp enable
switchport mode dot1q-tunnel
switchport trunk native vlan 102
speed 1000
duplex full
udld disable
no shutdown
```



VNタグも内部スイッチによって挿入され、アプリケーションにパケットを転送するために使用されます。これはシステムによって自動的に設定され、手動で変更することはできません。

ポートVLANタグとVNタグはアプリケーションと共有されます。アプリケーションは、それぞれの出カインターフェイスVLANタグとVNタグを各パケットに挿入します。アプリケーションからのパケットがバックプレーンインターフェイス上の内部スイッチによって受信されると、スイッチは出カインターフェイスのVLANタグとVNタグを読み取り、アプリケーションと出カインターフェイスを特定し、ポートのVLANタグとVNタグを削除して、パケットをネットワークに転送します。

## Secure Firewall 3100

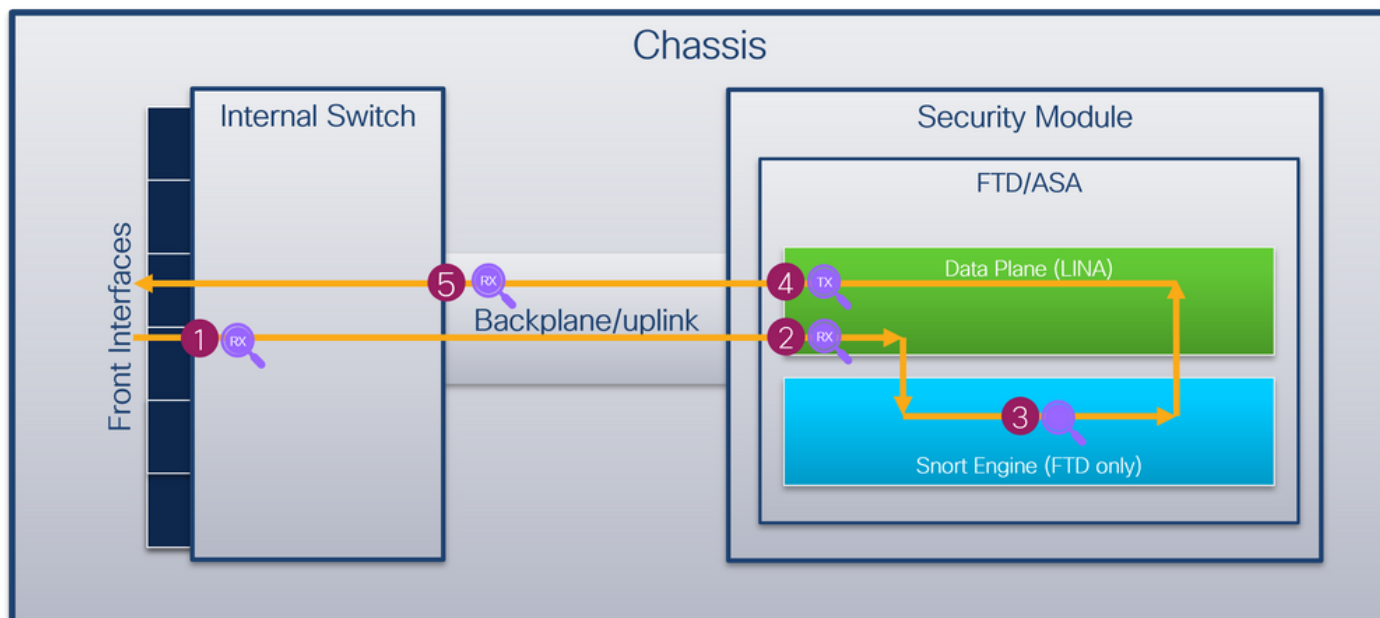
Firepower 4100/9300と同様に、ポートVLANタグはインターフェイスを識別するために内部スイッチによって使用されます。

ポートVLANタグはアプリケーションと共有されます。アプリケーションは、それぞれの出カインターフェイスVLANタグを各パケットに挿入します。アプリケーションからのパケットがアップリンクインターフェイス上の内部スイッチで受信されると、スイッチは出カインターフェイスのVLANタグを読み取り、出カインターフェイスを特定し、ポートのVLANタグを削除して、パケットをネットワークに転送します。

## パケットフローとキャプチャポイント

Firepower 4100/9300およびSecure Firewall 3100ファイアウォールは、内部スイッチのインターフェイスでのパケットキャプチャをサポートしています。

次の図に、シャーシとアプリケーション内のパケットパスに沿ったパケットキャプチャポイントを示します。



キャプチャポイントは次のとおりです。

1. 内部スイッチ前面インターフェイスの入力キャプチャポイント。前面インターフェイスは、スイッチなどのピアデバイスに接続されたインターフェイスです。
2. データプレーンインターフェイス入力キャプチャポイント
3. Snortキャプチャポイント

4. データプレーンインターフェイス出力キャプチャポイント

5. 内部スイッチバックプレーンまたはアップリンク入力キャプチャポイント。バックプレーンまたはアップリンクインターフェイスは、内部スイッチをアプリケーションに接続します。

内部スイッチは、入力インターフェイスキャプチャのみをサポートします。つまり、ネットワークまたはASA/FTDアプリケーションから受信したパケットだけをキャプチャできます。出力パケットキャプチャはサポートされていません。

## の設定と検証 Firepower 4100/9300

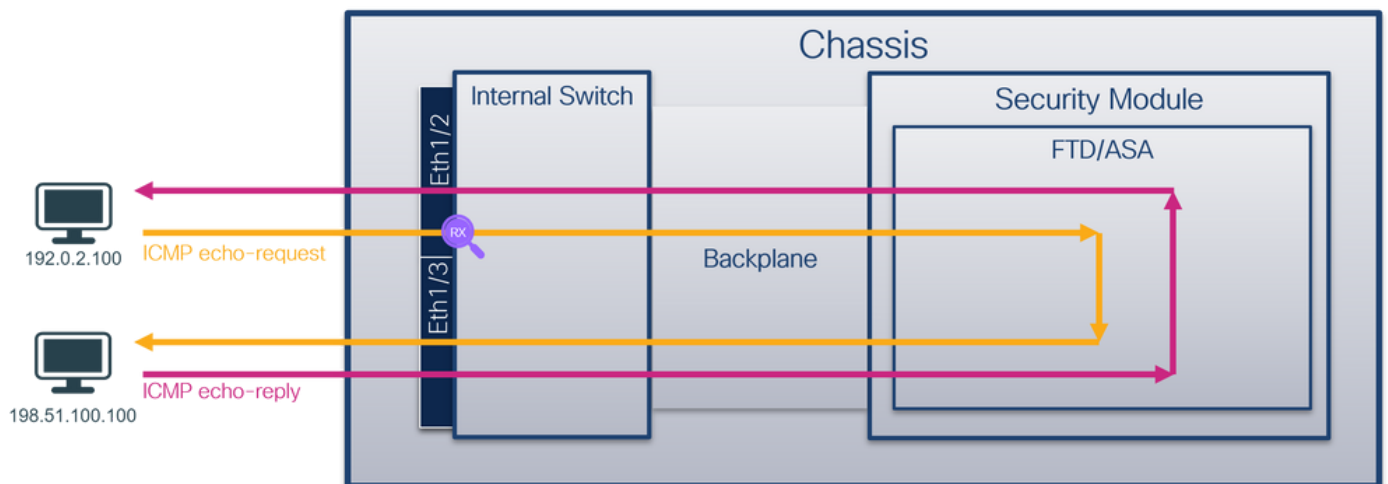
Firepower 4100/9300内部スイッチキャプチャは、FCMの[Tools] > [Packet Capture] またはFXOS CLIの[scope packet-capture] で設定できます。パケットキャプチャオプションの説明については、『Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide』または『Cisco Firepower 4100/9300 FXOS CLI Configuration Guide』の「Troubleshooting」の章の「Packet Capture」の項を参照してください。

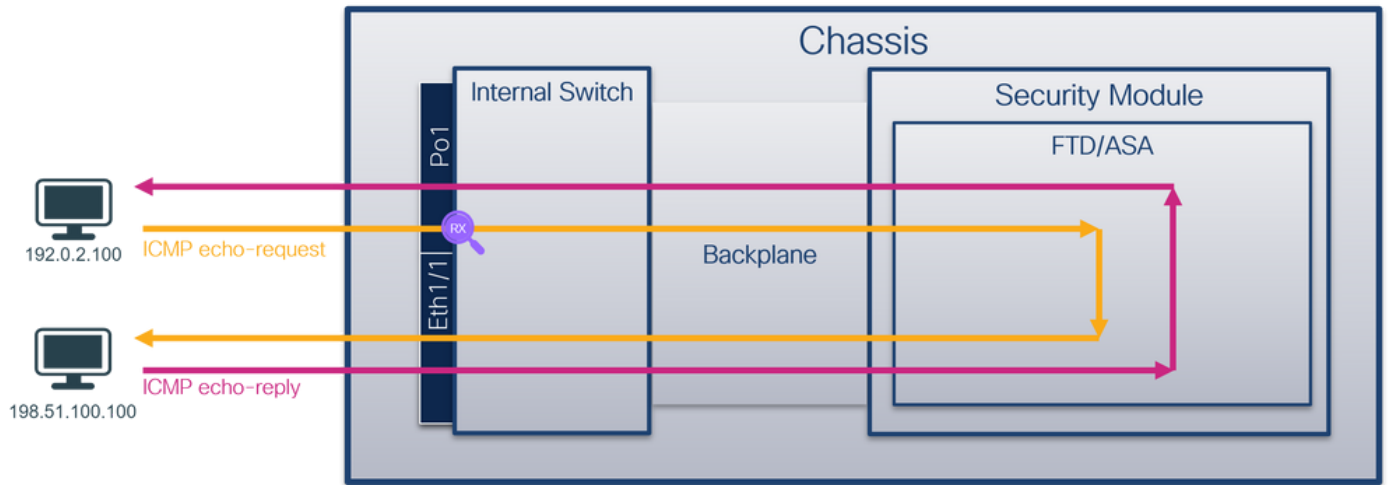
これらのシナリオは、Firepower 4100/9300内部スイッチキャプチャの一般的な使用例をカバーしています。

### 物理インターフェイスまたはポートチャンネルインターフェイスでのパケットキャプチャ

FCMとCLIを使用して、インターフェイスEthernet1/2またはPortchannel1インターフェイスのパケットキャプチャを設定および確認します。ポートチャンネルインターフェイスの場合は、すべての物理メンバーインターフェイスを選択してください。

### トポロジ、パケットフロー、およびキャプチャポイント



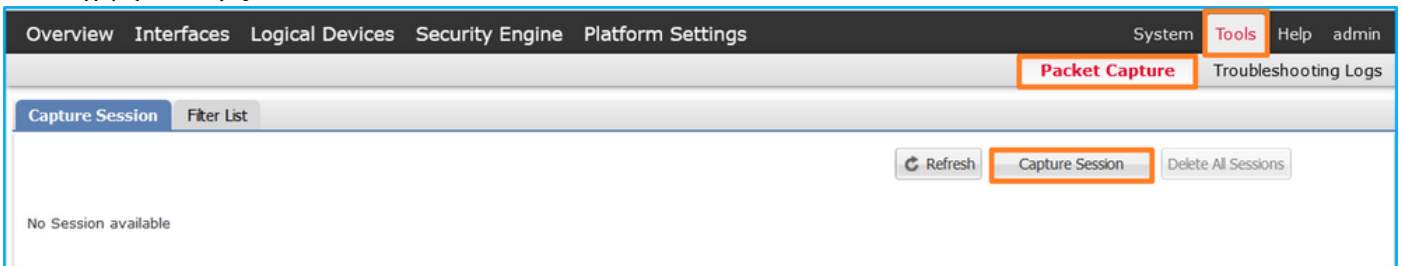


## コンフィギュレーション

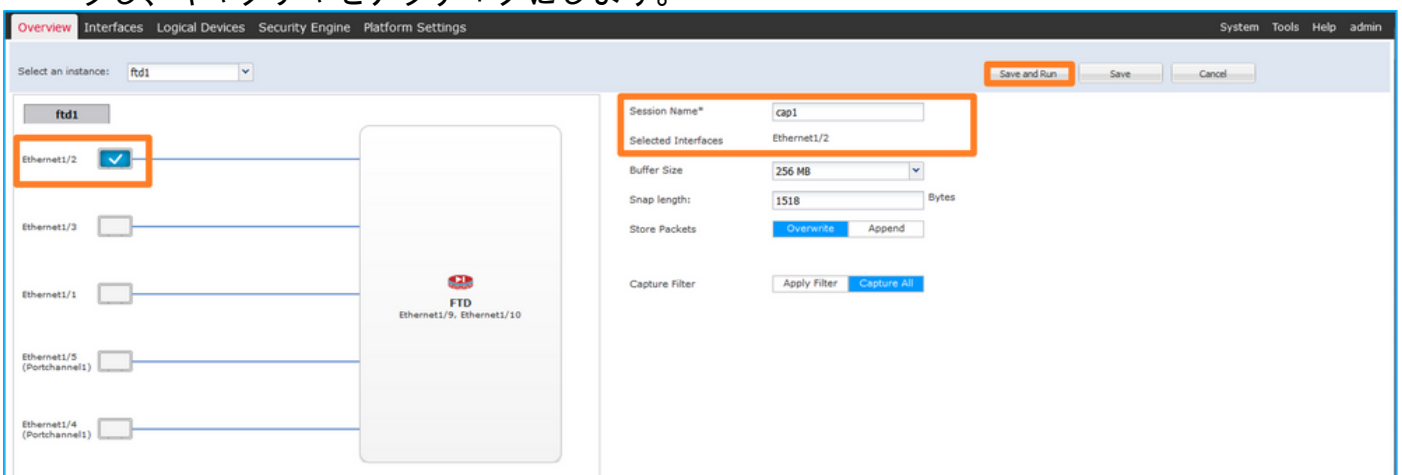
### FCM

インターフェイスEthernet1/2またはPortchannel1でパケットキャプチャを設定するには、FCMで次の手順を実行します。

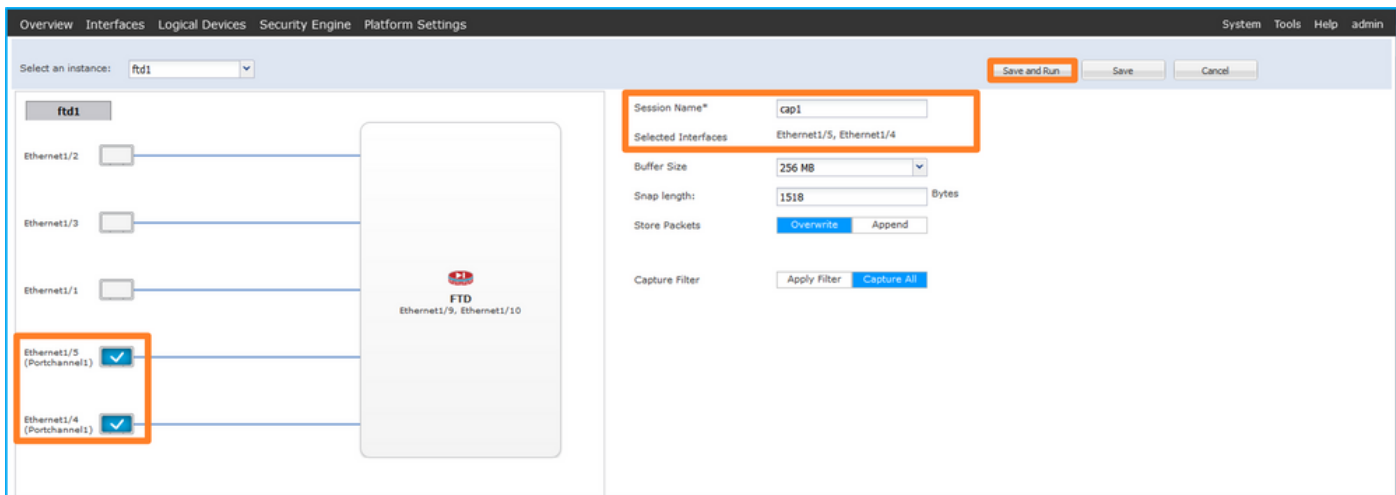
1. [Tools] > [Packet Capture] > [Capture Session] を使用して、新しいキャプチャセッションを作成します。



2. インターフェイスEthernet1/2を選択し、セッション名を指定して[Save and Run] をクリックし、キャプチャをアクティブにします。



3. ポートチャンネルインターフェイスの場合は、すべての物理メンバーインターフェイスを選択し、セッション名を指定して[Save and Run] をクリックし、キャプチャをアクティブにします。



## FXOS CLI

インターフェイスEthernet1/2またはPortchannel1でパケットキャプチャを設定するには、FXOS CLIで次の手順を実行します。

1. アプリケーションのタイプと識別子を特定します。

```
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. ポートチャネルインターフェイスの場合は、そのメンバーインターフェイスを特定します。

```
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. キャプチャセッションを作成します。

```
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 #
```

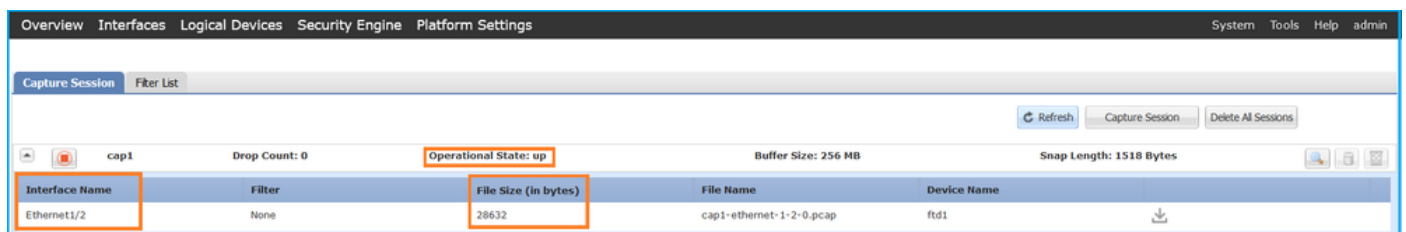
ポートチャネルインターフェイスの場合は、メンバーインターフェイスごとに個別のキャプチャが設定されます。

```
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 #
```

## 確認


## FCM

[Interface Name] を確認し、[Operational Status] が[up]になっており、[File Size (in bytes)] が増加していることを確認します。



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

メンバーインターフェイスEthernet1/4およびEthernet1/5を持つPortChannel1:



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

scope packet-captureでキャプチャの詳細を確認します。

```
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**

メンバーインターフェイスEthernet1/4およびEthernet1/5を持つポートチャンネル1:

```
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**

## キャプチャファイルの収集

「Firepower 4100/9300内部スイッチキャプチャファイルの収集」セクションの手順に従います。

## ファイル分析のキャプチャ

パケットキャプチャファイルリーダーアプリケーションを使用して、Ethernet1/2のキャプチャファイルを開きます。最初のパケットを選択し、キーポイントを確認します。

1. ICMPエコー要求パケットだけがキャプチャされます。各パケットはキャプチャされ、2回表



示されます。

- 元のパケットヘッダーにはVLANタグが付いていません。
- 内部スイッチは、入インターフェイスEthernet1/2を識別する追加ポートVLANタグ102を挿入します。
- 内部スイッチは、追加のVNタグを挿入します。

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-07-13 06:23:58.285080930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found)
2	2022-07-13 06:23:58.285082858	192.0.2.100	198.51.100.100	ICMP	102	0x9dec (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found)
3	2022-07-13 06:23:59.309048886	192.0.2.100	198.51.100.100	ICMP	108	0x9ed0 (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found)
4	2022-07-13 06:23:59.309193731	192.0.2.100	198.51.100.100	ICMP	102	0x9ed0 (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found)
5	2022-07-13 06:24:00.333054190	192.0.2.100	198.51.100.100	ICMP	108	0x9f20 (40736)	64	Echo (ping) request id=0x001a, seq=9/2304, ttl=64 (no response found)
6	2022-07-13 06:24:00.333056014	192.0.2.100	198.51.100.100	ICMP	102	0x9f20 (40736)	64	Echo (ping) request id=0x001a, seq=9/2304, ttl=64 (no response found)
7	2022-07-13 06:24:01.357173530	192.0.2.100	198.51.100.100	ICMP	108	0x9f2d (40749)	64	Echo (ping) request id=0x001a, seq=10/2560, ttl=64 (no response found)
8	2022-07-13 06:24:01.357174708	192.0.2.100	198.51.100.100	ICMP	102	0x9f2d (40749)	64	Echo (ping) request id=0x001a, seq=10/2560, ttl=64 (no response found)
9	2022-07-13 06:24:02.381073741	192.0.2.100	198.51.100.100	ICMP	108	0x9f88 (40840)	64	Echo (ping) request id=0x001a, seq=11/2816, ttl=64 (no response found)
10	2022-07-13 06:24:02.381074999	192.0.2.100	198.51.100.100	ICMP	102	0x9f88 (40840)	64	Echo (ping) request id=0x001a, seq=11/2816, ttl=64 (no response found)
11	2022-07-13 06:24:03.405199041	192.0.2.100	198.51.100.100	ICMP	108	0xa077 (41079)	64	Echo (ping) request id=0x001a, seq=12/3072, ttl=64 (no response found)
12	2022-07-13 06:24:03.405200261	192.0.2.100	198.51.100.100	ICMP	102	0xa077 (41079)	64	Echo (ping) request id=0x001a, seq=12/3072, ttl=64 (no response found)
13	2022-07-13 06:24:04.429155683	192.0.2.100	198.51.100.100	ICMP	108	0xa10f (41231)	64	Echo (ping) request id=0x001a, seq=13/3328, ttl=64 (no response found)
14	2022-07-13 06:24:04.429156831	192.0.2.100	198.51.100.100	ICMP	102	0xa10f (41231)	64	Echo (ping) request id=0x001a, seq=13/3328, ttl=64 (no response found)
15	2022-07-13 06:24:05.453156612	192.0.2.100	198.51.100.100	ICMP	108	0xa16a (41322)	64	Echo (ping) request id=0x001a, seq=14/3584, ttl=64 (no response found)
16	2022-07-13 06:24:05.453158052	192.0.2.100	198.51.100.100	ICMP	102	0xa16a (41322)	64	Echo (ping) request id=0x001a, seq=14/3584, ttl=64 (no response found)
17	2022-07-13 06:24:06.477127687	192.0.2.100	198.51.100.100	ICMP	108	0xa1e9 (41449)	64	Echo (ping) request id=0x001a, seq=15/3840, ttl=64 (no response found)
18	2022-07-13 06:24:06.477129899	192.0.2.100	198.51.100.100	ICMP	102	0xa1e9 (41449)	64	Echo (ping) request id=0x001a, seq=15/3840, ttl=64 (no response found)
19	2022-07-13 06:24:07.501291314	192.0.2.100	198.51.100.100	ICMP	108	0xa1f6 (41462)	64	Echo (ping) request id=0x001a, seq=16/4096, ttl=64 (no response found)
20	2022-07-13 06:24:07.501293041	192.0.2.100	198.51.100.100	ICMP	102	0xa1f6 (41462)	64	Echo (ping) request id=0x001a, seq=16/4096, ttl=64 (no response found)
21	2022-07-13 06:24:08.525089956	192.0.2.100	198.51.100.100	ICMP	108	0xa257 (41559)	64	Echo (ping) request id=0x001a, seq=17/4352, ttl=64 (no response found)
22	2022-07-13 06:24:08.525092088	192.0.2.100	198.51.100.100	ICMP	102	0xa257 (41559)	64	Echo (ping) request id=0x001a, seq=17/4352, ttl=64 (no response found)
23	2022-07-13 06:24:09.549236500	192.0.2.100	198.51.100.100	ICMP	108	0xa2a9 (41641)	64	Echo (ping) request id=0x001a, seq=18/4608, ttl=64 (no response found)
24	2022-07-13 06:24:09.549238564	192.0.2.100	198.51.100.100	ICMP	102	0xa2a9 (41641)	64	Echo (ping) request id=0x001a, seq=18/4608, ttl=64 (no response found)
25	2022-07-13 06:24:10.573110146	192.0.2.100	198.51.100.100	ICMP	108	0xa345 (41797)	64	Echo (ping) request id=0x001a, seq=19/4864, ttl=64 (no response found)
26	2022-07-13 06:24:10.573112504	192.0.2.100	198.51.100.100	ICMP	102	0xa345 (41797)	64	Echo (ping) request id=0x001a, seq=19/4864, ttl=64 (no response found)
27	2022-07-13 06:24:11.597086627	192.0.2.100	198.51.100.100	ICMP	108	0xa349 (41801)	64	Echo (ping) request id=0x001a, seq=20/5120, ttl=64 (no response found)
28	2022-07-13 06:24:11.597088170	192.0.2.100	198.51.100.100	ICMP	102	0xa349 (41801)	64	Echo (ping) request id=0x001a, seq=20/5120, ttl=64 (no response found)
29	2022-07-13 06:24:12.621061022	192.0.2.100	198.51.100.100	ICMP	108	0xa3dc (41948)	64	Echo (ping) request id=0x001a, seq=21/5376, ttl=64 (no response found)

> Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture\_u0\_1, id 0  
> Ethernet II, Src: Vmware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)

VLAN-Tag

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

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

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

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

Internet Control Message Protocol

```
0000 58 97 bd b9 77 0e 00 50 56 9d e8 be 81 00 00 66 X...w..P V.....f
0010 00 00 45 00 00 54 9d ec 40 00 40 01 af c0 c0 00 ..E..T..@....
0020 02 64 c6 33 64 64 08 00 4e a2 00 1a 00 07 f4 64 -d-3dd- N.....d
0030 ce 62 00 00 00 20 a2 07 00 00 00 00 00 11 11 -b.....
0040 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 |.....|
0050 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 *#558'()*+,-./01
0060 32 33 34 35 36 37 234567
```

2番目のパケットを選択し、キーポイントを確認します。

- ICMPエコー要求パケットだけがキャプチャされます。各パケットはキャプチャされ、2回表示されます。
- 元のパケットヘッダーにはVLANタグが付いていません。
- 内部スイッチは、入インターフェイスEthernet1/2を識別する追加ポートVLANタグ102を挿入します。

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-07-13 06:23:58.285080930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found)
2	2022-07-13 06:23:58.285082858	192.0.2.100	198.51.100.100	ICMP	102	0x9dec (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found)
3	2022-07-13 06:23:59.309048886	192.0.2.100	198.51.100.100	ICMP	108	0x9ed0 (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found)
4	2022-07-13 06:23:59.309193731	192.0.2.100	198.51.100.100	ICMP	102	0x9ed0 (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found)
5	2022-07-13 06:24:00.333054190	192.0.2.100	198.51.100.100	ICMP	108	0x9f20 (40736)	64	Echo (ping) request id=0x001a, seq=9/2304, ttl=64 (no response found)
6	2022-07-13 06:24:00.333056014	192.0.2.100	198.51.100.100	ICMP	102	0x9f20 (40736)	64	Echo (ping) request id=0x001a, seq=9/2304, ttl=64 (no response found)
7	2022-07-13 06:24:01.357173530	192.0.2.100	198.51.100.100	ICMP	108	0x9f2d (40749)	64	Echo (ping) request id=0x001a, seq=10/2560, ttl=64 (no response found)
8	2022-07-13 06:24:01.357174708	192.0.2.100	198.51.100.100	ICMP	102	0x9f2d (40749)	64	Echo (ping) request id=0x001a, seq=10/2560, ttl=64 (no response found)
9	2022-07-13 06:24:02.381073741	192.0.2.100	198.51.100.100	ICMP	108	0x9f88 (40840)	64	Echo (ping) request id=0x001a, seq=11/2816, ttl=64 (no response found)
10	2022-07-13 06:24:02.381074999	192.0.2.100	198.51.100.100	ICMP	102	0x9f88 (40840)	64	Echo (ping) request id=0x001a, seq=11/2816, ttl=64 (no response found)
11	2022-07-13 06:24:03.405199041	192.0.2.100	198.51.100.100	ICMP	108	0xa077 (41079)	64	Echo (ping) request id=0x001a, seq=12/3072, ttl=64 (no response found)
12	2022-07-13 06:24:03.405200261	192.0.2.100	198.51.100.100	ICMP	102	0xa077 (41079)	64	Echo (ping) request id=0x001a, seq=12/3072, ttl=64 (no response found)
13	2022-07-13 06:24:04.429155683	192.0.2.100	198.51.100.100	ICMP	108	0xa10f (41231)	64	Echo (ping) request id=0x001a, seq=13/3328, ttl=64 (no response found)
14	2022-07-13 06:24:04.429156831	192.0.2.100	198.51.100.100	ICMP	102	0xa10f (41231)	64	Echo (ping) request id=0x001a, seq=13/3328, ttl=64 (no response found)
15	2022-07-13 06:24:05.453156612	192.0.2.100	198.51.100.100	ICMP	108	0xa16a (41322)	64	Echo (ping) request id=0x001a, seq=14/3584, ttl=64 (no response found)
16	2022-07-13 06:24:05.453158052	192.0.2.100	198.51.100.100	ICMP	102	0xa16a (41322)	64	Echo (ping) request id=0x001a, seq=14/3584, ttl=64 (no response found)
17	2022-07-13 06:24:06.477127687	192.0.2.100	198.51.100.100	ICMP	108	0xa1e9 (41449)	64	Echo (ping) request id=0x001a, seq=15/3840, ttl=64 (no response found)
18	2022-07-13 06:24:06.477129899	192.0.2.100	198.51.100.100	ICMP	102	0xa1e9 (41449)	64	Echo (ping) request id=0x001a, seq=15/3840, ttl=64 (no response found)
19	2022-07-13 06:24:07.501291314	192.0.2.100	198.51.100.100	ICMP	108	0xa1f6 (41462)	64	Echo (ping) request id=0x001a, seq=16/4096, ttl=64 (no response found)
20	2022-07-13 06:24:07.501293041	192.0.2.100	198.51.100.100	ICMP	102	0xa1f6 (41462)	64	Echo (ping) request id=0x001a, seq=16/4096, ttl=64 (no response found)
21	2022-07-13 06:24:08.525089956	192.0.2.100	198.51.100.100	ICMP	108	0xa257 (41559)	64	Echo (ping) request id=0x001a, seq=17/4352, ttl=64 (no response found)
22	2022-07-13 06:24:08.525092088	192.0.2.100	198.51.100.100	ICMP	102	0xa257 (41559)	64	Echo (ping) request id=0x001a, seq=17/4352, ttl=64 (no response found)
23	2022-07-13 06:24:09.549236500	192.0.2.100	198.51.100.100	ICMP	108	0xa2a9 (41641)	64	Echo (ping) request id=0x001a, seq=18/4608, ttl=64 (no response found)
24	2022-07-13 06:24:09.549238564	192.0.2.100	198.51.100.100	ICMP	102	0xa2a9 (41641)	64	Echo (ping) request id=0x001a, seq=18/4608, ttl=64 (no response found)
25	2022-07-13 06:24:10.573110146	192.0.2.100	198.51.100.100	ICMP	108	0xa345 (41797)	64	Echo (ping) request id=0x001a, seq=19/4864, ttl=64 (no response found)
26	2022-07-13 06:24:10.573112504	192.0.2.100	198.51.100.100	ICMP	102	0xa345 (41797)	64	Echo (ping) request id=0x001a, seq=19/4864, ttl=64 (no response found)
27	2022-07-13 06:24:11.597086627	192.0.2.100	198.51.100.100	ICMP	108	0xa349 (41801)	64	Echo (ping) request id=0x001a, seq=20/5120, ttl=64 (no response found)
28	2022-07-13 06:24:11.597088170	192.0.2.100	198.51.100.100	ICMP	102	0xa349 (41801)	64	Echo (ping) request id=0x001a, seq=20/5120, ttl=64 (no response found)
29	2022-07-13 06:24:12.621061022	192.0.2.100	198.51.100.100	ICMP	108	0xa3dc (41948)	64	Echo (ping) request id=0x001a, seq=21/5376, ttl=64 (no response found)

> Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture\_u0\_1, id 0  
> Ethernet II, Src: Vmware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)

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

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

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

Internet Control Message Protocol

```
0000 58 97 bd b9 77 0e 00 50 56 9d e8 be 81 00 00 66 X...w..P V.....f
0010 08 00 45 00 00 54 9d ec 40 00 40 01 af c0 c0 00 ..E..T..@....
0020 02 64 c6 33 64 64 08 00 4e a2 00 1a 00 07 f4 64 -d-3dd- N.....d
0030 ce 62 00 00 00 20 a2 07 00 00 00 00 00 11 11 -b.....
0040 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 |.....|
0050 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 *#558'()*+,-./01
0060 32 33 34 35 36 37 234567
```



Portchannel1メンバーインターフェイスのキャプチャファイルを開きます。最初の packets を選択し、キーポイントを確認します。

1. ICMPエコー要求パケットだけがキャプチャされます。各パケットはキャプチャされ、2回表示されます。
2. 元のパケットヘッダーにはVLANタグが付いていません。
3. 内部スイッチは、入力インターフェイスPortchannel1を識別する追加ポートVLANタグ1001を挿入します。
4. 内部スイッチは、追加のVNタグを挿入します。

Packet 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture\_u0\_3, i

Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: a2:76:f2:00:00:25 (a2:76:f2:00:00:25)

VN-Tag

1. .... = Direction: From Bridge

.0. .... = Pointer: vif\_id

..00 0000 0101 0100 .... = Destination: 84

..... = 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: 1001

000. .... = Priority: Best Effort (default) (0)

...0 .... = DEI: Ineligible

.... 0011 1110 1001 = ID: 1001

Type: IPv4 (0x0800)

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

Internet Control Message Protocol

2番目の packets を選択し、キーポイントを確認します。

1. ICMPエコー要求パケットだけがキャプチャされます。各パケットはキャプチャされ、2回表示されます。
2. 元のパケットヘッダーにはVLANタグが付いていません。
3. 内部スイッチは、入力インターフェイスPortchannel1を識別する追加ポートVLANタグ1001を挿入します。

Packet 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture\_u0\_3, i

Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: a2:76:f2:00:00:25 (a2:76:f2:00:00:25)

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

000. .... = Priority: Best Effort (default) (0)

...0 .... = DEI: Ineligible

.... 0011 1110 1001 = ID: 1001

Type: IPv4 (0x0800)

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

Internet Control Message Protocol



## 説明

前面インターフェイスでパケットキャプチャが設定されると、スイッチは各パケットを同時に2回キャプチャします。

- ポートVLANタグの挿入後。
- VNタグの挿入後。

操作順では、VNタグはポートVLANタグの挿入よりも後の段階で挿入されます。ただし、キャプチャファイルでは、VNタグが付いたパケットがポートVLANタグが付いたパケットよりも前に表示されます。

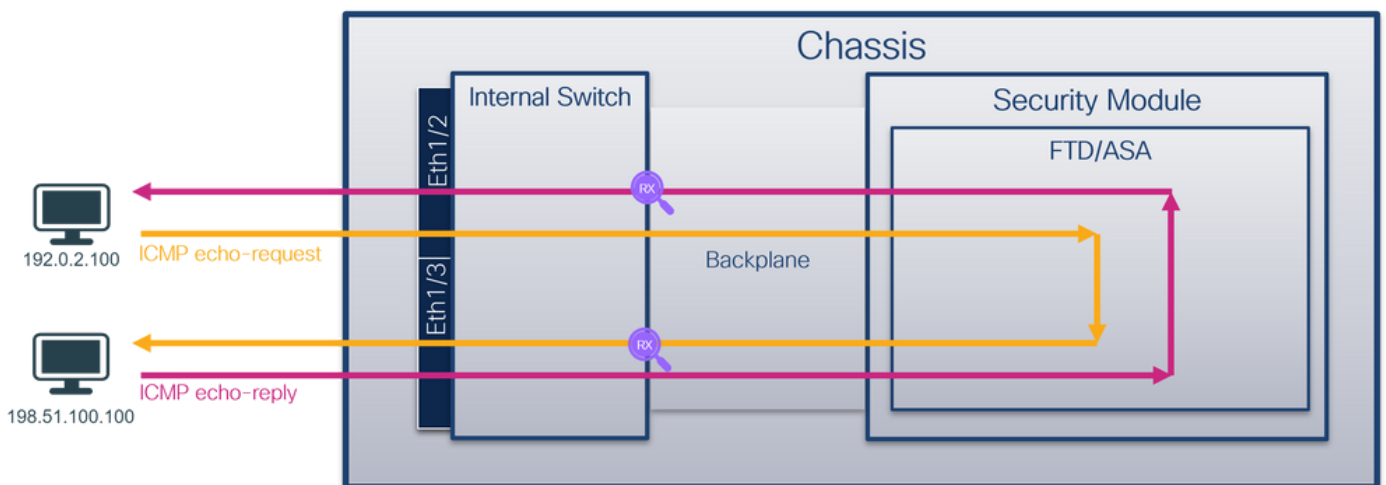
タスクの要約を次の表に示します。

タスク	キャプチャポイント	キャプチャされたパケットの内部ポートVLAN	方向	キャプチャされたトラフィック
インターフェイス Ethernet1/2でのパケットキャプチャの設定と確認	Ethernet1/2	102	入力のみ	ホスト192.0.2.100からホスト198.51.100.100へのICMPエコーリクエスト
メンバーインターフェイス Ethernet1/4および Ethernet1/5を持つインターフェイス Portchannel1でパケットキャプチャを設定および確認します	Ethernet1/4 Ethernet1/5	1001	入力のみ	ホスト192.0.2.100からホスト198.51.100.100へのICMPエコーリクエスト

## バックプレーンインターフェイスでのパケットキャプチャ

FCMとCLIを使用して、バックプレーンインターフェイスのパケットキャプチャを設定および確認します。

### トポロジ、パケットフロー、およびキャプチャポイント

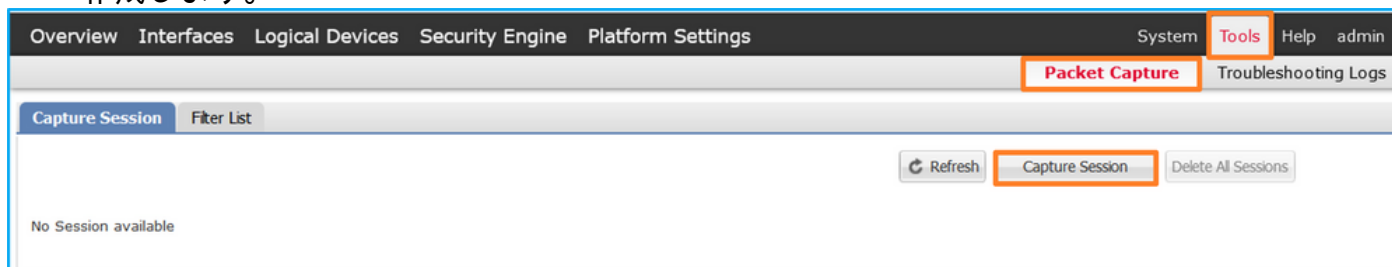


## コンフィギュレーション

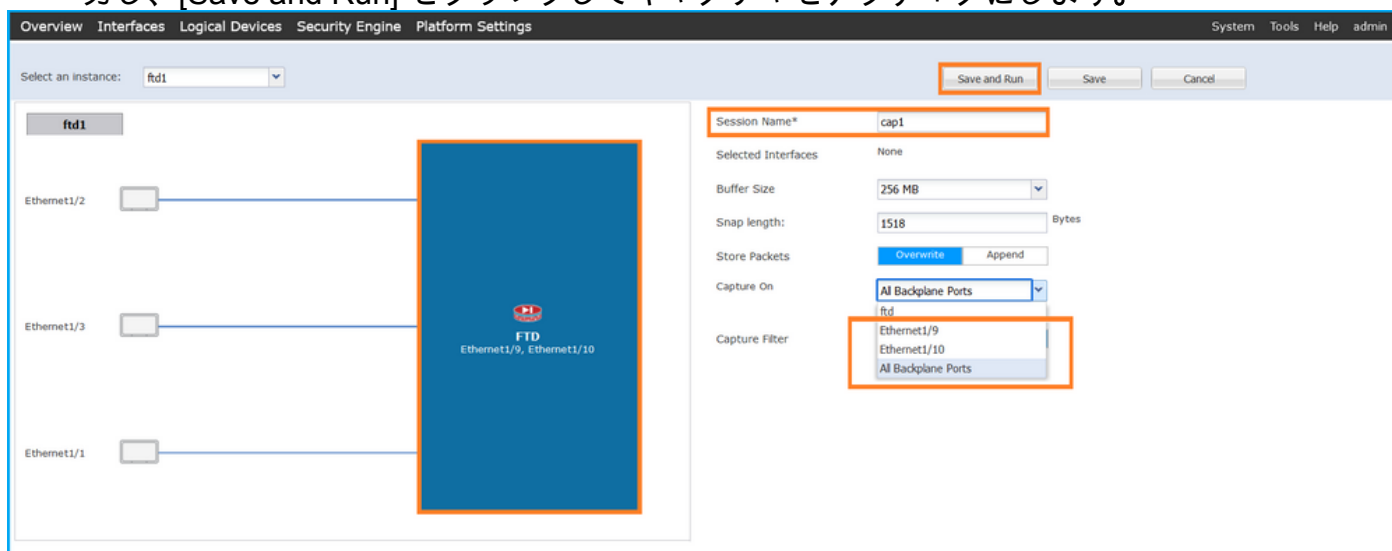
### FCM

バックプレーンインターフェイスでパケットキャプチャを設定するには、FCMで次の手順を実行します。

1. [Tools] > [Packet Capture] > [Capture Session] を使用して、新しいキャプチャセッションを作成します。



2. すべてのバックプレーンインターフェイスでパケットをキャプチャするには、アプリケーションを選択し、ドロップダウンリストの[Capture On] から[All Backplane Ports] を選択します。または、特定のバックプレーンインターフェイスを選択します。この場合、バックプレーンインターフェイスEthernet1/9およびEthernet1/10が使用可能です。[Session Name] を入力し、[Save and Run] をクリックしてキャプチャをアクティブにします。



## FXOS CLI

バックプレーンインターフェイスでパケットキャプチャを設定するには、FXOS CLIで次の手順を実行します。

1. アプリケーションのタイプと識別子を特定します。

```
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. キャプチャセッションを作成します。

```
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 #

```

## 確認

## FCM

[Interface Name] を確認し、[Operational Status] が[up]になっており、[File Size (in bytes)]が増加していることを確認します。

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

scope packet-captureでキャプチャの詳細を確認します。

```

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

### キャプチャファイルの収集

「Firepower 4100/9300内部スイッチキャプチャファイルの収集」セクションの手順に従います。

### ファイル分析のキャプチャ

パケットキャプチャファイルリーダーアプリケーションを使用して、キャプチャファイルを開きます。複数のバックプレーンインターフェイスがある場合は、各バックプレーンインターフェイスのすべてのキャプチャファイルを必ず開いてください。この場合、パケットはバックプレーンインターフェイスEthernet1/9でキャプチャされます。

最初と2番目のパケットを選択し、キーポイントを確認します。

1. 各ICMPエコー要求パケットがキャプチャされ、2回表示されます。
2. 元のパケットヘッダーにはVLANタグが付いていません。
3. 内部スイッチは、出カインターフェイスEthernet1/3を識別する追加のポートVLANタグ 103を挿入します。
4. 内部スイッチは、追加のVNタグを挿入します。

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	0xc2c (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	0xc2c (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64

```

> Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
> Ethernet II, Src: Cisco b9:77:2d (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
    .. .. = 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: 103
    000... .. = Priority: Best Effort (default) (0)
    ..0... .. = DEI: Ineligible
    .... 0000 0110 0111 = ID: 103
    Type: IPv4 (0x8000)
  > Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
  > Internet Control Message Protocol
  
```



No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-07-14 20:20:36.513854256	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (no response found!)
2	2022-07-14 20:20:36.513857289	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (reply in 3)
3	2022-07-14 20:20:36.514117394	198.51.100.100	192.0.2.100	ICMP	108	0xccc2c (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 2)
4	2022-07-14 20:20:37.537723822	192.0.2.100	198.51.100.100	ICMP	108	0xccc2c (52268)	64	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (request in 3)
5	2022-07-14 20:20:37.537723822	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040)	64	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (no response found!)
6	2022-07-14 20:20:37.537726588	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040)	64	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (reply in 7)
7	2022-07-14 20:20:37.538046165	198.51.100.100	192.0.2.100	ICMP	108	0xccc9b (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	0xccc9b (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 6)
9	2022-07-14 20:20:38.561776664	192.0.2.100	198.51.100.100	ICMP	108	0xccc9b (52379)	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	0xccc9b (52379)	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	0xccc4 (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	0xccc4 (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 10)
13	2022-07-14 20:20:39.585677043	192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366)	64	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (no response found!)
14	2022-07-14 20:20:39.585678455	192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366)	64	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (reply in 15)
15	2022-07-14 20:20:39.585936554	198.51.100.100	192.0.2.100	ICMP	108	0xcccdb (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	0xcccdb (52621)	64	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64 (request in 14)
17	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 (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	0xcccdb (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	0xcccdb (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64 (request in 18)
21	2022-07-14 20:20:41.633805153	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (no response found!)
22	2022-07-14 20:20:41.633806997	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (reply in 23)
23	2022-07-14 20:20:41.634084102	198.51.100.100	192.0.2.100	ICMP	108	0xccc36 (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	0xccc36 (52790)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64 (request in 22)
25	2022-07-14 20:20:42.657709988	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (no response found!)
26	2022-07-14 20:20:42.657711660	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (reply in 27)
27	2022-07-14 20:20:42.657980675	198.51.100.100	192.0.2.100	ICMP	108	0xccc49 (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	0xccc49 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64 (request in 26)
29	2022-07-14 20:20:43.681736697	192.0.2.100	198.51.100.100	ICMP	108	0x5c52 (23634)	64	Echo (ping) request id=0x0001, seq=22/5632, ttl=64 (no response found!)

Frame 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
..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: 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
  
```

3番目と4番目のパケットを選択し、キーポイントを確認します。

1. 各ICMPエコー応答はキャプチャされ、2回表示されます。
2. 元のパケットヘッダーにはVLANタグが付いていません。
3. 内部スイッチは、出カインターフェイスEthernet1/2を識別する追加のポートVLANタグ 102を挿入します。
4. 内部スイッチは、追加のVNタグを挿入します。

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	0xccc2c (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 2)
4	2022-07-14 20:20:37.537723822	192.0.2.100	198.51.100.100	ICMP	108	0xccc2c (52268)	64	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (request in 3)

Frame 3: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture\_u0\_8, id 0  
Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VMware 9d:e8:b6 (00:50:56:9d:e8:b6)

```

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
  
```

## 説明

バックプレーンインターフェイスでパケットキャプチャが設定されると、スイッチは各パケットを同時に2回キャプチャします。この場合、内部スイッチは、セキュリティモジュール上のアプリケーションによってポートVLANタグとVNタグですでにタグ付けされたパケットを受信します。VLANタグは、内部シャーシがパケットをネットワークに転送するために使用する出力インターフェイスを示します。ICMPエコー要求パケットのVLANタグ103はEthernet1/3を出力インターフェイスとして識別し、ICMPエコー応答パケットのVLANタグ102はEthernet1/2を出力インターフェイスとして識別します。内部スイッチは、パケットがネットワークに転送される前に、VNタグと内部インターフェイスVLANタグを削除します。

タスクの要約を次の表に示します。

タスク	キャプチャポイント	キャプチャされたパケットの内部ポートVLAN	方向	キャプチャされたトラフィック
バックプレーンインターフェイスでのパケットキャプチャの設定と確認	バックプレーンインターフェイス	102 103	入力のみ	ホスト192.0.2.100からホスト198.51.100.100へのICMPエコー ホスト198.51.100.100からホスト192.0.2.100へのICMPエコー応

## アプリケーションおよびアプリケーションポートでのパケットキャプチャ

アプリケーションまたはアプリケーションポートのパケットキャプチャは、常にバックプレーンインターフェイスに設定され、さらにユーザがアプリケーションキャプチャの方向を指定すると、前面インターフェイスにも設定されます。

主に2つの使用例があります。

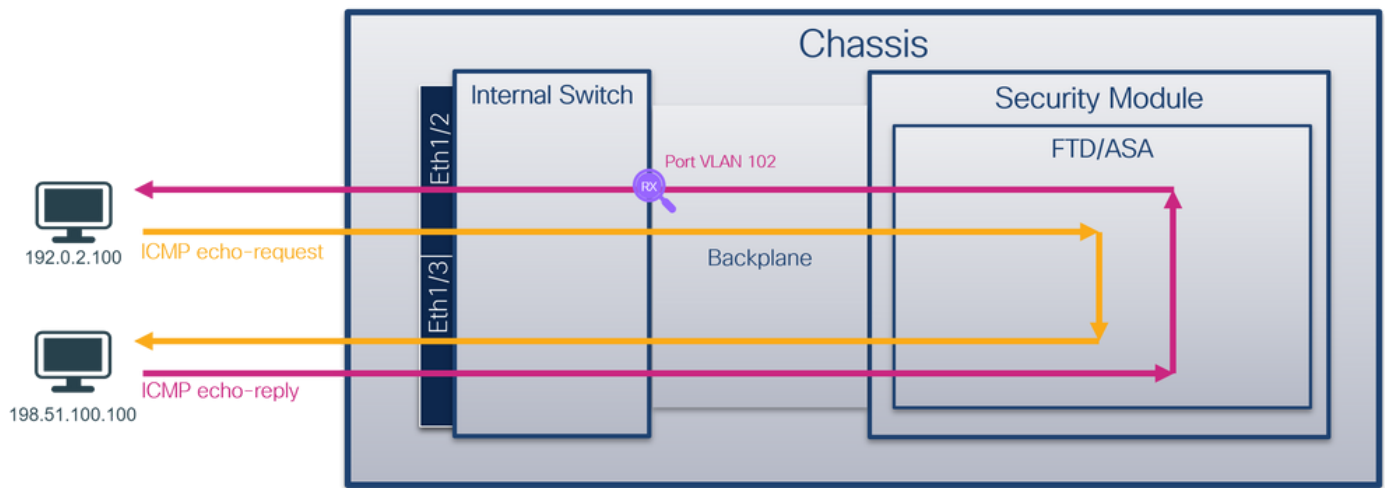
- 特定の前面インターフェイスから発信されるパケットのパケットキャプチャをバックプレーンインターフェイスで設定します。たとえば、インターフェイスEthernet1/2から発信されるパケットのパケットキャプチャをバックプレーンインターフェイスEthernet1/9に設定します。
- 特定の前面インターフェイスとバックプレーンインターフェイスで同時パケットキャプチャを設定します。たとえば、インターフェイスEthernet1/2を離れるパケットに対して、インターフェイスEthernet1/2とバックプレーンインターフェイスEthernet1/9で同時パケットキャプチャを設定します。

このセクションでは、両方の使用例について説明します。

### タスク 1

FCMとCLIを使用して、バックプレーンインターフェイスでパケットキャプチャを設定および確認します。アプリケーションポートEthernet1/2が出力インターフェイスとして識別されているパケットがキャプチャされます。この場合、ICMP応答がキャプチャされます。

### トポロジ、パケットフロー、およびキャプチャポイント

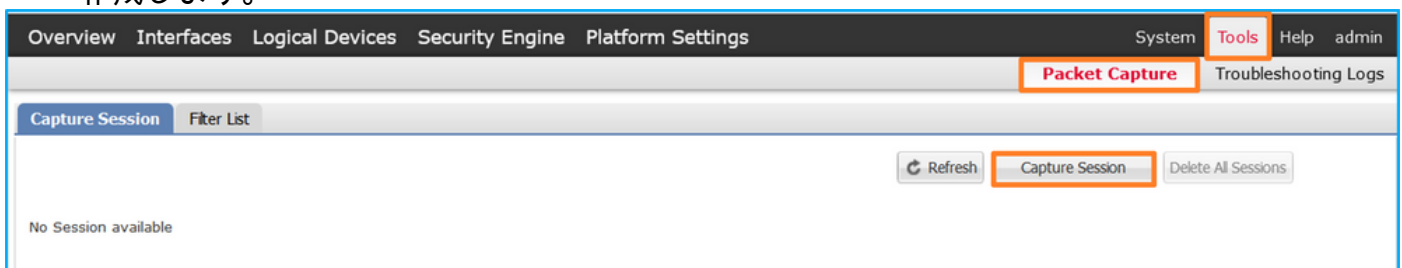


## コンフィギュレーション

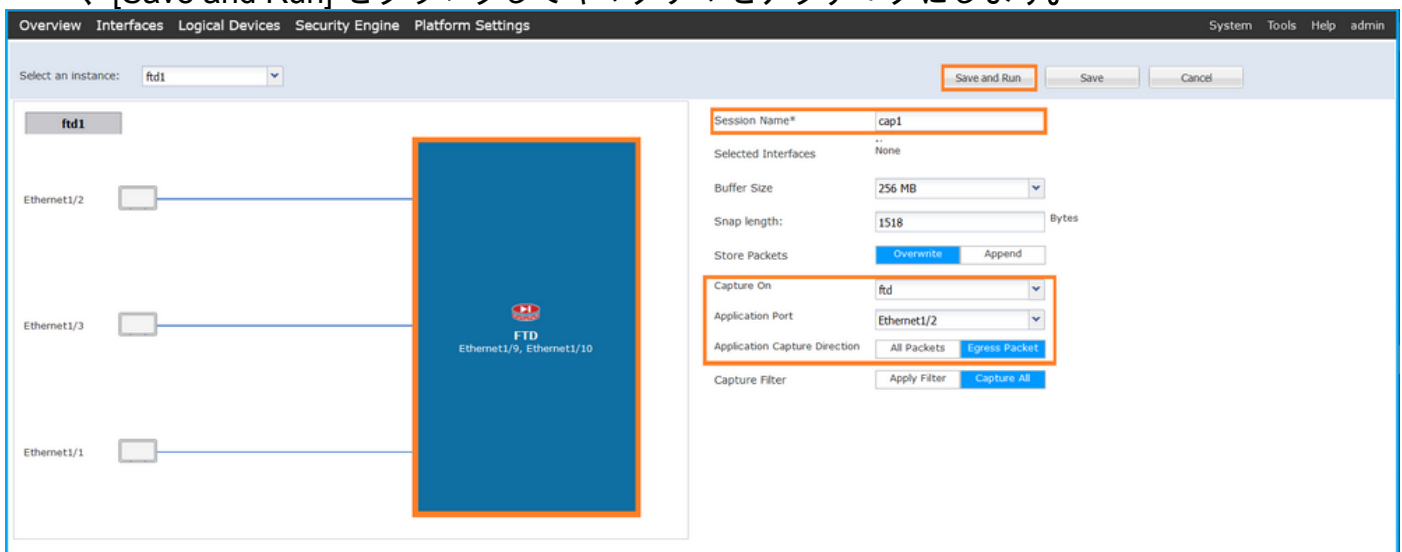
### FCM

FTDアプリケーションとアプリケーションポートEthernet1/2でパケットキャプチャを設定するには、FCMで次の手順を実行します。

1. [Tools] > [Packet Capture] > [Capture Session] を使用して、新しいキャプチャセッションを作成します。



2. [Application Port] ドロップダウンリストでアプリケーションEthernet1/2を選択し、[Application Capture Direction] で[Egress Packet] を選択します。[Session Name] を入力し、[Save and Run] をクリックしてキャプチャをアクティブにします。



### FXOS CLI

バックプレーンインターフェイスでパケットキャプチャを設定するには、FXOS CLIで次の手順を

実行します。

## 1. アプリケーションのタイプと識別子を特定します。

```
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
```

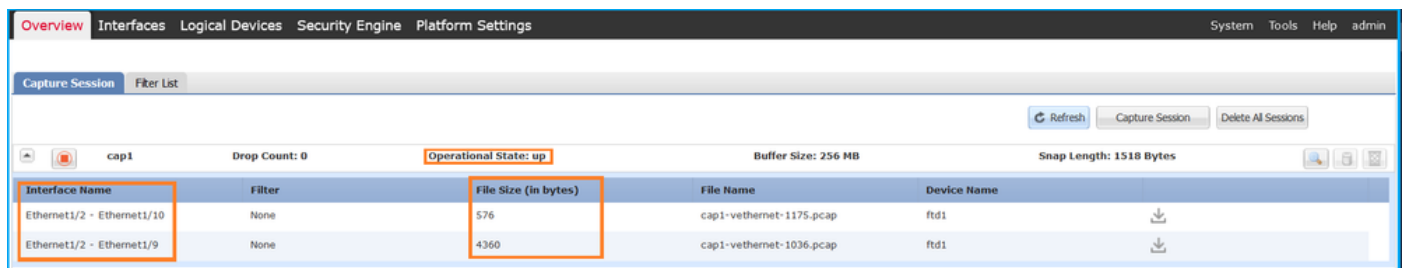
## 2. キャプチャセッションを作成します。

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

確認

## FCM

[Interface Name] を確認し、[Operational Status] が[up]になっており、[File Size (in bytes)] が増加していることを確認します。



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

## FXOS CLI

scope packet-captureでキャプチャの詳細を確認します。

```
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:

## キャプチャファイルの収集

「Firepower 4100/9300内部スイッチキャプチャファイルの収集」セクションの手順に従います。

## ファイル分析のキャプチャ

パケットキャプチャファイルリーダーアプリケーションを使用して、キャプチャファイルを開きます。複数のバックプレーンインターフェイスがある場合は、各バックプレーンインターフェイスのすべてのキャプチャファイルを必ず開いてください。この場合、パケットはバックプレーンインターフェイスEthernet1/9でキャプチャされます。

最初と2番目のパケットを選択し、キーポイントを確認します。

1. 各ICMPエコー応答はキャプチャされ、2回表示されます。
2. 元のパケットヘッダーにはVLANタグが付いていません。
3. 内部スイッチは、出カインターフェイスEthernet1/2を識別する追加のポートVLANタグ **102**を挿入します。
4. 内部スイッチは、追加のVNタグを挿入します。

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 10:03:29.354979591	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply
16	2022-08-01 10:03:29.354993706	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)

  VN-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
  
```

Offset	Hex	ASCII
0000	00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00	PV...X...M...&..
0010	00 0a 81 00 00 66 08 00 45 00 00 54 42 f8 00 00	...f...E...TB...
0020	40 01 4a b5 c6 33 64 64 c0 00 02 64 00 00 00 04	@J...3dd...d...
0030	00 12 00 01 dd a4 e7 62 00 00 00 e3 0d 09 00	...b... ..
0040	00 00 00 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	... !"# \$%&'()*+,-./:;<=>?@A
0060	2c 2d 2e 2f 30 31 32 33 34 35 36 37	...:;=>?@A

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 10:03:29.354979591	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply
16	2022-08-01 10:03:29.354993706	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)

  VN-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
  
```

Offset	Hex	ASCII
0000	00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00	PV...X...M...&..
0010	00 0a 81 00 00 66 08 00 45 00 00 54 42 f8 00 00	...f...E...TB...
0020	40 01 4a b5 c6 33 64 64 c0 00 02 64 00 00 00 04	@J...3dd...d...
0030	00 12 00 01 dd a4 e7 62 00 00 00 e3 0d 09 00	...b... ..
0040	00 00 00 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	... !"# \$%&'()*+,-./:;<=>?@A
0060	2c 2d 2e 2f 30 31 32 33 34 35 36 37	...:;=>?@A

### 説明

この場合、ポートVLANタグ102を持つEthernet1/2がICMPエコー応答パケットの出カインターフェイスです。

キャプチャオプションでアプリケーションキャプチャ方向がEgressに設定されている場合、イーサネットヘッダーにポートVLANタグ102が含まれるパケットは、入力方向のバックプレーンインターフェイスでキャプチャされます。

タスクの要約を次の表に示します。

タスク	キャプチャポイント	キャプチャされたパケットの内部ポートVLAN	方向	キャプチャされたトラフィック
アプリケーションおよびアプリケーションポートEthernet1/2でのキャプチャの設定と確認	バックプレーンインターフェイス	102	入力のみ	ホスト198.51.100.100からホスト192.0.2.100へのICMPエコー

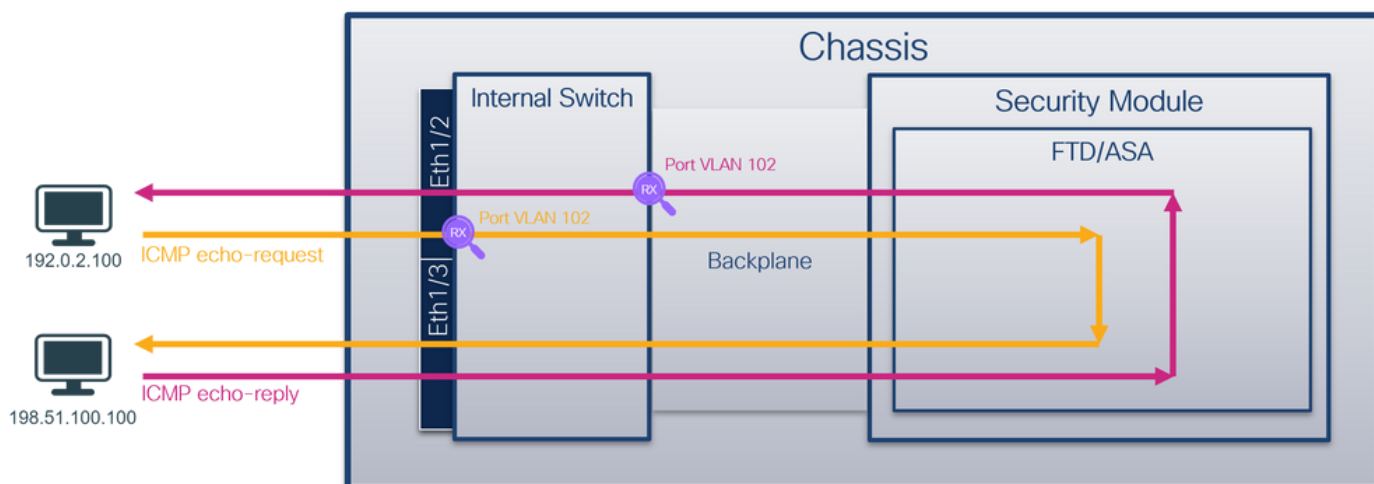
## タスク 2

FCMとCLIを使用して、バックプレーンインターフェイスと前面インターフェイスEthernet1/2の packets キャプチャを設定および確認します。

同時 packets キャプチャは次の場所で設定されます。

- 前面インターフェイス：インターフェイスEthernet1/2上のポートVLAN 102を持つ packets がキャプチャされます。キャプチャされた packets はICMPエコー要求です。
- バックプレーンインターフェイス：Ethernet1/2が出力インターフェイスとして識別される packets 、またはポートVLAN 102の packets がキャプチャされます。キャプチャされた packets はICMPエコー応答です。

### トポロジ、パケットフロー、およびキャプチャポイント

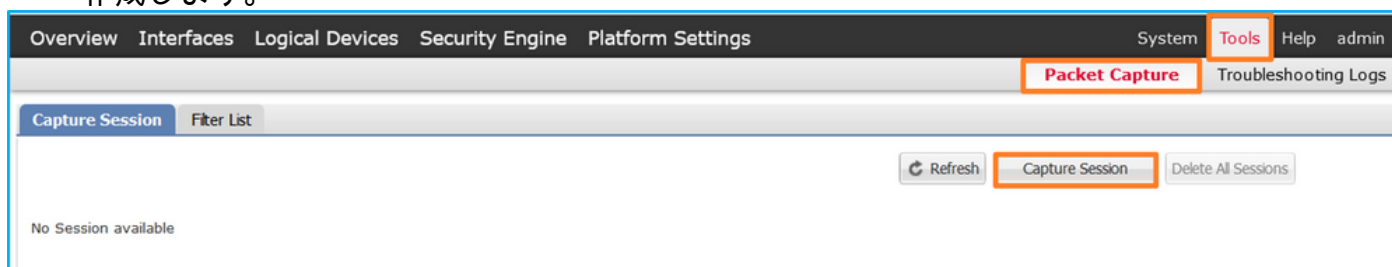


## コンフィギュレーション

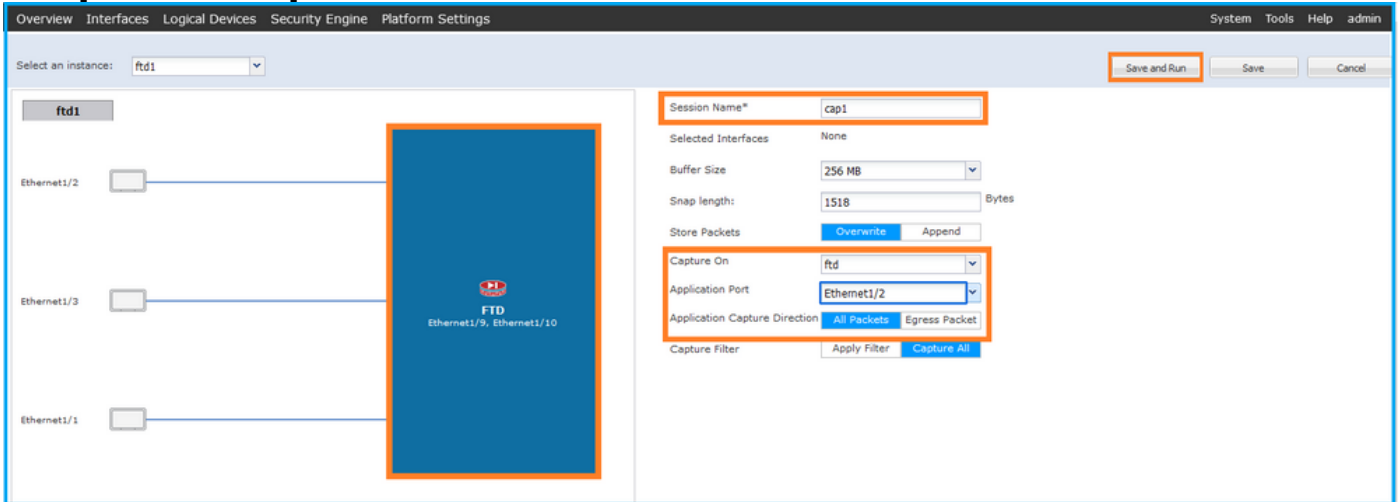
### FCM

FTDアプリケーションとアプリケーションポートEthernet1/2で packets キャプチャを設定するには、FCMで次の手順を実行します。

1. [Tools] > [Packet Capture] > [Capture Session] を使用して、新しいキャプチャセッションを作成します。



- [Application Port] ドロップダウンリストでFTDアプリケーションEthernet1/2を選択し、[Application Capture Direction] で[All Packets] を選択します。[Session Name] を入力し、[Save and Run] をクリックしてキャプチャをアクティブにします。



## FXOS CLI

バックプレーンインターフェイスでパケットキャプチャを設定するには、FXOS CLIで次の手順を実行します。

- アプリケーションのタイプと識別子を特定します。

```
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		

- キャプチャセッションを作成します。

```
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
```

## 確認

## FCM

[Interface Name] を確認し、[Operational Status] が[up]になっており、[File Size (in bytes)] が増加していることを確認します。

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

## FXOS CLI

scope packet-captureでキャプチャの詳細を確認します。

```
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:

### キャプチャファイルの収集

「Firepower 4100/9300内部スイッチキャプチャファイルの収集」セクションの手順に従います。

### ファイル分析のキャプチャ

パケットキャプチャファイルリーダーアプリケーションを使用して、キャプチャファイルを開きます。複数のバックプレーンインターフェイスがある場合は、各バックプレーンインターフェイスのすべてのキャプチャファイルを必ず開いてください。この場合、パケットはバックプレーンインターフェイスEthernet1/9でキャプチャされます。

インターフェイスEthernet1/2のキャプチャファイルを開き、最初のパケットを選択して、キーポイントを確認します。

1. ICMPエコー要求パケットだけがキャプチャされます。各パケットはキャプチャされ、2回表示されます。
2. 元のパケットヘッダーにはVLANタグが付いていません。
3. 内部スイッチは、入力インターフェイスEthernet1/2を識別する追加ポートVLANタグ102を挿入します。
4. 内部スイッチは、追加のVNタグを挿入します。

The screenshot displays a network traffic capture. The top table lists 29 ICMP Echo (ping) requests from source 192.0.2.100 to destination 198.51.100.100. The 'Info' column for each entry shows 'id=0x0013, seq=1/256, ttl=64 (no response found!)'. A red box highlights the first entry in this table.

Below the table, the packet details for the selected frame are shown:

- 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 (00:56:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e).
- VN-Tag:**
  - Direction: From Bridge
  - Pointer: vif1d
  - Destination: 10
  - Looped: No
  - Reserved: 0
  - Version: 0
  - Source: 0
  - Type: 802.1Q Virtual LAN (0x8100)
- 802.1Q Virtual LAN:**
  - Priority: Best Effort (default) (0)
  - DEI: Ineligible
  - ID: 102
  - Type: IPv4 (0x0800)
- Internet Protocol Version 4:** Src: 192.0.2.100, Dst: 198.51.100.100
- Internet Control Message Protocol:**

Red boxes and numbers 2, 3, and 4 in the image highlight the Ethernet II, 802.1Q Virtual LAN, and Internet Protocol Version 4 sections respectively.

2番目のパケットを選択し、キーポイントを確認します。

1. ICMPエコー要求パケットだけがキャプチャされます。各パケットはキャプチャされ、2回表示されます。
2. 元のパケットヘッダーにはVLANタグが付いていません。
3. 内部スイッチは、入力インターフェイスEthernet1/2を識別する追加ポートVLANタグ102を挿入します。

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 11:33:19.070693081	192.0.2.100	198.51.100.100	ICMP	108	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found!)
2	2022-08-01 11:33:19.070695347	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found!)
3	2022-08-01 11:33:19.071217121	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found!)
4	2022-08-01 11:33:19.071218458	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found!)
5	2022-08-01 11:33:20.072036625	192.0.2.100	198.51.100.100	ICMP	108	0xc0ae (49326)	64	Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found!)
6	2022-08-01 11:33:20.072038399	192.0.2.100	198.51.100.100	ICMP	102	0xc0ae (49326)	64	Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found!)
7	2022-08-01 11:33:21.073266030	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 11:33:23.075799089	192.0.2.100	198.51.100.100	ICMP	108	0xc208 (49672)	64	Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found!)
12	2022-08-01 11:33:23.075791513	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 11:33:24.081841306	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	0xc262 (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	0xc262 (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 11:33:28.178477175	192.0.2.100	198.51.100.100	ICMP	108	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found!)
22	2022-08-01 11:33:28.17849075	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found!)
23	2022-08-01 11:33:29.201804760	192.0.2.100	198.51.100.100	ICMP	108	0xc578 (50552)	64	Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found!)
24	2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	102	0xc578 (50552)	64	Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found!)
25	2022-08-01 11:33:30.225834765	192.0.2.100	198.51.100.100	ICMP	108	0xc585 (50565)	64	Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found!)
26	2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (50565)	64	Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found!)
27	2022-08-01 11:33:31.249828955	192.0.2.100	198.51.100.100	ICMP	108	0xc618 (50712)	64	Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found!)
28	2022-08-01 11:33:31.249831121	192.0.2.100	198.51.100.100	ICMP	102	0xc618 (50712)	64	Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found!)
29	2022-08-01 11:33:32.273867960	192.0.2.100	198.51.100.100	ICMP	108	0xc64f (50767)	64	Echo (ping) request id=0x0013, seq=14/3584, ttl=64 (no response found!)

```

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

インターフェイスEthernet1/9のキャプチャファイルを開き、最初と2番目のパケットを選択し、キーポイントを確認します。

1. 各ICMPエコー応答はキャプチャされ、2回表示されます。
2. 元のパケットヘッダーにはVLANタグが付いていません。
3. 内部スイッチは、出カインターフェイスEthernet1/2を識別する追加のポートVLANタグ 102を挿入します。
4. 内部スイッチは、追加のVNタグを挿入します。

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 11:33:19.071512698	198.51.100.100	192.0.2.100	ICMP	108	0x4f27 (20263)	64	Echo (ping) reply id=0x0013, seq=1/256, ttl=64
2	2022-08-01 11:33:19.071514882	198.51.100.100	192.0.2.100	ICMP	108	0x4f27 (20263)	64	Echo (ping) reply id=0x0013, seq=1/256, ttl=64
3	2022-08-01 11:33:20.072677302	198.51.100.100	192.0.2.100	ICMP	108	0x4ffb (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 (21748)	64	Echo (ping) reply id=0x0013, seq=11/2816, ttl=64
22	2022-08-01 11:33:29.202398067	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21748)	64	Echo (ping) reply id=0x0013, seq=11/2816, ttl=64
23	2022-08-01 11:33:30.226398735	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64	Echo (ping) reply id=0x0013, seq=12/3072, ttl=64
24	2022-08-01 11:33:30.226401017	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64	Echo (ping) reply id=0x0013, seq=12/3072, ttl=64
25	2022-08-01 11:33:31.250838708	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 11:33:31.250839971	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 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
  ....0. .... = Logged: 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
  
```



No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 11:33:19.071512698	198.51.100.100	192.0.2.100	ICMP	108	0x4f27 (20263)	64	Echo (ping) reply id=0x0013, seq=1/256, ttl=64
2	2022-08-01 11:33:19.071514882	198.51.100.100	192.0.2.100	ICMP	108	0x4f27 (20263)	64	Echo (ping) reply id=0x0013, seq=1/256, ttl=64
3	2022-08-01 11:33:20.072677302	198.51.100.100	192.0.2.100	ICMP	108	0x4ff0 (20475)	64	Echo (ping) reply id=0x0013, seq=2/512, ttl=64
4	2022-08-01 11:33:20.072679384	198.51.100.100	192.0.2.100	ICMP	108	0x4ffb (20475)	64	Echo (ping) reply id=0x0013, seq=2/512, ttl=64
5	2022-08-01 11:33:21.073913640	198.51.100.100	192.0.2.100	ICMP	108	0x50ac (20652)	64	Echo (ping) reply id=0x0013, seq=3/768, ttl=64
6	2022-08-01 11:33:21.073915690	198.51.100.100	192.0.2.100	ICMP	108	0x50ac (20652)	64	Echo (ping) reply id=0x0013, seq=3/768, ttl=64
7	2022-08-01 11:33:22.075239381	198.51.100.100	192.0.2.100	ICMP	108	0x513e (20798)	64	Echo (ping) reply id=0x0013, seq=4/1024, ttl=64
8	2022-08-01 11:33:22.075241491	198.51.100.100	192.0.2.100	ICMP	108	0x513e (20798)	64	Echo (ping) reply id=0x0013, seq=4/1024, ttl=64
9	2022-08-01 11:33:23.076447152	198.51.100.100	192.0.2.100	ICMP	108	0x51c9 (20937)	64	Echo (ping) reply id=0x0013, seq=5/1280, ttl=64
10	2022-08-01 11:33:23.076449303	198.51.100.100	192.0.2.100	ICMP	108	0x51c9 (20937)	64	Echo (ping) reply id=0x0013, seq=5/1280, ttl=64
11	2022-08-01 11:33:24.082407896	198.51.100.100	192.0.2.100	ICMP	108	0x528e (21134)	64	Echo (ping) reply id=0x0013, seq=6/1536, ttl=64
12	2022-08-01 11:33:24.082410099	198.51.100.100	192.0.2.100	ICMP	108	0x528e (21134)	64	Echo (ping) reply id=0x0013, seq=6/1536, ttl=64
13	2022-08-01 11:33:25.106382424	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64	Echo (ping) reply id=0x0013, seq=7/1792, ttl=64
14	2022-08-01 11:33:25.106384549	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64	Echo (ping) reply id=0x0013, seq=7/1792, ttl=64
15	2022-08-01 11:33:26.130437851	198.51.100.100	192.0.2.100	ICMP	108	0x53a6 (21414)	64	Echo (ping) reply id=0x0013, seq=8/2048, ttl=64
16	2022-08-01 11:33:26.130440320	198.51.100.100	192.0.2.100	ICMP	108	0x53a6 (21414)	64	Echo (ping) reply id=0x0013, seq=8/2048, ttl=64
17	2022-08-01 11:33:27.154398212	198.51.100.100	192.0.2.100	ICMP	108	0x5446 (21574)	64	Echo (ping) reply id=0x0013, seq=9/2304, ttl=64
18	2022-08-01 11:33:27.154400198	198.51.100.100	192.0.2.100	ICMP	108	0x5446 (21574)	64	Echo (ping) reply id=0x0013, seq=9/2304, ttl=64
19	2022-08-01 11:33:28.178469866	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64	Echo (ping) reply id=0x0013, seq=10/2560, ttl=64
20	2022-08-01 11:33:28.178471810	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64	Echo (ping) reply id=0x0013, seq=10/2560, ttl=64
21	2022-08-01 11:33:29.202395869	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21740)	64	Echo (ping) reply id=0x0013, seq=11/2816, ttl=64
22	2022-08-01 11:33:29.202398067	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21740)	64	Echo (ping) reply id=0x0013, seq=11/2816, ttl=64
23	2022-08-01 11:33:30.226398735	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64	Echo (ping) reply id=0x0013, seq=12/3072, ttl=64
24	2022-08-01 11:33:30.226401817	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 (58:9d:b9:77:0e), Dst: VMware 9d:e8:be (00:50:5e:9d:e8:be)		0000 00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00 --PV--X--m--&-- 0010 00 0a 81 00 00 66 08 00 45 00 00 54 4f 27 00 00 .....F--E--TO-- 0020 40 01 3e 86 c6 33 64 64 c0 00 02 64 00 00 95 7c @->-3dd --d...  0030 00 13 00 01 f2 b9 e7 62 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 \$%&'()*+ 0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 .....-/0123 4567
> VN-Tag 0..... = Direction: To Bridge .0..... = Pointer: vif_id ..00 0000 0000 0000 ..... = Destination: 0 .....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: 102 000..... = Priority: Best Effort (default) (0) ...0..... = DEI: Ineligible ....0000 0110 0110 = ID: 102 Type: 1Pv4 (0x0000)		
> Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100 > Internet Control Message Protocol		

## 説明

[Application Capture Direction] で[All Packets] オプションを選択すると、選択したアプリケーションポートEthernet1/2に関連する2つの同時パケットキャプチャが設定されます。前面インターフェイスEthernet1/2上のキャプチャと、選択したバックプレーンインターフェイス上のキャプチャ。

前面インターフェイスでパケットキャプチャが設定されると、スイッチは各パケットを同時に2回キャプチャします。

- ポートVLANタグの挿入後。
- VNタグの挿入後。

操作順では、VNタグはポートVLANタグの挿入よりも後の段階で挿入されます。ただし、キャプチャファイルでは、VNタグが付いたパケットは、ポートVLANタグが付いたパケットよりも前に表示されます。この例では、ICMPエコー要求パケットのVLANタグ102によって、Ethernet1/2が入カインターフェイスとして識別されます。

バックプレーンインターフェイスでパケットキャプチャが設定されると、スイッチは各パケットを同時に2回キャプチャします。内部スイッチは、セキュリティモジュール上のアプリケーションによってすでにタグ付けされたパケットを、ポートVLANタグとVNタグを使用して受信します。ポートVLANタグは、内部シャーシがパケットをネットワークに転送するために使用する出カインターフェイスを示します。この例では、ICMPエコー応答パケット内のVLANタグ102によって、Ethernet1/2が出カインターフェイスとして識別されます。

内部スイッチは、パケットがネットワークに転送される前に、VNタグと内部インターフェイスVLANタグを削除します。

タスクの要約を次の表に示します。

タスク	キャプチャポイント	キャプチャされたパケットの内部ポート	方向	キャプチャされたトラフィック
-----	-----------	--------------------	----	----------------

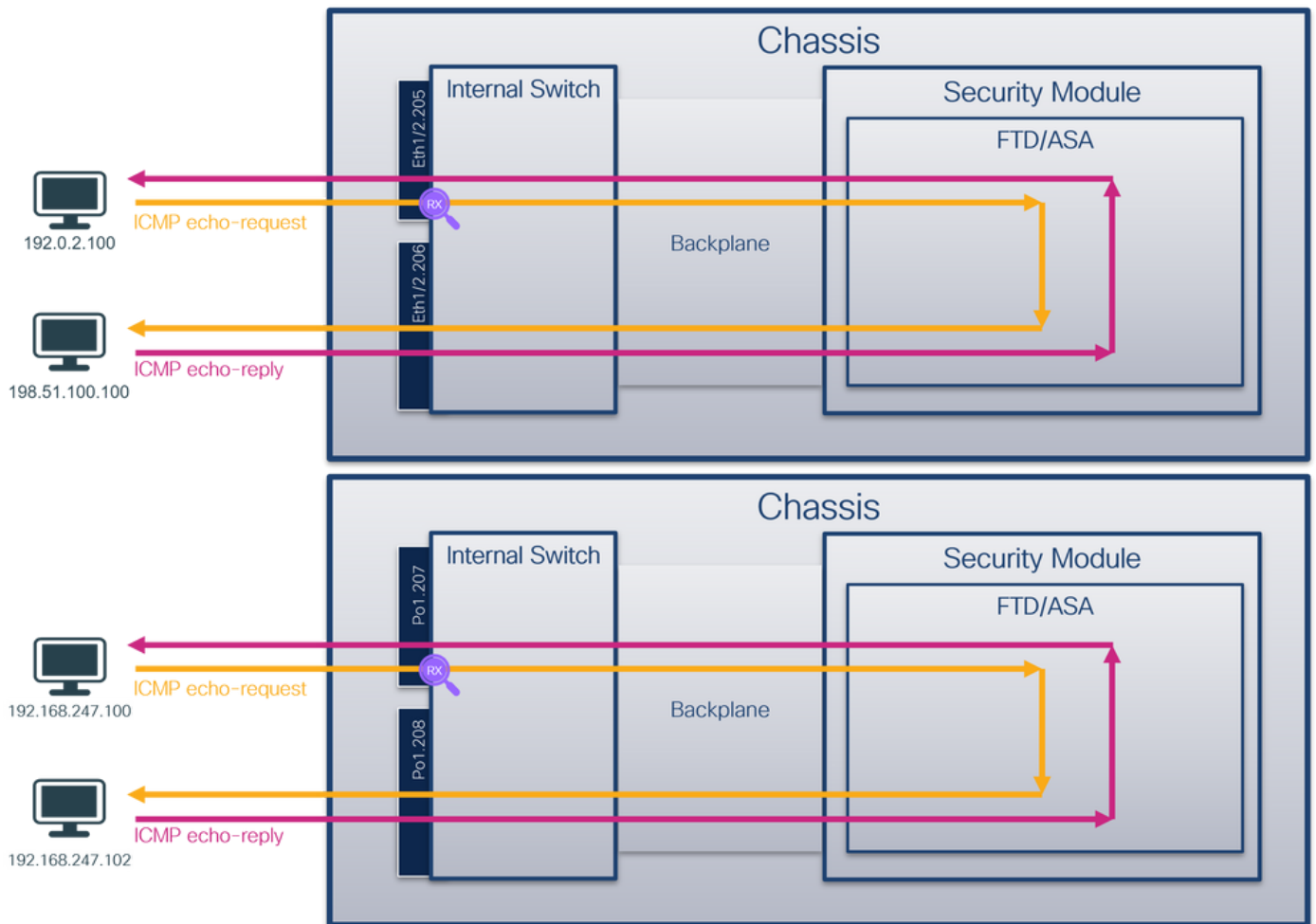


		VLAN		
アプリケーションおよびアプリケーションポート	バックプレインインターフェイス	102	入力のみ	ホスト198.51.100.100からホスト192.0.2.100へのICMPエコー
Ethernet1/2でのキャプチャの設定と確認	Interface Ethernet1/2	102	入力のみ	ホスト192.0.2.100からホスト198.51.100.100へのICMPエコー

## 物理インターフェイスまたはポートチャンネルインターフェイスのサブインターフェイスでのパケットキャプチャ

FCMおよびCLIを使用して、サブインターフェイスEthernet1/2.205またはポートチャンネルサブインターフェイスPortchannel1.207でのパケットキャプチャを設定および確認します。サブインターフェイスおよびサブインターフェイスでのキャプチャは、コンテナモードのFTDアプリケーションでのみサポートされます。この場合、Ethernet1/2.205とPortchannel1.207のパケットキャプチャが設定されています。

### トポロジ、パケットフロー、およびキャプチャポイント

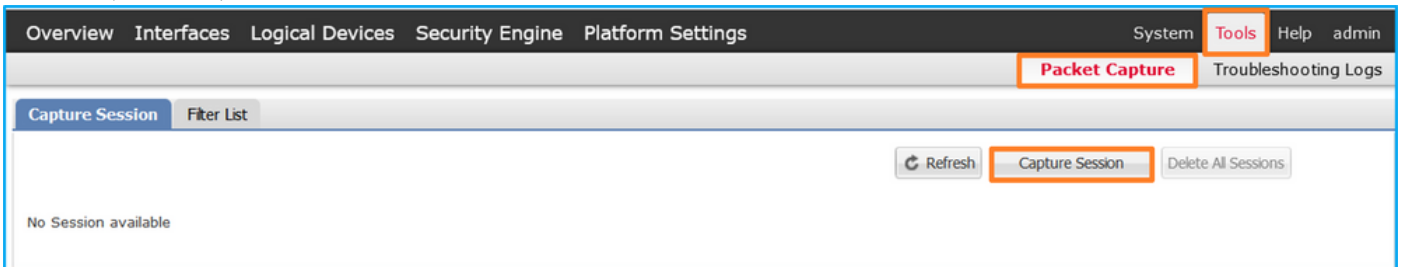


## コンフィギュレーション

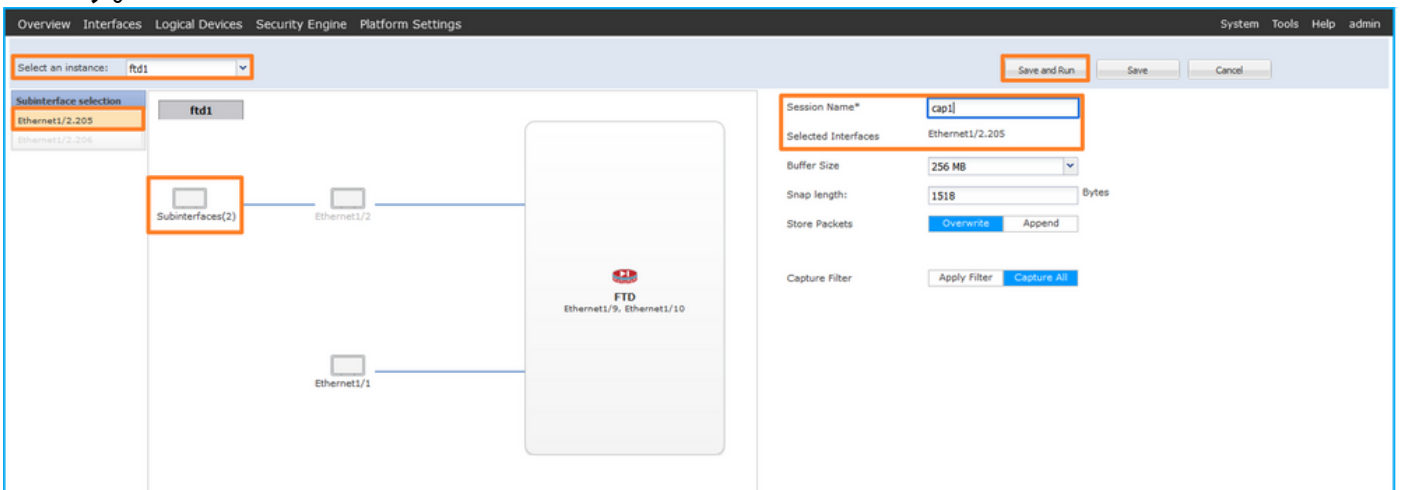
### FCM

FTDアプリケーションとアプリケーションポートEthernet1/2でパケットキャプチャを設定するには、FCMで次の手順を実行します。

1. [Tools] > [Packet Capture] > [Capture Session] を使用して、新しいキャプチャセッションを作成します。



2. 特定のアプリケーションインスタンス ftd1、サブインターフェイス Ethernet1/2.205 を選択し、セッション名を指定して、[Save and Run] をクリックしてキャプチャをアクティブにします。



3. ポートチャネルサブインターフェイスの場合、Cisco Bug ID [CSCcvq33119](https://tools.cisco.com/bugcenter/bug/?bugID=CSCcvq33119) により、サブインターフェイスは FCM に表示されません。FXOS CLI を使用して、ポートチャネルサブインターフェイスのキャプチャを設定します。

## FXOS CLI

サブインターフェイス Ethernet1/2.205 および Portchannel1.207 でパケットキャプチャを設定するには、FXOS CLI で次の手順を実行します。

1. アプリケーションのタイプと識別子を特定します。

```
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. ポートチャネルインターフェイスの場合は、そのメンバーインターフェイスを特定します。

```
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. キャプチャセッションを作成します。

```
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 #
```

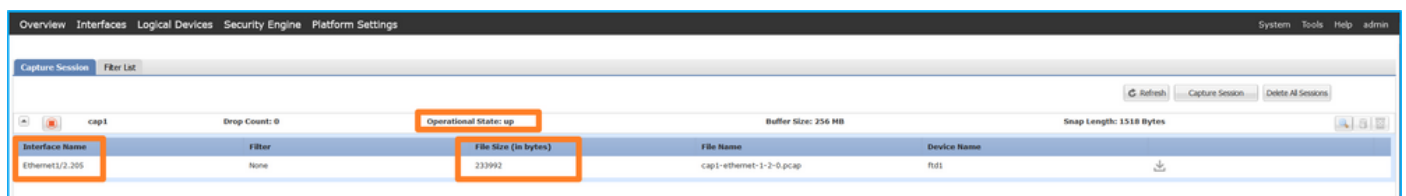
ポートチャネルサブインターフェイスの場合、各ポートチャネルメンバーインターフェイスのパケットキャプチャを作成します。

```
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 #
```

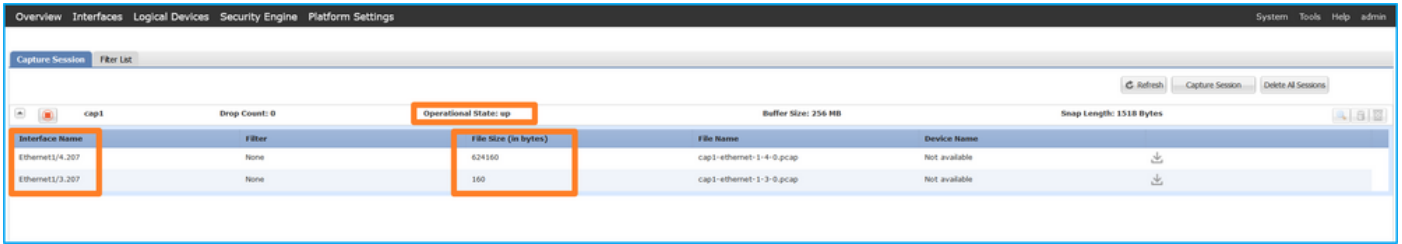
### 確認

### FCM

[Interface Name] を確認し、[Operational Status] が[up]になっており、[File Size (in bytes)] が増加していることを確認します。



FXOS CLIで設定されたポートチャンネルサブインターフェイスキャプチャもFCMで表示されます。ただし、次のように編集することはできません。



Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/3,207	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

scope packet-captureでキャプチャの詳細を確認します。

```
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
```

メンバーインターフェイスEthernet1/3およびEthernet1/4を持つポートチャンネル1:

```
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

## キャプチャファイルの収集

「Firepower 4100/9300内部スイッチキャプチャファイルの収集」セクションの手順に従います。

## ファイル分析のキャプチャ

パケットキャプチャファイルリーダーアプリケーションを使用して、キャプチャファイルを開きます。最初のパケットを選択し、キーポイントを確認します。

1. ICMPエコー要求パケットだけがキャプチャされます。各パケットはキャプチャされ、2回表示されます。
2. 元のパケットヘッダーにはVLANタグ205が付いています。
3. 内部スイッチは、入インターフェイスEthernet1/2を識別する追加ポートVLANタグ102を挿入します。
4. 内部スイッチは、追加のVNタグを挿入します。



2番目のパケットを選択し、キーポイントを確認します。

1. ICMPエコー要求パケットだけがキャプチャされます。各パケットはキャプチャされ、2回表示されます。
2. 元のパケットヘッダーにはVLANタグ205が付いています。

次に、Portchannel1.207のキャプチャファイルを開きます。最初のパケットを選択し、キーポイントを確認します

1. ICMPエコー要求パケットだけがキャプチャされます。各パケットはキャプチャされ、2回表示されます。
2. 元のパケットヘッダーにはVLANタグ207が付いています。
3. 内部スイッチは、入カインターフェイスPortchannel1を識別する追加ポートVLANタグ



1001を挿入します。

#### 4. 内部スイッチは、追加のVNタグを挿入します。

The image shows a Wireshark capture of ICMP Echo (ping) requests. The packet list pane shows 27 requests from 192.168.247.100 to 192.168.247.102. The packet details pane for the first packet (Frame 1) is highlighted with a red box and contains the following information:

- VN-Tag**: Direction: From Bridge, Pointer: vif\_id, 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**: Priority: Best Effort (default) (0), DEI: Ineligible, ID: 1001. Type: 802.1Q Virtual LAN (0x8100).
- 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 207**: Priority: Best Effort (default) (0), DEI: Ineligible, ID: 207. Type: IPv4 (0x0800).
- Internet Protocol Version 4, Src: 192.168.247.100, Dst: 192.168.247.102**
- Internet Control Message Protocol**

2番目のパケットを選択し、キーポイントを確認します。

1. ICMPエコー要求パケットだけがキャプチャされます。各パケットはキャプチャされ、2回表示されます。
2. 元のパケットヘッダーにはVLANタグ207が付いています。

The image shows a Wireshark capture of ICMP Echo (ping) requests. The packet list pane shows 27 requests from 192.168.247.100 to 192.168.247.102. The packet details pane for the second packet (Frame 2) is highlighted with a red box and contains the following information:

- 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 207**: Priority: Best Effort (default) (0), DEI: Ineligible, ID: 207. Type: IPv4 (0x0800).
- Internet Protocol Version 4, Src: 192.168.247.100, Dst: 192.168.247.102**
- Internet Control Message Protocol**

## 説明

前面インターフェイスでパケットキャプチャが設定されると、スイッチは各パケットを同時に2回キャプチャします。

- ポートVLANタグの挿入後。
- VNタグの挿入後。

操作順では、VNタグはポートVLANタグの挿入よりも後の段階で挿入されます。ただし、キャプチャファイルでは、VNタグが付いたパケットは、ポートVLANタグが付いたパケットよりも前に表示されます。また、サブインターフェイスの場合は、キャプチャファイル内の各2番目のパケットにポートVLANタグが含まれていません。

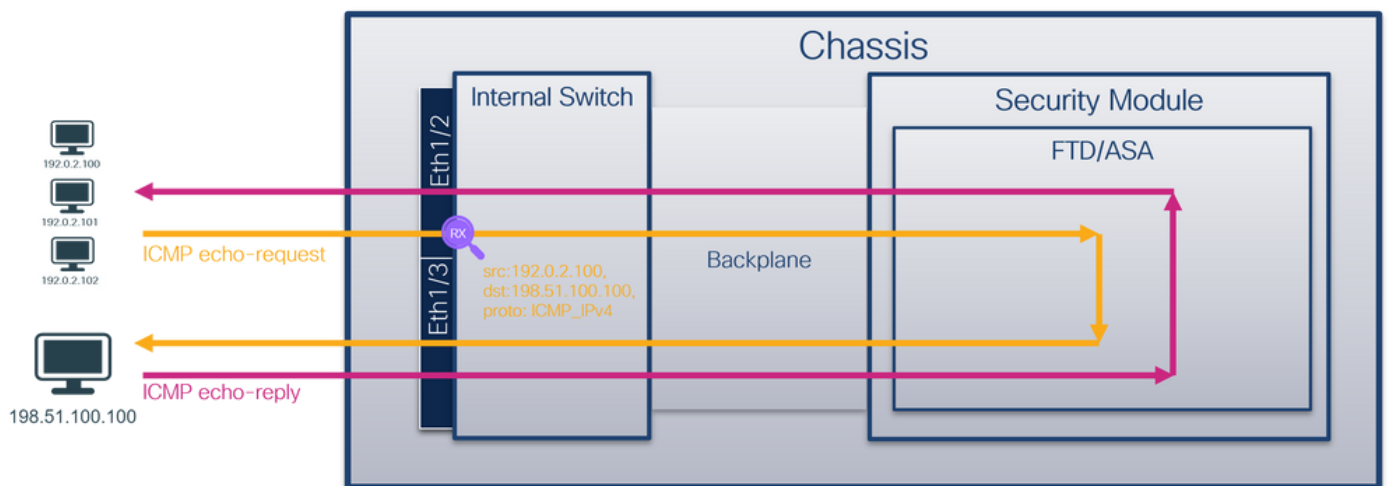
タスクの要約を次の表に示します。

タスク	キャプチャポイント	キャプチャされたパケットの内部ポートVLAN	方向	キャプチャされたトラフィック
サブインターフェイス Ethernet1/2.205でのパケットキャプチャの設定と確認	Ethernet1/2.205	102	入力のみ	ホスト192.0.2.100からホスト198.51.100.100へのICMPエコー
メンバーインターフェイス Ethernet1/3および Ethernet1/4を使用して、Portchannel1サブインターフェイスでパケットキャプチャを設定および確認します	Ethernet1/3 Ethernet1/4	1001	入力のみ	192.168.207.100からホスト192.168.207.102へのICMPエコー

## パケット キャプチャ フィルタ

FCMとCLIを使用して、インターフェイスEthernet1/2のパケットキャプチャをフィルタを使用して設定および確認します。

### トポロジ、パケットフロー、およびキャプチャポイント



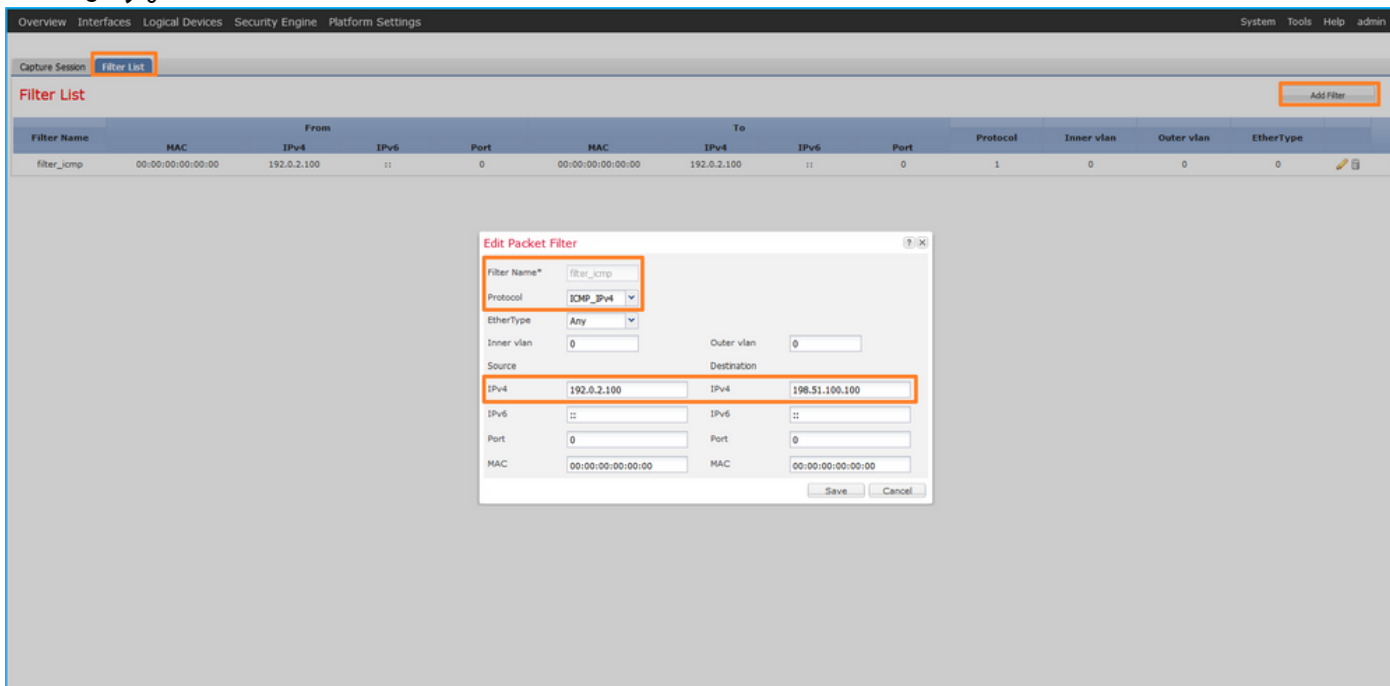
## コンフィギュレーション

### FCM

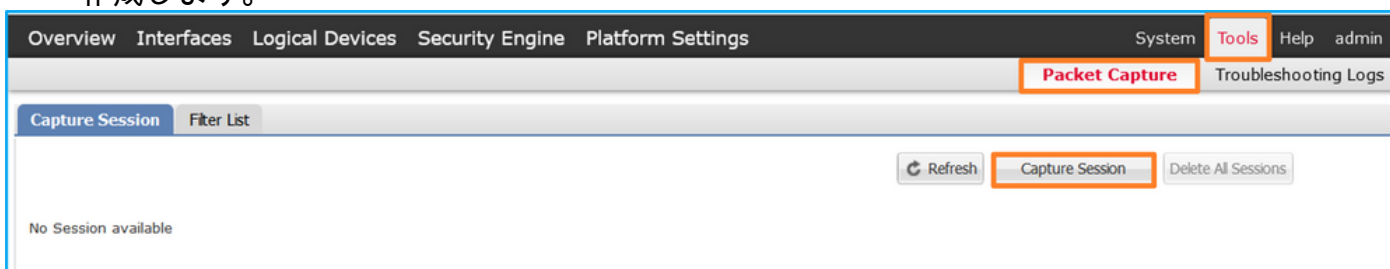
ホスト192.0.2.100からホスト198.51.100.100へのICMPエコー要求パケットのキャプチャフィルタを設定し、インターフェイスEthernet1/2のパケットキャプチャに適用するには、FCMで次の手順を実行します。



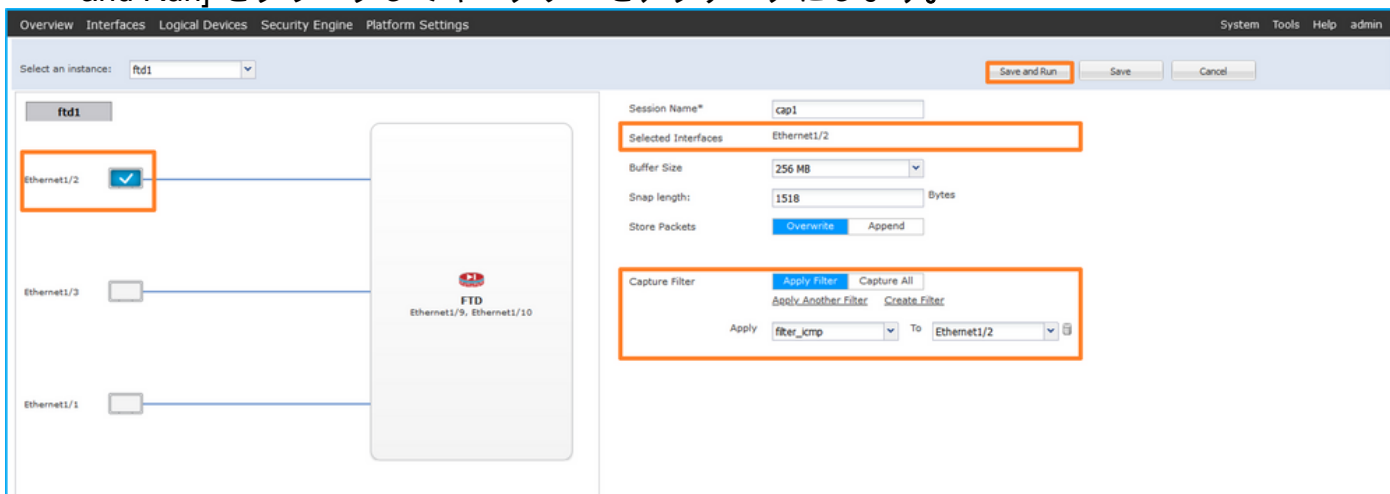
1. [Tools] > [Packet Capture] > [Filter List] > [Add Filter] を使用して、キャプチャフィルタを作成します。
2. [Filter Name]、[Protocol]、[Source IPv4]、[Destination IPv4] を指定し、[Save] をクリックします。



3. [Tools] > [Packet Capture] > [Capture Session] を使用して、新しいキャプチャセッションを作成します。



4. [Ethernet1/2]を選択し、[Session Name] を指定してキャプチャフィルタを適用し、[Save and Run] をクリックしてキャプチャをアクティブにします。



## FXOS CLI

バックプレーンインターフェイスでパケットキャプチャを設定するには、FXOS CLIで次の手順を

実行します。

### 1. アプリケーションのタイプと識別子を特定します。

```
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. <https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>でIPプロトコル番号を特定します。この場合、ICMPプロトコル番号は1です。

### 3. キャプチャセッションを作成します。

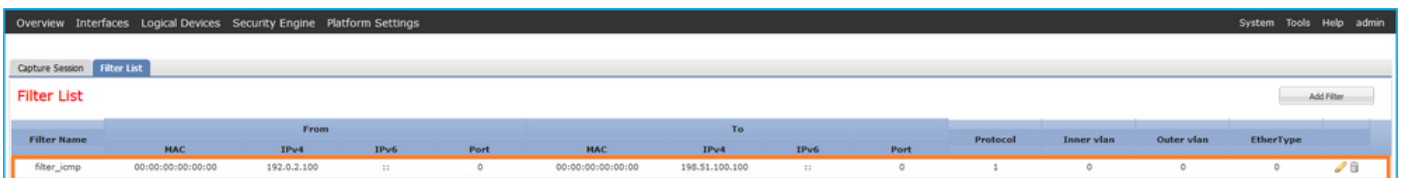
2.

```
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 #
```

### 確認

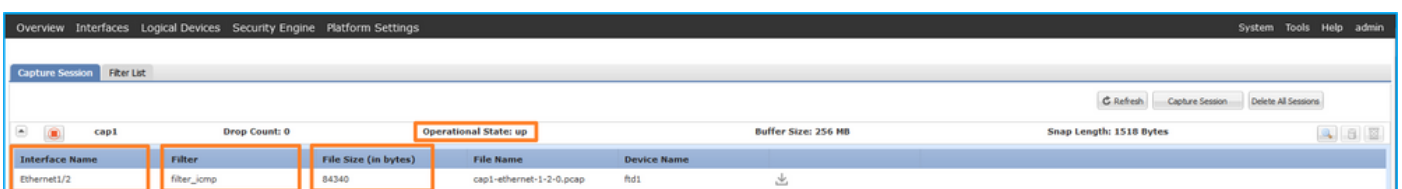
### FCM

[Interface Name] を確認し、[Operational Status] が[up]になっており、[File Size (in bytes)]が増加していることを確認します。



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

[Tools] > [Packet Capture] > [Capture Session] で、インターフェイス名、フィルタ、Operational Statusがupになっていることを確認し、ファイルサイズ(バイト単位)を増やします。



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

scope packet-captureでキャプチャの詳細を確認します。

```
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
```

## キャプチャファイルの収集

「Firepower 4100/9300内部スイッチキャプチャファイルの収集」セクションの手順に従います。

## ファイル分析のキャプチャ

パケットキャプチャファイルリーダーアプリケーションを使用して、キャプチャファイルを開きます。最初のパケットを選択し、キーポイントを確認します

1. ICMPエコー要求パケットだけがキャプチャされます。各パケットはキャプチャされ、2回表示されます。
2. 元のパケットヘッダーにはVLANタグが付いていません。
3. 内部スイッチは、入力インターフェイスEthernet1/2を識別する追加ポートVLANタグ102を挿入します。

#### 4. 内部スイッチは、追加のVNタグを挿入します。

The screenshot shows a Wireshark capture of ICMP Echo (ping) requests. The first packet is selected, and the packet details pane is expanded to show the following structure:

- 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
  - ... .. = 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

2番目のパケットを選択し、キーポイントを確認します。

1. ICMPエコー要求パケットだけがキャプチャされます。各パケットはキャプチャされ、2回表示されます。
2. 元のパケットヘッダーにはVLANタグが付いていません。
3. 内部スイッチは、入インターフェイスEthernet1/2を識別する追加ポートVLANタグ102を挿入します。

The screenshot shows a Wireshark capture of ICMP Echo (ping) requests. The second packet is selected, and the packet details pane is expanded to show the following structure:

- 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

#### 説明

前面インターフェイスでパケットキャプチャが設定されると、スイッチは各パケットを同時に2回キャプチャします。

- ポートVLANタグの挿入後。
- VNタグの挿入後。

操作順では、VNタグはポートVLANタグの挿入よりも後の段階で挿入されます。ただし、キャプチャファイルでは、VNタグが付いたパケットは、ポートVLANタグが付いたパケットよりも前に表示されます。

キャプチャフィルタが適用されると、入力方向のフィルタに一致するパケットだけがキャプチャされます。

タスクの要約を次の表に示します。

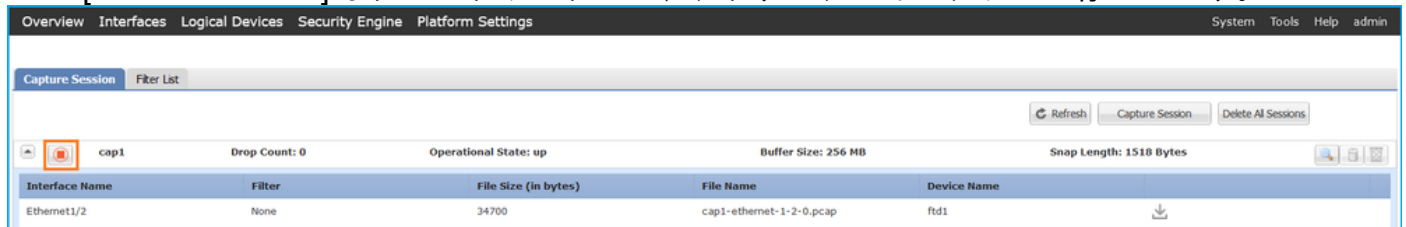
タスク	キャプチャポイント	キャプチャされたパケットの内部ポート VLAN	方向	ユーザフィルタ	キャプチャされたトラフィック
前面インターフェイス Ethernet1/2 のフィルタを使用してパケットキャプチャを設定および確認します	Ethernet1/2	102	入力の	プロトコル : ICMP Source: 192.0.2.100 送信先 : 198.51.100.100	ホスト 192.0.2.100 からホスト 198.51.100.100 への ICMP 要求

## Firepower 4100/9300 内部スイッチキャプチャファイルの収集

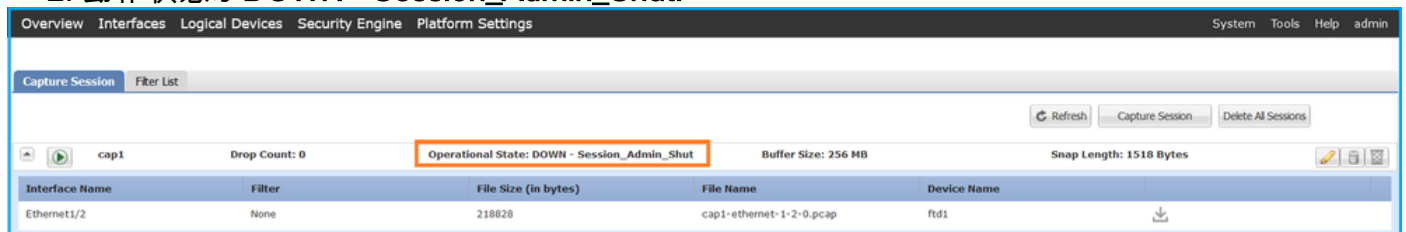
### FCM

内部スイッチキャプチャファイルを収集するには、FCMで次の手順を実行します。

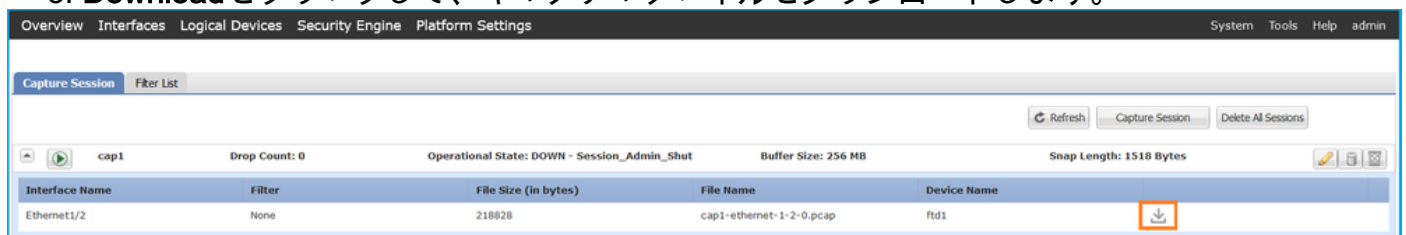
1. [Disable Session] ボタンをクリックして、アクティブなキャプチャを停止します。



2. 動作状態が DOWN - Session\_Admin\_Shut:



3. Download をクリックして、キャプチャファイルをダウンロードします。





ポートチャネルインターフェイスの場合は、メンバーインターフェイスごとにこの手順を繰り返します。

## FXOS CLI

キャプチャファイルを収集するには、FXOS CLIで次の手順を実行します。

### 1. アクティブなキャプチャを停止します。

```
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. local-mgmtコマンドスコープからキャプチャファイルをアップロードします。

```
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:
```

ポートチャネルインターフェイスの場合は、各メンバーインターフェイスのキャプチャファイルをコピーします。

## のガイドライン、制限事項、およびベストプラクティス 内部スイッチ パケット キャプチャ

Firepower 4100/9300の内部スイッチキャプチャに関連するガイドラインと制限事項については、『Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide』または『Cisco Firepower 4100/9300 FXOS CLI Configuration Guide』の第トラブルシューティング章の「Packet Capture」を参照してください。

TACケースでのパケットキャプチャの使用に基づくベストプラクティスのリストを次に示します。

- ガイドラインと制限事項に注意してください。
- すべてのポートチャネルメンバーインターフェイスでパケットをキャプチャし、すべてのキャプチャファイル进行分析します。
- キャプチャフィルタを使用します。
- キャプチャフィルタの設定時に、パケットIPアドレスに対するNATの影響を考慮してください。
- デフォルト値の1518バイトと異なる場合に、フレームサイズを指定するスナップ長を増減します。サイズが小さいほど、キャプチャされたパケットの数が増え、その逆も同様です。
- 必要に応じて[Buffer Size] を調整します。
- FCMまたはFXOS CLIのDrop Countに注意してください。バッファサイズの制限に達すると、廃棄カウントカウンタが増加します。
- Wiresharkでフィルタ!vntagを使用して、VNタグのないパケットだけを表示します。これは、前面インターフェイスのパケットキャプチャファイルでVNタグ付きパケットを非表示にする場合に便利です。
- Wiresharkでフィルタframe.number&1を使用して、奇数フレームだけを表示します。これは、バックプレーンインターフェイスのパケットキャプチャファイル内の重複パケットを非表示にする場合に便利です。
- TCPなどのプロトコルの場合、Wiresharkはデフォルトで、特定の条件を持つパケットを異なる色で表示する色付けルールを適用します。キャプチャファイル内の重複パケットが原因で内部スイッチキャプチャが発生した場合、パケットに色付けをして誤検出でマーキングすることができます。パケットキャプチャファイル进行分析してフィルタを適用した場合、表示されたパケットを新しいファイルにエクスポートし、代わりに新しいファイルを開きます。

## の設定と検証 Secure Firewall 3100

Firepower 4100/9300とは異なり、Secure Firewall 3100の内部スイッチキャプチャは、`capture <name> switch`コマンドを使用してアプリケーションコマンドラインインターフェイス(CLI)で設定されます。ここで、`switch`オプションは、キャプチャが内部スイッチで設定されていることを指定します。

次に、`switch`オプションを指定した`capture`コマンドを示します。

```
> 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>
```

パケットキャプチャ設定の一般的な手順は次のとおりです。

### 1. 入力インターフェイスを指定します。

スイッチのキャプチャ設定は、入力インターフェイスnameifを受け入れます。ユーザは、データインターフェイス名、内部アップリンク、または管理インターフェイスを指定できます。

```
> 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. イーサネットフレームのEtherTypeを指定します。デフォルトのEtherTypeはIPです。

**ethernet-type**オプションの値は、EtherTypeを指定します。

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

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

### 3. 一致条件を指定します。capture matchオプションは、一致基準を指定します。

```
> 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
snmp
spi      SPI value
tcp
udp
<cr>
```

4. バッファサイズ、パケット長など、他のオプションパラメータを指定します。
5. キャプチャを有効にします。コマンド `no capture <name> switch stop` は、キャプチャをアクティブにします。

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

6. キャプチャの詳細を確認します。

- 管理ステータスは `enabled` で、動作ステータスは `up` で `active` です。
- パケットキャプチャファイルサイズ: `Pcapsize`。
- `show capture <cap_name>` の出力に表示されるキャプチャされたパケットの数は0以外です。
- キャプチャパス `Pcapfile`。キャプチャされたパケットは `/mnt/disk0/packet-capture/フォルダ` に自動的に保存されます。
- 条件をキャプチャします。キャプチャ条件に基づいて、キャプチャフィルタが自動的に作成されます。

```
> 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. 必要に応じてキャプチャを停止します。

```
> 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. キャプチャファイルを収集します。「Secure Firewall 3100内部スイッチキャプチャファイルの収集」セクションの手順に従ってください。**

バージョン7.2では、内部スイッチのキャプチャ設定はFMCまたはFDMではサポートされていません。ASAソフトウェアバージョン9.18(1)以降の場合、内部スイッチキャプチャはASDMバージ



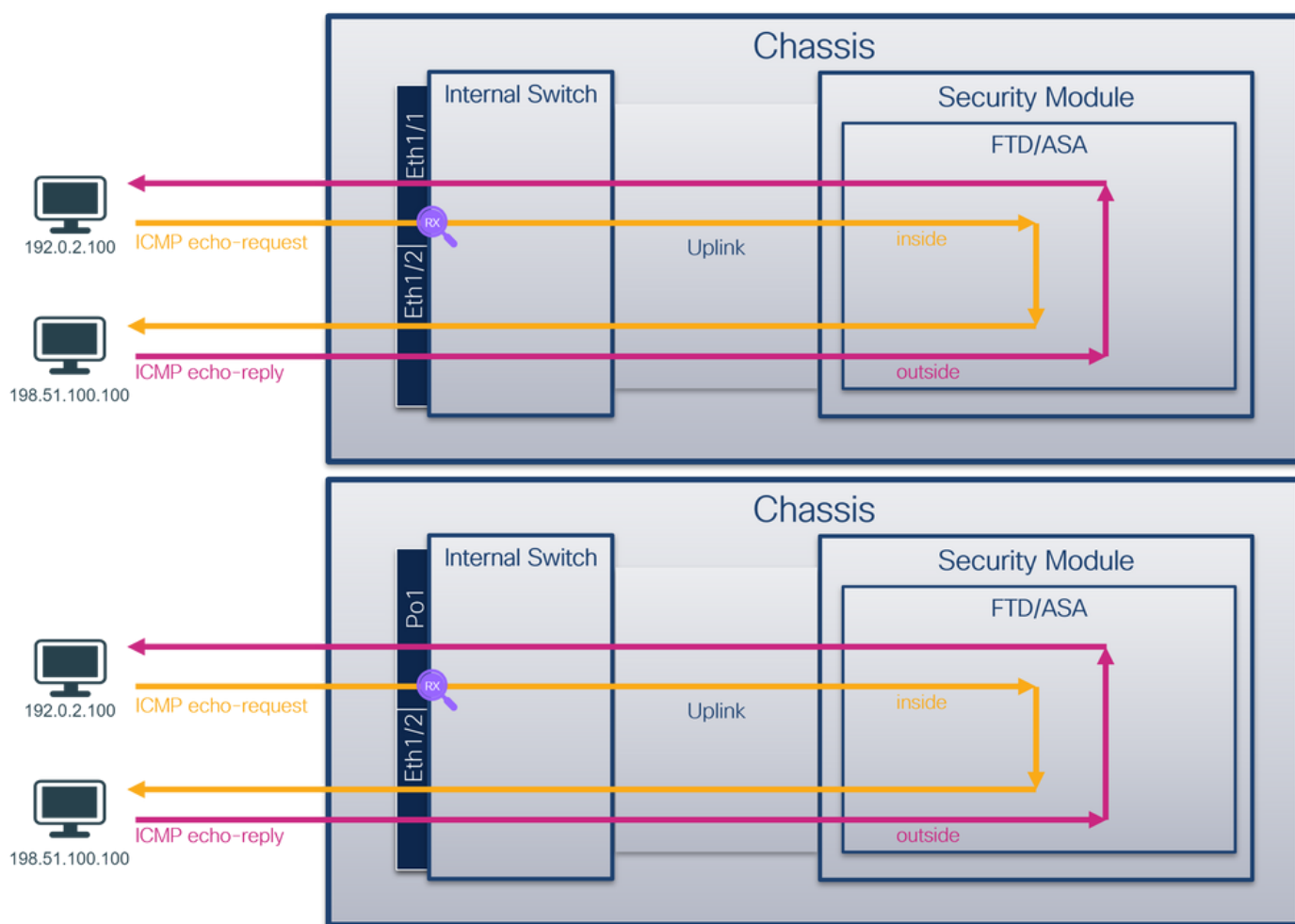
ョン7.18.1.x以降で設定できます。

これらのシナリオは、Secure Firewall 3100内部スイッチキャプチャの一般的な使用例をカバーしています。

## 物理インターフェイスまたはポートチャンネルインターフェイスでのパケットキャプチャ

FTDまたはASA CLIを使用して、インターフェイスEthernet1/1またはPortchannel1インターフェイスのパケットキャプチャを設定および確認します。両方のインターフェイスの名前はinsideです。

### トポロジ、パケットフロー、およびキャプチャポイント



### コンフィギュレーション

インターフェイスEthernet1/1またはPort-channel1でパケットキャプチャを設定するには、ASAまたはFTD CLIで次の手順を実行します。

1. nameifを確認します。

```
> 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. キャプチャセッションを作成します。

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

3. キャプチャセッションを有効にします。

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

## 確認

キャプチャセッション名、管理および動作の状態、インターフェイススロット、およびIDを確認します。Pcapsizeの値(バイト単位)が増加し、キャプチャされたパケットの数が0以外であることを確認します。

```
> 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

ポートチャネル1の場合、キャプチャはすべてのメンバーインターフェイスで設定されます。

> **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

ポートチャネルメンバーインターフェイスは、FXOSのlocal-mgmtコマンドシェルでshow portchannel summary コマンドを使用して確認できます。

```
> 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
```

ASAのFXOSにアクセスするには、connect fxos adminコマンドを実行します。マルチコンテキストの場合は、管理コンテキストでコマンドを実行します。

## キャプチャファイルの収集

「Secure Firewall 3100内部スイッチキャプチャファイルの収集」セクションの手順に従ってください。

## ファイル分析のキャプチャ

パケットキャプチャファイルリーダーアプリケーションを使用して、Ethernet1/1のキャプチャファイルを開きます。最初のパケットを選択し、キーポイントを確認します。

1. ICMPエコー要求パケットだけがキャプチャされます。
2. 元のパケットヘッダーにはVLANタグが付いていません。

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

Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)  
 Ethernet II, Src: VMware\_9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco\_34:9a:14 (bc:e7:12:34:9a:14)  
 Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100  
 Internet Control Message Protocol

```

0000 bc e7 12 34 9a 14 00 50 56 9d e8 be 08 00 45 00  ...4...P V...E-
0010 00 54 9a 10 40 00 40 01 b3 9c c0 00 02 64 c6 33  .T.@.-...d-3
0020 64 64 08 00 c6 91 00 34 00 01 61 17 f0 62 00 00  dd...4...a-b-
0030 00 00 18 ec 08 00 00 00 00 00 10 11 12 13 14 15  .....!...%$%
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  .....!...%$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
0060 36 37 55 55 55 55
  
```

Portchannel1メンバーインターフェイスのキャプチャファイルを開きます。最初のパケットを選択し、キーポイントを確認します。

1. ICMPエコー要求パケットだけがキャプチャされます。
2. 元のパケットヘッダーにはVLANタグが付いていません。

No.	Time	Source	Destination	Protocol	Length	IP ID	TTL	Info
1	2022-08-07 20:40:58.657533	192.0.2.100	198.51.100.100	ICMP	102	0x9296 (37526)	64	Echo (ping) request id=0x0035, seq=1/256, ttl=64 (no res
2	2022-08-07 20:40:59.658611	192.0.2.100	198.51.100.100	ICMP	102	0x9370 (37744)	64	Echo (ping) request id=0x0035, seq=2/512, ttl=64 (no res
3	2022-08-07 20:41:00.655662	192.0.2.100	198.51.100.100	ICMP	102	0x93f0 (37872)	64	Echo (ping) request id=0x0035, seq=3/768, ttl=64 (no res
4	2022-08-07 20:41:01.659749	192.0.2.100	198.51.100.100	ICMP	102	0x946f (37999)	64	Echo (ping) request id=0x0035, seq=4/1024, ttl=64 (no re
5	2022-08-07 20:41:02.660624	192.0.2.100	198.51.100.100	ICMP	102	0x94aa (38052)	64	Echo (ping) request id=0x0035, seq=5/1280, ttl=64 (no re
6	2022-08-07 20:41:03.663226	192.0.2.100	198.51.100.100	ICMP	102	0x952d (38189)	64	Echo (ping) request id=0x0035, seq=6/1536, ttl=64 (no re
7	2022-08-07 20:41:04.661262	192.0.2.100	198.51.100.100	ICMP	102	0x958d (38285)	64	Echo (ping) request id=0x0035, seq=7/1792, ttl=64 (no re
8	2022-08-07 20:41:05.665955	192.0.2.100	198.51.100.100	ICMP	102	0x95d8 (38360)	64	Echo (ping) request id=0x0035, seq=8/2048, ttl=64 (no re
9	2022-08-07 20:41:06.666538	192.0.2.100	198.51.100.100	ICMP	102	0x964b (38475)	64	Echo (ping) request id=0x0035, seq=9/2304, ttl=64 (no re
10	2022-08-07 20:41:07.667298	192.0.2.100	198.51.100.100	ICMP	102	0x972b (38699)	64	Echo (ping) request id=0x0035, seq=10/2560, ttl=64 (no r
11	2022-08-07 20:41:08.670540	192.0.2.100	198.51.100.100	ICMP	102	0x980a (38922)	64	Echo (ping) request id=0x0035, seq=11/2816, ttl=64 (no r
12	2022-08-07 20:41:09.668278	192.0.2.100	198.51.100.100	ICMP	102	0x9831 (38961)	64	Echo (ping) request id=0x0035, seq=12/3072, ttl=64 (no r
13	2022-08-07 20:41:10.672417	192.0.2.100	198.51.100.100	ICMP	102	0x98a2 (39074)	64	Echo (ping) request id=0x0035, seq=13/3328, ttl=64 (no r
14	2022-08-07 20:41:11.671369	192.0.2.100	198.51.100.100	ICMP	102	0x98f7 (39159)	64	Echo (ping) request id=0x0035, seq=14/3584, ttl=64 (no r
15	2022-08-07 20:41:12.675462	192.0.2.100	198.51.100.100	ICMP	102	0x99e4 (39396)	64	Echo (ping) request id=0x0035, seq=15/3840, ttl=64 (no r
16	2022-08-07 20:41:13.674903	192.0.2.100	198.51.100.100	ICMP	102	0x9a84 (39556)	64	Echo (ping) request id=0x0035, seq=16/4096, ttl=64 (no r
17	2022-08-07 20:41:14.674093	192.0.2.100	198.51.100.100	ICMP	102	0x9af3 (39667)	64	Echo (ping) request id=0x0035, seq=17/4352, ttl=64 (no r
18	2022-08-07 20:41:15.676904	192.0.2.100	198.51.100.100	ICMP	102	0x9b8e (39822)	64	Echo (ping) request id=0x0035, seq=18/4608, ttl=64 (no r

Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)  
 Ethernet II, Src: VMware\_9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco\_34:9a:2c (bc:e7:12:34:9a:2c)  
 Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100  
 Internet Control Message Protocol

```

0000 bc e7 12 34 9a 2c 00 50 56 9d e8 be 08 00 45 00  ...4...P V...E-
0010 00 54 92 96 40 00 40 01 bb 16 c0 00 02 64 c6 33  .T.@.-...d-3
0020 64 64 08 00 58 a8 00 35 00 01 4d 23 f0 62 00 00  dd...X-5...MH-b-
0030 00 00 0e c8 04 00 00 00 00 00 10 11 12 13 14 15  .....!...%$%
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  .....!...%$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
0060 36 37 55 55 55 55
  
```

説明

スイッチキャプチャは、インターフェイスEthernet1/1またはPortchannel1で設定されます。

タスクの要約を次の表に示します。

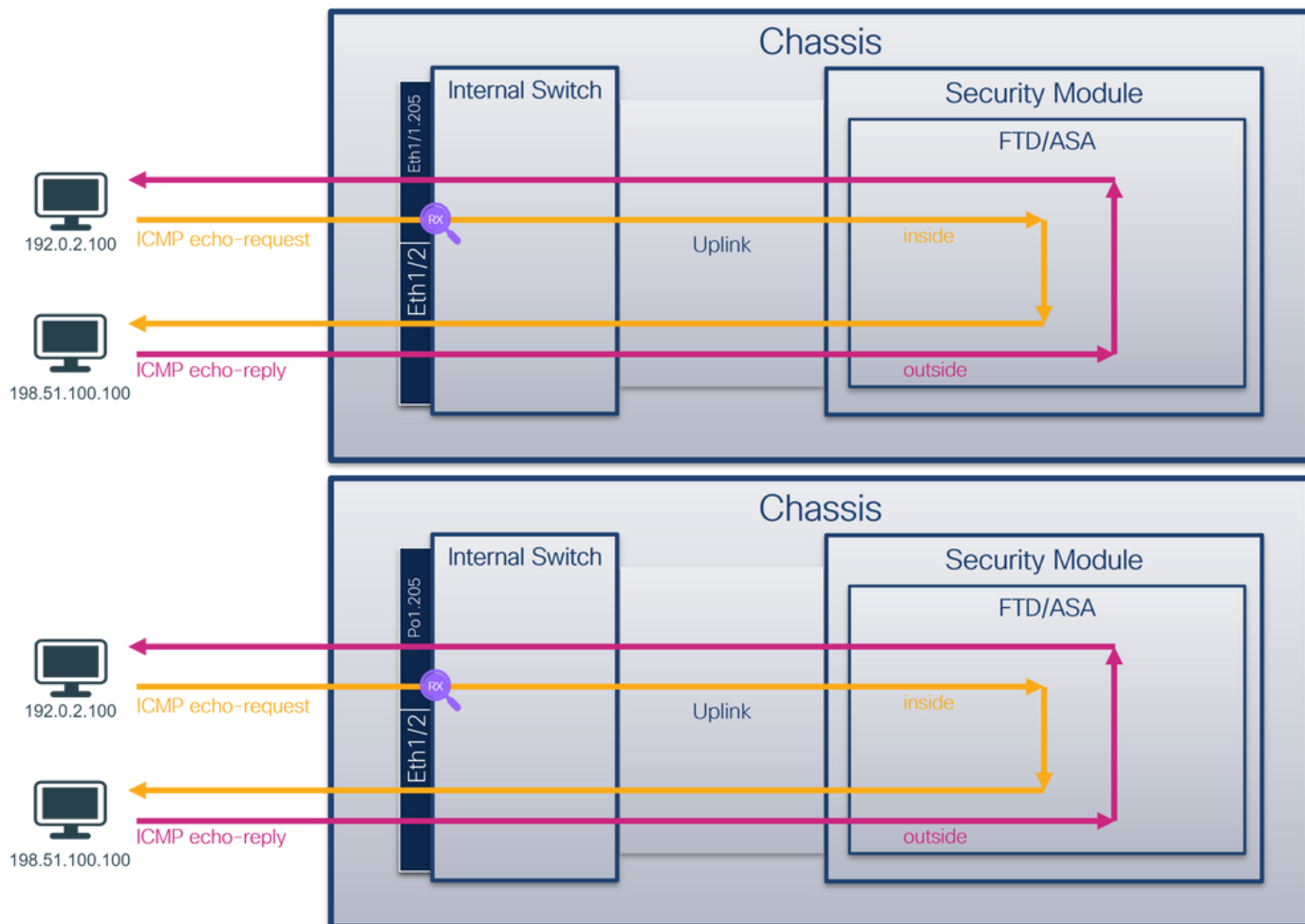
タスク	キャプチャポイント	内部フィルタ	方向	キャプチャされたトラフィック
インターフェイスEthernet1/1でのパケットキャプチャの設定と確認	Ethernet1/1	なし	入力の	ホスト192.0.2.100からホスト198.51.100.100へのICMPエコー要求
メンバーインターフェイスEthernet1/3およびEthernet1/4を持つ	Ethernet1/3	なし	入力の	ホスト192.0.2.100からホスト198.51.100.100へのICMPエコー要求
インターフェイスPortchannel1でパケットキャプチャを設定および確認します	Ethernet1/4	なし	入力の	ホスト192.0.2.100からホスト198.51.100.100へのICMPエコー要求

物理インターフェイスまたはポートチャネルインターフェイスのサブインターフェイスでのパケットキャプチャ



FTDまたはASA CLIを使用して、サブインターフェイスEthernet1/1.205またはPortchannel1.205上のパケットキャプチャを設定および確認します。両方のサブインターフェイスの名前はinsideです。

## トポロジ、パケットフロー、およびキャプチャポイント



## コンフィギュレーション

インターフェイスEthernet1/1またはPort-channel1でパケットキャプチャを設定するには、ASAまたはFTD CLIで次の手順を実行します。

1. nameifを確認します。

```
> 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. キャプチャセッションを作成します。

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

3. キャプチャセッションを有効にします。

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

## 確認

キャプチャセッション名、管理および動作の状態、インターフェイススロット、およびIDを確認します。Pcapsize値(バイト単位)が増加し、キャプチャされたパケットの数がゼロ以外であることを確認します。

```
> 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

この場合、外部VLAN Ovlan=205のフィルタが作成され、インターフェイスに適用されます。

Port-channel1の場合、フィルタOvlan=205を使用したキャプチャがすべてのメンバーインターフェイスで設定されます。

> **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

ポートチャネルメンバーインターフェイスは、FXOSのlocal-mgmtコマンドシェルでshow portchannel summary コマンドを使用して確認できます。

```
> 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
```

ASAのFXOSにアクセスするには、connect fxos adminコマンドを実行します。マルチコンテキストの場合は、管理コンテキストでこのコマンドを実行します。

## キャプチャファイルの収集

「Secure Firewall 3100内部スイッチキャプチャファイルの収集」セクションの手順に従ってください。

## ファイル分析のキャプチャ

パケットキャプチャファイルリーダーアプリケーションを使用して、Ethernet1/1.205のキャプチャファイルを開きます。最初のパケットを選択し、キーポイントを確認します。

1. ICMPエコー要求パケットだけがキャプチャされます。
2. 元のパケットヘッダーにはVLANタグ205が付いています。

Portchannel1メンバーインターフェイスのキャプチャファイルを開きます。最初の packets を選択し、キーポイントを確認します。

1. ICMPエコー要求パケットだけがキャプチャされます。
2. 元のパケットヘッダーにはVLANタグ205が付いています。

### 説明

スイッチキャプチャは、外部VLAN 205に一致するフィルタを使用して、サブインターフェイス Ethernet1/1.205またはPortchannel1.205で設定されます。

タスクの要約を次の表に示します。

タスク	キャプチャポイント	内部フィルタ	方向	キャプチャされたトラフィック
サブインターフェイス Ethernet1/1.205でのパケットキャプチャの設定と確認	Ethernet 1/1	外部 VLAN 205	入力のみに	ホスト192.0.2.100からホスト198.51.100.100へのICMPエコー要求
サブインターフェイス Portchannel1.205で、メンバーインターフェイスEthernet1/3および	Ethernet 1/3 Ethernet	外部 VLAN 205	入力のみに	ホスト192.0.2.100からホスト198.51.100.100へのICMPエコー要求



Ethernet1/4を使用してパケットキャプチャを設定および確認します 1/4

## 内部インターフェイスでのパケットキャプチャ

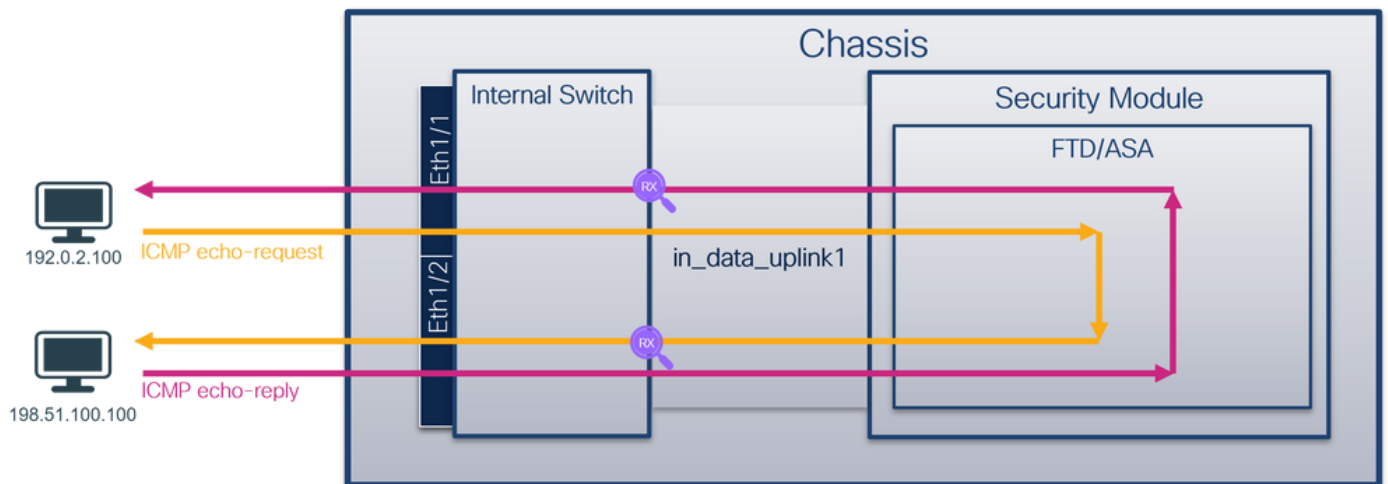
セキュアファイアウォールには、2つの内部インターフェイスがあります。

- `in_data_uplink1` : アプリケーションを内部スイッチに接続します。
- `in_mgmt_uplink1` : 管理インターフェイスへのSSHなど、管理接続用の専用パケットパス、またはFMCとFTD間の管理接続 ( `sftunnel`とも呼ばれる ) を提供します。

### タスク 1

FTDまたはASA CLIを使用して、アップリンクインターフェイス`in_data_uplink1`でパケットキャプチャを設定および確認します。

### トポロジ、パケットフロー、およびキャプチャポイント



## コンフィギュレーション

インターフェイス`in_data_uplink1`でパケットキャプチャを設定するには、ASAまたはFTD CLIで次の手順を実行します。

1. キャプチャセッションを作成します。

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

2. キャプチャセッションを有効にします。

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

### 確認

キャプチャセッション名、管理および動作の状態、インターフェイススロット、およびIDを確認します。`Pcapsize`値 ( バイト単位 ) が増加し、キャプチャされたパケットの数がゼロ以外であることを確認します。

```
> show capture capsw detail
```

```
Packet Capture info
```

**Name:** capsu  
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-capsu-data-uplink1.pcap  
**Pcapsize:** 7704  
Filter: capsu-1-18

Packet Capture Filter Info

Name: capsu-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

この場合、キャプチャは内部ID 18 (セキュアファイアウォール3130のin\_data\_uplink1インターフェイス) を持つインターフェイスで作成されます。FXOS local-mgmtコマンドシエルのshow portmanager switch statusコマンドは、インターフェイスIDを示します。

> 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

ASAのFXOSにアクセスするには、**connect fxos admin**コマンドを実行します。マルチコンテキストの場合は、管理コンテキストでこのコマンドを実行します。

## キャプチャファイルの収集

「Secure Firewall 3100内部スイッチキャプチャファイルの収集」セクションの手順に従ってください。

## ファイル分析のキャプチャ

パケットキャプチャファイルリーダーアプリケーションを使用して、インターフェイス in\_data\_uplink1のキャプチャファイルを開きます。キーポイントを確認します。この場合、ICMPエコー要求パケットとエコー応答パケットがキャプチャされます。これらは、アプリケーションから内部スイッチに送信されるパケットです。

The screenshot displays a list of captured network packets. The selected packet (No. 1) is an ICMP Echo (ping) request from source 192.0.2.100 to destination 198.51.100.100. Below the packet list, the raw data is shown in hexadecimal and ASCII, along with a protocol analysis pane.

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	0x40e8 (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 d9 93 40 00 40 01 00 1a c0 00 02 64 c6 33  .TM@.-...d3
0020  64 64 08 00 7f 15 00 00 00 21 39 3f f0 62 00 00  dd...-197-b...
0030  00 00 8b 1a 05 00 00 00 00 00 10 11 12 13 14 15  .-...-...
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  .-...-!%$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
0060  36 37 55 55 55 55  .67UUU
  
```

## 説明

アップリンクインターフェイスでスイッチキャプチャが設定されると、アプリケーションから内部スイッチに送信されるパケットだけがキャプチャされます。アプリケーションに送信されたパケットはキャプチャされません。

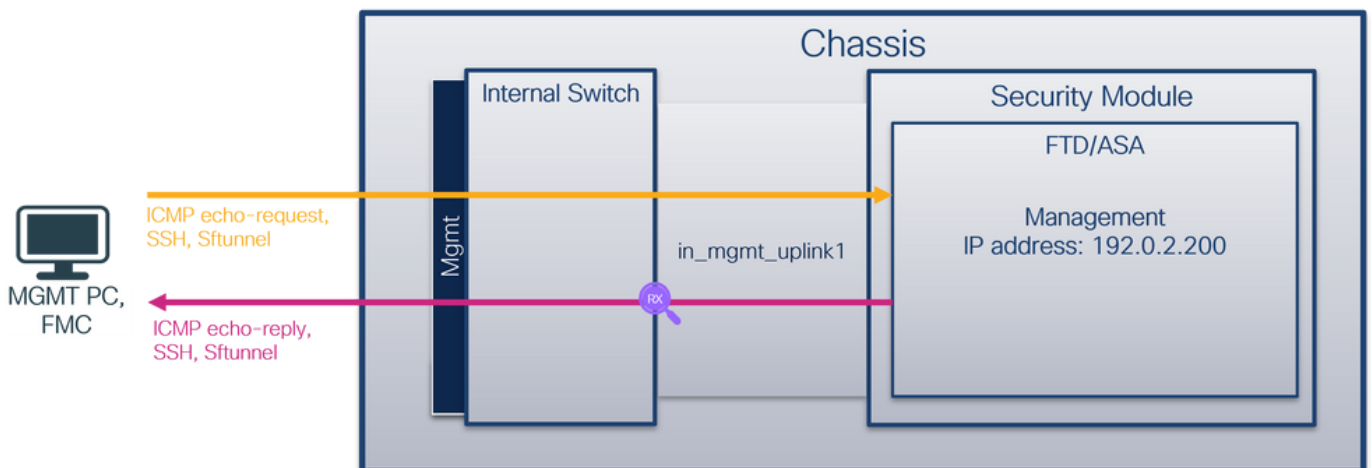
タスクの要約を次の表に示します。

タスク	キャプチャポイント	内部ファイラ	方向	キャプチャされたトラフィック
アップリンクインターフェイス in_data_uplink1でパケットキャプチャを設定および確認する	in_data_uplink1	なし	入力のみ	ホスト192.0.2.100からホスト198.51.100.100へのICMPエコーリクエスト ホスト198.51.100.100からホスト192.0.2.100へのICMPエコー応答

## タスク 2

FTDまたはASA CLIを使用して、アップリンクインターフェイスin\_mgmt\_uplink1でパケットキャプチャを設定および確認します。管理プレーン接続のパケットのみがキャプチャされます。

### トポロジ、パケットフロー、およびキャプチャポイント



## コンフィギュレーション

インターフェイスin\_mgmt\_uplink1でパケットキャプチャを設定するには、ASAまたはFTD CLIで次の手順を実行します。

1. キャプチャセッションを作成します。

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

2. キャプチャセッションを有効にします。

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

### 確認

キャプチャセッション名、管理および動作の状態、インターフェイススロット、およびIDを確認します。Pcapsize値 (バイト単位) が増加し、キャプチャされたパケットの数がゼロ以外であることを確認します。

> 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

この場合、キャプチャは内部ID 19を持つインターフェイス上で作成されます。この内部ID 19は、セキュアファイアウォール3130上のin\_mgmt\_uplink1インターフェイスです。FXOS local-mgmtコマンドシエルのshow portmanager switch statusコマンドは、インターフェイスIDを表示します。

> 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

ASAのFXOSにアクセスするには、**connect fxos admin**コマンドを実行します。マルチコンテキストの場合は、管理コンテキストでこのコマンドを実行します。

## キャプチャファイルの収集

「Secure Firewall 3100内部スイッチキャプチャファイルの収集」セクションの手順に従ってください。

## ファイル分析のキャプチャ

パケットキャプチャファイルリーダーアプリケーションを使用して、インターフェイス **in\_mgmt\_uplink1**のキャプチャファイルを開きます。キーポイントを確認します。この場合、管理IPアドレス192.0.2.200からのパケットのみが表示されます。例としては、SSH、Sftunnel、ICMPエコー応答パケットなどがあります。これらは、アプリケーション管理インターフェイスから内部スイッチ経由でネットワークに送信されるパケットです。

No.	Time	Source	Destination	Protocol	Length	IP ID	Flags	Info
196	2022-08-07 23:21:45.133362	192.0.2.200	192.0.2.101	TCP	1518	0xb7d0 (47056)	64	39181 → 8305 [ACK] Seq=61372 Ack=875 Win=1384 Len=1448 TS
197	2022-08-07 23:21:45.133385	192.0.2.200	192.0.2.101	TCP	1518	0xb7d1 (47057)	64	39181 → 8305 [ACK] Seq=62820 Ack=875 Win=1384 Len=1448 TS
198	2022-08-07 23:21:45.133388	192.0.2.200	192.0.2.101	TLSv1.2	990	0xb7d2 (47058)	64	Application Data
199	2022-08-07 23:21:45.928772	192.0.2.200	192.0.2.100	ICMP	78	0xbd48 (48456)	64	Echo (ping) reply id=0x0001, seq=4539/47889, ttl=64
200	2022-08-07 23:21:45.949024	192.0.2.200	192.0.2.101	TLSv1.2	128	0x4a97 (19095)	64	Application Data
201	2022-08-07 23:21:45.949027	192.0.2.200	192.0.2.101	TCP	70	0x4a98 (19096)	64	8305 → 58885 [ACK] Seq=21997 Ack=26244 Win=4116 Len=0 TSv
202	2022-08-07 23:21:46.019895	192.0.2.200	192.0.2.101	TLSv1.2	100	0x4a99 (19097)	64	Application Data
203	2022-08-07 23:21:46.019899	192.0.2.200	192.0.2.101	TLSv1.2	96	0x4a9a (19098)	64	Application Data
204	2022-08-07 23:21:46.019903	192.0.2.200	192.0.2.101	TCP	70	0x4a9b (19099)	64	8305 → 58885 [ACK] Seq=22053 Ack=26274 Win=4116 Len=0 TSv
205	2022-08-07 23:21:46.019906	192.0.2.200	192.0.2.101	TCP	70	0x4a9c (19100)	64	8305 → 58885 [ACK] Seq=22053 Ack=26300 Win=4116 Len=0 TSv
206	2022-08-07 23:21:46.136415	192.0.2.200	192.0.2.101	TCP	70	0xb7d3 (47059)	64	39181 → 8305 [ACK] Seq=65188 Ack=921 Win=1384 Len=0 TSval
207	2022-08-07 23:21:46.958148	192.0.2.200	192.0.2.100	ICMP	78	0xbd9e (48542)	64	Echo (ping) reply id=0x0001, seq=4540/48145, ttl=64
208	2022-08-07 23:21:47.980409	192.0.2.200	192.0.2.100	ICMP	78	0xbd9f (48543)	64	Echo (ping) reply id=0x0001, seq=4541/48146, ttl=64
209	2022-08-07 23:21:48.406312	192.0.2.200	192.0.2.101	TCP	70	0x4a9d (19101)	64	8305 → 58885 [ACK] Seq=22053 Ack=26366 Win=4116 Len=0 TSv
210	2022-08-07 23:21:48.903236	192.0.2.200	192.0.2.101	TLSv1.2	747	0x4a9e (19102)	64	Application Data
211	2022-08-07 23:21:48.994386	192.0.2.200	192.0.2.100	ICMP	78	0xbe48 (48712)	64	Echo (ping) reply id=0x0001, seq=4542/48657, ttl=64
212	2022-08-07 23:21:50.008576	192.0.2.200	192.0.2.100	ICMP	78	0xbe49 (48713)	64	Echo (ping) reply id=0x0001, seq=4543/48658, ttl=64
213	2022-08-07 23:21:50.140167	192.0.2.200	192.0.2.101	TCP	1518	0xb7d4 (47060)	64	39181 → 8305 [ACK] Seq=65188 Ack=921 Win=1384 Len=0 TSval
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=0 TSv
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	0xbfd8 (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	0xbfd9 (48899)	64	Echo (ping) reply id=0x0001, seq=4546/49681, ttl=64
220	2022-08-07 23:21:53.073144	192.0.2.200	192.0.2.100	SSH	170	0xad34 (44340)	64	Server: Encrypted packet (len=112)
221	2022-08-07 23:21:53.194906	192.0.2.200	192.0.2.100	TCP	64	0xad35 (44341)	64	22 → 53249 [ACK] Seq=1025 Ack=881 Win=946 Len=0
222	2022-08-07 23:21:53.905480	192.0.2.200	192.0.2.101	TLSv1.2	747	0x4a9f (19103)	64	Application Data
223	2022-08-07 23:21:54.102899	192.0.2.200	192.0.2.100	ICMP	78	0xbf63 (48995)	64	Echo (ping) reply id=0x0001, seq=4547/49937, ttl=64
224	2022-08-07 23:21:54.903675	192.0.2.200	192.0.2.101	TCP	70	0x4aa0 (19104)	64	8305 → 58885 [ACK] Seq=23407 Ack=26424 Win=4116 Len=0 TSv
225	2022-08-07 23:21:55.136700	192.0.2.200	192.0.2.100	TCP	70	0xbf64 (48996)	64	Echo (ping) reply id=0x0001, seq=4548/50103, ttl=64

## 説明

管理アップリンクインターフェイスでスイッチキャプチャが設定されると、アプリケーション管理インターフェイスから送信された入力パケットだけがキャプチャされます。アプリケーション管理インターフェイス宛てのパケットはキャプチャされません。

タスクの要約を次の表に示します。

タスク	キャプチャポイント	内部フィルタ	方向	キャプチャされたトラフィック
管理アップリンクインターフェイスでのパケットキャプチャの設定と確認	in_mgmt_uplink1	なし	入力のみ (管理インターフェイスから内部スイッチを介してネットワークへ)	FTD管理IPアドレス192.0.2.200からホス 192.0.2.100へのICMPエコー応答 Ftd管理IPアドレス192.0.2.200からFMC アドレス192.0.2.101へのSFTUNNEL FTD管理IPアドレス192.0.2.200からホス 192.0.2.100へのSSH

## パケット キャプチャ フィルタ

内部スイッチのパケットキャプチャフィルタは、データプレーンのキャプチャと同じように設定されます。フィルタを設定するには、**ethernet-type**および**match**オプションを使用します。

## コンフィギュレーション

ASAまたはFTD CLIで次の手順に従って、インターフェイスEthernet1/1のホスト198.51.100.100からのARPフレームまたはICMPパケットと一致するフィルタを使用してパケットキャプチャを設定します。

1. nameifを確認します。

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

2. ARPまたはICMPのキャプチャセッションを作成します。

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

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

## 確認

キャプチャセッション名とフィルタを確認します。Ethertype値は、10進数では2054、16進数では0x0806です。

```
> 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

これは、ICMPのフィルタの検証です。IPプロトコル1はICMPです。

> **show capture capsw detail**

Packet Capture info

<b>Name:</b>	<b>capsw</b>
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
<b>Filter:</b>	<b>capsw-1-1</b>

**Packet Capture Filter Info**

<b>Name:</b>	<b>capsw-1-1</b>
<b>Protocol:</b>	<b>1</b>
Ivlan:	0
Ovlan:	0
<b>Src Ip:</b>	<b>198.51.100.100</b>
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

## Secure Firewall 3100内部スイッチキャプチャファイルの収集

ASAまたはFTD CLIを使用して、内部スイッチキャプチャファイルを収集します。FTDでは、キャプチャファイルは、CLIのcopyコマンドを使用して、データインターフェイスまたは診断インターフェイス経由で到達可能な宛先にエクスポートすることもできます。

あるいは、エキスパートモードで/ngfw/var/commonにファイルをコピーし、File Downloadオプションを使用してFMCからダウンロードすることもできます。

ポートチャネルインターフェイスの場合は、すべてのメンバーインターフェイスからパケットキャプチャファイルを収集してください。

## 平均応答時間

ASA CLIで内部スイッチキャプチャファイルを収集するには、次の手順に従います。

1. キャプチャを停止します。

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

2. キャプチャセッションが停止していることを確認し、キャプチャファイル名をメモします。

```
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. CLIのcopyコマンドを使用して、リモート接続先にファイルをエクスポートします。

```
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

次の手順に従って、FTD CLIで内部スイッチキャプチャファイルを収集し、データまたは診断インターフェイス経由で到達可能なサーバにコピーします。

### 1. 診断CLIに移動します。

```
> 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. キャプチャを停止します。

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

### 3. キャプチャセッションが停止していることを確認し、キャプチャファイル名をメモします。

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

Total Physical ports involved in Packet Capture: 1
Physical port:
Slot Id:         1
Port Id:         1
Pcapfile:     /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize:        139826
Filter:          caps-1-1
```

Packet Capture Filter Info

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

Total Physical breakout ports involved in Packet Capture: 0

886 packets captured on disk using switch capture

Reading of capture file from disk is not supported

#### 4. CLIのcopyコマンドを使用して、リモート接続先にファイルをエクスポートします。

```
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
```

File Downloadオプションを使用してFMCからキャプチャファイルを収集するには、次の手順に従います。

##### 1. キャプチャを停止します。

```
> capture capsw switch stop
```

##### 2. キャプチャセッションが停止していることを確認し、ファイル名と完全なキャプチャファイルパスをメモします。

```
> 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. エキスパートモードに移行し、ルートモードに切り替えます。

> **expert**

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

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

4. キャプチャファイルを/ngfw/var/common/:

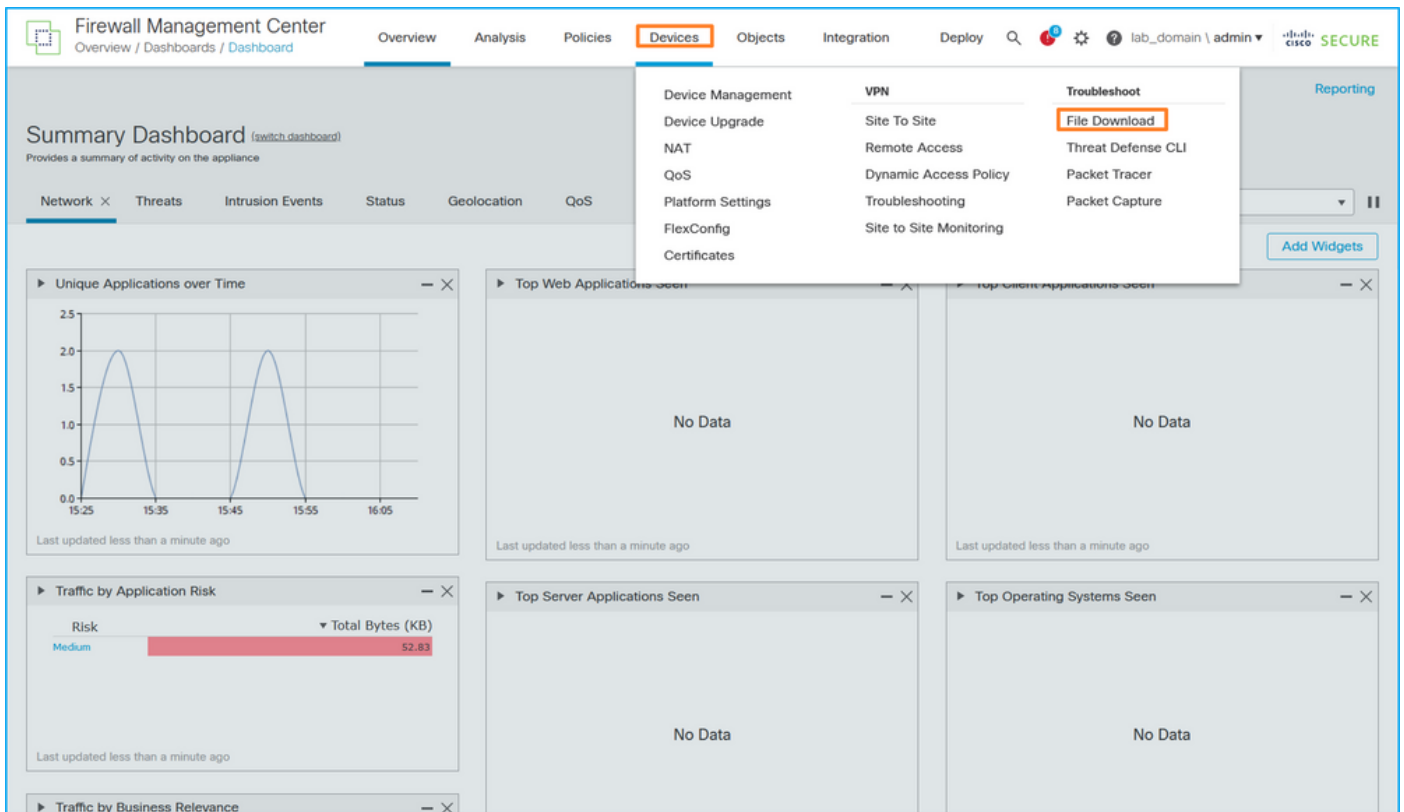
```
root@KSEC-FPR3100-1:/home/admin cp /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
/ngfw/var/common/
```

```
root@KSEC-FPR3100-1:/home/admin ls -l /ngfw/var/common/sess*
```

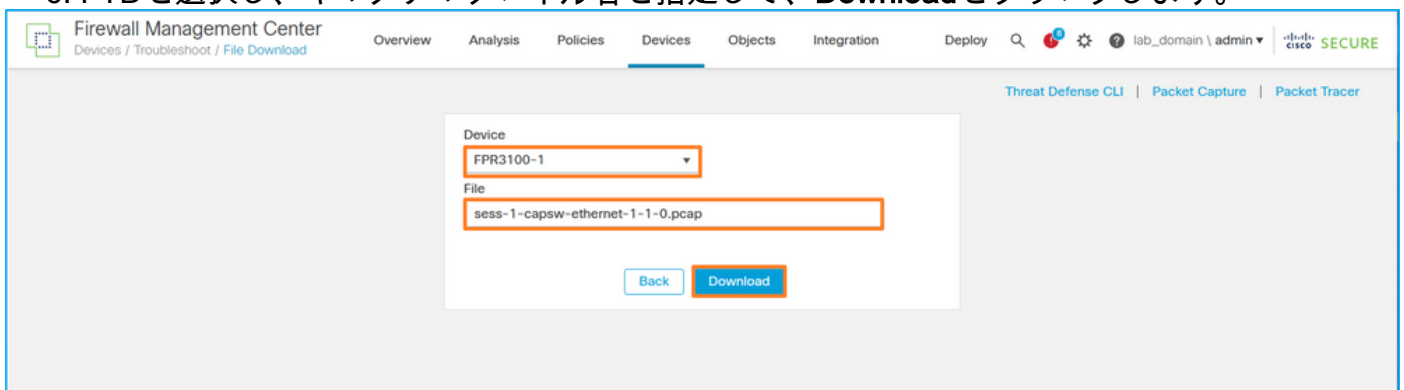
```
-rwxr-xr-x 1 root admin 139826 Aug 7 20:14 /ngfw/var/common/sess-1-capsw-ethernet-1-1-0.pcap
```

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

5. FMCで、[Devices] > [File Download] を選択します。



## 6. FTDを選択し、キャプチャファイル名を指定して、Downloadをクリックします。



## 内部スイッチパケットキャプチャのガイドライン、制限事項、およびベストプラクティス

### ガイドラインと制限事項:

- 複数のスイッチキャプチャ設定セッションがサポートされますが、一度にアクティブにできるスイッチキャプチャセッションは1つだけです。2つ以上のキャプチャセッションを有効にしようとする、エラー「**ERROR:Failed to enable session, as limit of maximum 1 active packet capture sessions reached**」が表示されます。
- アクティブなスイッチキャプチャは削除できません。
- アプリケーションでスイッチキャプチャを読み取ることができません。ユーザはファイルをエクスポートする必要があります。
- dump、decode、packet-number、traceなどの特定のデータプレーンキャプチャオプションは、スイッチキャプチャではサポートされていません。
- マルチコンテキストASAの場合、データインターフェイスのスイッチキャプチャはユーザコンテキストで設定されます。in\_data\_uplink1およびin\_mgmt\_uplink1インターフェイスでのスイッチキャプチャは、管理コンテキストでのみサポートされます。

TACケースでのパケットキャプチャの使用に基づくベストプラクティスのリストを次に示します。

- ガイドラインと制限事項に注意してください。
- キャプチャフィルタを使用します。
- キャプチャフィルタの設定時に、パケットIPアドレスに対するNATの影響を考慮してください。
- フレームサイズを指定する`packet-length`を増減します。デフォルト値の1518バイトと異なる場合に使用します。サイズが小さいほど、キャプチャされたパケットの数が増え、その逆も同様です。
- 必要に応じてバッファサイズを調整します。
- `show cap <cap_name> detail`コマンドの出力のDrop Countに注意してください。バッファサイズの制限に達すると、廃棄カウントカウンタが増加します。

## 関連情報

- [Firepower 4100/9300シャーシマネージャおよびFXOS CLIコンフィギュレーションガイド](#)
- [Cisco Secure Firewall 3100スタートアップガイド](#)
- [Cisco Firepower 4100/9300 FXOSコマンドリファレンス](#)



## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。