

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

[はじめに](#)

[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](#)

[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](#)

[セキュアファイアウォール3100/4200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](#)

[セキュアファイアウォール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](#)

はじめに

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

製品に関する基礎知識、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、クリアな（デフォルト）設定で作業を開始しています。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。

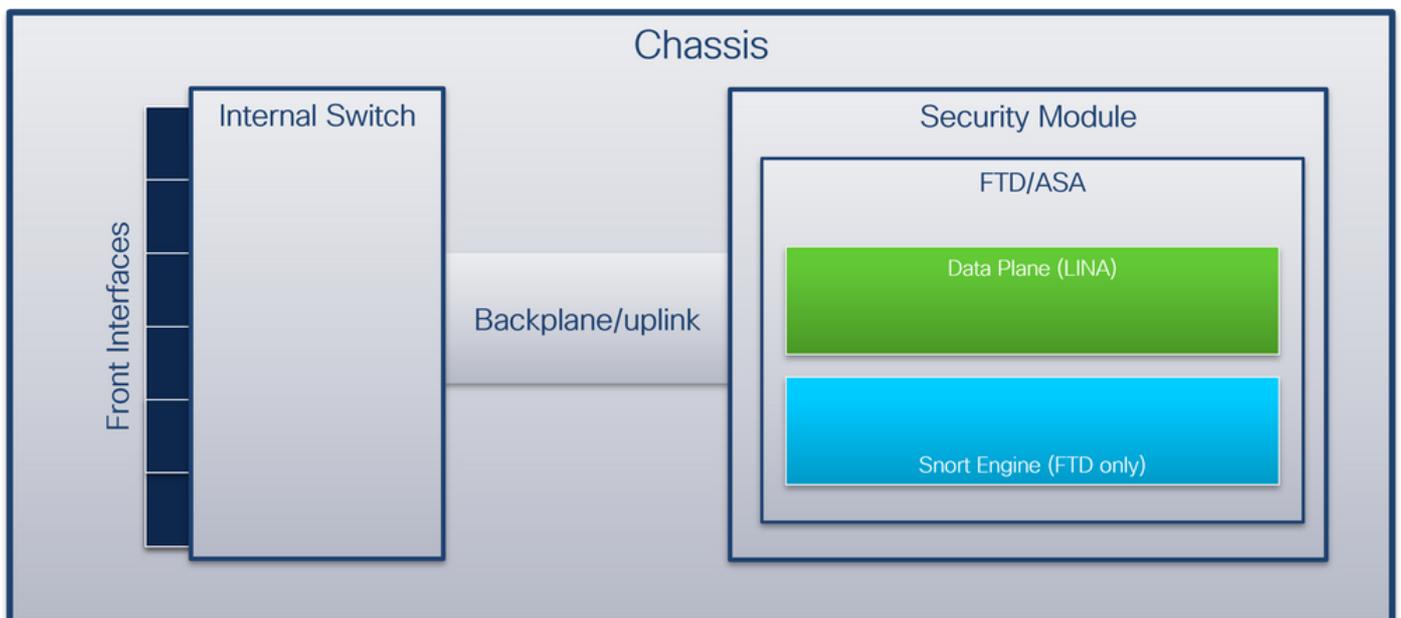
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- セキュアファイアウォール31xx、42xx
- 火力41xx
- 火力93xx
- Cisco Secure eXtensible Operating System(FXOS)2.12.0.x
- Cisco Secure Firewall Threat Defense(FTD)7.2.0.x、7.4.1-172
- Cisco Secure Firewall Management Center(FMC)7.2.0.x、7.4.1-172
- 適応型セキュリティアプライアンス(ASA)9.18(1)x、9.20(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およびセキュアファイアウォール3100/4200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、および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します。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」

は強力な技術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や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。
- 管理アップリンク：内部スイッチとアプリケーション間の管理トラフィックパスを提供する、Secure Firewall 3100/4200専用の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3100/4200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	管理アップリンクインターフェイス	マップされたアプリケーションインターフェイス
Firepower 4100 (Firepower 4110/4112を除く)	1	SM1: イーサネット1/9 Ethernet1/10	N/A	内部データ0/0 内部データ0/1
Firepower 4110/4112	1	イーサネット1/9	N/A	内部データ0/0 内部データ0/1
FirePOWER 9300	3	SM1: イーサネット1/9 Ethernet1/10 SM2: Ethernet1/11 Ethernet1/12 SM3: Ethernet1/13 Ethernet1/14	N/A	内部データ0/0 内部データ0/1 内部データ0/0 内部データ0/1 内部データ0/0 内部データ0/1

Cisco Secure Firewall 3100	1	SM1:in_data_uplink1	in_mgmt_uplink1	内部データ0/1 管理1/1
Cisco Secure Firewall 4200	1	SM1:in_data_uplink1 SM1:in_data_uplink2 (4245のみ)	in_mgmt_uplink1 in_mgmt_uplink2	内部データ0/1 Internal-Data0/2 (4245のみ) 管理1/1 管理1/2

モジュールあたり2つのバックプレーンインターフェイスを備えたFirepower 4100/9300または2つのデータアップリンクインターフェイスを備えたセキュアファイアウォール4245の場合、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のバックプレーンまたはアップリンクインターフェイスの名前。

show interface detailコマンドを使用して、内部インターフェイスを確認します。

```
<#root>
```

```
>
```

```
show interface detail | grep Interface
```

```
Interface Internal-Control0/0 "ha_ctl_nlp_int_tap", is up, line protocol is up
```

```
Control Point Interface States:
  Interface number is 6
  Interface config status is active
  Interface state is active
```

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

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

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

```
Control Point Interface States:
  Interface number is 3
  Interface config status is active
  Interface state is active
```

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

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(PVLAN)またはポートVLANタグ、および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、内部スイッチがインターフェイスを識別するために使用します。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コマンドシエルで確認できます。

```
<#root>
```

```
firepower#
```

```
connect fxos
```

```
...
```

```
firepower(fxos)#
```

```
show run int e1/2
```

```
!Command: show running-config interface Ethernet1/2
```

```
!Time: Tue Jul 12 22:32:11 2022
```

```
version 5.0(3)N2(4.120)
```

```
interface Ethernet1/2
  description U: Uplink
  no lldp transmit
  no lldp receive
  no cdp enable
```

```
switchport mode dot1q-tunnel
```

```
switchport trunk native vlan 102
```

```
speed 1000  
duplex full  
udld disable  
no shutdown
```

VN-tagも内部スイッチによって挿入され、パケットをアプリケーションに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-tag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。

セキュアファイアウォール3100/4200

Firepower 4100/9300と同様に、ポートVLANタグは内部スイッチがインターフェイスを識別するために使用されます。

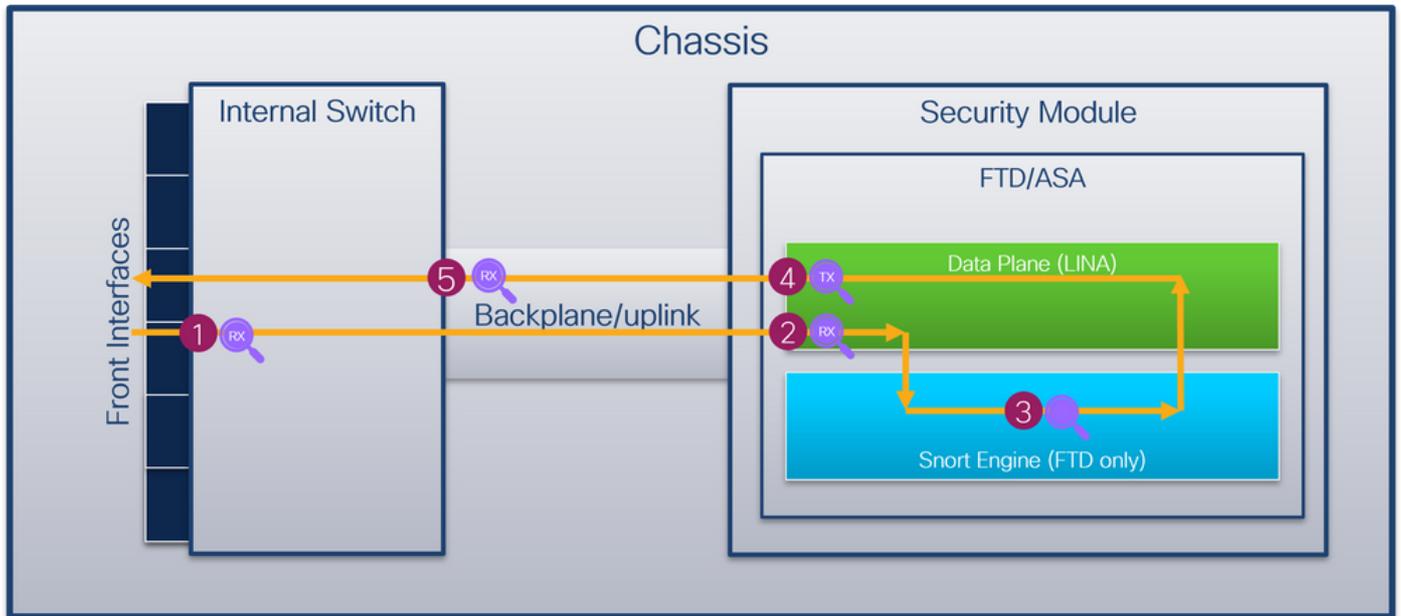
ポートVLANタグはアプリケーションと共有されます。アプリケーションは、それぞれの出カインターフェイスVLANタグを各パケットに挿入します。アプリケーションからのパケットがアップリンクインターフェイス上の内部スイッチによって受信されると、スイッチは出カインターフェイスのVLANタグを読み取り、出カインターフェイスを識別し、ポートのVLANタグを削除して、パケットをネットワークに転送します。

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

Firepower 4100/9300およびセキュアファイアウォール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。

次の図は、シャーシおよび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ています。



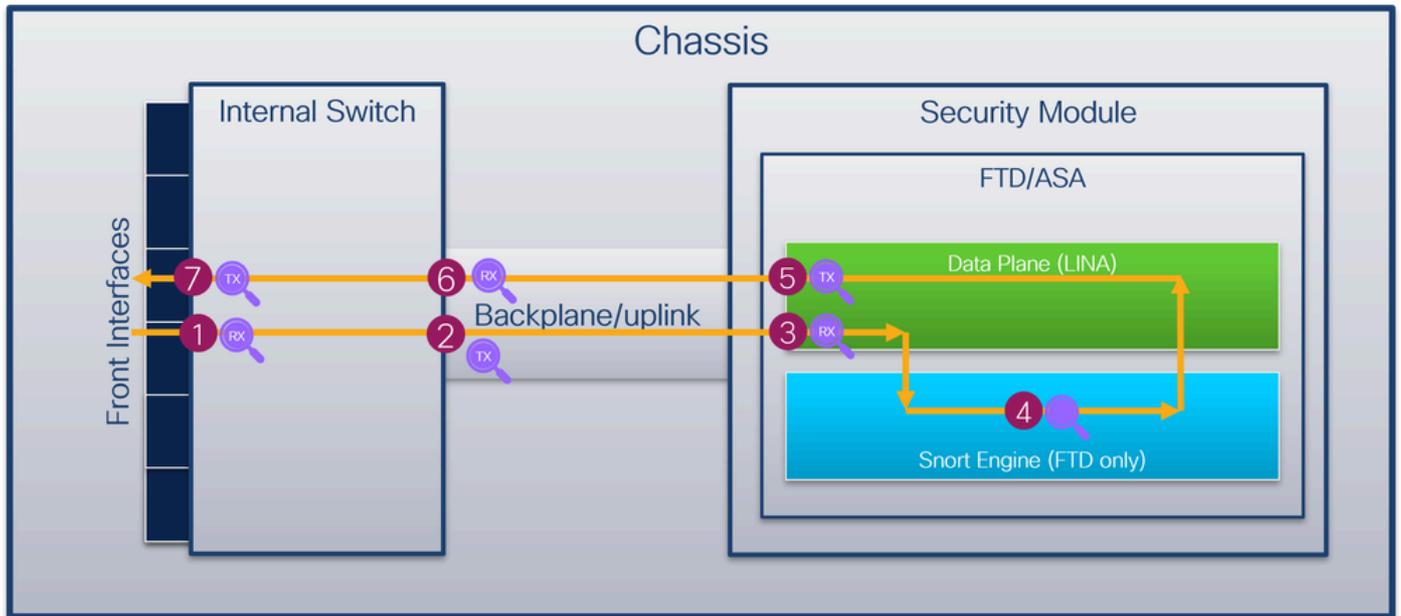
キャプチャポイントは次のとおりです。

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。

内部スイッチでは、入力インターフェイスのキャプチャだけがサポートされます。キャプチャできるのは、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です。出力パケットキャプチャはサポートされていません。

Cisco Secure Firewall 4200

セキュアファイアウォール4200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。次の図は、シャーシおよび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ています。



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. 内部スイッチバックプレーンインターフェイス出力キャプチャポイント。
3. 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
4. Snortキャプチャポイント
5. 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
6. 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。
7. 内部スイッチ前面インターフェイス出力キャプチャポイント。

内部スイッチは、双方向（入力と出力の両方）キャプチャをオプションでサポートします。デフォルトでは、内部スイッチは入力方向の packets をキャプチャします。

Firepower 4100/9300の設定と検証

Firepower 4100/9300内部スイッチのキャプチャは、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詳細については、『Cisco Firepower 4100/9300 FXOSシャーシマネージャコンフィギュレーションガイド』または『Cisco Firepower 4100/9300 FXOS CLIコンフィギュレーションガイド』の「トラブルシューティング」章の「パケットキャプチャ」セクションを参照してください。

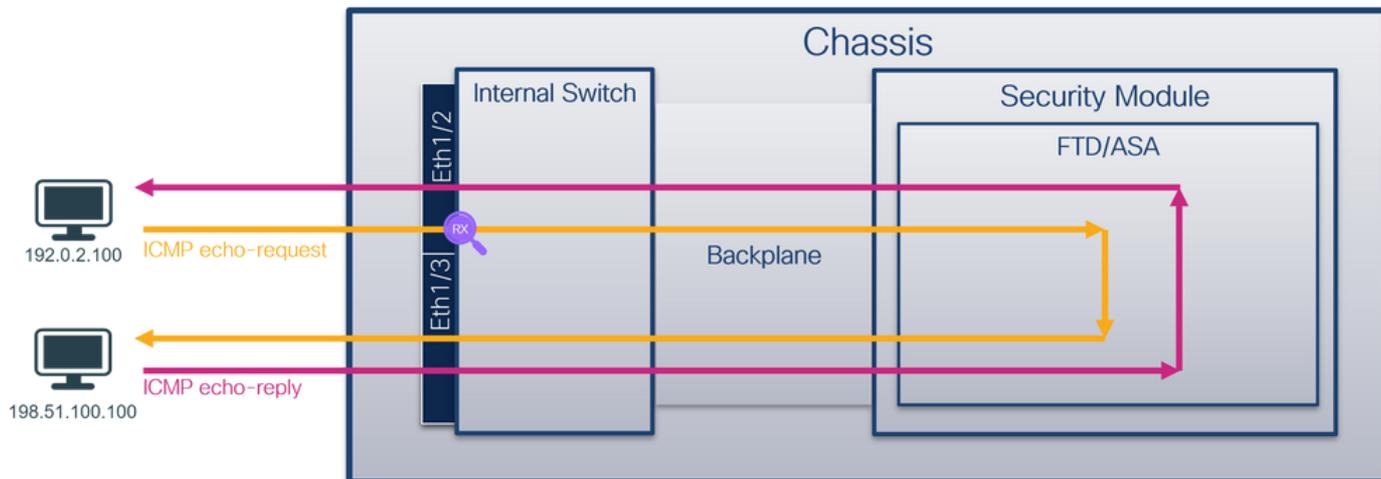
これらのシナリオは、Firepower 4100/9300内部スイッチのキャプチャの一般的な使用例をカバーしています。

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およびCLIを使用して、インターフェイスEthernet1/2またはPortchannel1インターフェイス上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必ず選択してください。

トポロジ、パケットフロー、およびキャプチャポイント

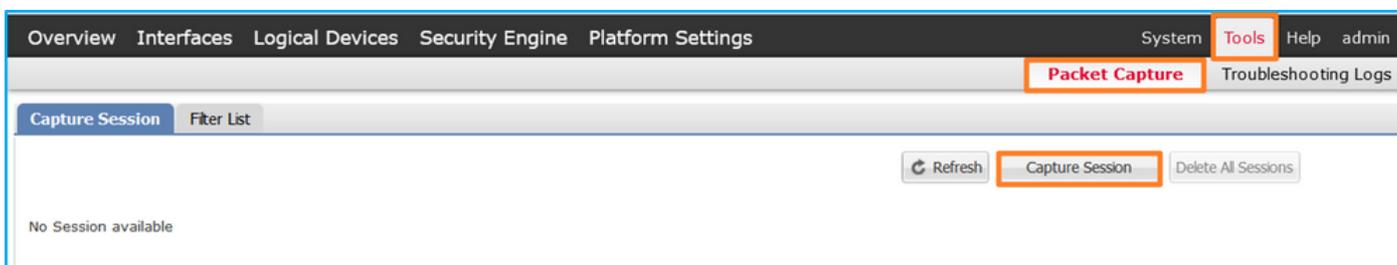


コンフィギュレーション

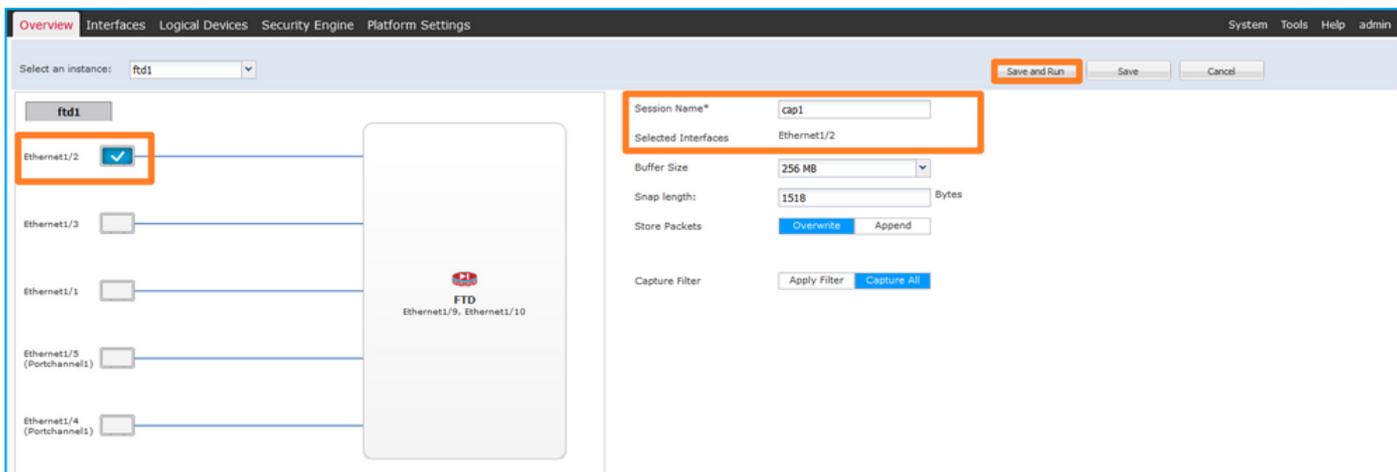
FCM (必須)

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。

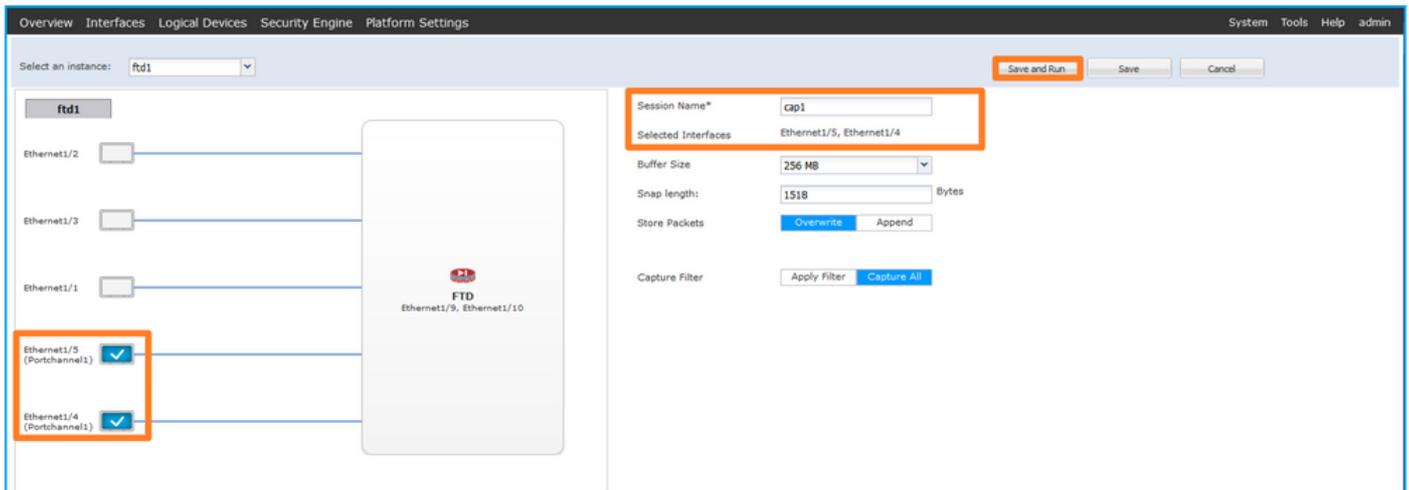
1. Tools > Packet Capture > Capture Sessionの順に選択して、新しいキャプチャセッションを作成します。



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てセッション名を指定し、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の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IDを識別します。

```
<#root>
```

```
firepower#
```

```
scope ssa
```

```
firepower /ssa #
```

```
show app-instance
```

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

2. ポートチャン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識別します。

```
<#root>
```

```
firepower#
```

```
connect fxos
```

```
<output skipped>
```

```
firepower(fxos)#
```

```
show port-channel summary
```

```
Flags: D - Down          P - Up in port-channel (members)
       I - Individual    H - Hot-standby (LACP only)
       s - Suspended     r - Module-removed
       S - Switched      R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
```

```
-----
Group Port-      Type      Protocol  Member Ports
Channel
-----
1      Po1(SU)    Eth       LACP      Eth1/4(P)  Eth1/5(P)
```

3. キャプチャセッションを作成します。

```
<#root>
```

```
firepower#
```

```
scope packet-capture
```

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

```
create session cap1
```

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

```
create phy-port Eth1/2
```

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

```
set app ftd
```

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

```
set app-identifier ftd1
```

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

```
up
```

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

```
enable
```

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

```
commit
```

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

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。

```
<#root>
```

```
firepower#
```

```
scope packet-capture
```

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

```
create session cap1
```

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

```
create phy-port Eth1/4
```

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

```
set app ftd
```

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

```
set app-identifier ftd1
```

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

```
up
```

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

```
create phy-port Eth1/5
```

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

```
set app ftd
```

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

```
set app-identifier ftd1
```

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

```
up
```

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

```
enable
```

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

```
commit
```

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

検証

FCM (必須)

Interface Nameを確認し、Operational Statusがupであること、File Size (バイト単位) 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	29632	cap1-ethernet-1-2-0.pcap	fd1

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	fd1
Ethernet1/4	None	85000	cap1-ethernet-1-4-0.pcap	fd1

FXOSのCLI

scope packet-captureでキャプチャの詳細を確認します。

```
<#root>
```

```
firepower#
```

```
scope packet-capture
```

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

```
show session cap1
```

Traffic Monitoring Session:

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

```
Session: 1
```

```
Admin State: Enabled
```

```
Oper State: Up
```

Oper State Reason: Active

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

Physical ports involved in Packet Capture:

Slot Id: 1

Port Id: 2

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

Pcapsize: 75136 bytes

Filter:
Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

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:

<#root>

firepower#

scope packet-capture

firepower /packet-capture #

show session cap1

Traffic Monitoring Session:

Packet Capture Session Name: cap1

Session: 1

Admin State: Enabled

Oper State: Up

Oper State Reason: Active

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

Physical ports involved in Packet Capture:

Slot Id: 1

Port Id: 4

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

Pcapsize: 310276 bytes

Filter:
Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

Slot Id: 1

Port Id: 5

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

Pcapsize: 160 bytes

Filter:
Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

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」セクションの手順を実行します。

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2回取得されて表示されます。
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。

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

Packet List:

No.	Time	Source	Destination	Protocol	Length	IP ID	TTL	Info
1	2022-07-13 06:23:58.285080930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found!)
2	2022-07-13 06:23:58.285082858	192.0.2.100	198.51.100.100	ICMP	102	0x9dec (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found!)
3	2022-07-13 06:23:59.309048886	192.0.2.100	198.51.100.100	ICMP	108	0x9ed0 (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found!)
4	2022-07-13 06:23:59.309193731	192.0.2.100	198.51.100.100	ICMP	102	0x9ed0 (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found!)
5	2022-07-13 06:24:00.333054190	192.0.2.100	198.51.100.100	ICMP	108	0x9f20 (40736)	64	Echo (ping) request id=0x001a, seq=9/2304, ttl=64 (no response found!)
6	2022-07-13 06:24:00.333056014	192.0.2.100	198.51.100.100	ICMP	102	0x9f20 (40736)	64	Echo (ping) request id=0x001a, seq=9/2304, ttl=64 (no response found!)
7	2022-07-13 06:24:01.357173530	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 06:24:11.597066277	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 06:24:11.597068170	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 06:24:12.612061022	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!)

Packet Details (Frame 1):

- VN-Tag:** Direction: From Bridge; Pointer: vif_id; Destination: 10; Looped: No; Reserved: 0; Version: 0; Source: 0.
- 802.1Q Virtual LAN (0x8100):** 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:**

Raw Packet Data:

```

0000 58 97 bd b9 77 0e 00 50 56 9d e8 be 89 26 80 0a X...w..P V...&..
0010 00 00 81 00 00 06 08 00 45 00 00 54 9d ec 40 00 .....f..E.T.:@
0020 40 01 af c0 c0 00 02 64 c6 33 64 64 08 00 4e a2 @.....d 3dd..N
0030 00 1a 00 07 fa 64 ce 62 00 00 00 20 32 07 00 .....d.b.....
0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b .....
0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b .... !"# $%&'()*+
0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,-. /0123 4567
    
```

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2回取得されて表示されます。
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を識別する追加のポート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 06:23:58.28508930	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	0x9e0d (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	0x9e0d (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 (41599)	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 (41599)	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
  
```

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。各パケットは2回取得されて表示されます。
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を識別する追加のポート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。

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-05 23:07:31.865872877	192.0.2.100	198.51.100.100	ICMP	108	0x322e (12846)	64	Echo (ping) request id=0x002d, seq=245/62720, ttl=64 (no response found)
2	2022-08-05 23:07:31.865875131	192.0.2.100	198.51.100.100	ICMP	102	0x322e (12846)	64	Echo (ping) request id=0x002d, seq=245/62720, ttl=64 (no response found)
3	2022-08-05 23:07:32.867144598	192.0.2.100	198.51.100.100	ICMP	108	0x32b9 (12985)	64	Echo (ping) request id=0x002d, seq=246/62976, ttl=64 (no response found)
4	2022-08-05 23:07:32.867145852	192.0.2.100	198.51.100.100	ICMP	102	0x32b9 (12985)	64	Echo (ping) request id=0x002d, seq=246/62976, ttl=64 (no response found)
5	2022-08-05 23:07:33.881902485	192.0.2.100	198.51.100.100	ICMP	108	0x32d8 (13016)	64	Echo (ping) request id=0x002d, seq=247/63232, ttl=64 (no response found)
6	2022-08-05 23:07:33.881904911	192.0.2.100	198.51.100.100	ICMP	102	0x32d8 (13016)	64	Echo (ping) request id=0x002d, seq=247/63232, ttl=64 (no response found)
7	2022-08-05 23:07:34.883049425	192.0.2.100	198.51.100.100	ICMP	108	0x3373 (13171)	64	Echo (ping) request id=0x002d, seq=248/63488, ttl=64 (no response found)
8	2022-08-05 23:07:34.883051649	192.0.2.100	198.51.100.100	ICMP	102	0x3373 (13171)	64	Echo (ping) request id=0x002d, seq=248/63488, ttl=64 (no response found)
9	2022-08-05 23:07:35.883478016	192.0.2.100	198.51.100.100	ICMP	108	0x3427 (13351)	64	Echo (ping) request id=0x002d, seq=249/63744, ttl=64 (no response found)
10	2022-08-05 23:07:35.883479190	192.0.2.100	198.51.100.100	ICMP	102	0x3427 (13351)	64	Echo (ping) request id=0x002d, seq=249/63744, ttl=64 (no response found)
11	2022-08-05 23:07:36.889741625	192.0.2.100	198.51.100.100	ICMP	108	0x34de (13534)	64	Echo (ping) request id=0x002d, seq=250/64000, ttl=64 (no response found)
12	2022-08-05 23:07:36.889742853	192.0.2.100	198.51.100.100	ICMP	102	0x34de (13534)	64	Echo (ping) request id=0x002d, seq=250/64000, ttl=64 (no response found)
13	2022-08-05 23:07:37.913770117	192.0.2.100	198.51.100.100	ICMP	108	0x354c (13644)	64	Echo (ping) request id=0x002d, seq=251/64256, ttl=64 (no response found)
14	2022-08-05 23:07:37.913772219	192.0.2.100	198.51.100.100	ICMP	102	0x354c (13644)	64	Echo (ping) request id=0x002d, seq=251/64256, ttl=64 (no response found)
15	2022-08-05 23:07:38.937829879	192.0.2.100	198.51.100.100	ICMP	108	0x3602 (13826)	64	Echo (ping) request id=0x002d, seq=252/64512, ttl=64 (no response found)
16	2022-08-05 23:07:38.937831215	192.0.2.100	198.51.100.100	ICMP	102	0x3602 (13826)	64	Echo (ping) request id=0x002d, seq=252/64512, ttl=64 (no response found)
17	2022-08-05 23:07:39.961786128	192.0.2.100	198.51.100.100	ICMP	108	0x36ed (14061)	64	Echo (ping) request id=0x002d, seq=253/64768, ttl=64 (no response found)
18	2022-08-05 23:07:39.961787284	192.0.2.100	198.51.100.100	ICMP	102	0x36ed (14061)	64	Echo (ping) request id=0x002d, seq=253/64768, ttl=64 (no response found)
19	2022-08-05 23:07:40.985773090	192.0.2.100	198.51.100.100	ICMP	108	0x37d5 (14293)	64	Echo (ping) request id=0x002d, seq=254/65024, ttl=64 (no response found)

Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_3, id 0
 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2回取得されて表示されます。
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Portchannel1を識別する追加のポートVLANタグ1001を挿入します。

説明

前面インターフェイスの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。

動作の順序では、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先に表示されます。

タスクの要約を次の表に示します。

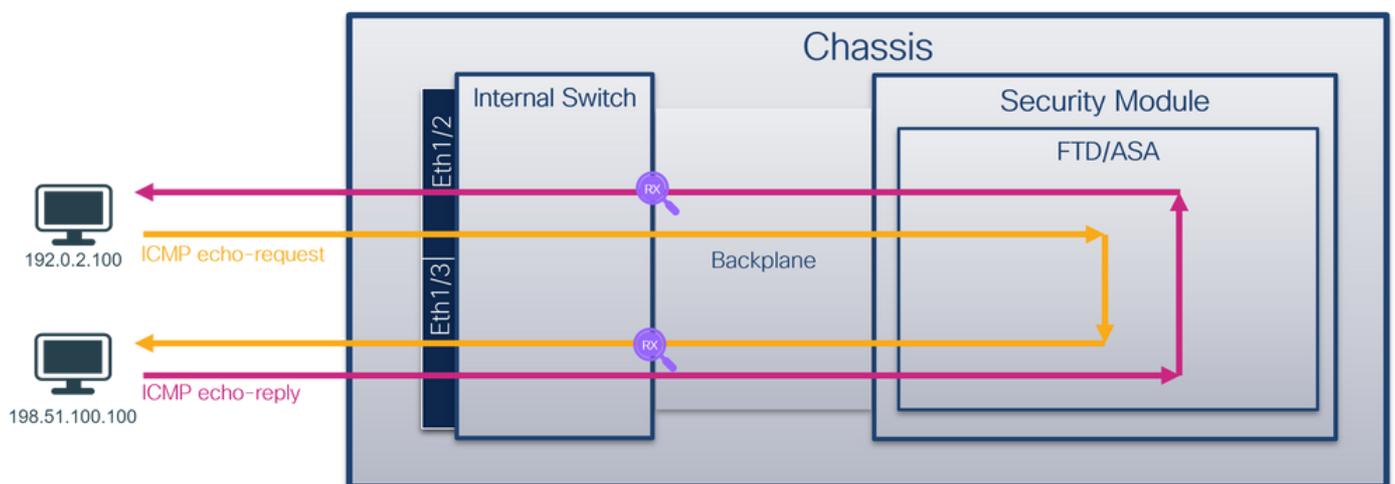
タスク	キャプチャポイント	キャプチャされたパケットの内部ポートVLAN	方向	キャプチャされたトラフィック
インターフェイス Ethernet1/2のパケットキャプチャの設定と確認	イーサネット1/2	102	入力のみ	ホスト192.0.2.100からホスト198.51.100.100へのICMPエコー要求
インターフェイス Portchannel1で、メン	Ethernet1/4 Ethernet1/5	1001	入力のみ	ホスト192.0.2.100からホスト198.51.100.100へのICMPエコー

バックプレーンインターフェイス Ethernet1/4および Ethernet1/5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			要求
---	--	--	----

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

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には、FCMとCLIを使用します。

トポロジ、パケットフロー、およびキャプチャポイント

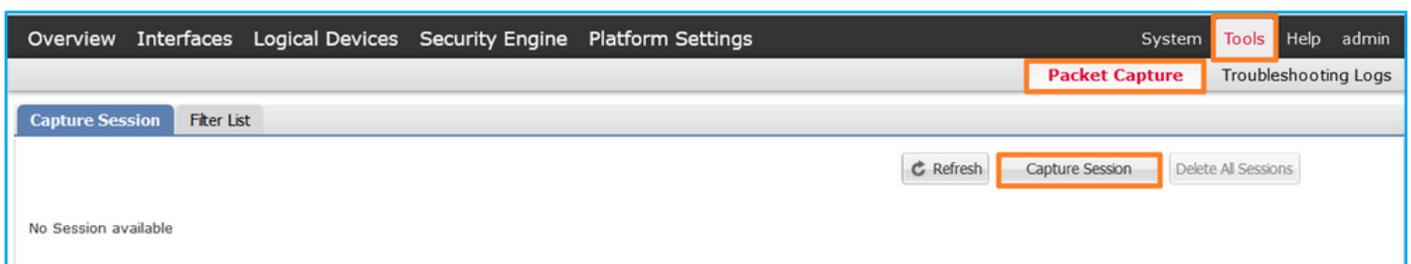


コンフィギュレーション

FCM (必須)

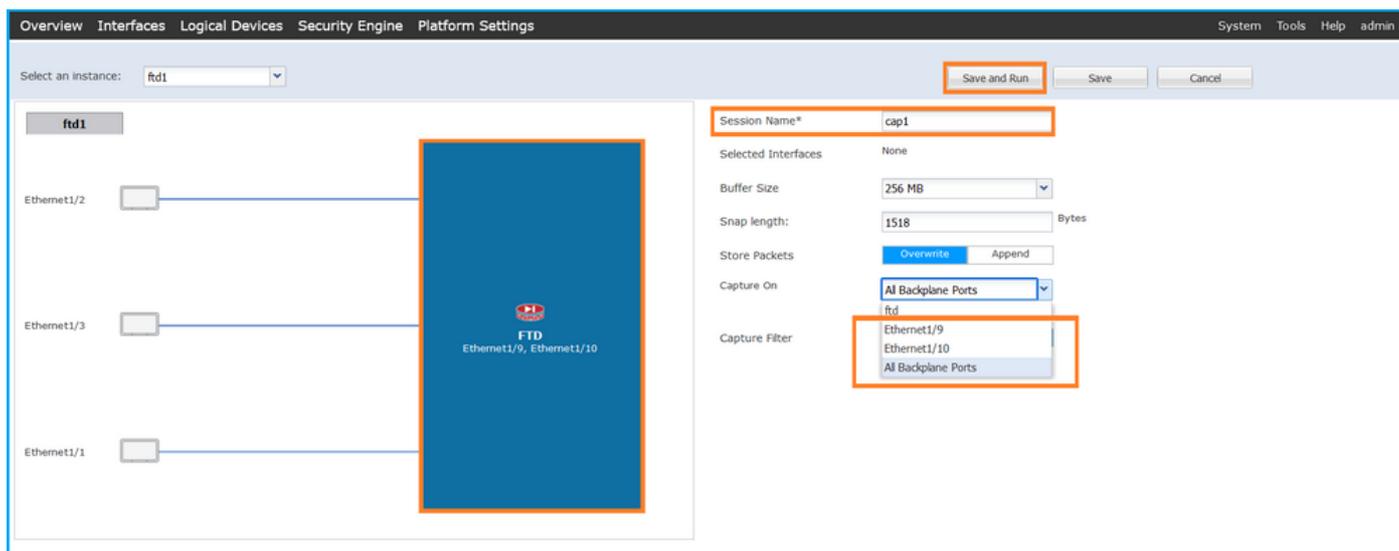
バックプレーンインターフェイスでパケットキャプチャを設定するには、FCMで次の手順を実行します。

1. Tools > Packet Capture > Capture Sessionの順に選択して、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、ドロップダウンリストでCapture Onを選択し、アプリケーション、All Backplane Portsの順に選択します。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

ンインターフェイスEthernet1/9とEthernet1/10が使用できます。セッション名を入力し、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の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IDを識別します。

```
<#root>
```

```
firepower#
```

```
scope ssa
```

```
firepower /ssa#
```

```
show app-instance
```

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

2. キャプチャセッションを作成します。

```
<#root>
```

```
firepower#
```

```
scope packet-capture
```

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

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

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

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

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

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

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

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

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

firepower /packet-capture/session* #
enable

firepower /packet-capture/session* #
commit

firepower /packet-capture/session #
```

検証

FCM (必須)

Interface Nameを確認し、Operational Statusがupであること、File Size (バイト単位) 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のCLI

scope packet-captureでキャプチャの詳細を確認します。

```
<#root>
```

```
firepower#
```

```
scope packet-capture
```

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

```
show session cap1
```

Traffic Monitoring Session:

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

```
Session: 1
```

```
Admin State: Enabled
```

```
Oper State: Up
```

```
Oper State Reason: Active
```

```
Config Success: Yes
```

```
Config Fail Reason:
```

```
Append Flag: Overwrite
```

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

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

```
Error Code: 0
```

```
Drop Count: 0
```

Physical ports involved in Packet Capture:

```
slot Id: 1
```

```
Port Id: 10
```

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

Pcapsize: 1017424 bytes

Filter:
Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

Slot Id: 1

Port Id: 9

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

Pcapsize: 1557432 bytes

Filter:
Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

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」セクションの手順を実行します。

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て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	0xc2c2 (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 2)
4	2022-07-14 20:20:36.514119312	198.51.100.100	192.0.2.100	ICMP	108	0xc2c2 (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64


```

> Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
> Ethernet II, Src: Cisco b9:77:2d (58:97:bd:b9:77:2d), Dst: VMware 9d:e7:50 (00:50:56:9d:e7:50)
  0000  00 50 56 9d e7 50 58 97 bd b9 77 2d 89 26 00 00  |PV..PX. .w.-&.
  0010  00 0a 81 00 00 67 08 00 45 00 00 54 59 90 40 00  |.....g..E..TY.@
  0020  40 01 f4 1c c0 00 02 64 c6 33 64 64 08 00 22 68  |@....d..3dd..h
  0030  00 01 00 0f 89 7a d0 62 00 00 00 00 b3 d7 09 00  |.....z-b.....
  0040  00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b  |.....!*" $%&'()*+
  0050  1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b  |
  0060  2c 2d 2e 2f 30 31 32 33 34 35 36 37  |,./:0123 4567
  
```



```

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



```

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 103
  000. .... = Priority: Best Effort (default) (0)
  ...0 .. = DEI: Ineligible
  ... 0000 0110 0111 = ID: 103
  Type: IPv4 (0x0800)
  
```



```

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

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エコー応答がキャプチャされて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。

説明

バックプレーンインターフェイスの packets キャプチャが設定されると、スイッチは各パケットを2回ずつ同時にキャプチャします。この場合、内部スイッチは、ポートVLANタグとVNタグを持つ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ているパケットを受信します。VLANタグは、内部シャーシがネットワークにパケットを転送するために使用する出カインターフェイスを識別します。ICMPエコー要求パケット内のVLANタグ103はEthernet1/3を出カインターフェイスとして識別し、ICMPエコー応答パケット内のVLANタグ102はEthernet1/2を出カ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の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 エコー要求 ホスト 198.51.100.100 から ホスト 192.0.2.100 への ICMP エコー応答

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で設定され、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でも設定されます。

主に2つの使用例があります。

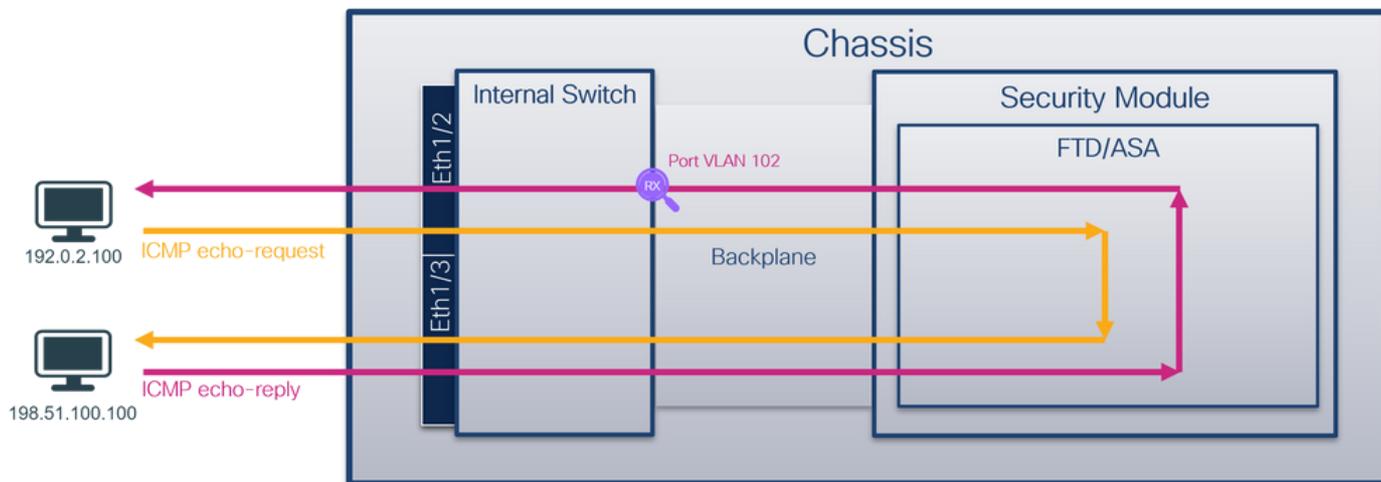
- 特定の前面インターフェイスから発信されるパケットのパケットキャプチャをバックプレーンインターフェイスで設定します。たとえば、インターフェイスEthernet1/2から送信されるパケットのパケットキャプチャをバックプレーンインターフェイスEthernet1/9で設定します。
- 特定の前面インターフェイスとバックプレーンインターフェイスで同時パケットキャプチャを設定します。たとえば、インターフェイスEthernet1/2から出るパケットに対して、インターフェイスEthernet1/2とバックプレーンインターフェイスEthernet1/9で同時パケットキャプチャを設定します。

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

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には、FCMとCLIを使用します。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



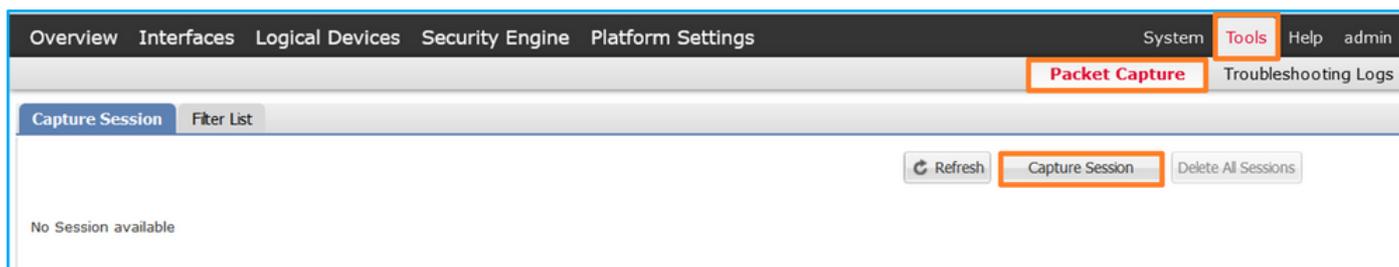
コンフィギュレーション

FCM (必須)

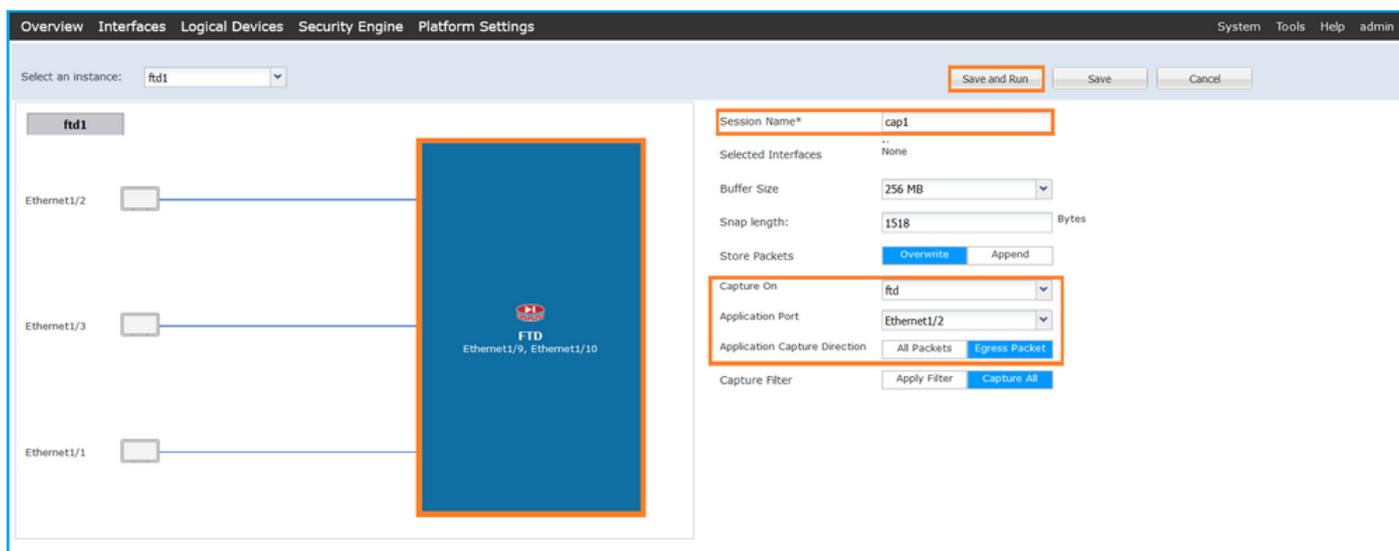
FTDアプリケーションおよびアプリケーションポートEthernet1/2でパケットキャプチャを設定するには、FCMで次の手順を実行します。

1. Tools > Packet Capture > Capture Sessionの順に選択して、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。セッション名を入力し、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の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IDを識別します。

```
<#root>
```

```
firepower#
```

```
scope ssa
```

```
firepower /ssa#
```

```
show app-instance
```

```
App Name   Identifier Slot ID   Admin State Oper State   Running Version Startup Version Deploy Ty
-----
```

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

2. キャプチャセッションを作成します。

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

firepower /packet-capture #
create session cap1

firepower /packet-capture/session* #
create app-port 1 112 Ethernet1/2 ftd

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

firepower /packet-capture/session/app-port* #
set filter ""

firepower /packet-capture/session/app-port* #
set subinterface 0

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

firepower /packet-capture/session* #
commit

firepower /packet-capture/session #
```

検証

FCM (必須)

Interface Nameを確認し、Operational Statusがupであること、File Size (バイト単位) 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のCLI

scope packet-captureでキャプチャの詳細を確認します。

```
<#root>
```

```
firepower#
```

```
scope packet-capture
```

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

```
show session cap1
```

Traffic Monitoring Session:

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

```
Session: 1
```

```
Admin State: Enabled
```

```
Oper State: Up
```

```
Oper State Reason: Active
```

```
Config Success: Yes
```

```
Config Fail Reason:
```

```
Append Flag: Overwrite
```

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

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

```
Error Code: 0
```

```
Drop Count: 0
```

Application ports involved in Packet Capture:

```
Slot Id: 1
```

```
Link Name: 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」セクションの手順を実行します。

。

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エコー応答がキャプチャされて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。

The screenshot displays a network capture analysis tool interface. The top section shows a list of captured packets. The second packet is highlighted, and its details are expanded in the bottom section. The packet list shows ICMP Echo (ping) replies from 198.51.100.100 to 192.0.2.100. The detailed view of the second packet shows the following headers:

- VLAN-Tag: Direction: To Bridge, Pointer: vif_id, 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. Priority: Best Effort (default) (0), DEI: Ineligible, ID: 102. Type: IPv4 (0x0800).
- Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100.
- Internet Control Message Protocol.

The packet data section shows the raw bytes of the packet, including the Ethernet II header, the 802.1Q VLAN tag, and the ICMP Echo (ping) reply data.

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をEgressに設定すると、イーサネットヘッダー内のポートVLANタグ102を持つパケットが、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エコー応答

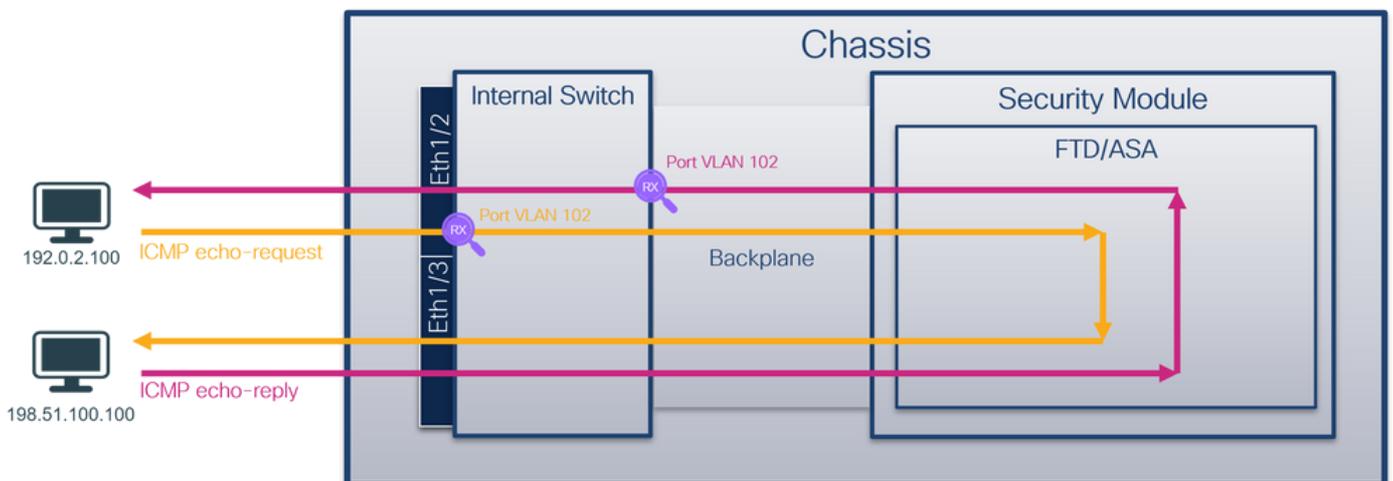
タスク 2

FCMおよびCLIを使用して、バックプレーンインターフェイスおよび前面インターフェイスEthernet1/2のパケットキャプチャを設定および確認します。

同時パケットキャプチャは次のように設定されます。

- 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を持つパケットがキャプチャされます。キャプチャされたパケットは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が出カインターフェイスとして識別されるパケット、またはポートがVLAN 102のパケットがキャプチャされます。キャプチャされたパケットは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

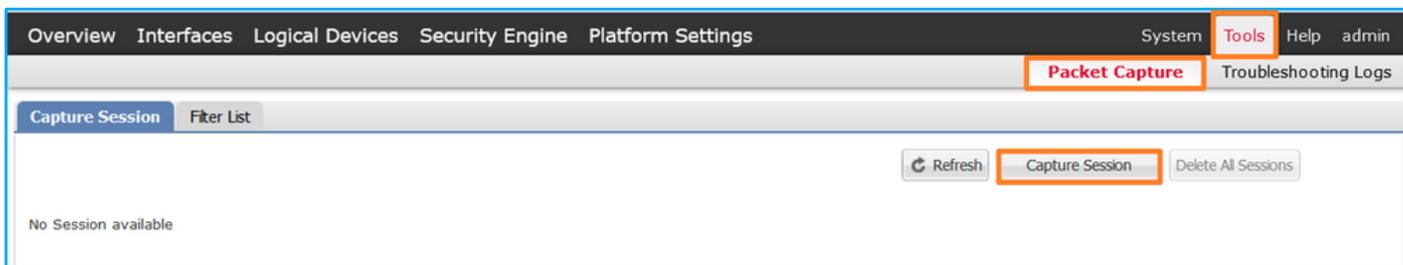


コンフィギュレーション

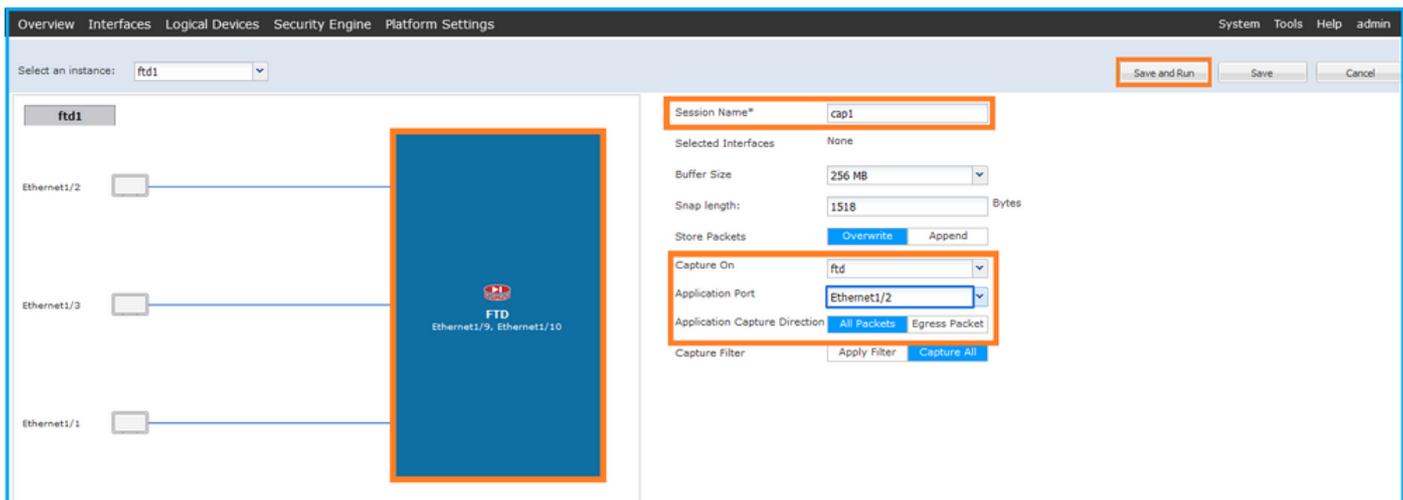
FCM (必須)

FTD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の順に選択して、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。セッション名を入力し、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の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IDを識別します。

```
<#root>
```

```
firepower#
```

```
scope ssa
```

```
firepower /ssa#
```

```
show app-instance
```

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

2. キャプチャセッションを作成します。

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

firepower /packet-capture #
create session cap1

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

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

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

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

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

firepower /packet-capture/session* #
enable

firepower /packet-capture/session* #
commit

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

検証

FCM (必須)

Interface Nameを確認し、Operational Statusがupであること、File Size (バイト単位) 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.pcap	fd1
Ethernet1/2 - Ethernet1/10	None	368	cap1-vethernet-1175.pcap	fd1
Ethernet1/2 - Ethernet1/9	None	13040	cap1-vethernet-1036.pcap	fd1

FXOSのCLI

scope packet-captureでキャプチャの詳細を確認します。

```
<#root>
```

```
firepower#
```

```
scope packet-capture
```

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

```
show session cap1
```

Traffic Monitoring Session:

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

```
Session: 1
```

```
Admin State: Enabled
```

```
Oper State: Up
```

```
Oper State Reason: Active
```

```
Config Success: Yes
```

```
Config Fail Reason:
```

```
Append Flag: Overwrite
```

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

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

```
Error Code: 0
```

```
Drop Count: 0
```

Physical ports involved in Packet Capture:

```
Slot Id: 1
```

```
Port Id: 2
```

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

Pcapsize: 410444 bytes

Filter:

Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

Application ports involved in Packet Capture:

Slot Id: 1

Link Name: link12

Port Name: Ethernet1/2

App Name: ftd

Sub Interface: 0

Application Instance Identifier: ftd1

Application ports resolved to:

Name: vnic1

Eq Slot Id: 1

Eq Port Id: 9

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

Pcapsize: 128400 bytes

Vlan: 102

Filter:

Name: vnic2

Eq Slot Id: 1

Eq Port Id: 10

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

Pcapsize: 2656 bytes

Vlan: 102

Filter:

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」セクションの手順を実行します。

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2回取得されて表示されます。
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 11:33:19.070693081	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 11:33:19.070693347	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 11:33:21.073268327	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 11:33:23.075781513	192.0.2.100	198.51.100.100	ICMP	102	0xc208 (49672)	64	Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found!)
13	2022-08-01 11:33:24.081839490	192.0.2.100	198.51.100.100	ICMP	108	0xc211 (49681)	64	Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found!)
14	2022-08-01 11:33:24.081841386	192.0.2.100	198.51.100.100	ICMP	102	0xc211 (49681)	64	Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found!)
15	2022-08-01 11:33:25.105806249	192.0.2.100	198.51.100.100	ICMP	108	0xc2e2 (49890)	64	Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found!)
16	2022-08-01 11:33:25.105807895	192.0.2.100	198.51.100.100	ICMP	102	0xc2e2 (49890)	64	Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found!)
17	2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	ICMP	108	0xc3b4 (50100)	64	Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found!)
18	2022-08-01 11:33:26.129838114	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100)	64	Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found!)
19	2022-08-01 11:33:27.153828653	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found!)
20	2022-08-01 11:33:27.153830201	192.0.2.100	198.51.100.100	ICMP	102	0xc476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found!)
21	2022-08-01 11:33:28.17847175	192.0.2.100	198.51.100.100	ICMP	108	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found!)
22	2022-08-01 11:33:28.17849075	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found!)
23	2022-08-01 11:33:29.201804760	192.0.2.100	198.51.100.100	ICMP	108	0xc578 (50552)	64	Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found!)
24	2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	102	0xc578 (50552)	64	Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found!)
25	2022-08-01 11:33:30.225834765	192.0.2.100	198.51.100.100	ICMP	108	0xc585 (50565)	64	Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found!)
26	2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (50565)	64	Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found!)
27	2022-08-01 11:33:31.249828955	192.0.2.100	198.51.100.100	ICMP	108	0xc618 (50712)	64	Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found!)
28	2022-08-01 11:33:31.249831121	192.0.2.100	198.51.100.100	ICMP	102	0xc618 (50712)	64	Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found!)
29	2022-08-01 11:33:32.273867960	192.0.2.100	198.51.100.100	ICMP	108	0xc64f (50767)	64	Echo (ping) request id=0x0013, seq=14/3584, ttl=64 (no response found!)

```

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

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2回取得されて表示されます。
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を識別する追加のポート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 11:33:19.070693347	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 11:33:21.073268327	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 11:33:23.075781513	192.0.2.100	198.51.100.100	ICMP	102	0xc208 (49672)	64	Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found!)
13	2022-08-01 11:33:24.081839490	192.0.2.100	198.51.100.100	ICMP	108	0xc211 (49681)	64	Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found!)
14	2022-08-01 11:33:24.081841386	192.0.2.100	198.51.100.100	ICMP	102	0xc211 (49681)	64	Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found!)
15	2022-08-01 11:33:25.105806249	192.0.2.100	198.51.100.100	ICMP	108	0xc2e2 (49890)	64	Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found!)
16	2022-08-01 11:33:25.105807895	192.0.2.100	198.51.100.100	ICMP	102	0xc2e2 (49890)	64	Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found!)
17	2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	ICMP	108	0xc3b4 (50100)	64	Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found!)
18	2022-08-01 11:33:26.129838114	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100)	64	Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found!)
19	2022-08-01 11:33:27.153828653	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found!)
20	2022-08-01 11:33:27.153830201	192.0.2.100	198.51.100.100	ICMP	102	0xc476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found!)
21	2022-08-01 11:33:28.17847175	192.0.2.100	198.51.100.100	ICMP	108	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found!)
22	2022-08-01 11:33:28.17849075	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found!)
23	2022-08-01 11:33:29.201804760	192.0.2.100	198.51.100.100	ICMP	108	0xc578 (50552)	64	Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found!)
24	2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	102	0xc578 (50552)	64	Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found!)
25	2022-08-01 11:33:30.225834765	192.0.2.100	198.51.100.100	ICMP	108	0xc585 (50565)	64	Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found!)
26	2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (50565)	64	Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found!)
27	2022-08-01 11:33:31.249828955	192.0.2.100	198.51.100.100	ICMP	108	0xc618 (50712)	64	Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found!)
28	2022-08-01 11:33:31.249831121	192.0.2.100	198.51.100.100	ICMP	102	0xc618 (50712)	64	Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found!)
29	2022-08-01 11:33:32.273867960	192.0.2.100	198.51.100.100	ICMP	108	0xc64f (50767)	64	Echo (ping) request id=0x0013, seq=14/3584, ttl=64 (no response found!)

```

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

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てキーポイントを確認します。

1. 各ICMPエコー応答がキャプチャされて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	TTL	Info
1	2022-08-01 11:33:19.071512698	198.51.100.100	192.0.2.100	ICMP	108	0x4f2f (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	0x4f2f (20263)	64	Echo (ping) reply id=0x0013, seq=1/256, ttl=64
3	2022-08-01 11:33:20.072677382	198.51.100.100	192.0.2.100	ICMP	108	0x4f10 (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 11:33:29.202398869	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 11:33:29.202398867	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 11:33:30.226401817	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 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
> Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VMware 9d:e8:be (00:50:56:9d:e8:be)
  > VN-Tag
    0... .. = Direction: To Bridge
    .0... .. = Pointer: vif_id
    ..00 0000 0000 0000 .. = Destination: 0
    .. .. .. .. = Looped: No
    .. .. .. .. = Reserved: 0
    .. .. .. .. = Version: 0
    .. .. .. .. 0000 0000 1010 = Source: 10
    Type: 802.1Q Virtual LAN (0x8100)
  > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
    000... .. = Priority: Best Effort (default) (0)
    ...0 .. .. = DEI: Ineligible
    ... 0000 0110 0110 = ID: 102
    Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100
  > Internet Control Message Protocol
  
```

説明

All Packets in the Application Capture Direction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 (前面インターフェイスEthernet1/2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のキャプチャ) が設定されます。

前面インターフェイスの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。

動作の順序では、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先に示されます。この例では、ICMPエコー要求パケット内の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の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2回ずつ同時にキャプチャします。内部スイッチは、ポートVLANタグとVNタグを持つ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ているパケットを受信します。ポートVLANタグは、内部シャーシがネットワークにパケットを転送するために使用する出力

インターフェイスを識別します。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、出カインターフェイスとしてEthernet1/2が識別されます。

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のVLANタグを削除します。

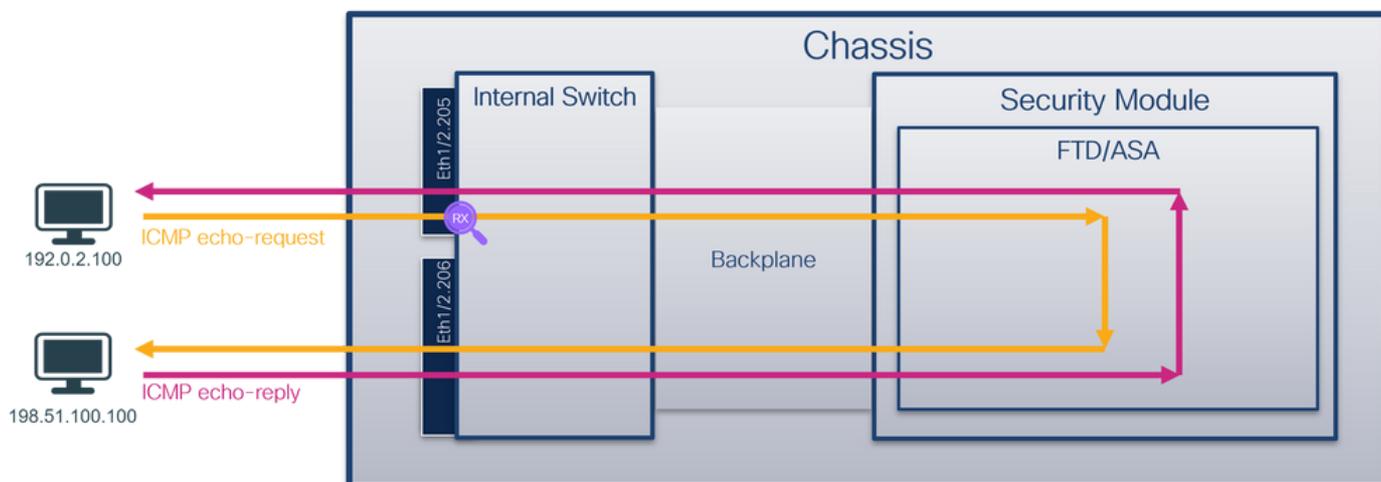
タスクの要約を次の表に示します。

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
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エコー応答
	インターフェイス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エコー要求

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上のサブインターフェイスとキャプチャは、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。この例では、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

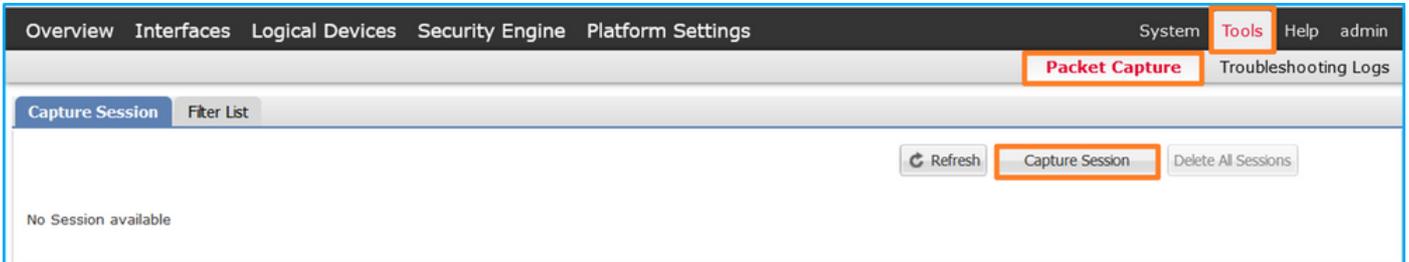


コンフィギュレーション

FCM (必須)

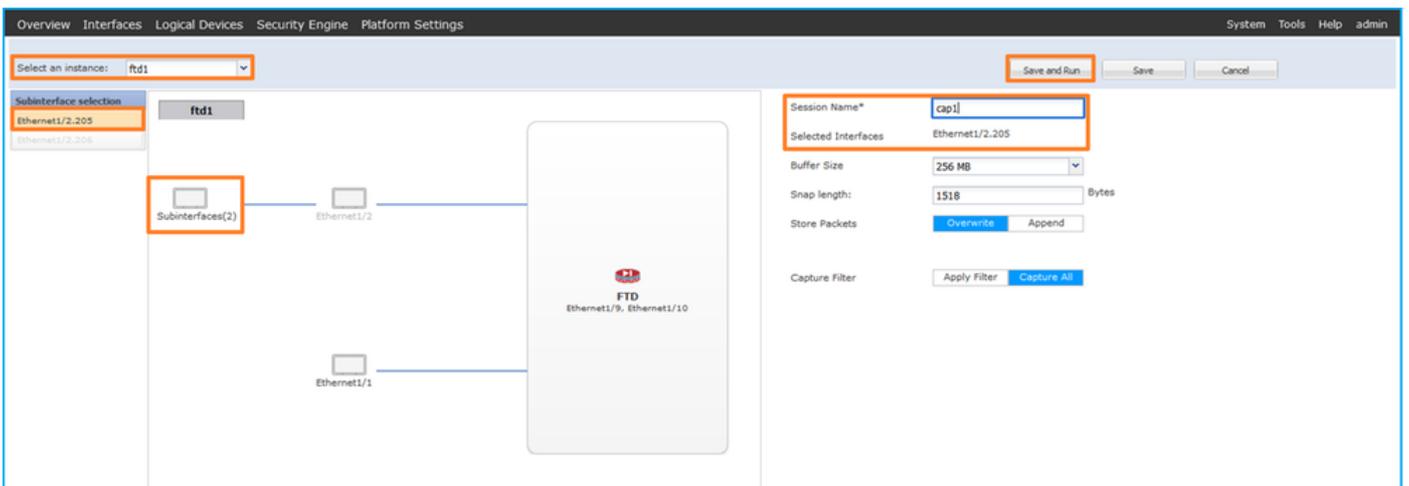
FTDアプリケーションおよびアプリケーションポートEthernet1/2でパケットキャプチャを設定するには、FCMで次の手順を実行します。

1. Tools > Packet Capture > Capture Sessionの順に選択して、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を選択してセッション名を指定し、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

o



3. ポートチャンネルサブインターフェイスの場合は、Cisco Bug ID [CSCvq33119](#)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、ポートチャン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の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IDを識別します。

```
<#root>
```

```
firepower#
```

```
scope ssa
```

```
firepower /ssa #
show app-instance
```

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

2. ポートチャン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識別します。

```
<#root>
```

```
firepower#
```

```
connect fxos
```

```
<output skipped>
```

```
firepower(fxos)#
```

```
show port-channel summary
```

```
Flags: D - Down          P - Up in port-channel (members)
       I - Individual    H - Hot-standby (LACP only)
       s - Suspended     r - Module-removed
       S - Switched      R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
```

Group	Port-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。

```
<#root>
```

```
firepower#
```

```
scope packet-capture
```

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

```
create session cap1
```

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

```
create phy-port Eth1/2
```

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

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

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

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

firepower /packet-capture/session* #
enable

firepower /packet-capture/session* #
commit

firepower /packet-capture/session #
```

ポートチャンネルサブインターフェイスの場合は、各ポートチャン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。

```
<#root>
```

```
firepower#
scope packet-capture

firepower /packet-capture #
create filter vlan207

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

firepower /packet-capture/filter* #
up

firepower /packet-capture* #
create session cap1

firepower /packet-capture/session*
```

```
create phy-port Eth1/3

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

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

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

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

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

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

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

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

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

firepower /packet-capture/session* #
enable

firepower /packet-capture/session* #
commit

firepower /packet-capture/session #
```

検証

FCM (必須)

Interface Nameを確認し、Operational Statusがupであること、File Size (バイト単位) 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のキャプチャもFCMで表示されますが、次のように編集することはできません。



FXOSのCLI

scope packet-captureでキャプチャの詳細を確認します。

```
<#root>
```

```
firepower#
```

```
scope packet-capture
```

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

```
show session cap1
```

Traffic Monitoring Session:

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

```
Session: 1
```

```
Admin State: Enabled
```

```
Oper State: Up
```

```
Oper State Reason: Active
```

```
Config Success: Yes
```

```
Config Fail Reason:
```

```
Append Flag: Overwrite
```

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

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

```
Error Code: 0
```

Drop Count: 0

Physical ports involved in Packet Capture:

slot Id: 1

Port Id: 2

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

Pcapsize: 9324 bytes

Filter:

Sub Interface: 205

Application Instance Identifier: ftd1

Application Name: ftd

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:

<#root>

firepower#

scope packet-capture

firepower /packet-capture # show session cap1

Traffic Monitoring Session:

Packet Capture Session Name: cap1

Session: 1

Admin State: Enabled

Oper State: Up

Oper State Reason: Active

Config Success: Yes

Config Fail Reason:

Append Flag: Overwrite

Session Mem Usage: 256 MB
Session Pcap Snap Len: 1518 Bytes
Error Code: 0
Drop Count: 0

Physical ports involved in Packet Capture:

slot Id: 1

Port Id: 3

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

Pcapsize: 160 bytes

Filter:

Sub Interface: 207

Application Instance Identifier: ftd1

Application Name: ftd

Slot Id: 1

Port Id: 4

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

Pcapsize: 624160 bytes

Filter:

Sub Interface: 207

Application Instance Identifier: ftd1

Application Name: ftd

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」セクションの手順を実行します。

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2回取得されて表示されます。
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。

The screenshot displays a network traffic capture analysis tool. The top section shows a list of captured packets, with the second packet selected. The packet details are expanded to show the following structure:

- VN-Tag:** Contains fields for Direction, Pointer, Destination, Looped, Reserved, and Version.
- 802.1Q Virtual LAN (802.1Q):** Contains Priority, DEI, and ID (102).
- 802.1Q Virtual LAN (802.1Q):** Contains Priority, DEI, and ID (205).
- Internet Protocol Version 4:** Contains Source and Destination IP addresses (192.0.2.100 and 198.51.100.100).
- Internet Control Message Protocol:** The protocol type for the selected packet.

Red boxes and numbers 1, 2, 3, and 4 are overlaid on the image to highlight these specific components in the packet headers.

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2回取得されて表示されます。
2. 元のパケットヘッダーにはVLANタグ205が付いています。

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-04 07:21:56.993302102	192.0.2.100	198.51.100.100	ICMP	112	0x9574 (38260)	64	Echo (ping) request id=0x0022, seq=1/256, ttl=64 (no response found!)
2	2022-08-04 07:21:56.993303597	192.0.2.100	198.51.100.100	ICMP	102	0x9574 (38260)	64	Echo (ping) request id=0x0022, seq=1/256, ttl=64 (no response found!)
3	2022-08-04 07:22:06.214264777	192.0.2.100	198.51.100.100	ICMP	112	0x9a81 (39533)	64	Echo (ping) request id=0x0022, seq=10/2560, ttl=64 (no response found!)
4	2022-08-04 07:22:06.214267373	192.0.2.100	198.51.100.100	ICMP	102	0x9a81 (39533)	64	Echo (ping) request id=0x0022, seq=10/2560, ttl=64 (no response found!)
5	2022-08-04 07:22:07.215113393	192.0.2.100	198.51.100.100	ICMP	112	0x9a81 (39533)	64	Echo (ping) request id=0x0022, seq=11/2816, ttl=64 (no response found!)
6	2022-08-04 07:22:07.215115445	192.0.2.100	198.51.100.100	ICMP	102	0x9a81 (39533)	64	Echo (ping) request id=0x0022, seq=11/2816, ttl=64 (no response found!)
7	2022-08-04 07:22:08.229938577	192.0.2.100	198.51.100.100	ICMP	112	0x9b33 (39731)	64	Echo (ping) request id=0x0022, seq=12/3072, ttl=64 (no response found!)
8	2022-08-04 07:22:08.229940829	192.0.2.100	198.51.100.100	ICMP	102	0x9b33 (39731)	64	Echo (ping) request id=0x0022, seq=12/3072, ttl=64 (no response found!)
9	2022-08-04 07:22:09.253944601	192.0.2.100	198.51.100.100	ICMP	112	0x9c0e (39950)	64	Echo (ping) request id=0x0022, seq=13/3328, ttl=64 (no response found!)
10	2022-08-04 07:22:09.253946899	192.0.2.100	198.51.100.100	ICMP	102	0x9c0e (39950)	64	Echo (ping) request id=0x0022, seq=13/3328, ttl=64 (no response found!)
11	2022-08-04 07:22:10.277953070	192.0.2.100	198.51.100.100	ICMP	112	0x9c0e (39950)	64	Echo (ping) request id=0x0022, seq=14/3584, ttl=64 (no response found!)
12	2022-08-04 07:22:10.277954736	192.0.2.100	198.51.100.100	ICMP	102	0x9c0e (39950)	64	Echo (ping) request id=0x0022, seq=14/3584, ttl=64 (no response found!)
13	2022-08-04 07:22:11.301931282	192.0.2.100	198.51.100.100	ICMP	112	0x9d84 (40324)	64	Echo (ping) request id=0x0022, seq=15/3840, ttl=64 (no response found!)
14	2022-08-04 07:22:11.301933600	192.0.2.100	198.51.100.100	ICMP	102	0x9d84 (40324)	64	Echo (ping) request id=0x0022, seq=15/3840, ttl=64 (no response found!)
15	2022-08-04 07:22:12.325936521	192.0.2.100	198.51.100.100	ICMP	112	0x9da2 (40354)	64	Echo (ping) request id=0x0022, seq=16/4096, ttl=64 (no response found!)
16	2022-08-04 07:22:12.325937895	192.0.2.100	198.51.100.100	ICMP	102	0x9da2 (40354)	64	Echo (ping) request id=0x0022, seq=16/4096, ttl=64 (no response found!)
17	2022-08-04 07:22:13.326988040	192.0.2.100	198.51.100.100	ICMP	112	0x9e07 (40455)	64	Echo (ping) request id=0x0022, seq=17/4352, ttl=64 (no response found!)
18	2022-08-04 07:22:13.326990258	192.0.2.100	198.51.100.100	ICMP	102	0x9e07 (40455)	64	Echo (ping) request id=0x0022, seq=17/4352, ttl=64 (no response found!)
19	2022-08-04 07:22:14.341944773	192.0.2.100	198.51.100.100	ICMP	112	0x9e6a (40554)	64	Echo (ping) request id=0x0022, seq=18/4608, ttl=64 (no response found!)
20	2022-08-04 07:22:14.341946249	192.0.2.100	198.51.100.100	ICMP	102	0x9e6a (40554)	64	Echo (ping) request id=0x0022, seq=18/4608, ttl=64 (no response found!)
21	2022-08-04 07:22:15.365941588	192.0.2.100	198.51.100.100	ICMP	112	0x9efb (40699)	64	Echo (ping) request id=0x0022, seq=19/4864, ttl=64 (no response found!)
22	2022-08-04 07:22:15.365942566	192.0.2.100	198.51.100.100	ICMP	102	0x9efb (40699)	64	Echo (ping) request id=0x0022, seq=19/4864, ttl=64 (no response found!)
23	2022-08-04 07:22:16.389973843	192.0.2.100	198.51.100.100	ICMP	112	0x9f68 (40936)	64	Echo (ping) request id=0x0022, seq=20/5120, ttl=64 (no response found!)
24	2022-08-04 07:22:16.389975129	192.0.2.100	198.51.100.100	ICMP	102	0x9f68 (40936)	64	Echo (ping) request id=0x0022, seq=20/5120, ttl=64 (no response found!)
25	2022-08-04 07:22:17.413936452	192.0.2.100	198.51.100.100	ICMP	112	0xa079 (41081)	64	Echo (ping) request id=0x0022, seq=21/5376, ttl=64 (no response found!)
26	2022-08-04 07:22:17.413938090	192.0.2.100	198.51.100.100	ICMP	102	0xa079 (41081)	64	Echo (ping) request id=0x0022, seq=21/5376, ttl=64 (no response found!)
27	2022-08-04 07:22:18.437954335	192.0.2.100	198.51.100.100	ICMP	112	0xa11e (41246)	64	Echo (ping) request id=0x0022, seq=22/5632, ttl=64 (no response found!)

Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture_u0_1, id 0
 Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: a2:76:f2:00:00:1b (a2:76:f2:00:00:1b)

```

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 205
000. .... = Priority: Best Effort (default) (0)
...0 .... = DEI: Ineligible
... 0000 1100 1101 = ID: 205
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
Internet Control Message Protocol
  
```

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2回取得されて表示されます。
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、入インターフェイスPortchannel1を識別する追加のポート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。

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-04 08:18:24.572548869	192.168.247.100	192.168.247.102	ICMP	128	0x609e (24734)	255	Echo (ping) request id=0x007b, seq=0/0, ttl=255 (no response found!)
2	2022-08-04 08:18:24.572550073	192.168.247.100	192.168.247.102	ICMP	118	0x609e (24734)	255	Echo (ping) request id=0x007b, seq=0/0, ttl=255 (no response found!)
3	2022-08-04 08:18:24.573286630	192.168.247.100	192.168.247.102	ICMP	128	0x609f (24735)	255	Echo (ping) request id=0x007b, seq=1/256, ttl=255 (no response found!)
4	2022-08-04 08:18:24.573287640	192.168.247.100	192.168.247.102	ICMP	118	0x609f (24735)	255	Echo (ping) request id=0x007b, seq=1/256, ttl=255 (no response found!)
5	2022-08-04 08:18:24.573795748	192.168.247.100	192.168.247.102	ICMP	128	0x60a0 (24736)	255	Echo (ping) request id=0x007b, seq=2/512, ttl=255 (no response found!)
6	2022-08-04 08:18:24.573795748	192.168.247.100	192.168.247.102	ICMP	118	0x60a0 (24736)	255	Echo (ping) request id=0x007b, seq=2/512, ttl=255 (no response found!)
7	2022-08-04 08:18:24.574368638	192.168.247.100	192.168.247.102	ICMP	128	0x60a1 (24737)	255	Echo (ping) request id=0x007b, seq=3/768, ttl=255 (no response found!)
8	2022-08-04 08:18:24.574369574	192.168.247.100	192.168.247.102	ICMP	118	0x60a1 (24737)	255	Echo (ping) request id=0x007b, seq=3/768, ttl=255 (no response found!)
9	2022-08-04 08:18:24.574914512	192.168.247.100	192.168.247.102	ICMP	128	0x60a2 (24738)	255	Echo (ping) request id=0x007b, seq=4/1024, ttl=255 (no response found!)
10	2022-08-04 08:18:24.574914512	192.168.247.100	192.168.247.102	ICMP	118	0x60a2 (24738)	255	Echo (ping) request id=0x007b, seq=4/1024, ttl=255 (no response found!)
11	2022-08-04 08:18:24.575442569	192.168.247.100	192.168.247.102	ICMP	128	0x60a3 (24739)	255	Echo (ping) request id=0x007b, seq=5/1280, ttl=255 (no response found!)
12	2022-08-04 08:18:24.575442569	192.168.247.100	192.168.247.102	ICMP	118	0x60a3 (24739)	255	Echo (ping) request id=0x007b, seq=5/1280, ttl=255 (no response found!)
13	2022-08-04 08:18:24.575918119	192.168.247.100	192.168.247.102	ICMP	128	0x60a4 (24740)	255	Echo (ping) request id=0x007b, seq=6/1536, ttl=255 (no response found!)
14	2022-08-04 08:18:24.575918119	192.168.247.100	192.168.247.102	ICMP	118	0x60a4 (24740)	255	Echo (ping) request id=0x007b, seq=6/1536, ttl=255 (no response found!)
15	2022-08-04 08:18:24.576407671	192.168.247.100	192.168.247.102	ICMP	128	0x60a5 (24741)	255	Echo (ping) request id=0x007b, seq=7/1792, ttl=255 (no response found!)
16	2022-08-04 08:18:24.576408585	192.168.247.100	192.168.247.102	ICMP	118	0x60a5 (24741)	255	Echo (ping) request id=0x007b, seq=7/1792, ttl=255 (no response found!)
17	2022-08-04 08:18:24.576885643	192.168.247.100	192.168.247.102	ICMP	128	0x60a6 (24742)	255	Echo (ping) request id=0x007b, seq=8/2048, ttl=255 (no response found!)
18	2022-08-04 08:18:24.576885643	192.168.247.100	192.168.247.102	ICMP	118	0x60a6 (24742)	255	Echo (ping) request id=0x007b, seq=8/2048, ttl=255 (no response found!)
19	2022-08-04 08:18:24.577394328	192.168.247.100	192.168.247.102	ICMP	128	0x60a7 (24743)	255	Echo (ping) request id=0x007b, seq=9/2304, ttl=255 (no response found!)
20	2022-08-04 08:18:24.577394328	192.168.247.100	192.168.247.102	ICMP	118	0x60a7 (24743)	255	Echo (ping) request id=0x007b, seq=9/2304, ttl=255 (no response found!)
21	2022-08-04 08:18:24.577987632	192.168.247.100	192.168.247.102	ICMP	128	0x60a8 (24744)	255	Echo (ping) request id=0x007b, seq=10/2560, ttl=255 (no response found!)
22	2022-08-04 08:18:24.577989290	192.168.247.100	192.168.247.102	ICMP	118	0x60a8 (24744)	255	Echo (ping) request id=0x007b, seq=10/2560, ttl=255 (no response found!)
23	2022-08-04 08:18:24.578448781	192.168.247.100	192.168.247.102	ICMP	128	0x60a9 (24745)	255	Echo (ping) request id=0x007b, seq=11/2816, ttl=255 (no response found!)
24	2022-08-04 08:18:24.578449999	192.168.247.100	192.168.247.102	ICMP	118	0x60a9 (24745)	255	Echo (ping) request id=0x007b, seq=11/2816, ttl=255 (no response found!)
25	2022-08-04 08:18:24.578900043	192.168.247.100	192.168.247.102	ICMP	128	0x60aa (24746)	255	Echo (ping) request id=0x007b, seq=12/3072, ttl=255 (no response found!)
26	2022-08-04 08:18:24.578900897	192.168.247.100	192.168.247.102	ICMP	118	0x60aa (24746)	255	Echo (ping) request id=0x007b, seq=12/3072, ttl=255 (no response found!)
27	2022-08-04 08:18:24.579426962	192.168.247.100	192.168.247.102	ICMP	128	0x60ab (24747)	255	Echo (ping) request id=0x007b, seq=13/3328, ttl=255 (no response found!)

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

```

VN-Tag
1. .... = Direction: From Bridge
..0. .... = Pointer: vif_id
..00 0000 0011 1101 .... = Destination: 61
..... = 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: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 207
000. .... = Priority: Best Effort (default) (0)
...0 .... = DEI: Ineligible
... 0000 1100 1111 = ID: 207
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.247.100, Dst: 192.168.247.102
Internet Control Message Protocol
  
```

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2回取得されて表示されます。
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 screenshot shows a list of 27 ICMP Echo (ping) requests. The first packet is selected, and its details pane is expanded to show the 802.1Q Virtual LAN header. The details pane shows:

- 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 207
- 000. = Priority: Best Effort (default) (0)
- ...0 = DEI: Ineligible
-0000 1100 1111 = ID: 207
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.247.100, Dst: 192.168.247.102
- Internet Control Message Protocol

 The packet bytes pane shows the raw data of the packet, including the Ethernet II header and the ICMP Echo request data.

説明

前面インターフェイスの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。

動作の順序では、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先に示されます。また、サブインターフェイスの場合、キャプチャファイルでは、1秒ごとのパケットにポートVLANタグは含まれません。

タスクの要約を次の表に示します。

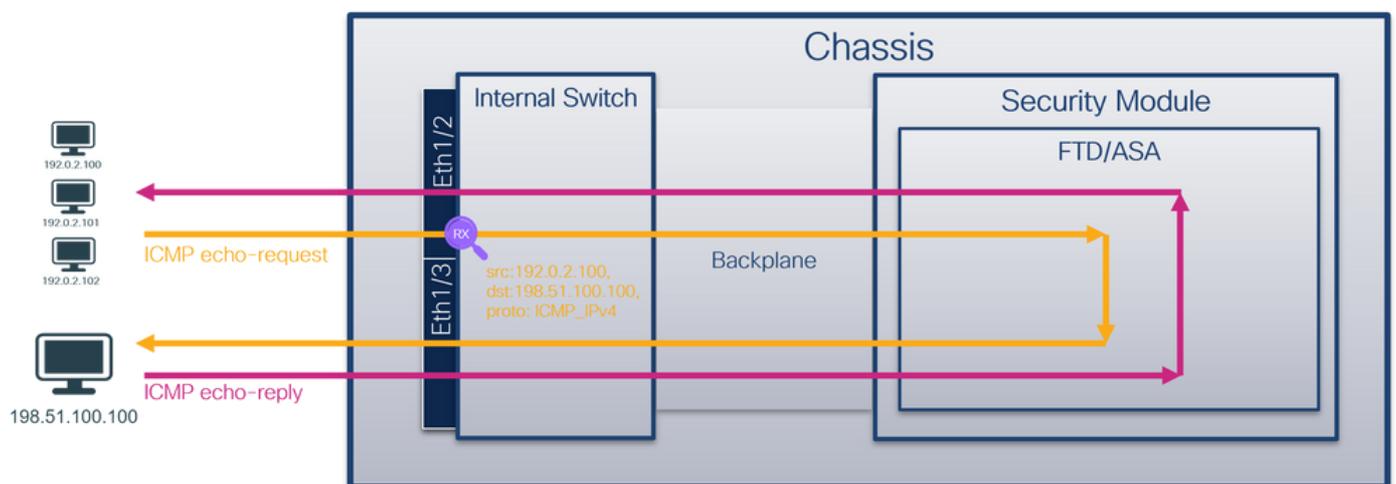
タスク	キャプチャポイント	キャプチャされたパケットの内部ポートVLAN	方向	キャプチャされたトラフィック
サブインターフェイス Ethernet1/2.205でのパケットキャプチャの設定と確認	Ethernet1/2.205	102	入力のみ	ホスト192.0.2.100からホスト198.51.100.100へのICMPエコー要求
メンバーインターフェイス Ethernet1/3および	Ethernet1/3	1001	入力のみ	192.168.207.100からホスト192.168.207.102へのICMPエコー要求

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	イーサネット1/4			一要求
--	-----------	--	--	-----

パケット キャプチャ フィルタ

FCMおよびCLIを使用して、フィルタ付きのインターフェイスEthernet1/2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

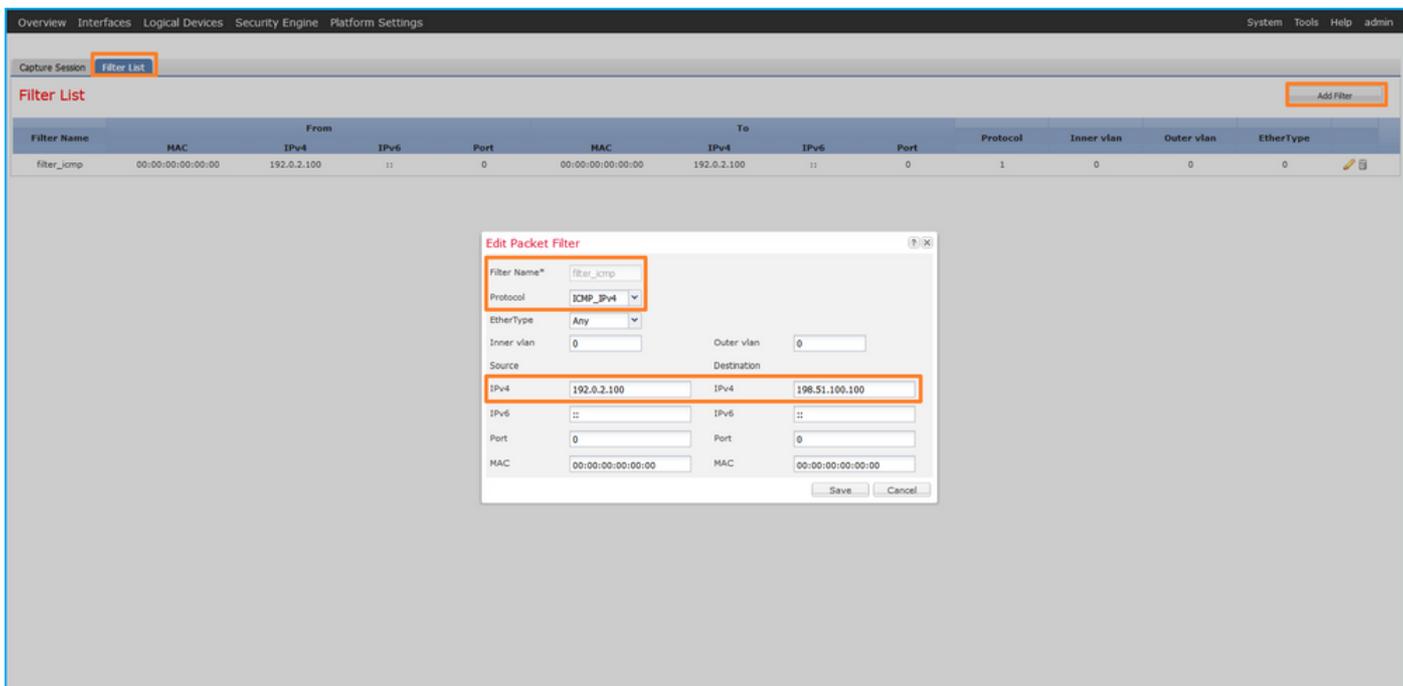


コンフィギュレーション

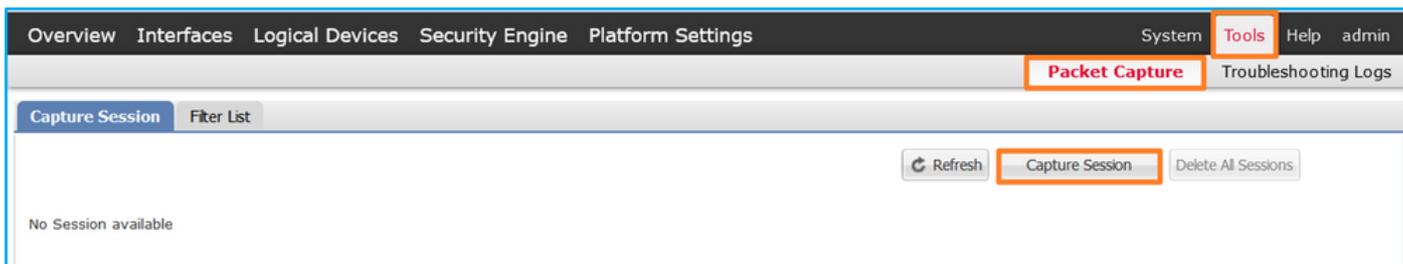
FCM (必須)

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。

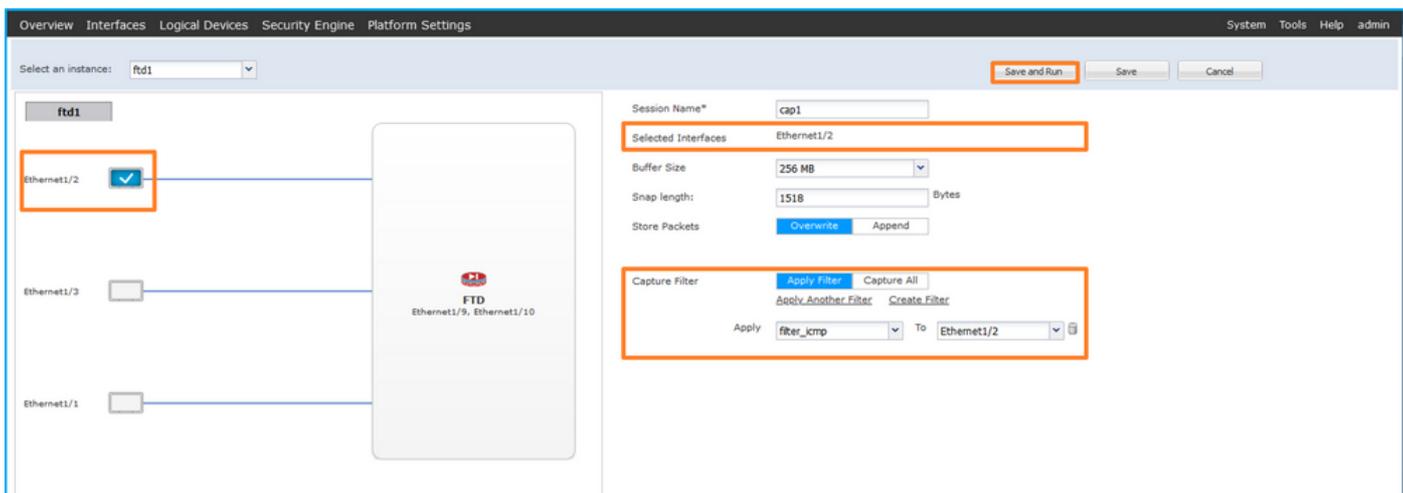
1. キャプチャフィルタを作成するには、Tools > Packet Capture > Filter List > Add Filterの順に選択します。
2. フィルタ名、プロトコル、送信元IPv4、宛先IPv4を指定し、Save:をクリックします。



3. Tools > Packet Capture > Capture Sessionの順に選択して、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、セッション名を指定してキャプチャフィルタを適用し、保存して実行をクリックしてキャプチャをアクティブにします。



FXOSの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IDを識別します。

```
<#root>
```

```
firepower#
```

```
scope ssa
```

```
firepower /ssa#
```

```
show app-instance
```

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

2. <https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>でIPプロトコル番号を識別します。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。

```
<#root>
```

```
firepower#
```

```
scope packet-capture
```

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

```
create filter filter_icmp
```

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

```
set destip 198.51.100.100
```

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

```
set protocol 1
```

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

```
set srcip 192.0.2.100
```

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

```
exit
```

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

```

create session cap1

firepower /packet-capture/session* #
create phy-port Ethernet1/2

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

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

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

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

firepower /packet-capture/session* #
enable

firepower /packet-capture/session* #
commit

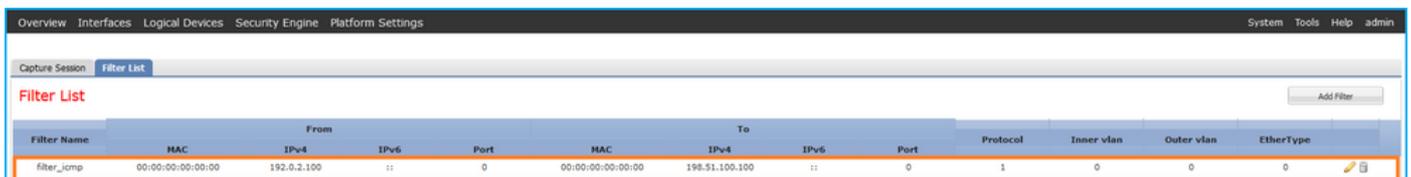
firepower /packet-capture/session #

```

検証

FCM (必須)

Interface Nameを確認し、Operational Statusがupであること、File Size (バイト単位) が増加していることを確認します。



The screenshot shows the 'Filter List' configuration page in the Palo Alto Networks GUI. The table below represents the data shown in the interface.

Filter Name	MAC	From	IPv4	IPv6	Port	MAC	To	IPv4	IPv6	Port	Protocol	Inser 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、Interface Name、Filter、Operational Statusがup、およびFile Size(bytes)の値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	filter_icmp	84340	cap1-ethernet-1-2-0.pcap	fd1

FXOSのCLI

scope packet-captureでキャプチャの詳細を確認します。

```
<#root>
```

```
firepower#
```

```
scope packet-capture
```

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

```
show filter detail
```

Configure a filter for packet capture:

```
Name: filter_icmp
```

```
Protocol: 1
```

```
Ivlan: 0
```

```
Ovlan: 0
```

```
Src Ip: 192.0.2.100
```

```
Dest Ip: 198.51.100.100
```

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

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

```
Src Port: 0
```

```
Dest Port: 0
```

```
Ethertype: 0
```

```
Src Ipv6: ::
```

```
Dest Ipv6: ::
```

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

```
show session cap1
```

Traffic Monitoring Session:

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

```
Session: 1
```

Admin State: Enabled

Oper State: Up

Oper State Reason: Active

Config Success: Yes

Config Fail Reason:

Append Flag: Overwrite

Session Mem Usage: 256 MB

Session Pcap Snap Len: 1518 Bytes

Error Code: 0

Drop Count: 0

Physical ports involved in Packet Capture:

Slot Id: 1

Port Id: 2

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

Pcapsize: 213784 bytes

Filter: filter_icmp

Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

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」セクションの手順を実行します。

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2回取得されて表示され

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。
- 内部スイッチは、追加のVNタグを挿入します。

The image shows a Wireshark packet capture analysis. The top pane displays a list of 20 ICMP Echo (ping) requests. The second packet is highlighted with a red box and a red '1' in the Length column. The bottom pane shows the details of this packet, with several fields highlighted by red boxes and numbered 2, 3, and 4:

- 2**: Internet Control Message Protocol (ICMP) - Echo (ping) request
- 3**: 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
- 4**: VN-Tag

The packet bytes pane shows the raw data for the selected packet, with a red box highlighting the beginning of the packet structure.

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2回取得されて表示されます。
- 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。

説明

前面インターフェイスの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。

動作の順序では、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先に示されます。

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

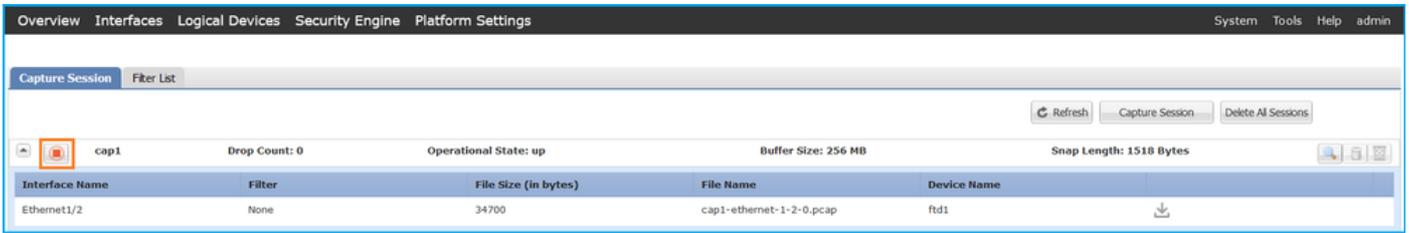
タスク	キャプチャポイント	キャプチャされたパケットの内部ポートVLAN	方向	ユーザフィルタ	キャプチャされたトラフィック
前面インターフェイスEthernet1/2のフィルタを使用したパケットキャプチャの設定と確認	イーサネット1/2	102	入力のみ	プロトコル : ICMP Source:192.0.2.100 Destination:198.51.100.100	ホスト192.0.2.100からホスト198.51.100.100へのICMPエコー要求

Firepower 4100/9300内部スイッチキャプチャファイルの収集

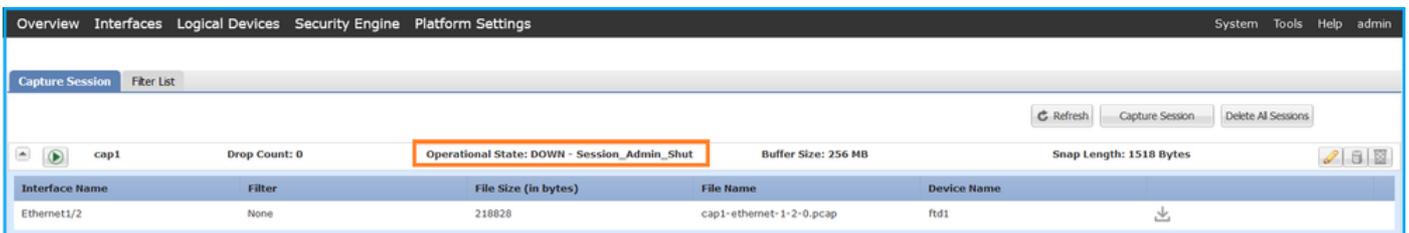
FCM (必須)

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。



ポートチャン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の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。

```
<#root>
```

```
firepower#
```

```
scope packet-capture
```

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

```
scope session cap1
```

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

disable

firepower /packet-capture/session* #

commit

firepower /packet-capture/session #

up

firepower /packet-capture #

show session cap1 detail

Traffic Monitoring Session:

Packet Capture Session Name:

cap1

Session: 1

Admin State: Disabled

Oper State: Down

Oper State Reason: Admin Disable

Config Success: Yes

Config Fail Reason:

Append Flag: Overwrite

Session Mem Usage: 256 MB

Session Pcap Snap Len: 1518 Bytes

Error Code: 0

Drop Count: 0

Physical ports involved in Packet Capture:

Slot Id: 1

Port Id: 2

Pcapfile:

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

Pcapsize: 115744 bytes

Filter:

Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

2. 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。

<#root>

```
firepower#
```

```
connect local-mgmt
```

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

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

```
ftp:          Dest File URI
http:         Dest File URI
https:        Dest File URI
scp:          Dest File URI
sftp:         Dest File URI
tftp:         Dest File URI
usbdrive:     Dest File URI
volatile:     Dest File URI
workspace:    Dest File URI
```

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

```
copy /packet-capture/session-1/cap1-ethernet-1-2-0.pcap ftp://ftuser@10.10.10.1/cap1-ethernet-1-2-0.pcap
```

```
Password:
```

ポートチャン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。

内部スイッチの packets キャプチャに関するガイドライン、制限事項、およびベストプラクティス

Firepower 4100/9300 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 シャーシマネージャ コンフィギュレーションガイド』または『Cisco Firepower 4100/9300 FXOS CLI コンフィギュレーションガイド』の「トラブルシューティング」の章の「パケットキャプチャ」の項を参照してください。

次に、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ン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を分析します。
- キャプチャフィルタを使用します。
- キャプチャフィルタを設定する際は、パケットの 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備えて、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、キャプチャされるパケットの数が増加し、サイズが小さいほどキャプチャされるパケットの数が増加します。
- 必要に応じてバッファサイズを調整します。
- FCM または FXOS CLI のドロップ数に注意してください。バッファサイズの制限に達すると、廃棄カウンターのカウンタが増加します。

- VN-tagのないパケットだけを表示するには、Wiresharkでフィルタ!vntagを使用します。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で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による内部スイッチキャプチャの場合、パケットは誤検出の方法で色付けおよびマーキングされることがあります。パケットキャプチャファイルを分析してフィルタを適用した場合は、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。

セキュアファイアウォール3100/4200の設定と検証

Firepower 4100/9300とは異なり、セキュアファイアウォール3100/4200の内部スイッチのキャプチャは、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)で設定します。switchオプションでは、キャプチャが内部スイッチで設定されるように指定します。

次に、switchオプションを指定したcaptureコマンドの出力を示します。

```
<#root>
```

```
> 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では、入力インターフェイスの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。

```
<#root>
```

```
>
```

```
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
```

セキュアファイアウォール4200は、双方向キャプチャをサポートしています。特に指定のない限り、デフォルト値はingressです。

```
<#root>
```

```
>
```

```
capture capi switch interface inside direction
```

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

さらに、セキュアファイアウォール4245には、2つの内部データと2つの管理アップリンクインターフェイスがあります。

```
<#root>
```

```
>
```

```
capture capsw switch interface
```

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

- 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、次のようにEtherTypeを指定します。

```
<#root>
```

```
>
```

```
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。

```
<#root>
```

```
>
```

```
capture capsw switch interface inside match ?
```

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

4. バッファサイズやパケット長など、その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。no capture <name> switch stop コマンドは、キャプチャをアクティブ化します。

```
<#root>
```

```
>
```

```
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のサイズPcapsizeが増加します。
- show capture <cap_name>の出力でキャプチャされたパケットの数が0以外になっている。
- Pcapfileパスをキャプチャします。キャプチャされたパケットは自動的に/mnt/disk0/packet-capture/フォルダに保存されます。
- 条件の取得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。

```
<#root>
```

```
>
```

```
show capture capsw
```

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

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

```
>
```

```
show capture capsw detail
```

```
Packet Capture info
```

```
Name:                capsw
```

```
Session:             1
```

```
Admin State:        enabled
```

```
Oper State:         up
```

```
Oper State Reason:  Active
```

```
Config Success:     yes
```

```
Config Fail Reason:
```

```
Append Flag:        overwrite
```

```
Session Mem Usage:  256
```

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

```
Error Code:         0
```

```
Drop Count:         0
```

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1
Port Id: 1

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

Pcapsize: 18838

Filter: 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。

<#root>

>

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。「セキュアファイアウォール内部スイッチキャプチャファイルの収集」セクションの手順を実行します。

Secure Firewallソフトウェアバージョン7.4では、内部スイッチキャプチャ設定は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。

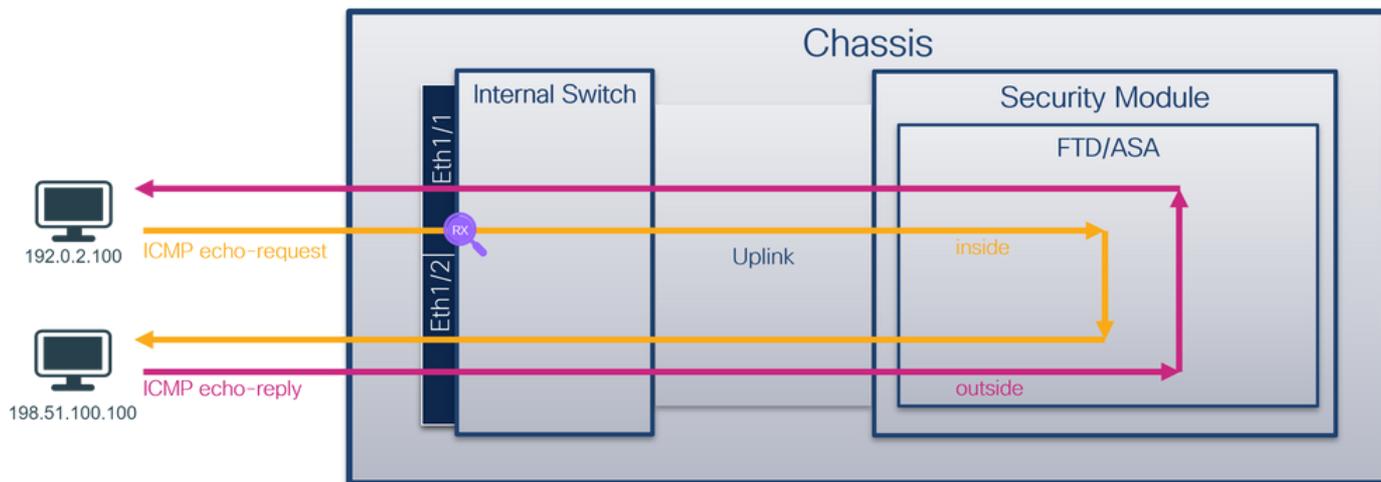
これらのシナリオでは、Secure Firewall 3100/4200内部スイッチのキャプチャの一般的な使用例を取り上げています。

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

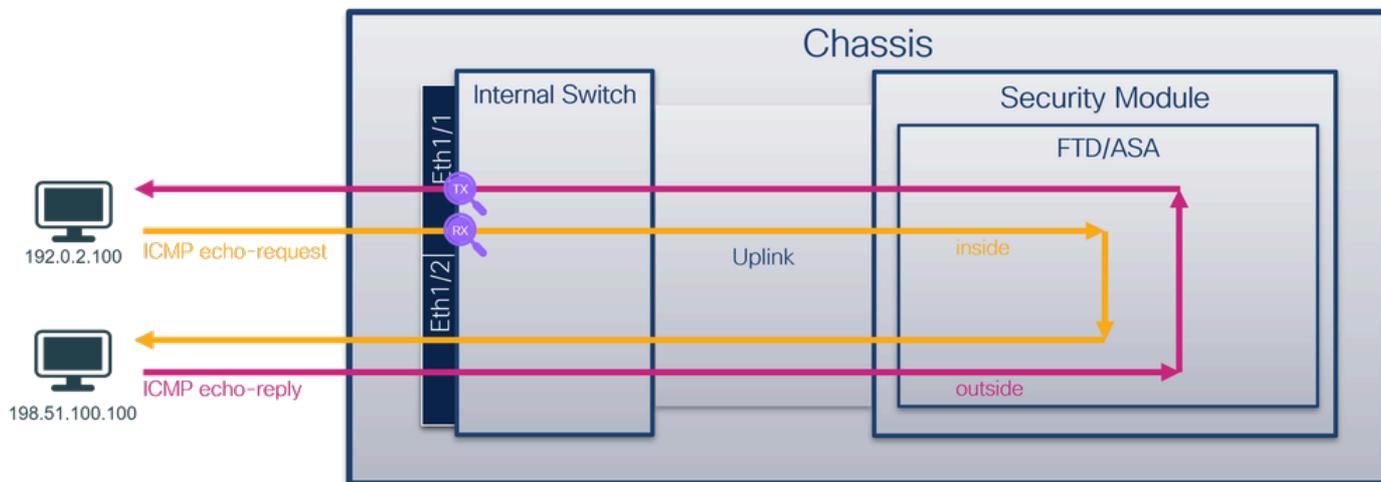
FTDまたはASA CLIを使用して、インターフェイスEthernet1/1またはPortchannel1インターフェイスのパケットキャプチャを設定および確認します。どちらのインターフェイスもnameifはinsideです。

トポロジ、パケットフロー、およびキャプチャポイント

Cisco Secure Firewall 3100:



双方向キャプチャを使用するセキュアファイアウォール4200:



コンフィギュレーション

インターフェイスEthernet1/1またはポートチャンネル1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。

```
<#root>
```

```
>
```

```
show nameif
```

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

```
<#root>
```

```
>
```

```
show nameif
```

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

2. キャプチャセッションの作成

```
<#root>
```

```
>
```

```
capture capsw switch interface inside
```

セキュアファイアウォール4200は、キャプチャの方向性をサポートしています。

```
<#root>
```

```
> capture capsw switch interface inside direction ?
```

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

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

3. キャプチャセッションを有効にします。

```
<#root>
```

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

検証

キャプチャセッションの名前、管理ステートと動作ステート、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)が増加していること、および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。

```
<#root>
```

```
>
```

```
show capture capsw detail
```

Packet Capture info

```
Name:                capsw

Session:             1

Admin State:         enabled

Oper State:          up
```

```
Oper State Reason:  Active
```

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

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

Physical port:

```
slot Id:            1

Port Id:            1

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

Pcapsize:           12653

Filter:             capsw-1-1
```

Packet Capture Filter Info

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

Protocol: 0
Vlan: 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

セキュアなファイアウォール4200:

<#root>

>

show cap 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: 0

Direction: both

Drop: disable
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

33 packet captured on disk using switch capture

Reading of capture file from disk is not supported

ポートチャンネル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。

<#root>

>

show capture capsw detail

Packet Capture info

Name: capsw

Session: 1
Admin State: enabled

Oper State: up

Oper State Reason: Active

Config Success: yes

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

Total Physical ports involved in Packet Capture: 2

Physical port:

Slot Id: 1

Port Id: 4

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

Filter: 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。

<#root>

>

connect fxos

...

firewall#

connect local-mgmt

firewall(local-mgmt)#

show portchannel summary

Flags: D - Down P - Up in port-channel (members)
I - Individual H - Hot-standby (LACP only)
s - Suspended r - Module-removed
S - Switched R - Routed
U - Up (port-channel)
M - Not in use. Min-links not met

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

LACP KeepAlive Timer:

```
-----  
Channel PeerKeepAliveTimerFast  
-----  
1      Po1(U)      False
```

Cluster LACP Status:

Channel	ClusterSpanned	ClusterDetach	ClusterUnitID	ClusterSysID	
1	Po1(U)	False	False	0	clust

ASA上の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

「セキュアファイアウォール内部スイッチキャプチャファイルの収集」セクションの手順を実行します。

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、Ethernet1/1のキャプチャファイルを開きます。この例では、Secure Firewall 3100でのパケットキャプチャが分析されます。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。

The screenshot displays a network traffic capture analysis. The top table lists 18 ICMP Echo (ping) requests. The first packet is highlighted with a red box and a '1' in the ID column. Below the table, the packet details for the first packet are shown, with the 'Internet Control Message Protocol' header highlighted by a yellow box and a '2' in the ID column.

No.	Time	Source	Destination	Protocol	Length	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

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 20:41:00.659662	192.0.2.100	198.51.100.100	ICMP	102	0x93f0 (37872)	64	Echo (ping) request id=0x0035, seq=3/768, ttl=64 (no res
4	2022-08-07 20:41:01.659749	192.0.2.100	198.51.100.100	ICMP	102	0x946f (37999)	64	Echo (ping) request id=0x0035, seq=4/1024, ttl=64 (no re
5	2022-08-07 20:41:02.660624	192.0.2.100	198.51.100.100	ICMP	102	0x94a4 (38052)	64	Echo (ping) request id=0x0035, seq=5/1280, ttl=64 (no re
6	2022-08-07 20:41:03.663226	192.0.2.100	198.51.100.100	ICMP	102	0x952d (38189)	64	Echo (ping) request id=0x0035, seq=6/1536, ttl=64 (no re
7	2022-08-07 20:41:04.661262	192.0.2.100	198.51.100.100	ICMP	102	0x958d (38285)	64	Echo (ping) request id=0x0035, seq=7/1792, ttl=64 (no re
8	2022-08-07 20:41:05.665955	192.0.2.100	198.51.100.100	ICMP	102	0x95d8 (38360)	64	Echo (ping) request id=0x0035, seq=8/2048, ttl=64 (no re
9	2022-08-07 20:41:06.666538	192.0.2.100	198.51.100.100	ICMP	102	0x964b (38475)	64	Echo (ping) request id=0x0035, seq=9/2304, ttl=64 (no re
10	2022-08-07 20:41:07.667298	192.0.2.100	198.51.100.100	ICMP	102	0x972b (38699)	64	Echo (ping) request id=0x0035, seq=10/2560, ttl=64 (no r
11	2022-08-07 20:41:08.670540	192.0.2.100	198.51.100.100	ICMP	102	0x980a (38922)	64	Echo (ping) request id=0x0035, seq=11/2816, ttl=64 (no r
12	2022-08-07 20:41:09.668278	192.0.2.100	198.51.100.100	ICMP	102	0x9831 (38961)	64	Echo (ping) request id=0x0035, seq=12/3072, ttl=64 (no r
13	2022-08-07 20:41:10.672417	192.0.2.100	198.51.100.100	ICMP	102	0x98a2 (39074)	64	Echo (ping) request id=0x0035, seq=13/3328, ttl=64 (no r
14	2022-08-07 20:41:11.671369	192.0.2.100	198.51.100.100	ICMP	102	0x98f7 (39159)	64	Echo (ping) request id=0x0035, seq=14/3584, ttl=64 (no r
15	2022-08-07 20:41:12.675462	192.0.2.100	198.51.100.100	ICMP	102	0x99e4 (39396)	64	Echo (ping) request id=0x0035, seq=15/3840, ttl=64 (no r
16	2022-08-07 20:41:13.674993	192.0.2.100	198.51.100.100	ICMP	102	0x9a84 (39556)	64	Echo (ping) request id=0x0035, seq=16/4096, ttl=64 (no r
17	2022-08-07 20:41:14.674093	192.0.2.100	198.51.100.100	ICMP	102	0x9af3 (39667)	64	Echo (ping) request id=0x0035, seq=17/4352, ttl=64 (no r
18	2022-08-07 20:41:15.676904	192.0.2.100	198.51.100.100	ICMP	102	0x9b8e (39822)	64	Echo (ping) request id=0x0035, seq=18/4608, ttl=64 (no r

> Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)	0000 bc e7 12 34 9a 2c 00 50 56 9d e8 be 08 00 45 00 ...4.,.P V.....E-
> Ethernet II, Src: VMware_9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco_34:9a:2c (bc:e7:12:34:9a:2c)	0010 00 54 92 96 40 00 40 01 bb 16 c0 00 02 64 c6 33 ...T:@:.....d-3
> Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100	0020 64 64 08 00 58 a8 00 35 00 01 4d 23 f0 62 00 00 ...dd.X.5...MM.b...
> Internet Control Message Protocol	0030 00 00 9e c8 04 00 00 00 00 00 10 11 12 13 14 15!"#\$%&'()*+,-./01234567UUUU
	0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25!"#\$%&'()*+,-./01234567UUUU
	0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35!"#\$%&'()*+,-./01234567UUUU
	0060 36 37 55 55 55 55

説明

スイッチのキャプチャは、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の パケットキャプチャの設定と確認	イーサネット1/1	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エコー要求
インターフェイスPortchannel1で、メンバーインターフェイスEthernet1/3および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	Ethernet1/3 イーサネット1/4	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エコー要求

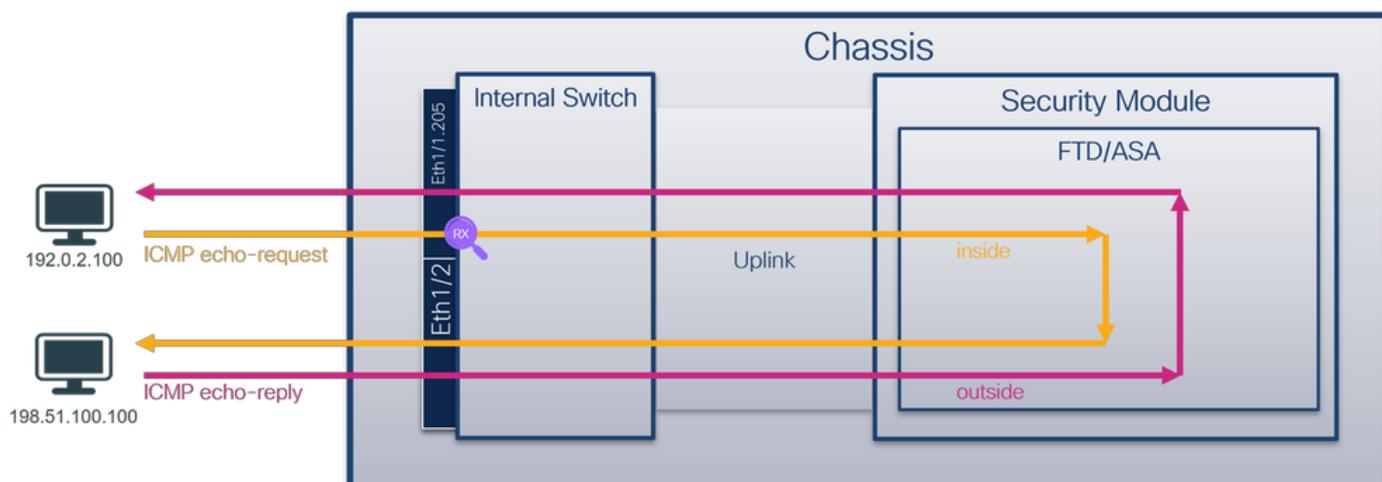
* 3100とは異なり、セキユアファイアウォール4200は双方向（入力および出力）キャプチャをサポートします。

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

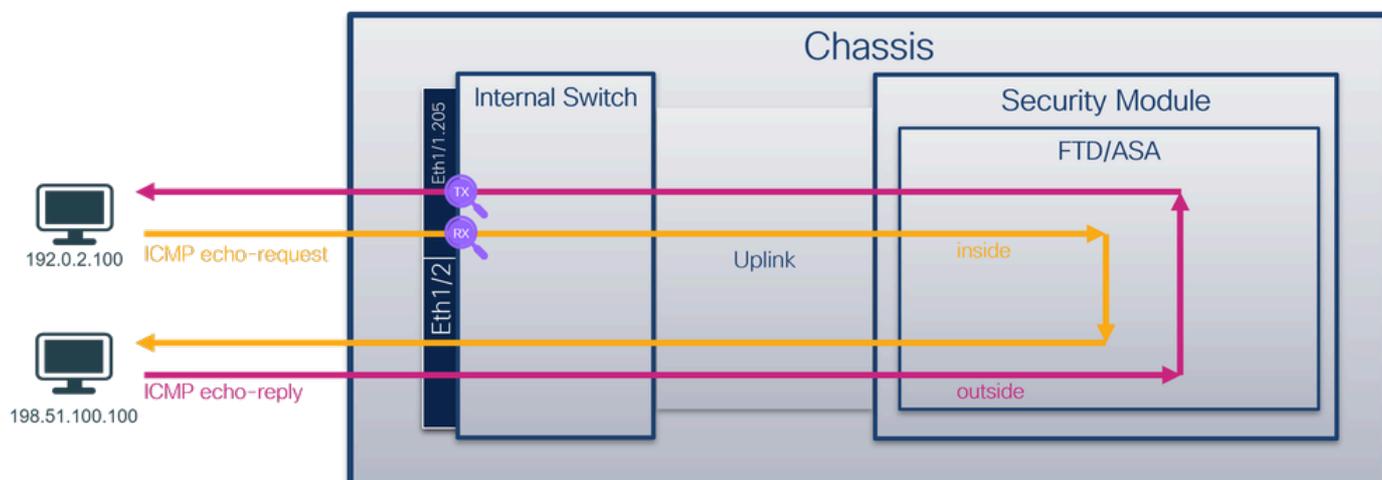
FTDまたはASA CLIを使用して、サブインターフェイスEthernet1/1.205またはPortchannel1.205上のパケットキャプチャを設定および確認します。どちらのサブインターフェイスもnameifはinsideです。

トポロジ、パケットフロー、およびキャプチャポイント

Cisco Secure Firewall 3100:



Cisco Secure Firewall 4200:



コンフィギュレーション

インターフェイスEthernet1/1またはポートチャンネル1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。

```
<#root>
```

```
>
```

```
show nameif
```

Interface	Name	Security
Ethernet1/1.205	inside	0
Ethernet1/2	outside	0

```
Management1/1          diagnostic          0
```

```
<#root>
```

```
>
```

```
show nameif
```

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

2. キャプチャセッションを作成します。

```
<#root>
```

```
>
```

```
capture capsw switch interface inside
```

セキュアファイアウォール4200は、キャプチャの方向性をサポートしています。

```
<#root>
```

```
> capture capsw switch interface inside direction ?
```

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

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

3. キャプチャセッションを有効にします。

```
<#root>
```

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

検証

キャプチャセッションの名前、管理ステートと動作ステート、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)が増加していること、および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。

```
<#root>
```

```
>
```

```
show capture capsw detail
```

```
Packet Capture info
```

```
Name: capsw
```

```
Session: 1
```

```
Admin State: enabled
```

```
Oper State: up
```

```
Oper State Reason: Active
```

```
Config Success: yes
```

```
Config Fail Reason:
```

```
Append Flag: overwrite
```

```
Session Mem Usage: 256
```

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

```
Error Code: 0
```

```
Drop Count: 0
```

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

```
Physical port:
```

```
slot Id: 1
```

```
Port Id: 1
```

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

```
Pcapsize: 6360
```

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

```
Packet Capture Filter Info
```

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

```
Protocol: 0
```

```
Ivlan: 0
```

```
Ovlan: 205
```

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

Total Physical breakout ports involved in Packet Capture: 0

46 packets captured on disk using switch capture

Reading of capture file from disk is not supported

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のキャプチャは、すべてのメンバーインターフェイスで設定されます。

<#root>

>

show capture capsw detail

Packet Capture info

Name: capsw

Session: 1

Admin State: enabled

Oper State: up

Oper State Reason: Active

Config Success: yes

Config Fail Reason:

Append Flag: overwrite

Session Mem Usage: 256

Session Pcap Snap Len: 1518

Error Code: 0

Drop Count: 0

Total Physical ports involved in Packet Capture: 2

Physical port:

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

<#root>

>

connect fxos

...

firewall#

connect local-mgmt

firewall(local-mgmt)#

show portchannel summary

Flags: D - Down P - Up in port-channel (members)
I - Individual H - Hot-standby (LACP only)
s - Suspended r - Module-removed
S - Switched R - Routed
U - Up (port-channel)
M - Not in use. Min-links not met

Group	Port-Channel	Type	Protocol	Member Ports
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上の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、このコマンドを管理コンテキストで実行します。

キャプチャファイルの収集

「セキュアファイアウォール内部スイッチキャプチャファイルの収集」セクションの手順を実行します。

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、Ethernet1/1.205のキャプチャファイルを開きます。この例では、Secure Firewall 3100でのパケットキャプチャが分析されます。最初のパケットを選択し、キーポイントを確認します。

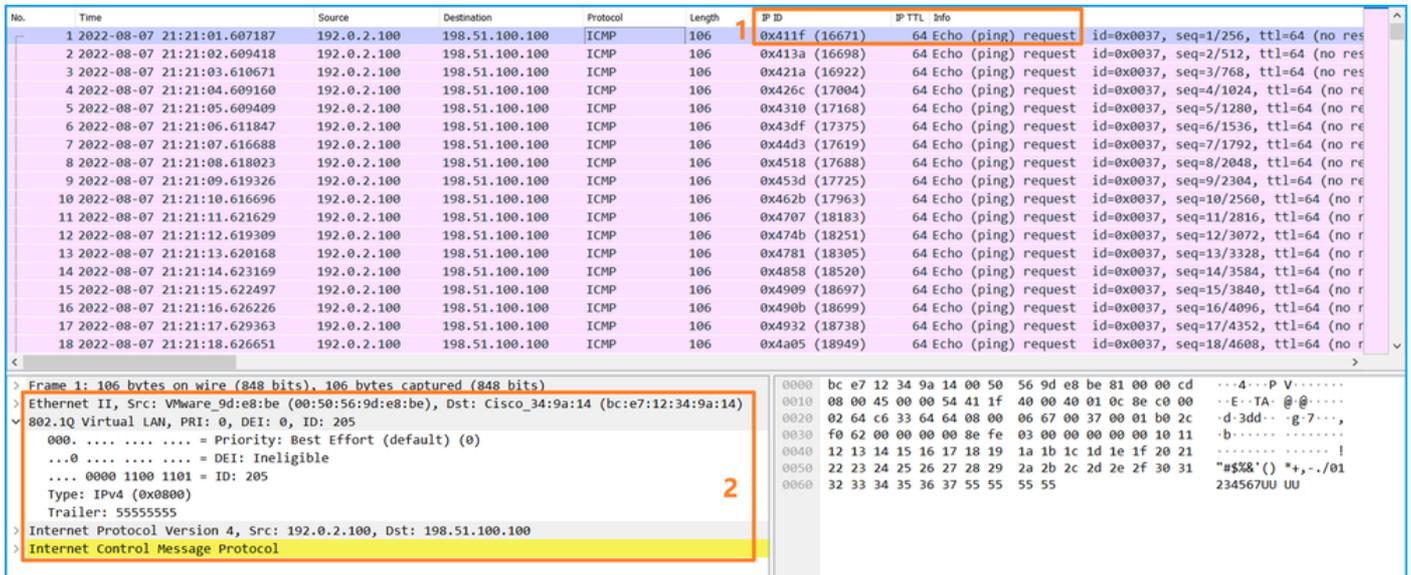
1. ICMPエコー要求パケットだけがキャプチャされます。
2. 元のパケットヘッダーにはVLANタグ205が付いています。

The screenshot displays a network traffic capture analysis tool. The top section shows a list of captured packets. The first packet is highlighted, showing it is an ICMP Echo (ping) request from 192.0.2.100 to 198.51.100.100. The packet length is 106 bytes. The IP ID is 0x411f (16671) and the TTL is 64. The info field indicates it is an Echo (ping) request with id=0x0037, seq=1/256, and ttl=64.

The bottom section shows a detailed view of the first packet's header. The packet is identified as Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits). The Ethernet II header shows the source as VMware_9d:e8:be (00:50:56:9d:e8:be) and the destination as Cisco_34:9a:14 (bc:e7:12:34:9a:14). The 802.1Q Virtual LAN header shows a priority of 0, DEI of 0, and ID of 205. The Internet Protocol Version 4 header shows the source as 192.0.2.100 and the destination as 198.51.100.100. The Internet Control Message Protocol header is also visible.

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205が付いています。



説明

スイッチのキャプチャは、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	イーサネット1/1	外部VLAN 205	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	Ethernet1/3 イーサネット1/4	外部VLAN 205	入力のみ*	ホスト192.0.2.100からホスト198.51.100.100へのICMPエコー要求

* 3100とは異なり、セキュアファイアウォール4200は双方向（入力および出力）キャプチャをサポートします。

内部インターフェイスでのパケットキャプチャ

Secure Firewall 3100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:FMCとFTD間の管理インターフェイスへのSSHなど、またはsftunnelとも呼ばれる管理接続のための専用パケットパスを提供します。

Secure Firewall 4200には、最大4つの内部インターフェイスがあります。

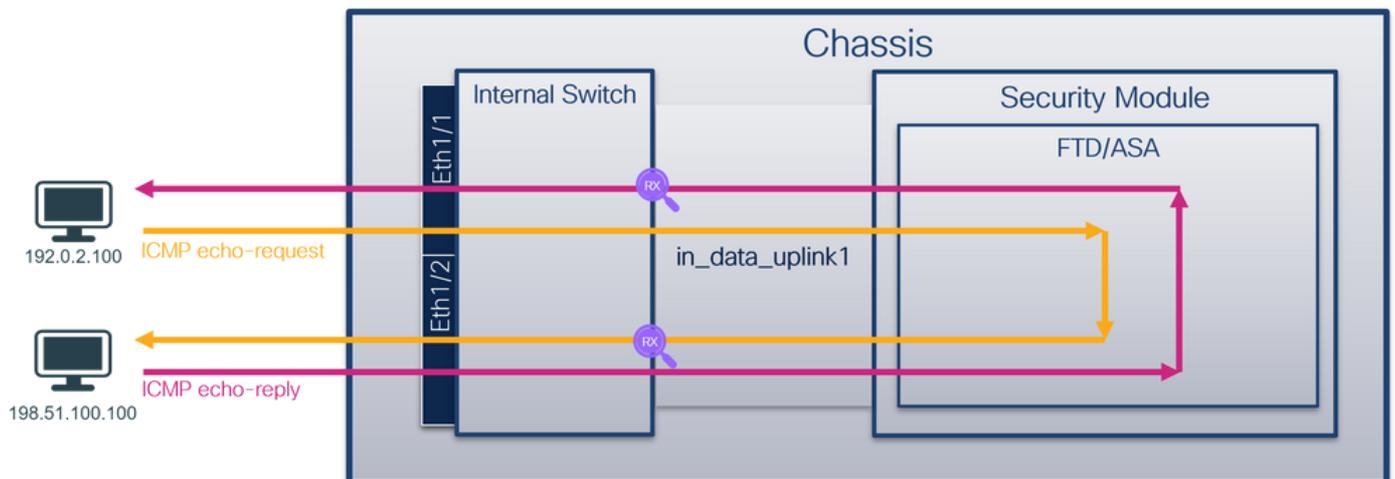
- in_data_uplink1およびin_data_uplink2 (4245のみ) : これらのインターフェイスは、アプリケーションを内部スイッチに接続します。4245の場合、パケットは2つのアップリンクインターフェイス間でロードバランスされます。
- in_mgmt_uplink1およびin_mgmt_uplink2 – これらのインターフェイスは、FMCとFTD間の管理インターフェイス (またはsftunnelとも呼ばれる) へのSSHなどの管理接続のための専用パケットパスを提供します。セキュアファイアウォール4200は、2つの管理インターフェイスをサポートしています。

タスク 1

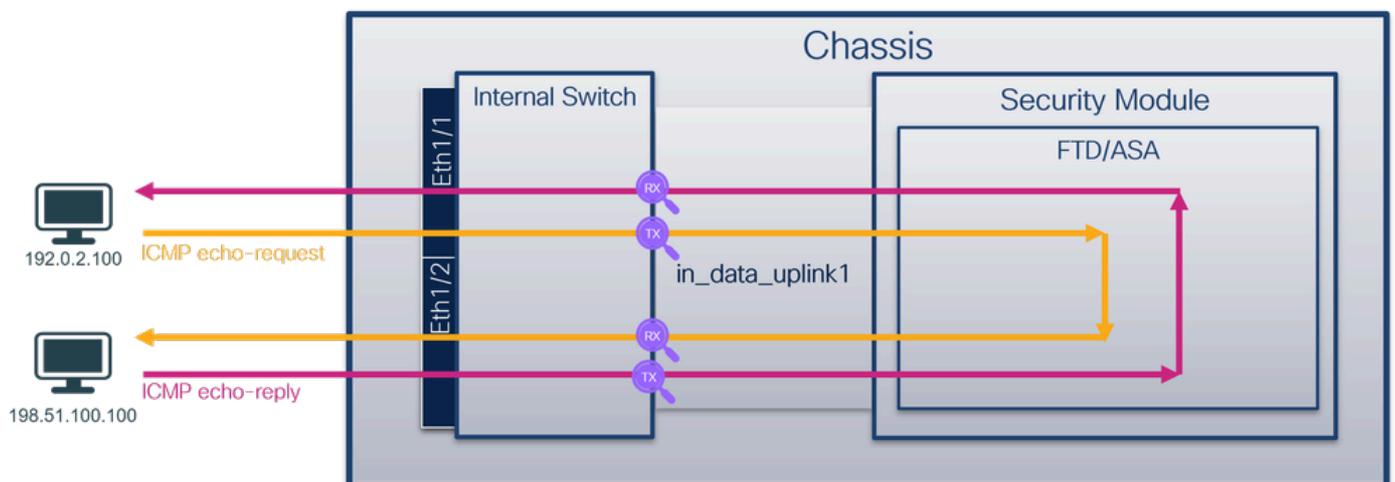
FTDまたはASA CLIを使用して、アップリンクインターフェイスin_data_uplink1上のパケットキャプチャを設定および確認します。

トポロジ、パケットフロー、およびキャプチャポイント

Cisco Secure Firewall 3100:



Cisco Secure Firewall 4200:



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。

```
<#root>
```

```
>
```

```
capture capsw switch interface in_data_uplink1
```

セキュアファイアウォール4200は、キャプチャの方向性をサポートしています。

```
<#root>
```

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

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

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

2. キャプチャセッションを有効にします。

```
<#root>
```

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

検証

キャプチャセッションの名前、管理ステートと動作ステート、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)が増加していること、および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。

```
<#root>
```

```
>
```

```
show capture capsw detail
```

Packet Capture info

```
Name:                capsw
```

Session: 1
Admin State: enabled

Oper State: up

Oper State Reason: Active

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

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1

Port Id: 18

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

Pcapsize: 7704

Filter: capsw-1-18

Packet Capture Filter Info

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

Total Physical breakout ports involved in Packet Capture: 0

66 packets captured on disk using switch capture

Reading of capture file from disk is not supported

この場合、キャプチャは内部ID 18のインターフェイス (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) で作成されます。FXOSのlocal-mgmtコマンドシェルでshow portmanager switch statusコマンドを実行すると、インターフェイスIDが表示されます。

```
<#root>
```

```
>
```

```
connect fxos
```

```
...
```

```
firewall#
```

```
connect local-mgmt
```

```
firewall(local-mgmt)#
```

```
show portmanager switch status
```

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

ASA上の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、このコマンドを管理コンテキストで実行します。

キャプチャファイルの収集

「セキュアファイアウォール内部スイッチキャプチャファイルの収集」セクションの手順を実行します。

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、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。この例では、Secure Firewall 3100でのパケットキャプチャが分析されます。

キーポイントを確認します。この場合、ICMPエコー要求および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。

No.	Time	Source	Destination	Protocol	Length	IP ID	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	0x4de8 (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...4...E-
0010  00 54 4d 93 40 00 40 01 00 1a c0 00 02 64 c6 33  ..TM@.@...d-3
0020  64 64 08 00 7f 15 00 3a 00 21 39 3f f0 62 00 00  dd...!9?-b...
0030  00 00 8b 1a 05 00 00 00 00 00 10 11 12 13 14 15  .....,.....
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  .....,...!#$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  .....,...&'()*+,-./:012345
0060  36 37 55 55 55 55  .....,...67UUUU

```

説明

アップリンクインターフェイスの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	内部フィルタ	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でのパケットキャプチャの設定と確認	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エコー要求

				ホスト198.51.100.100からホスト192.0.2.100へのICMPエコー応答
--	--	--	--	--

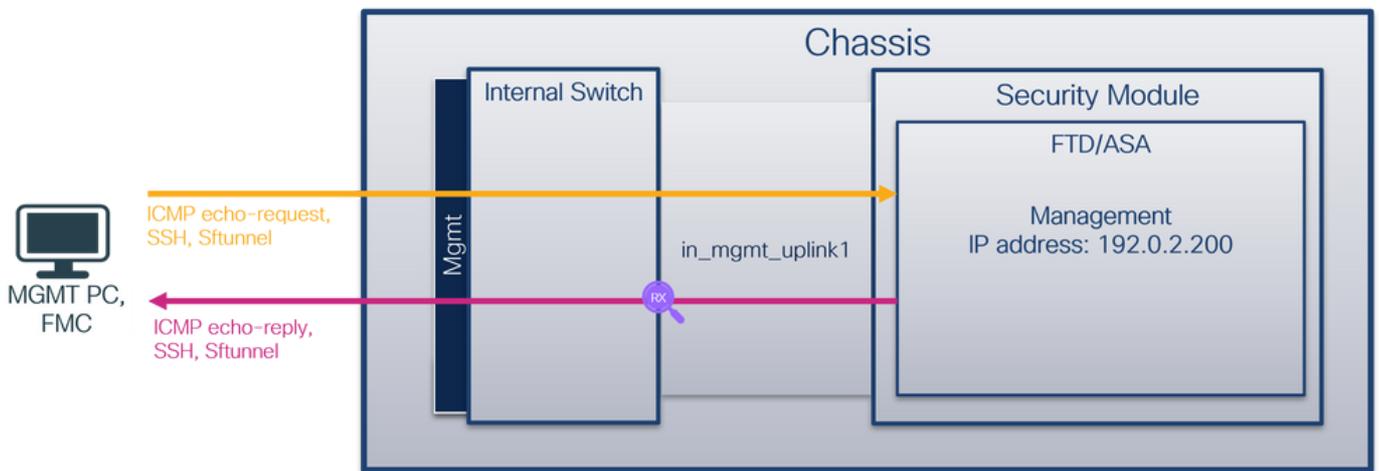
* 3100とは異なり、セキュアファイアウォール4200は双方向（入力および出力）キャプチャをサポートします。

タスク 2

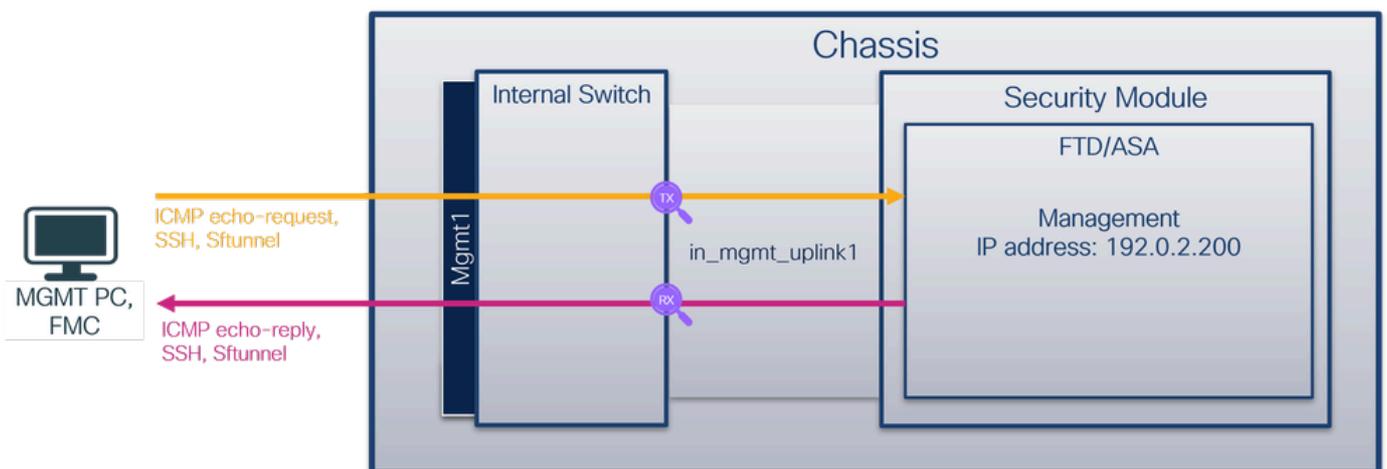
FTDまたはASA CLIを使用して、アップリンクインターフェイスin_mgmt_uplink1上のパケットキャプチャを設定および確認します。管理プレーン接続のパケットだけがキャプチャされます。

トポロジ、パケットフロー、およびキャプチャポイント

Cisco Secure Firewall 3100:



Cisco Secure Firewall 4200:



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。

```
<#root>
```

```
>
```

```
capture capsw switch interface in_mgmt_uplink1
```

セキュアファイアウォール4200は、キャプチャの方向性をサポートしています。

```
<#root>
```

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

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

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

2. キャプチャセッションを有効にします。

```
<#root>
```

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

検証

キャプチャセッションの名前、管理ステートと動作ステート、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)が増加していること、および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。

```
<#root>
```

```
> show capture capsw detail
```

Packet Capture info

Name: capsw

Session: 1

Admin State: enabled

Oper State: up

Oper State Reason: Active

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

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1

Port Id: 19

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

Pcapsize: 137248

Filter: 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(セキュアファイアウォール3130の in_mgmt_uplink1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を表示します。

```
<#root>
```

```
>
```

```
connect fxos
```

```
...
```

```
firewall#
```

```
connect local-mgmt
```

```
firewall(local-mgmt)#
```

```
show portmanager switch status
```

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

ASA上の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、このコマンドを管理コンテキストで実行します。

キャプチャファイルの収集

「セキュアファイアウォール内部スイッチキャプチャファイルの収集」セクションの手順を実行します。

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、in_mgmt_uplink1インターフェイスのキャプチャファイルを開きます。この例では、Secure Firewall 3100でのパケットキャプチャが分析されます。

キーポイントを確認します。この例では、管理IPアドレス192.0.2.200からのパケットだけが表示されています。例としては、SSH、Sftunnel、またはICMPエコー応答パケットがあります。これらは、内部スイッチを介してアプリケーション管理インターフェイスから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	IP TTL	Info
196	2022-08-07 23:21:45.133362	192.0.2.200	192.0.2.101	TCP	1518	0xb7d0 (47056)	64	39181 → 8305 [ACK] Seq=61372 Ack=875 Win=1384 Len=1448 TS
197	2022-08-07 23:21:45.133385	192.0.2.200	192.0.2.101	TCP	1518	0xb7d1 (47057)	64	39181 → 8305 [ACK] Seq=62820 Ack=875 Win=1384 Len=1448 TS
198	2022-08-07 23:21:45.133388	192.0.2.200	192.0.2.101	TLSv1.2	990	0xb7d2 (47058)	64	Application Data
199	2022-08-07 23:21:45.928772	192.0.2.200	192.0.2.100	ICMP	78	0xbd48 (48456)	64	Echo (ping) reply id=0x0001, seq=4539/47889, ttl=64
200	2022-08-07 23:21:45.949024	192.0.2.200	192.0.2.101	TLSv1.2	128	0x4a97 (19095)	64	Application Data
201	2022-08-07 23:21:45.949027	192.0.2.200	192.0.2.101	TCP	70	0x4a98 (19096)	64	8305 → 58885 [ACK] Seq=21997 Ack=26244 Win=4116 Len=0 TSv
202	2022-08-07 23:21:46.019895	192.0.2.200	192.0.2.101	TLSv1.2	100	0x4a99 (19097)	64	Application Data
203	2022-08-07 23:21:46.019899	192.0.2.200	192.0.2.101	TLSv1.2	96	0x4a9a (19098)	64	Application Data
204	2022-08-07 23:21:46.019903	192.0.2.200	192.0.2.101	TCP	70	0x4a9b (19099)	64	8305 → 58885 [ACK] Seq=22053 Ack=26274 Win=4116 Len=0 TSv
205	2022-08-07 23:21:46.019906	192.0.2.200	192.0.2.101	TCP	70	0x4a9c (19100)	64	8305 → 58885 [ACK] Seq=22053 Ack=26300 Win=4116 Len=0 TSv
206	2022-08-07 23:21:46.136415	192.0.2.200	192.0.2.101	TCP	70	0xb7d3 (47059)	64	39181 → 8305 [ACK] Seq=65188 Ack=921 Win=1384 Len=0 TSval
207	2022-08-07 23:21:46.958148	192.0.2.200	192.0.2.100	ICMP	78	0xbd9e (48542)	64	Echo (ping) reply id=0x0001, seq=4540/48145, ttl=64
208	2022-08-07 23:21:47.980409	192.0.2.200	192.0.2.100	ICMP	78	0xbdf2 (48626)	64	Echo (ping) reply id=0x0001, seq=4541/48401, ttl=64
209	2022-08-07 23:21:48.406312	192.0.2.200	192.0.2.101	TCP	70	0x4a9d (19101)	64	8305 → 58885 [ACK] Seq=22053 Ack=26366 Win=4116 Len=0 TSv
210	2022-08-07 23:21:48.903236	192.0.2.200	192.0.2.101	TLSv1.2	747	0x4a9e (19102)	64	Application Data
211	2022-08-07 23:21:48.994386	192.0.2.200	192.0.2.100	ICMP	78	0xbe48 (48712)	64	Echo (ping) reply id=0x0001, seq=4542/48657, ttl=64
212	2022-08-07 23:21:50.008576	192.0.2.200	192.0.2.100	ICMP	78	0xbea6 (48806)	64	Echo (ping) reply id=0x0001, seq=4543/48913, ttl=64
213	2022-08-07 23:21:50.140167	192.0.2.200	192.0.2.101	TCP	1518	0xb7d4 (47060)	64	39181 → 8305 [ACK] Seq=65188 Ack=921 Win=1384 Len=1448 TS
214	2022-08-07 23:21:50.140171	192.0.2.200	192.0.2.101	TCP	1518	0xb7d5 (47061)	64	39181 → 8305 [ACK] Seq=66636 Ack=921 Win=1384 Len=1448 TS
215	2022-08-07 23:21:50.140175	192.0.2.200	192.0.2.101	TLSv1.2	990	0xb7d6 (47062)	64	Application Data
216	2022-08-07 23:21:51.015884	192.0.2.200	192.0.2.100	ICMP	78	0xbec1 (48833)	64	Echo (ping) reply id=0x0001, seq=4544/49169, ttl=64
217	2022-08-07 23:21:51.142842	192.0.2.200	192.0.2.101	TCP	70	0xb7d7 (47063)	64	39181 → 8305 [ACK] Seq=69004 Ack=967 Win=1384 Len=0 TSval
218	2022-08-07 23:21:52.030118	192.0.2.200	192.0.2.100	ICMP	78	0xbf02 (48898)	64	Echo (ping) reply id=0x0001, seq=4545/49425, ttl=64
219	2022-08-07 23:21:53.042744	192.0.2.200	192.0.2.100	ICMP	78	0xbf59 (48985)	64	Echo (ping) reply id=0x0001, seq=4546/49681, ttl=64
220	2022-08-07 23:21:53.073144	192.0.2.200	192.0.2.100	SSH	170	0xad34 (44340)	64	Server: Encrypted packet (len=112)
221	2022-08-07 23:21:53.194906	192.0.2.200	192.0.2.100	TCP	64	0xad35 (44341)	64	22 → 53249 [ACK] Seq=1025 Ack=881 Win=946 Len=0
222	2022-08-07 23:21:53.905480	192.0.2.200	192.0.2.101	TLSv1.2	747	0x4a9f (19103)	64	Application Data
223	2022-08-07 23:21:54.102899	192.0.2.200	192.0.2.100	ICMP	78	0xbf63 (48995)	64	Echo (ping) reply id=0x0001, seq=4547/49937, ttl=64
224	2022-08-07 23:21:54.903675	192.0.2.200	192.0.2.101	TCP	70	0x4aa0 (19104)	64	8305 → 58885 [ACK] Seq=23407 Ack=26424 Win=4116 Len=0 TSv
225	2022-08-07 23:21:55.136700	192.0.2.200	192.0.2.100	ICMP	78	0xbf64 (48996)	64	Echo (ping) reply id=0x0001, seq=4548/50103, ttl=64

```

> Frame 1: 747 bytes on wire (5976 bits), 747 bytes captured (5976 bits)
> Ethernet II, Src: Cisco_34:9a:a00 (bc:e7:12:34:9a:a00), Dst: Cisco_11:38:2a (a4:53:0e:11:38:2a)
> Internet Protocol Version 4, Src: 192.0.2.200, Dst: 192.0.2.101
> Transmission Control Protocol, Src Port: 8305, Dst Port: 58885, Seq: 1, Ack: 1, Len: 677
> Transport Layer Security
0000 a4 53 0e 11 38 2a bc e7 12 34 9a 00 08 00 45 00  :S-8*...4....E-
0010 02 d9 4a 3d 40 00 40 06 68 b4 c0 00 02 c8 c0 00  :...@.h.....
0020 02 65 20 71 e6 05 67 1b 2a c5 db e3 6b d4 80 18  :e q . g . * * k . . .
0030 10 14 27 cc 00 00 01 01 08 0a 08 76 95 7f 91 02  :.....j.....
0040 3d 41 17 03 03 02 a0 22 6a 01 e0 ff cc 98 f9 af  :=A.....j.....
0050 07 40 75 19 a4 d5 df 64 d8 fe 66 8e 9b cc 8d 2f  :@u....d..f....-/
0060 92 b2 1a 64 e7 20 36 03 8e 48 02 5a 7c 85 30 d4  :...d . 6 . H . Z | . 0
0070 fa c0 a8 56 b8 ad a7 7e 19 3a c1 9c 4b 57 0e e0  :...V...:..:KM-
0080 be ef 95 22 84 c1 c1 9d 9f 24 78 b4 15 1c 44 0e  :...:..:$.D-
0090 ea cb 43 9e 1f fd a7 70 75 e5 6b a4 f8 2b ee 47  :..C...p u . k . + . G
00a0 2f 86 73 8f b1 e1 b5 c6 57 e3 a8 46 0e cb 26 b7  :/ . s . . . . W . F . &
00b0 5b c7 e3 09 54 f3 c1 ff 26 d9 87 ea 51 3d 20 08  : [ . . . T . . . & . . . Q = .
00c0 16 fd cb f5 4f 91 98 5e 86 15 17 55 68 6f 5d 04  :...O...^..Uho].

```

説明

管理アップリンクインターフェイスの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る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
管理アプリケーショ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	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経由でネットワークへ)	FTD管理IPアドレス192.0.2.200からホスト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 IPアドレス192.0.2.101へのSFTUNNEL FTD管理IPアドレス192.0.2.200からホスト192.0.2.100へのSSH

* 3100とは異なり、セキュアファイアウォール4200は双方向（入力および出力）キャプチャをサポートします。

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方法で設定します。ethernet-typeオプションとmatchオプションを使用して、フィルタを設定します。

コンフィギュレーション

ASAまたはFTD CLIで次の手順を実行し、インターフェイスEthernet1/1上のホスト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。

```
<#root>
```

```
>
```

```
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。

```
<#root>
```

>

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

<#root>

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

検証

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。

<#root>

>

```
show capture capsw detail
```

Packet Capture info

```
Name:                capsw

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

Total Physical ports involved in Packet Capture: 1

Physical port:

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

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

Packet Capture Filter Info

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

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

Ethertype: 2054

Total Physical breakout ports involved in Packet Capture: 0

0 packet captured on disk using switch capture

Reading of capture file from disk is not supported

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。

<#root>

>

show capture capsw detail

Packet Capture info

Name: capsw

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

Total Physical ports involved in Packet Capture: 1

Physical port:

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

Filter: capsw-1-1

Packet Capture Filter Info

Name: caps-1-1

Protocol: 1

Ivlan: 0
Ovlan: 0

Src Ip: 198.51.100.100

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

Total Physical breakout ports involved in Packet Capture: 0

0 packets captured on disk using switch capture

Reading of capture file from disk is not supported

セキュアファイアウォール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、CLIのcopyコマンドを使用して、キャプチャファイルを、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。

または、エキスパートモードで/ngfw/var/commonにコピーし、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、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。

ASA

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、次の手順を実行します。

1. キャプチャを停止します。

<#root>

```
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。

```
<#root>
```

```
asa#
show capture capsw detail
```

Packet Capture info

Name: capsw

Session: 1

Admin State: disabled

Oper State: down

Oper State Reason: Session_Admin_Shut

Config Success: yes

Config Fail Reason:

Append Flag: overwrite

Session Mem Usage: 256

Session Pcap Snap Len: 1518

Error Code: 0

Drop Count: 0

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1

Port Id: 1

Pcapfile:

/mnt/disk0/packet-capture/

sess-1-capsw-ethernet-1-1-0.pcap

Pcapsize: 139826

Filter: capsw-1-1

Packet Capture Filter Info

Name: capsw-1-1

Protocol: 0

Ivlan: 0

Ovlan: 0

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

Total Physical breakout ports involved in Packet Capture: 0

886 packets captured on disk using switch capture

Reading of capture file from disk is not supported

3. CLIのcopyコマンドを使用して、リモートの宛先にファイルをエクスポートします。

```
<#root>
```

```
asa#
```

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

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

```
asa#
```

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

```
Source filename [/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap]?
```

```
Destination filename [sess-1-capsw-ethernet-1-1-0.pcap]?
```

```
Copy in progress...C
```

```
139826 bytes copied in 0.532 secs
```

FTD

次の手順を実行して、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サーバにコピーします。

1. 診断CLIに移動します。

```
<#root>
```

```
>
```

```
system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Click 'Ctrl+a then d' to detach.  
Type help or '?' for a list of available commands.
```

```
firepower>
```

```
enable
```

```
Password:
```

```
<-- Enter
```

```
firepower#
```

2. キャプチャを停止します。

```
<#root>
```

```
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。

```
<#root>
```

```
firepower#
```

```
show capture capsw detail
```

```
Packet Capture info
```

```
Name:                capsw
```

```
Session:             1
```

```
Admin State:         disabled
```

```
Oper State:          down
```

```
Oper State Reason:   Session_Admin_Shut
```

```
Config Success:      yes
```

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

Total Physical ports involved in Packet Capture: 1

Physical port:
Slot Id: 1
Port Id: 1

Pcapfile:

/mnt/disk0/packet-capture/

sess-1-capsw-ethernet-1-1-0.pcap

Pcapsize: 139826
Filter: capsw-1-1

Packet Capture Filter Info

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

Total Physical breakout ports involved in Packet Capture: 0

886 packets captured on disk using switch capture

Reading of capture file from disk is not supported

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

<#root>

firepower#

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

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

```
startup-config Copy to startup configuration
system:         Copy to system: file system
tftp:           Copy to tftp: file system
```

```
firepower#
```

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

```
Source filename [/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap]?
```

```
Destination filename [sess-1-capsw-ethernet-1-1-0.pcap]?
```

```
Copy in progress...C
```

```
139826 bytes copied in 0.532 secs
```

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、次の手順を実行します。

1. キャプチャを停止します。

```
<#root>
```

```
>
```

```
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。

```
<#root>
```

```
>
```

```
show capture capsw detail
```

```
Packet Capture info
```

```
Name:                capsw
```

```
Session:             1
```

```
Admin State:         disabled
```

```
Oper State:          down
```

```
Oper State Reason:   Session_Admin_Shut
```

```
Config Success:      yes
```

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

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1
Port Id: 1

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

Pcapsize: 139826
Filter: capsw-1-1

Packet Capture Filter Info

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

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

3. 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。

```
<#root>
```

```
>
```

```
expert
```

```
admin@firepower:~$
```

```
sudo su
```

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

4. キャプチャファイルを/ngfw/var/common/にコピーします。

<#root>

```
root@KSEC-FPR3100-1:/home/admin
```

```
cp /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap /ngfw/var/common/
```

```
root@KSEC-FPR3100-1:/home/admin
```

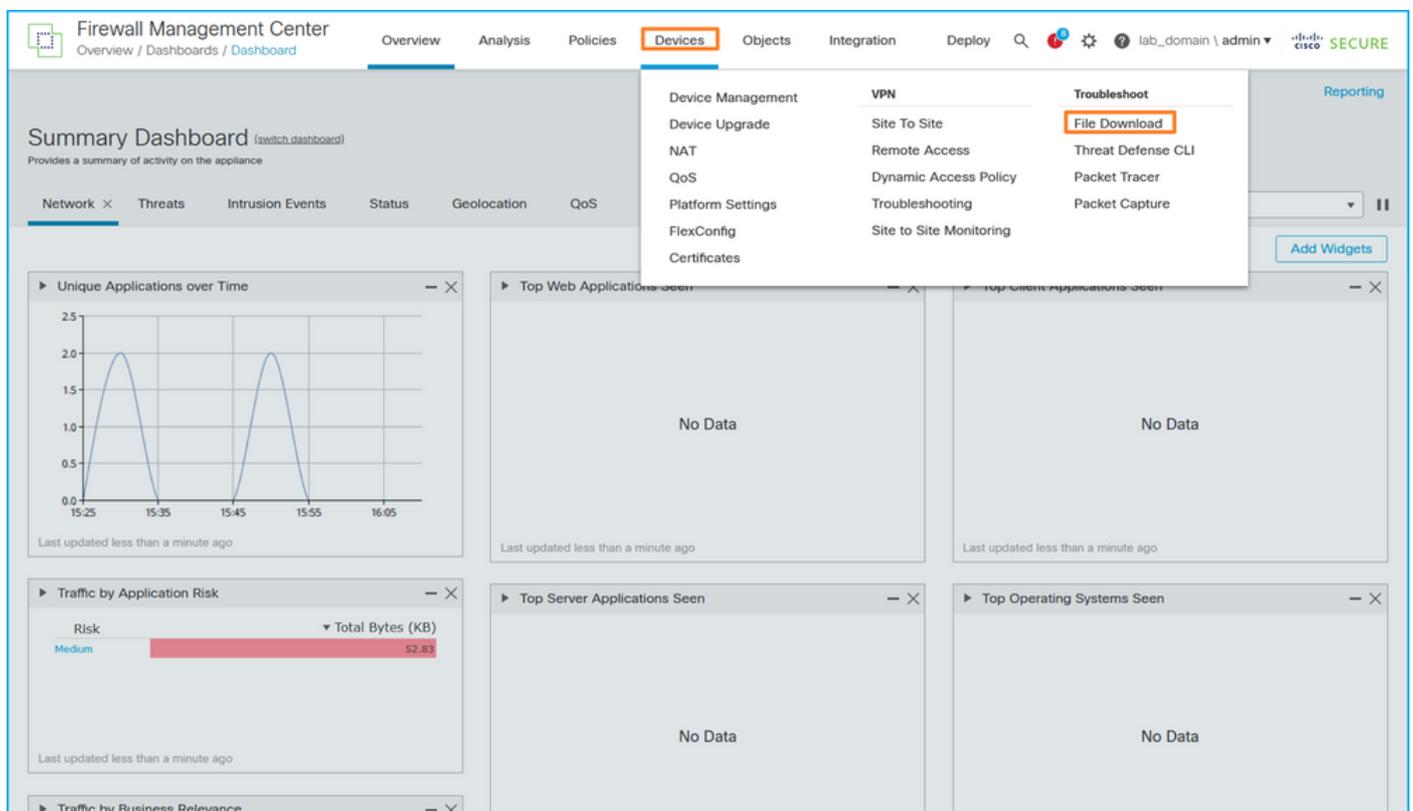
```
ls -l /ngfw/var/common/sess*
```

```
-rwxr-xr-x 1 root admin 139826 Aug  7 20:14
```

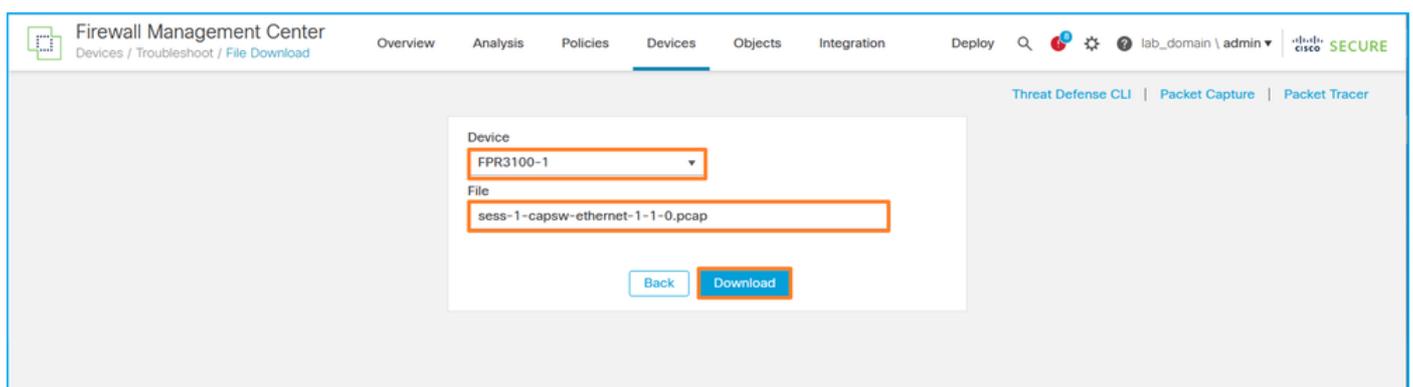
```
/ngfw/var/common/sess-1-capsw-ethernet-1-1-0.pcap
```

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

5. FMCで、Devices > File Downloadの順に選択します。

The screenshot shows the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'Integration', and 'Deploy'. The 'Devices' menu is expanded, showing options like 'Device Management', 'VPN', and 'Troubleshoot'. The 'File Download' option under 'Troubleshoot' is highlighted with an orange box. The main dashboard area contains several widgets: 'Unique Applications over Time' (line graph), 'Top Web Applications Seen' (No Data), 'Top Server Applications Seen' (No Data), 'Top Operating Systems Seen' (No Data), and 'Traffic by Application Risk' (bar chart showing Medium risk with 52.83 KB total bytes).

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

The screenshot shows the 'File Download' configuration page in the FMC. The 'Device' dropdown menu is set to 'FPR3100-1' and the 'File' text input field contains 'sess-1-capsw-ethernet-1-1-0.pcap'. Both the dropdown and the text field are highlighted with orange boxes. At the bottom of the form, there are 'Back' and 'Download' buttons, with the 'Download' button highlighted in orange.

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と、エラー「ERROR: Failed to enable session, as limit of maximum 1 active packet capture sessions reached」が発生します。
- 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の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。
- ダンプ、デコード、パケット番号、トレース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上のスイッチのキャプチャはユーザコンテキストで設定されます。インターフェイスin_data_uplink1とin_mgmt_uplink1でのスイッチのキャプチャは、管理コンテキストでのみサポートされています。

次に、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を設定する際は、パケットの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パケット長を、デフォルト値の1518バイトと異なる場合に増減します。サイズが小さいほど、キャプチャされるパケットの数が増加し、サイズが小さいほどキャプチャされるパケットの数が増加します。
- 必要に応じてバッファサイズを調整します。
- show cap <cap_name> detailコマンドの出力にある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、廃棄カウントのカウントが増加します。

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。