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

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。

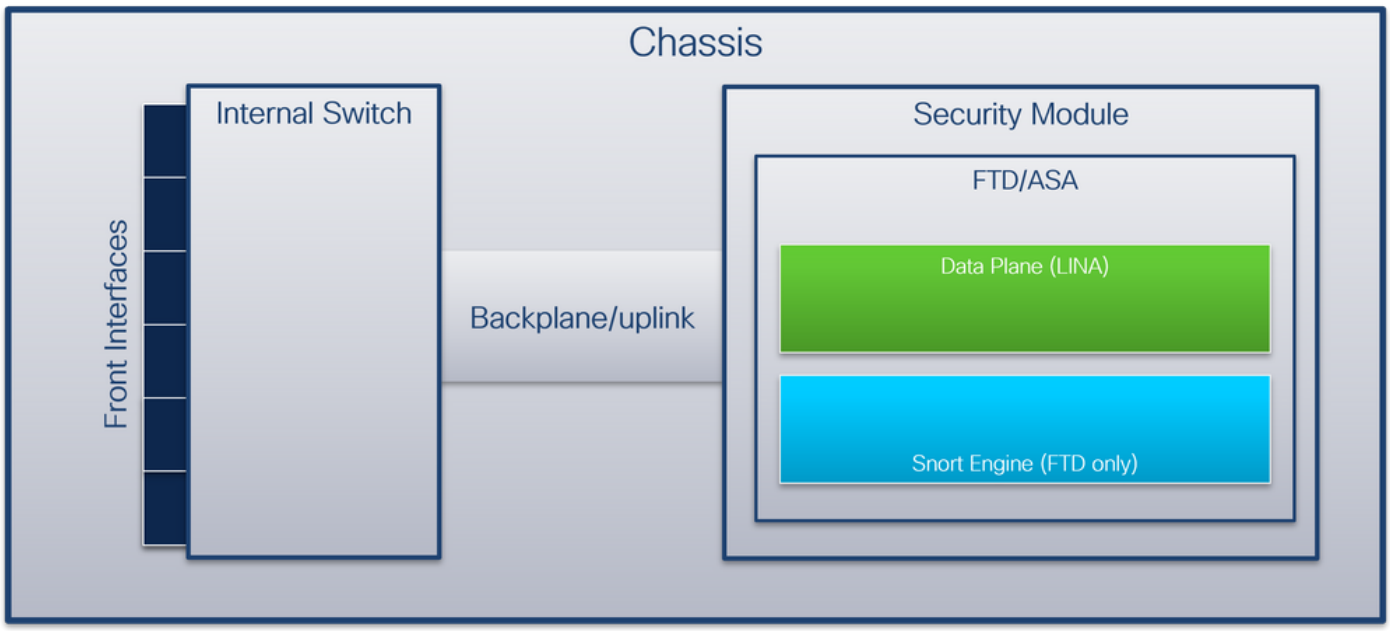
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 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コマンドシェルで確認できます。

<#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、それぞれの出力インターフェイス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、スイッチは出力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力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。

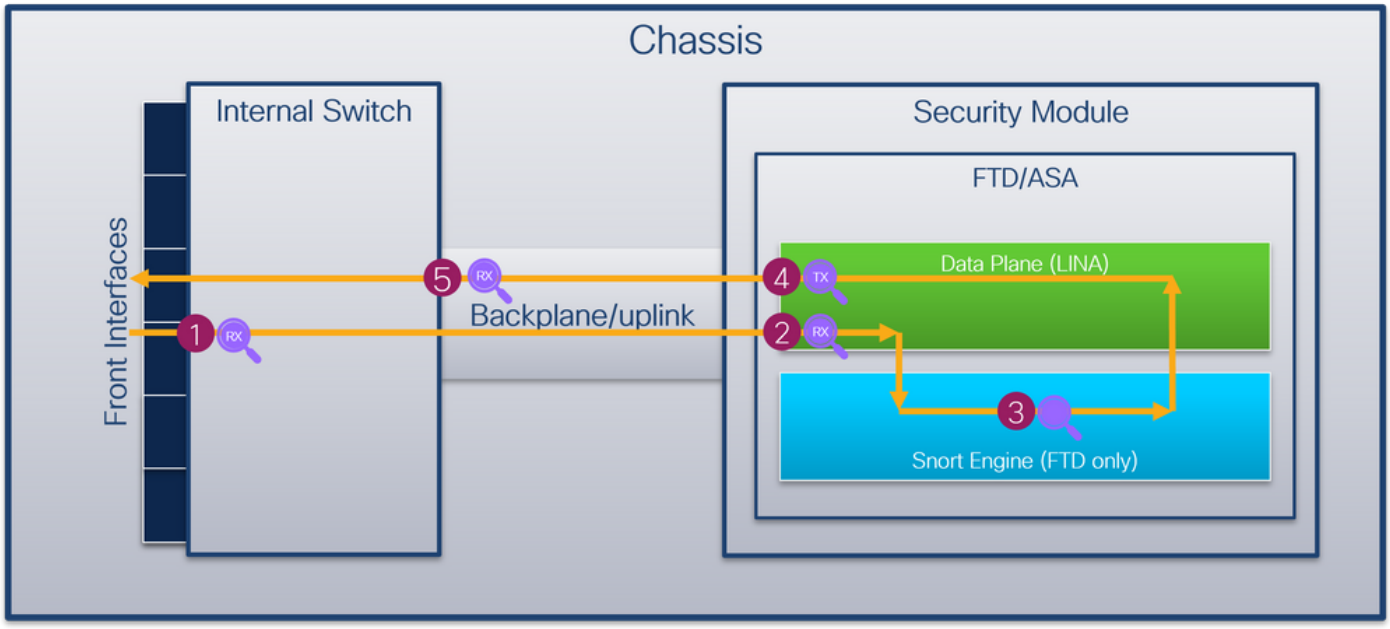
ポートVLANタグはアプリケーションと共有されます。アプリケーションは、それぞれの出力インターフェイスVLANタグを各パケットに挿入します。アプリケーションからのパケットがアップリンクインターフェイス上の内部スイッチによって受信されると、スイッチは出力インターフェイスのVLANタグを読み取り、出力インターフェイスを識別し、ポートのVLANタグを削除して、パケットをネットワークに転送します。

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。



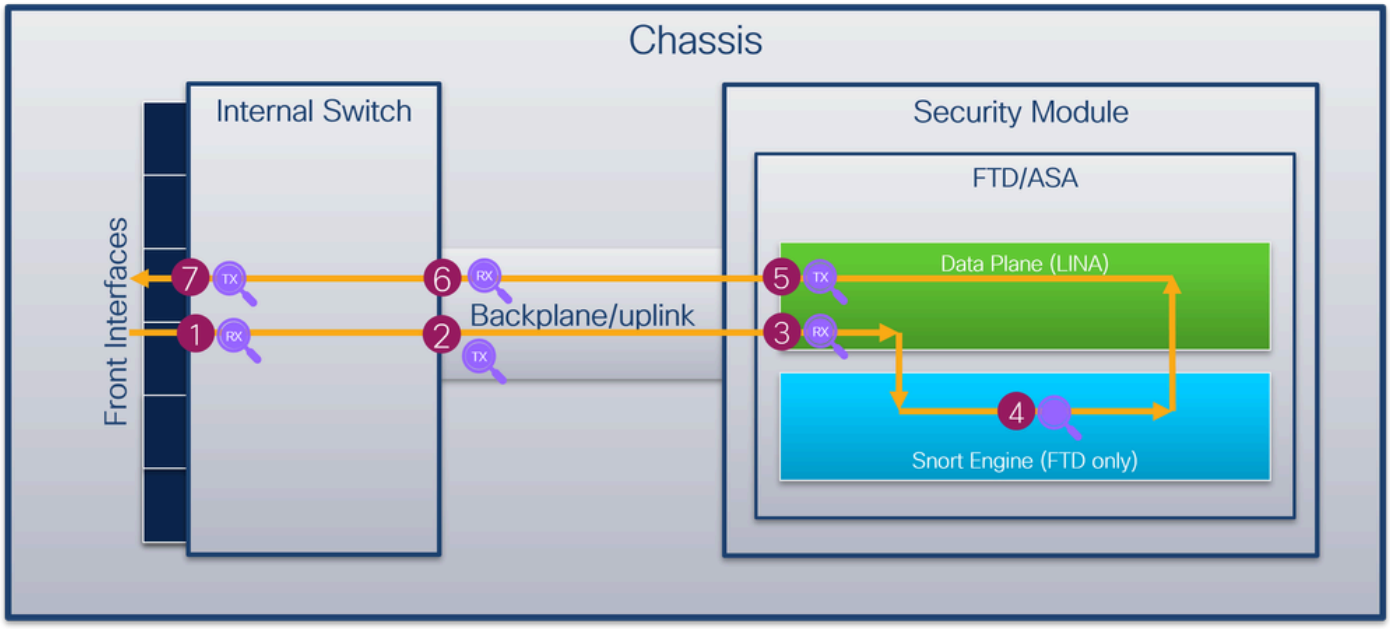
キャプチャポイントは次のとおりです。

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パケット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。

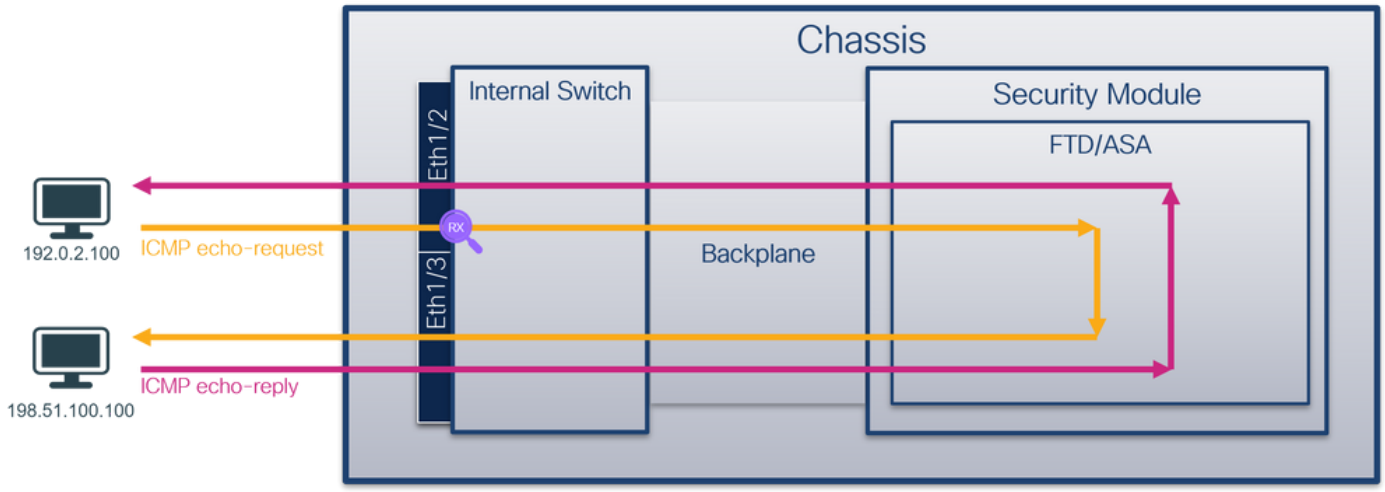
これらのシナリオは、Firepower 4100/9300内部スイッチのキャプチャの一般的な使用例をカバーしています。

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

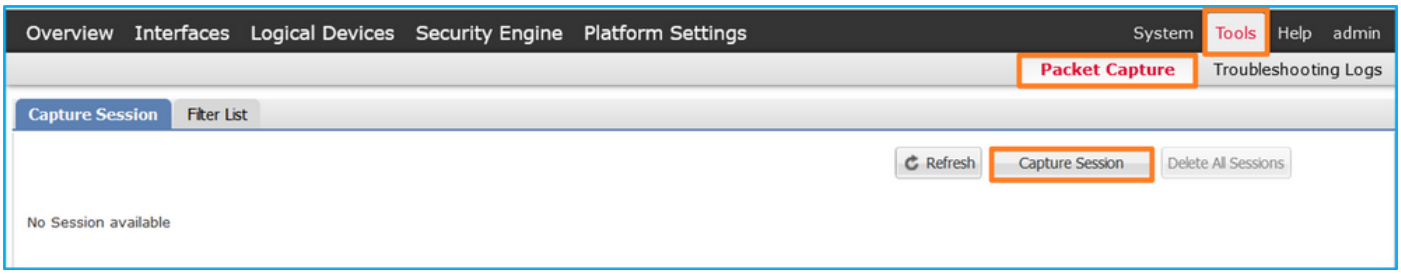


コンフィギュレーション

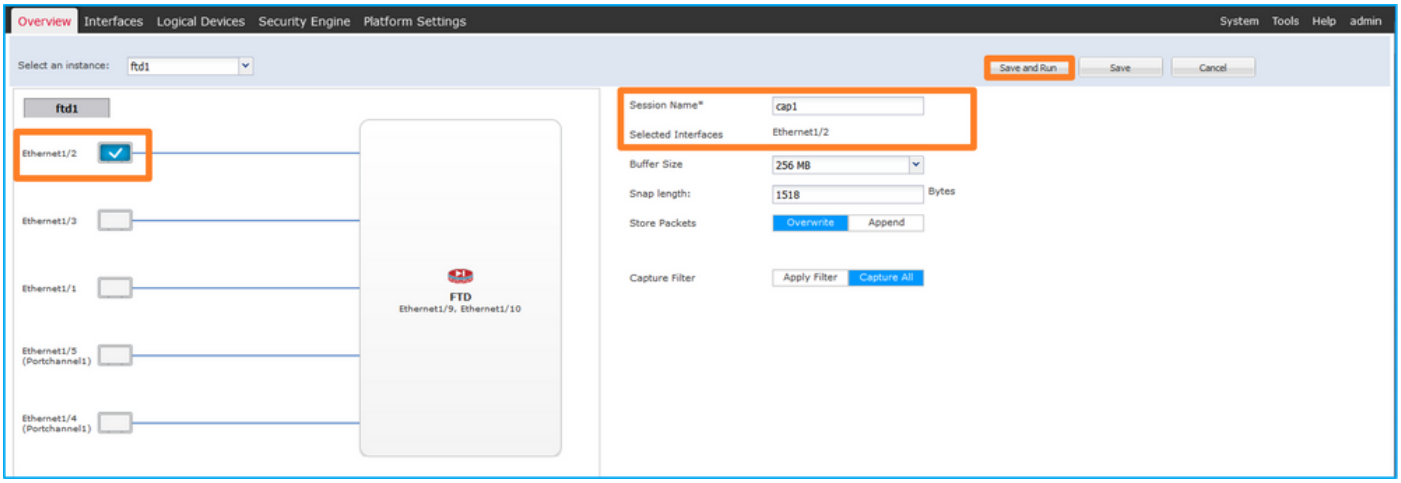
FCM（必須）

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。

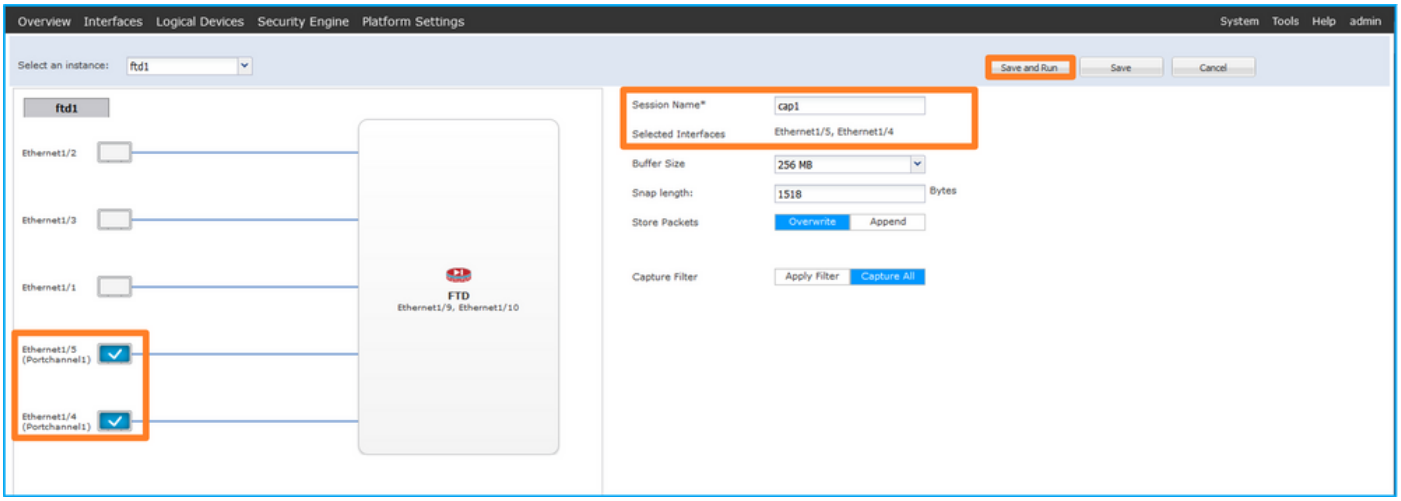
1. Tools > Packet Capture > Capture Sessionの順に選択して、新しいキャプチャセッションを作成します。



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。

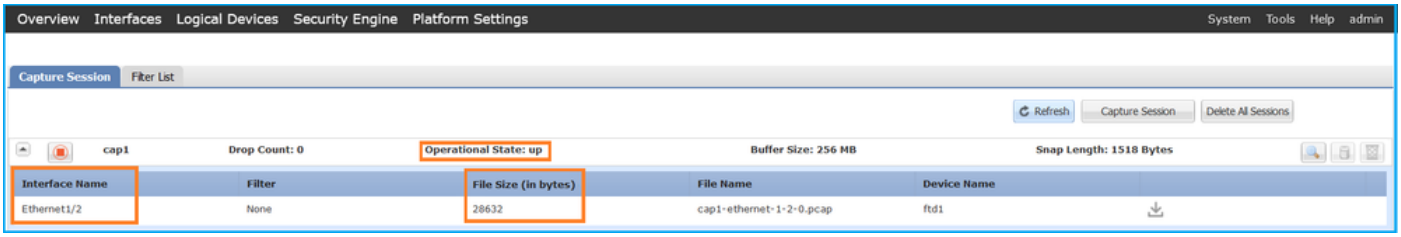
```
<#root>
firepower#
scope packet-capture

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 #
```

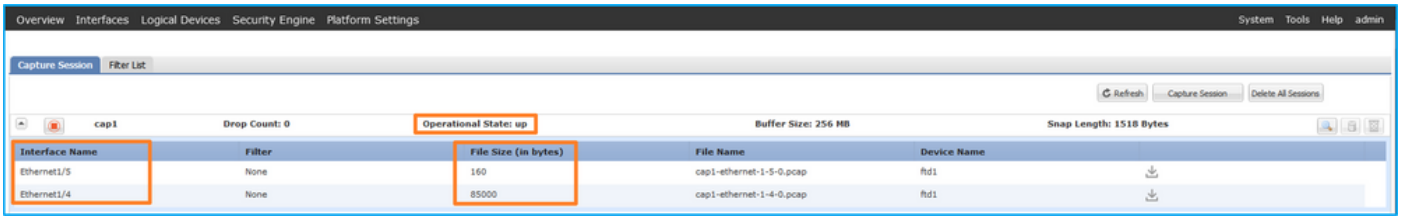
検証

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。



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



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

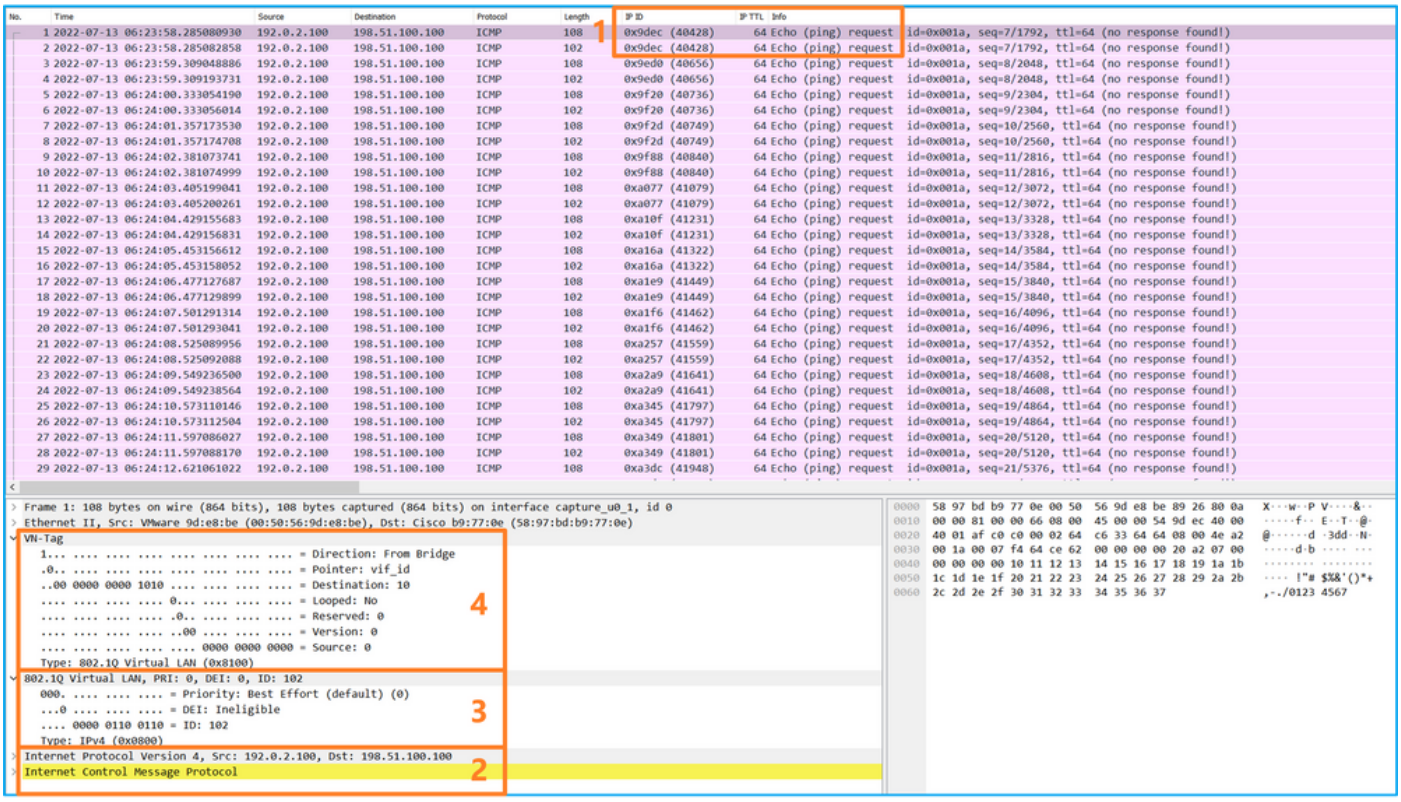
キャプチャファイルの収集

「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

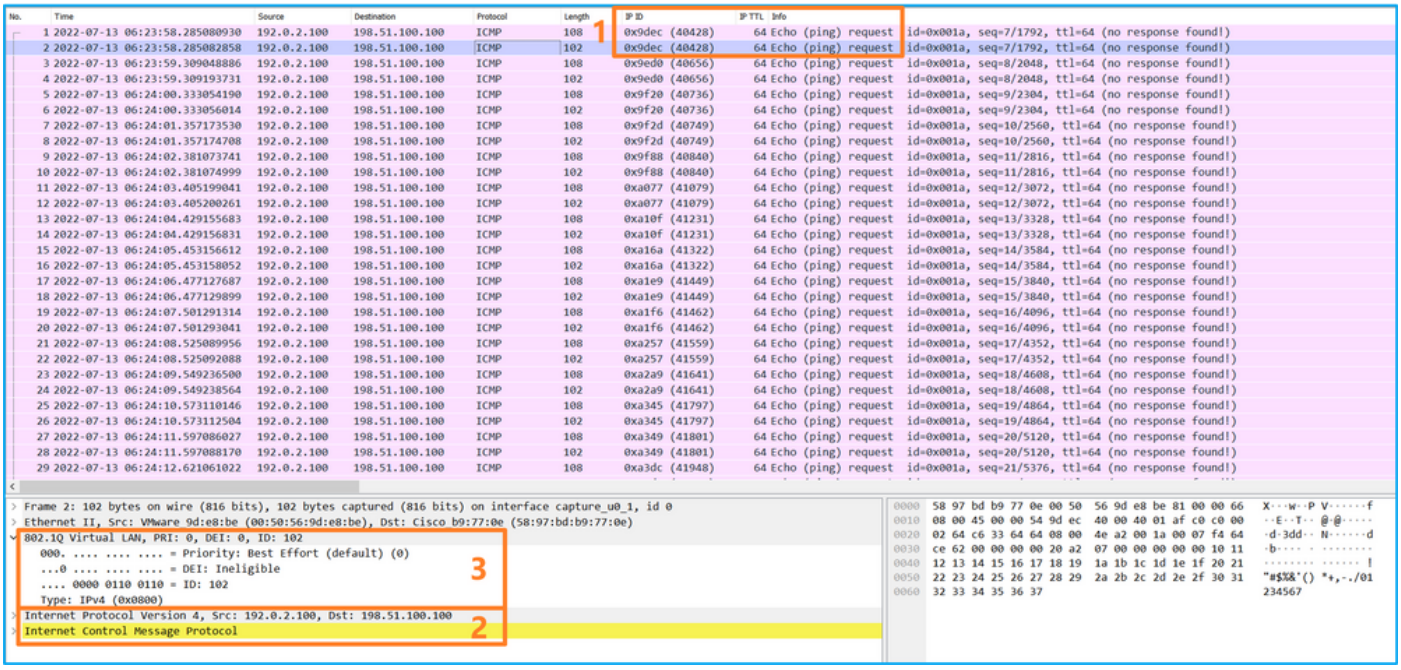
パケットキャプチャファイルリーダーアプリケーションを使用して、Ethernet1/2のキャプチャファイルを開きます。最初のパケットを選択し、キーポイントを確認します。

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。



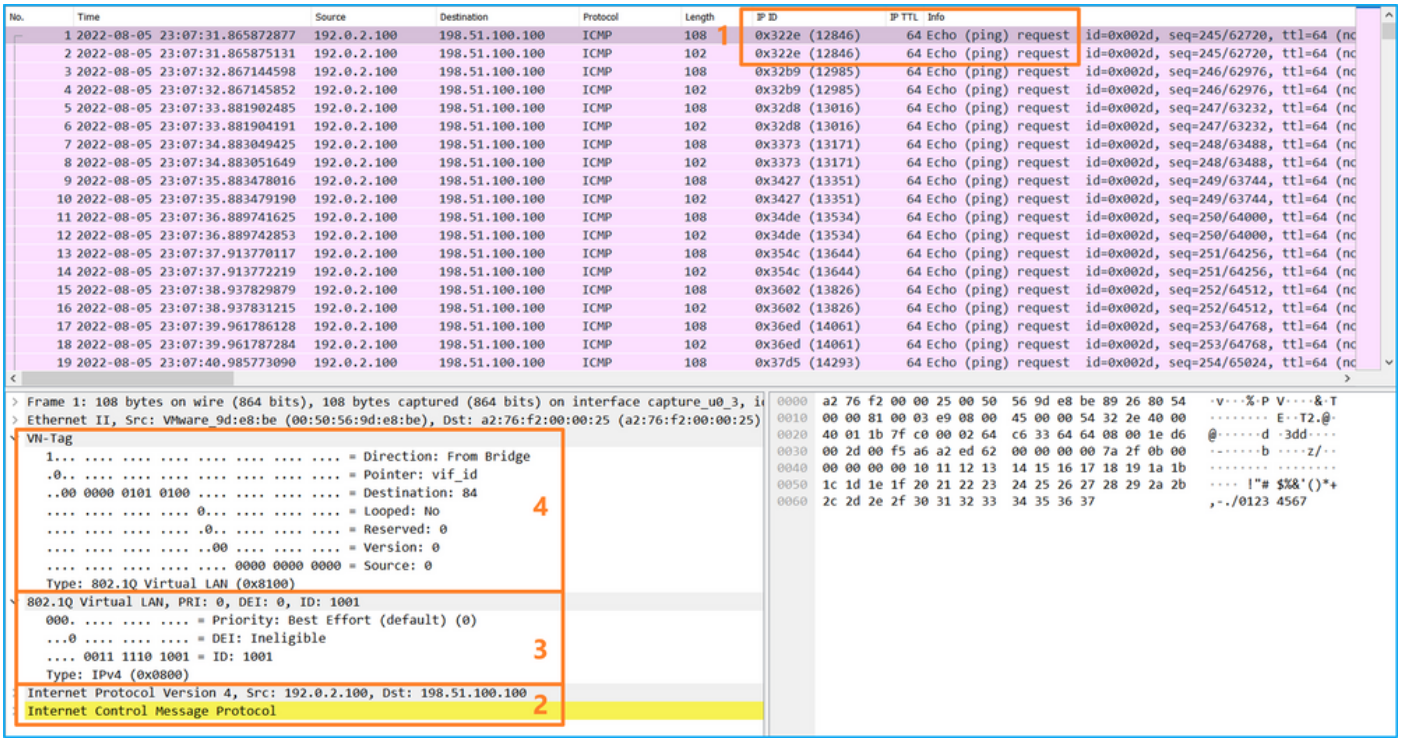
2番目のパケットを選択し、キーポイントを確認します。

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。



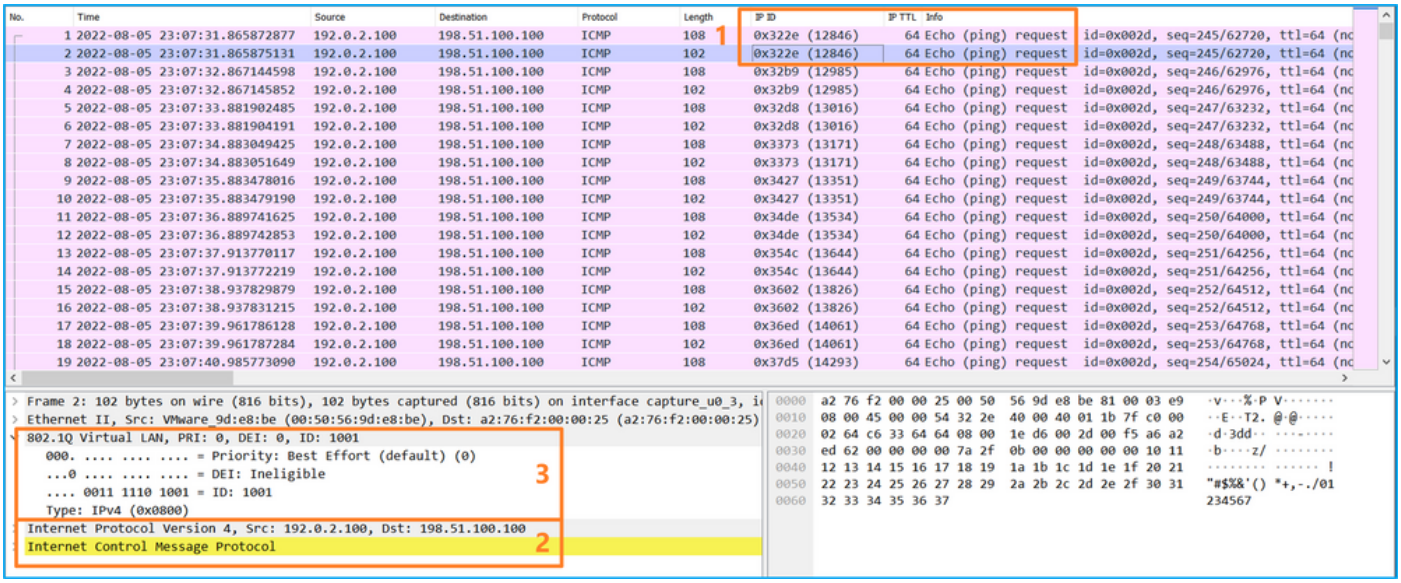
Portchannel1メンバーインターフェイスのキャプチャファイルを開きます。最初のパケットを選択し、キーポイントを確認します。

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。



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。



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。

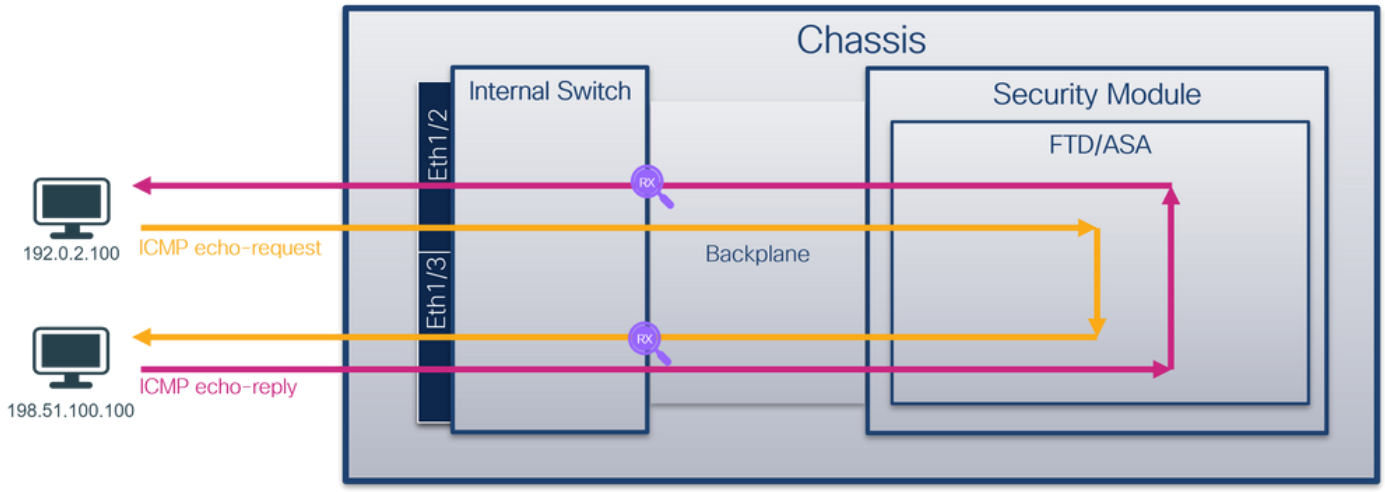
タスク	キャプチャポイント	キャプチャされたパケットの内部ポートVLAN	方向	キャプチャされたトラフィック
インターフェイスEthernet1/2のパケットキャプチャの設定と確認	イーサネット1/2	102	入力のみ	ホスト192.0.2.100からホスト198.51.100.100へのICMPエコー要求
インターフェイスPortchannel1で、メン	Ethernet1/4 Ethernet1/5	1001	入力のみ	ホスト192.0.2.100からホスト198.51.100.100へのICMPエコー

バーインターフェイス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

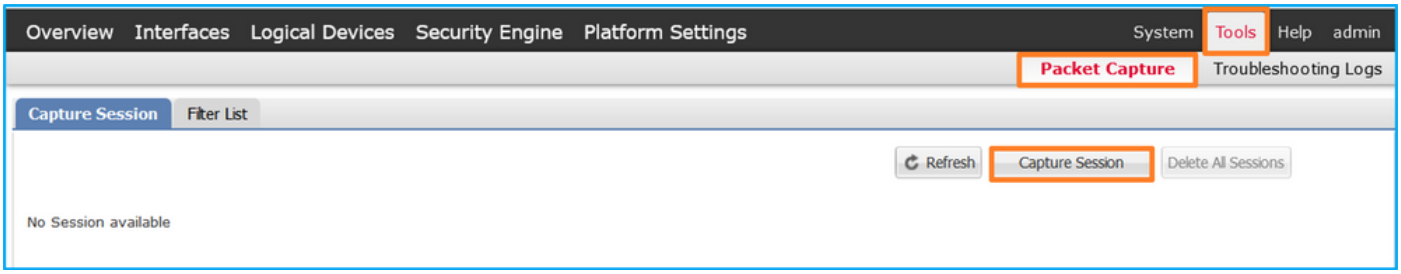


コンフィギュレーション

FCM（必須）

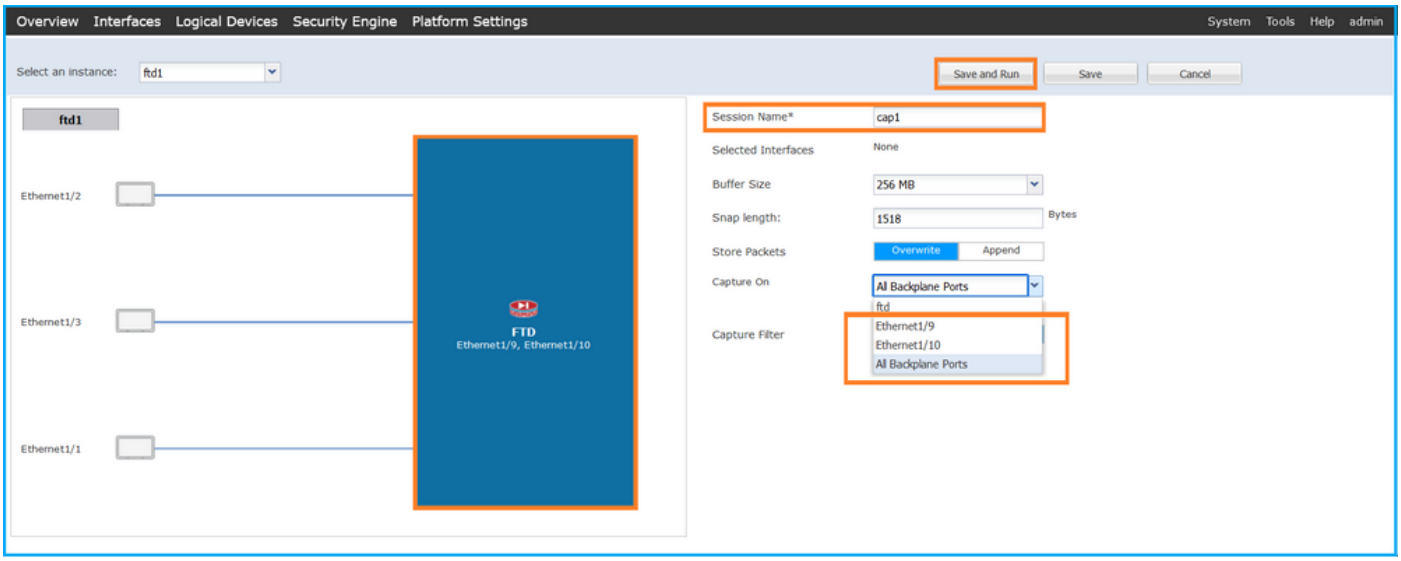
バックプレーンインターフェイスでパケットキャプチャを設定するには、FCMで次の手順を実行します。

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。

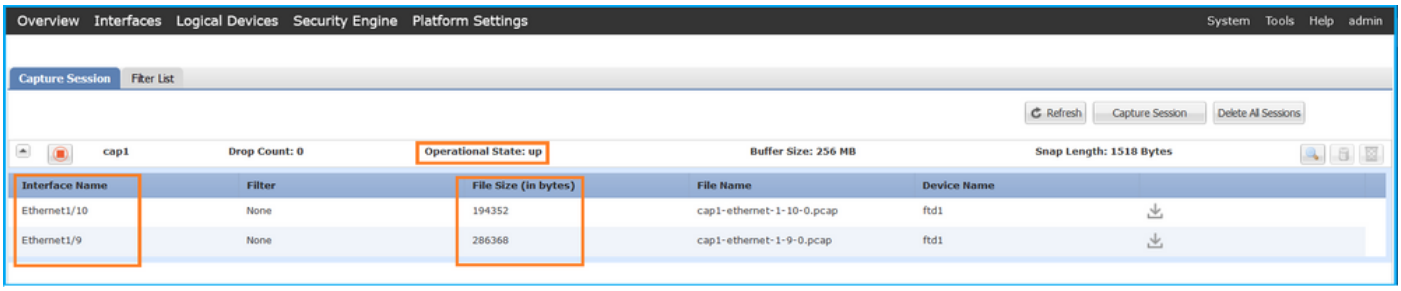
```
<#root>

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。



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。

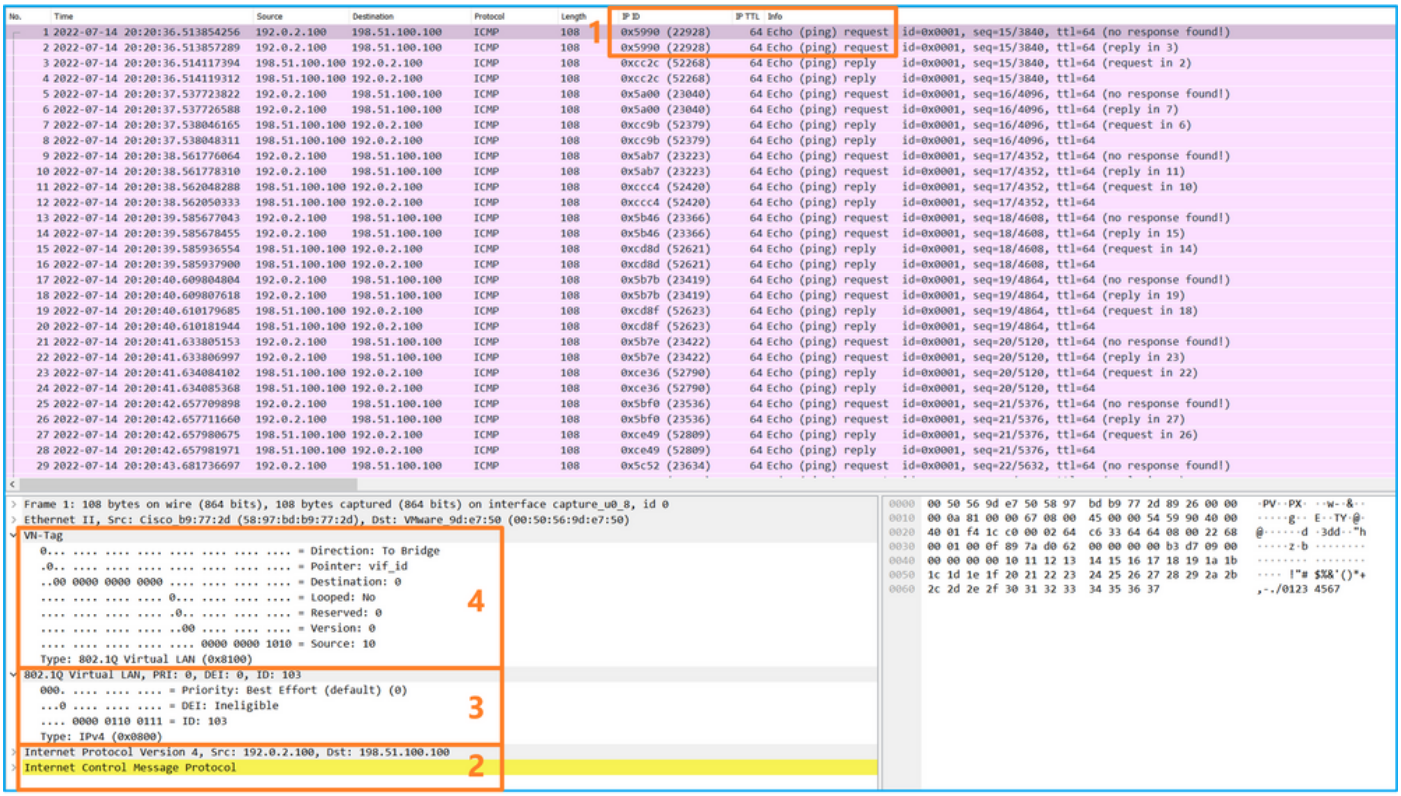
ファイル分析のキャプチャ

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。

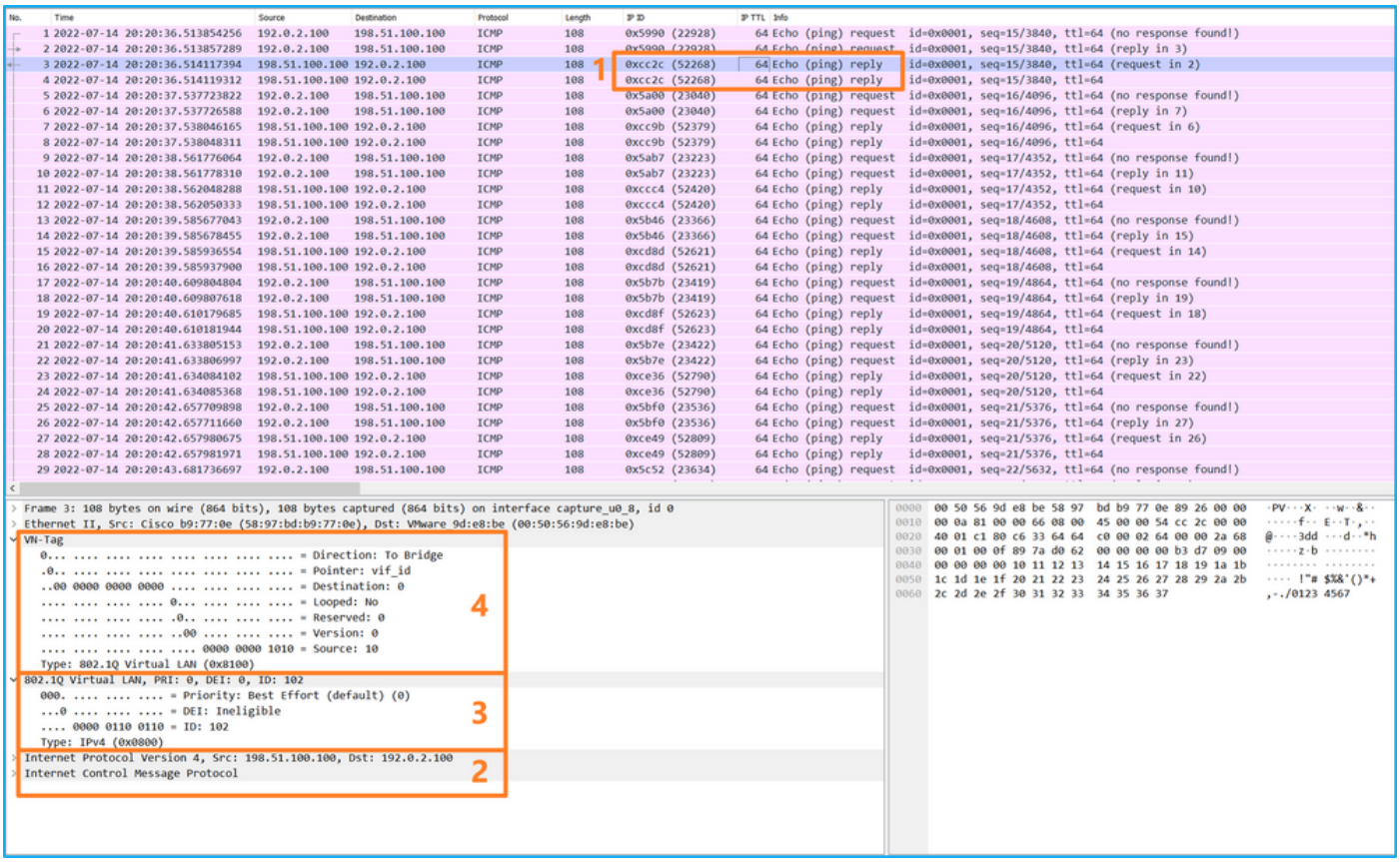
1. 各ICMPエコー要求パケットがキャプチャされて2回表示されます。
2. 元のパケットヘッダーにはVLANタグが付いていません。
3. 内部スイッチは、出力インターフェイスEthernet1/3を識別する追加のポートVLANタグ

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。



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。



説明

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。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力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を出力インターフェイスとして識別し、ICMPエコー応答パケット内のVLANタグ102はEthernet1/2を出力インターフェイスとして識別します。内部スイッチは、パケットがネットワークに転送される前に、VNタグと内部インターフェイスの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。

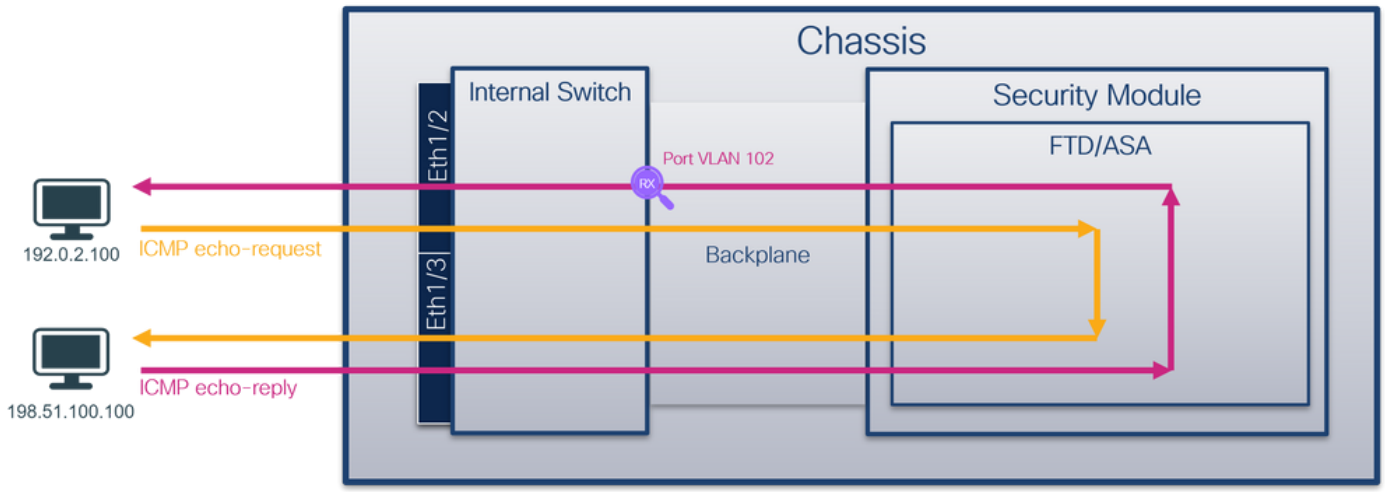
- 特定の前面インターフェイスから発信されるパケットのパケットキャプチャをバックプレーンインターフェイスで設定します。たとえば、インターフェイスEthernet1/2から送信されるパケットのパケットキャプチャをバックプレーンインターフェイスEthernet1/9で設定します。
- 特定の前面インターフェイスとバックプレーンインターフェイスで同時パケットキャプチャを設定します。たとえば、インターフェイスEthernet1/2から出るパケットに対して、インターフェイスEthernet1/2とバックプレーンインターフェイスEthernet1/9で同時パケットキャプチャを設定します。

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



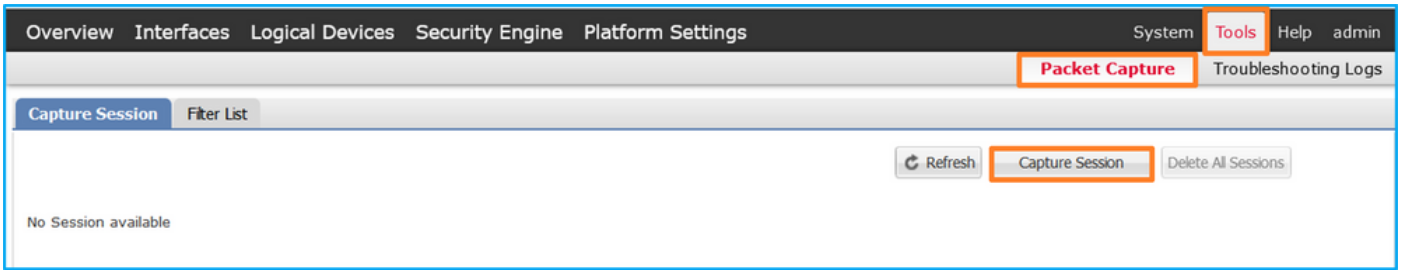
コンフィギュレーション

FCM（必須）

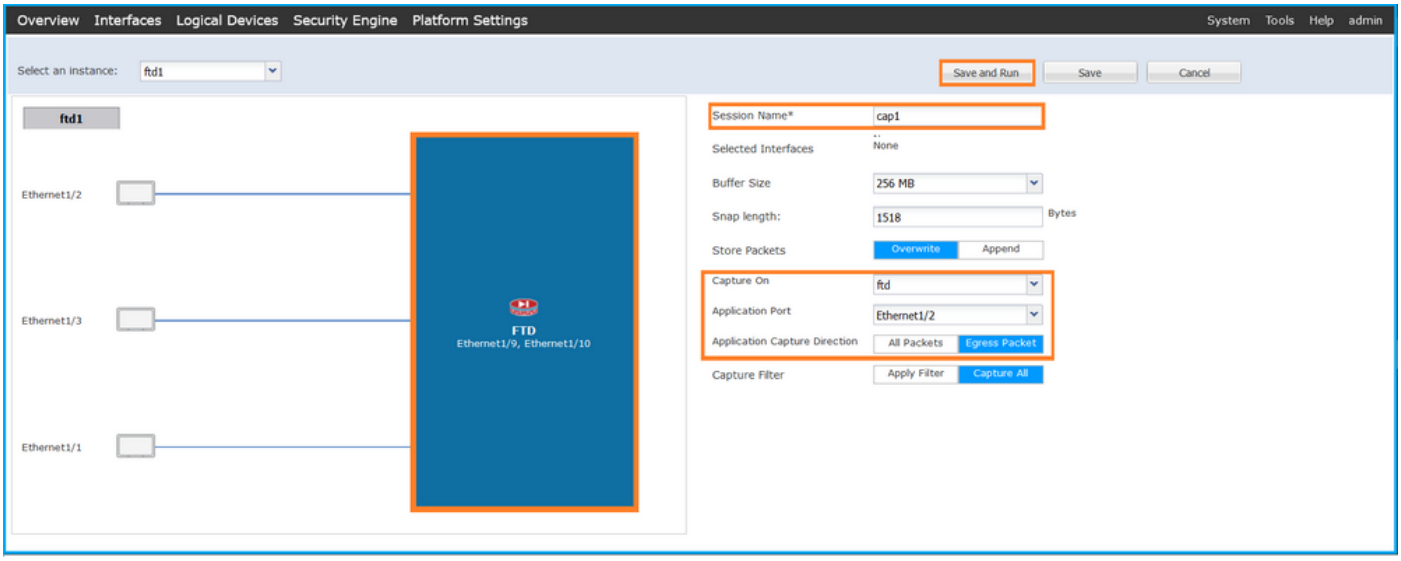
FTDアプリケーションおよびアプリケーションポートEthernet1/2でパケットキャプチャを設定するには、FCMで次の手順を実行します。

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
---------- ---------- ---------- ----------- --------------- -------------- -------------- ---------

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。

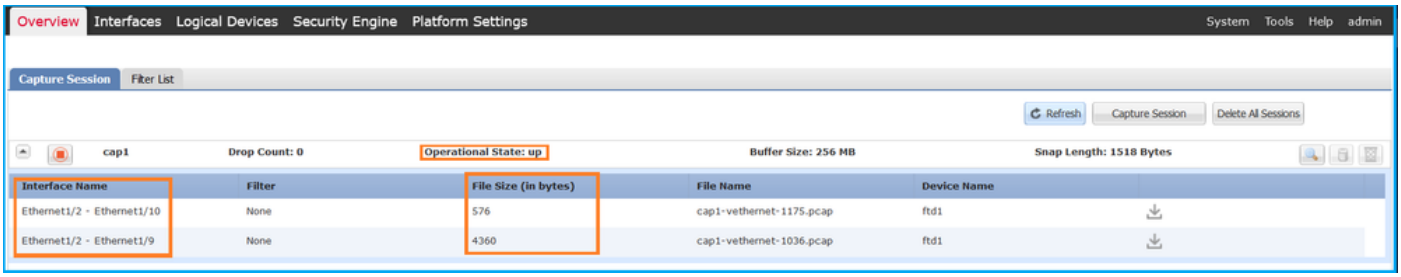
<#root>

```
firepower#
scope packet-capture

firepower /packet-capture #
create session cap1

firepower /packet-capture/session* #
create app-port 1 l12 Ethernet1/2 ftd

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

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

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

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

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

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: l12

Port Name: Ethernet1/2

App Name: ftd
Sub Interface: 0

Application Instance Identifier: ftd1

Application ports resolved to:

Name: vnic1

Eq Slot Id: 1

Eq Port Id: 9

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

Pcapsize: 53640 bytes

Vlan: 102

Filter:

Name: vnic2

Eq Slot Id: 1

Eq Port Id: 10

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

Pcapsize: 1824 bytes

Vlan: 102

Filter:

キャプチャファイルの収集

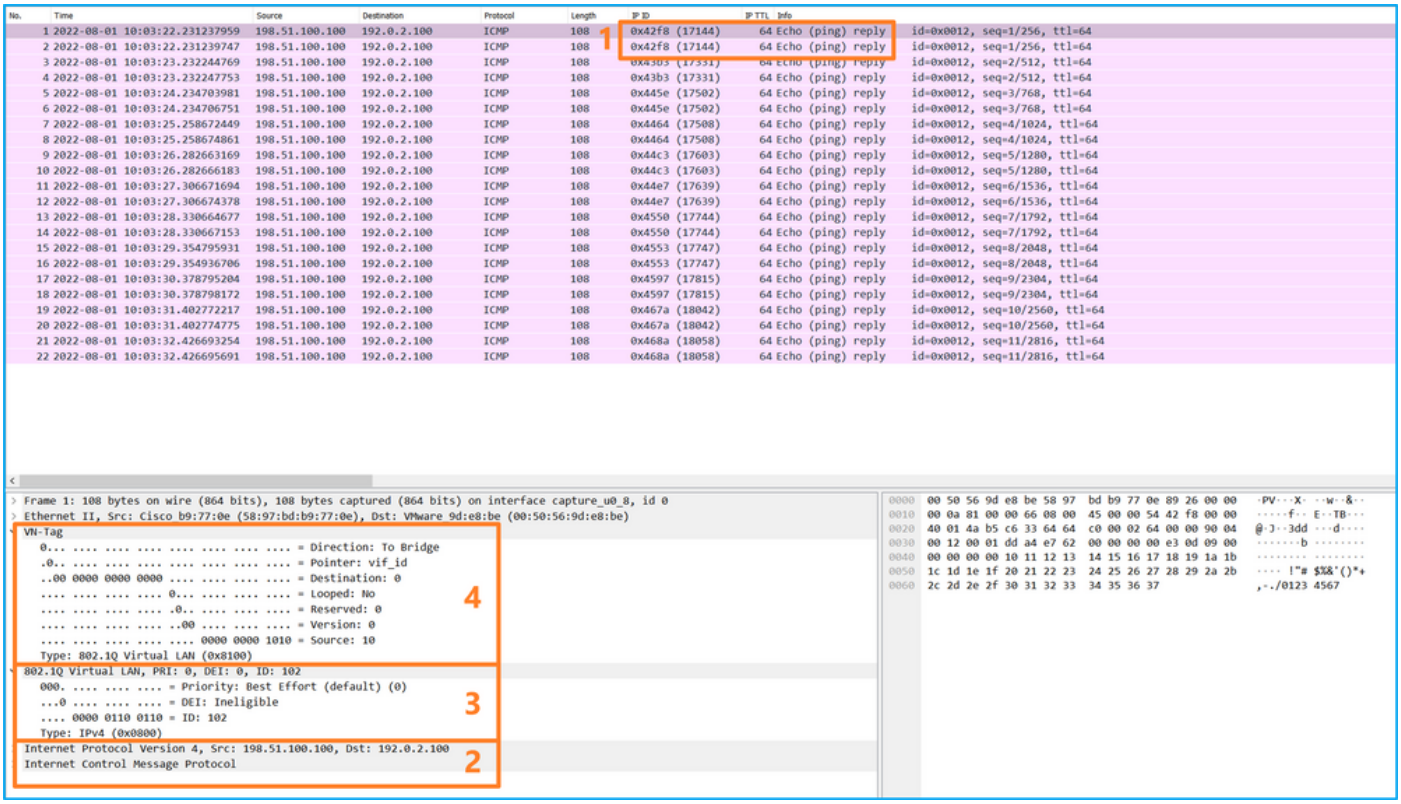
「Firepower 4100/9300内部スイッチキャプチャファイルの収集」セクションの手順を実行します。

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。



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力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

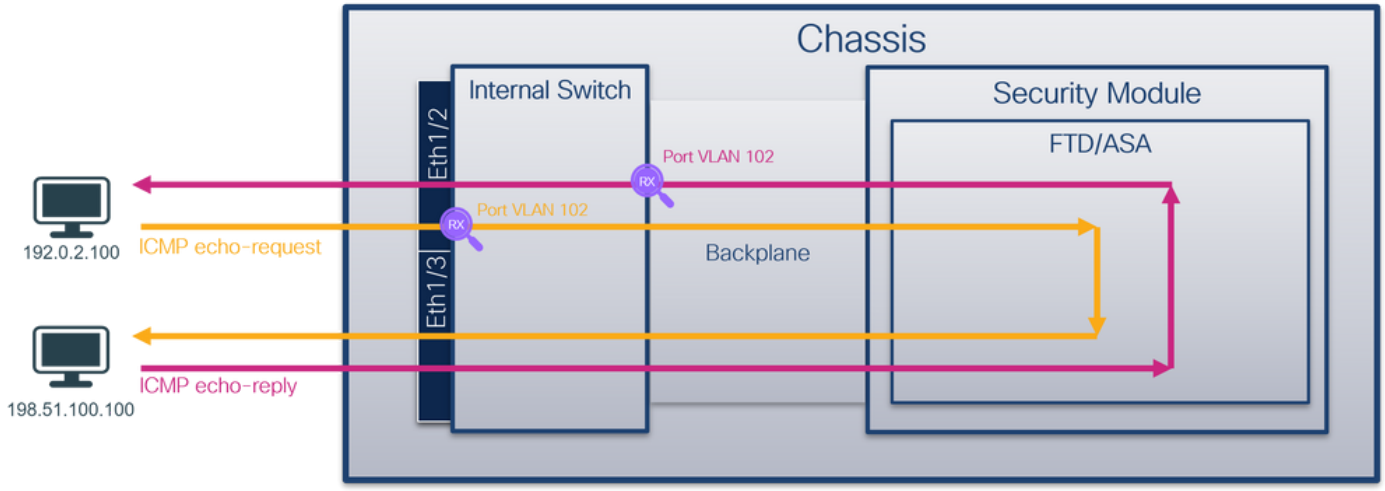
タスク 2

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が出力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

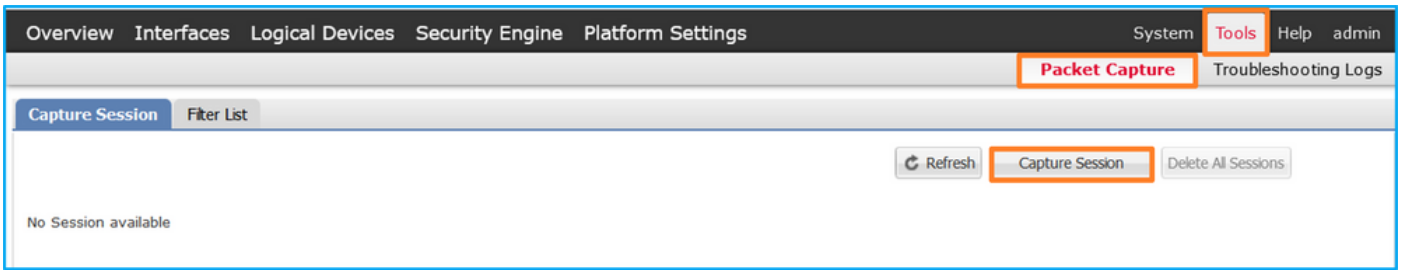


コンフィギュレーション

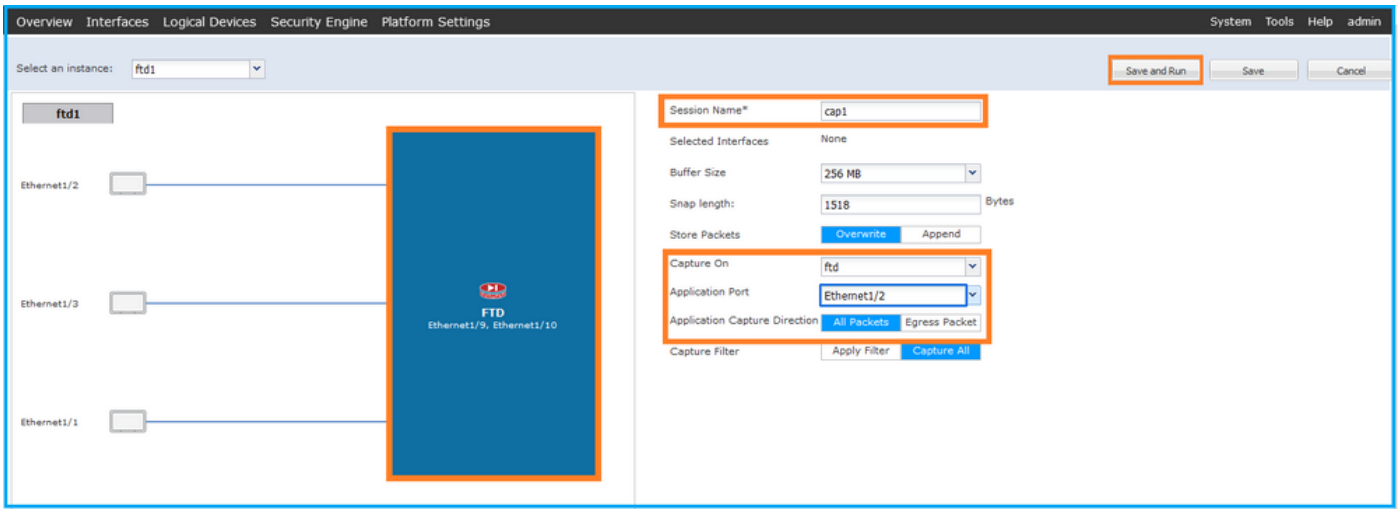
FCM（必須）

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         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。

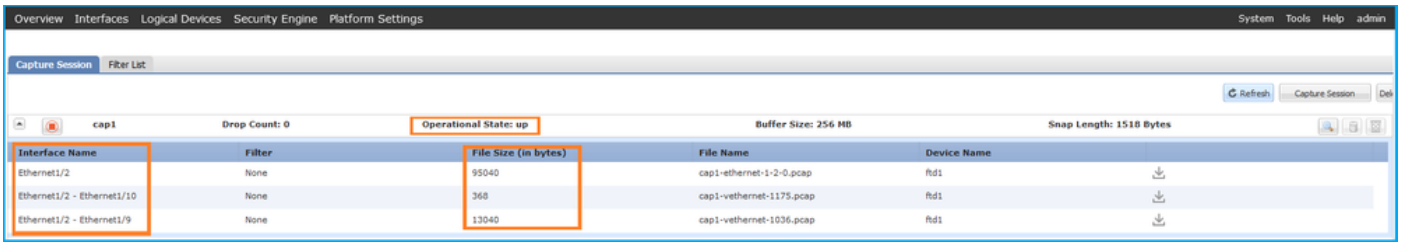
<#root>

```
firepower#
scope packet-capture

firepower /packet-capture #
create session cap1

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

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。



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

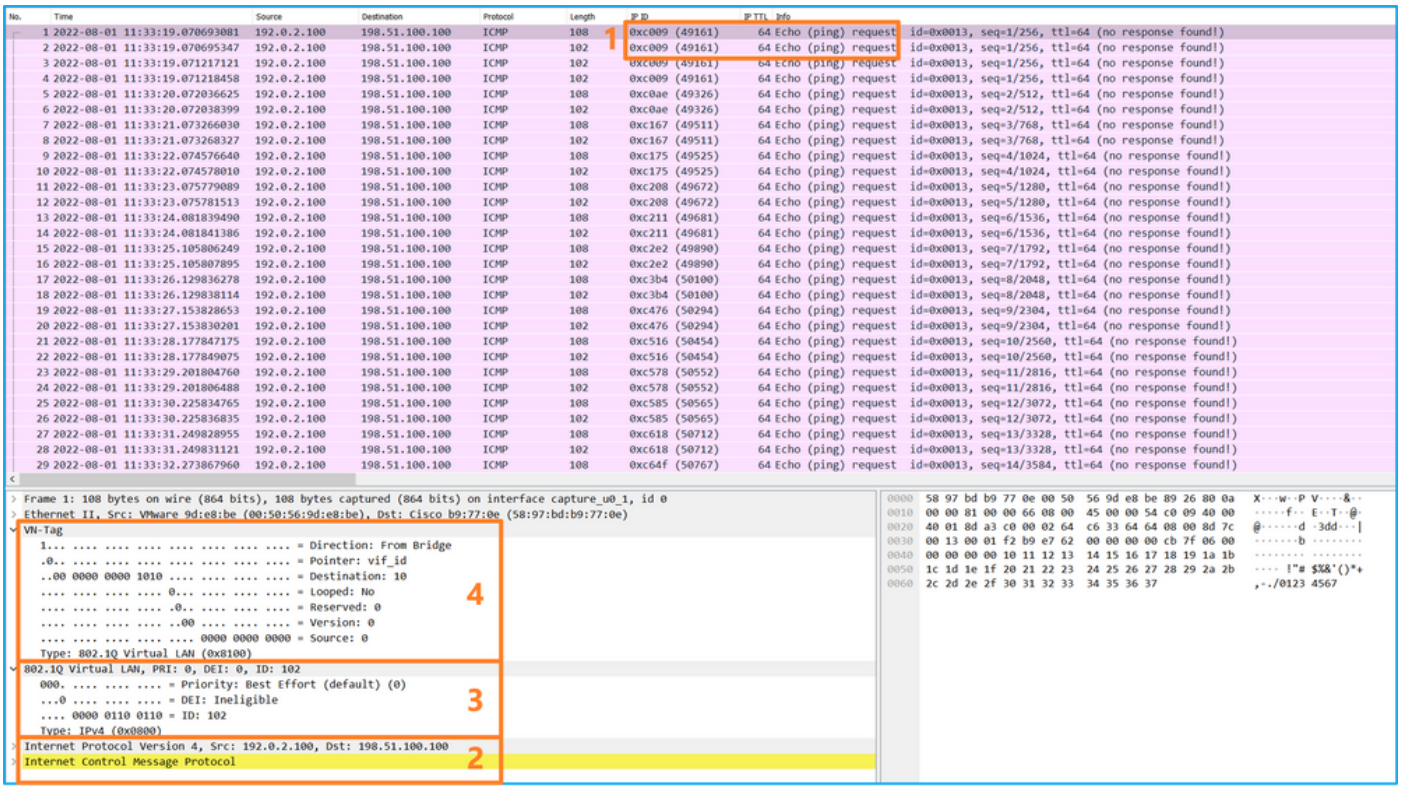
「Firepower 4100/9300内部スイッチキャプチャファイルの収集」セクションの手順を実行します。

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。

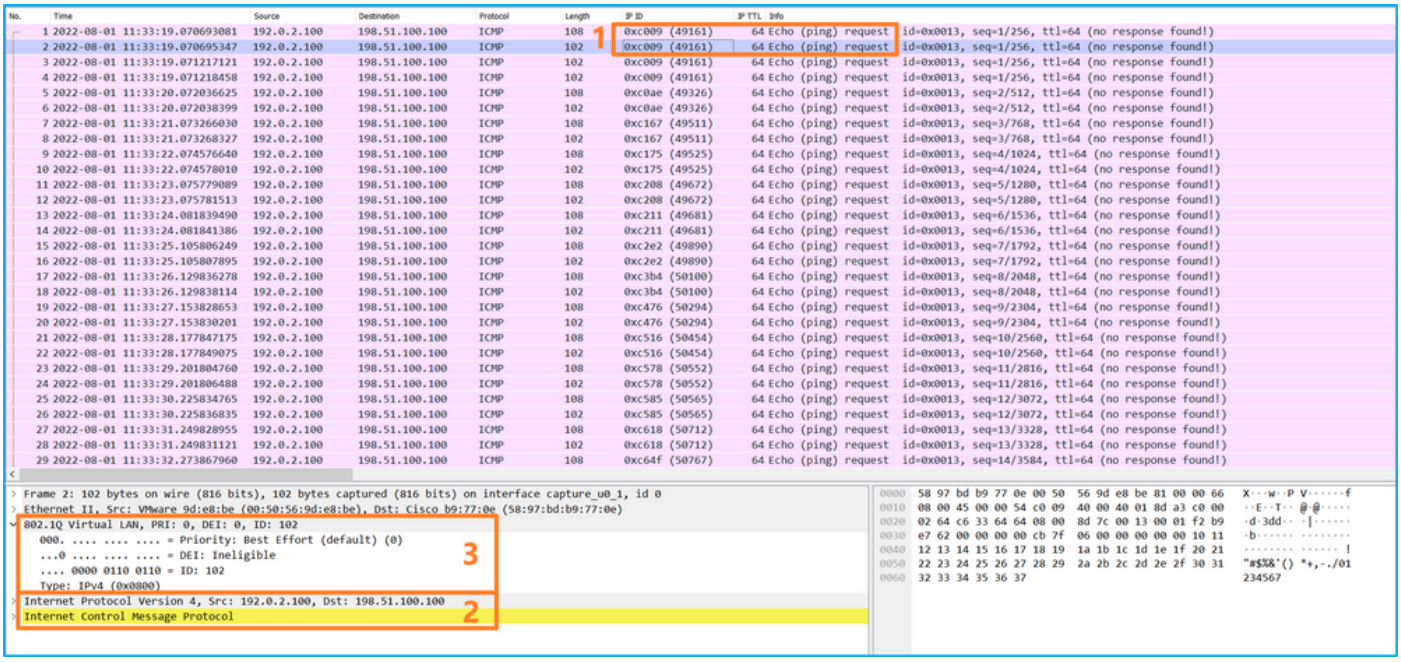
インターフェイスEthernet1/2のキャプチャファイルを開き、最初のパケットを選択してキーポイントを確認します。

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。



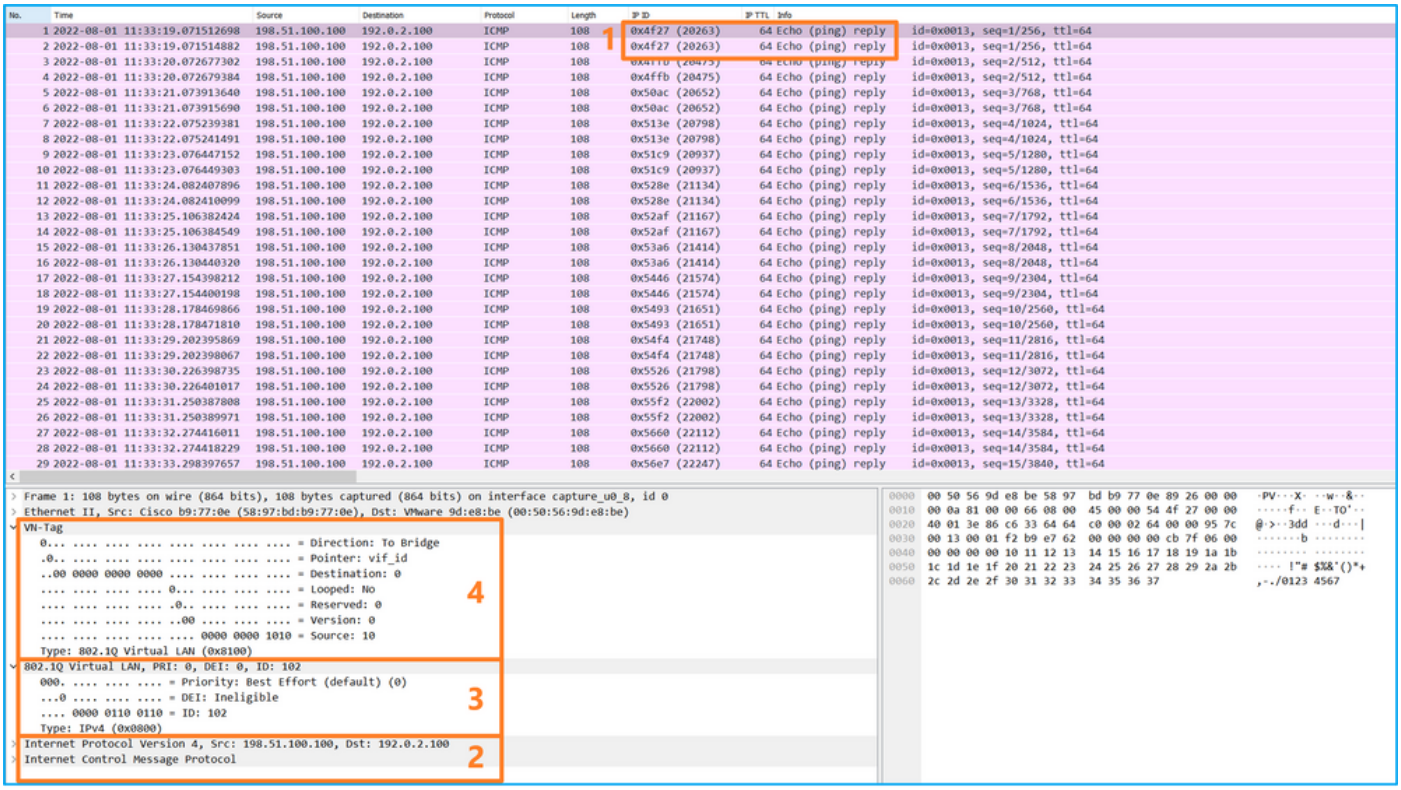
2番目のパケットを選択し、キーポイントを確認します。

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。



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。



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が入力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、出力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。

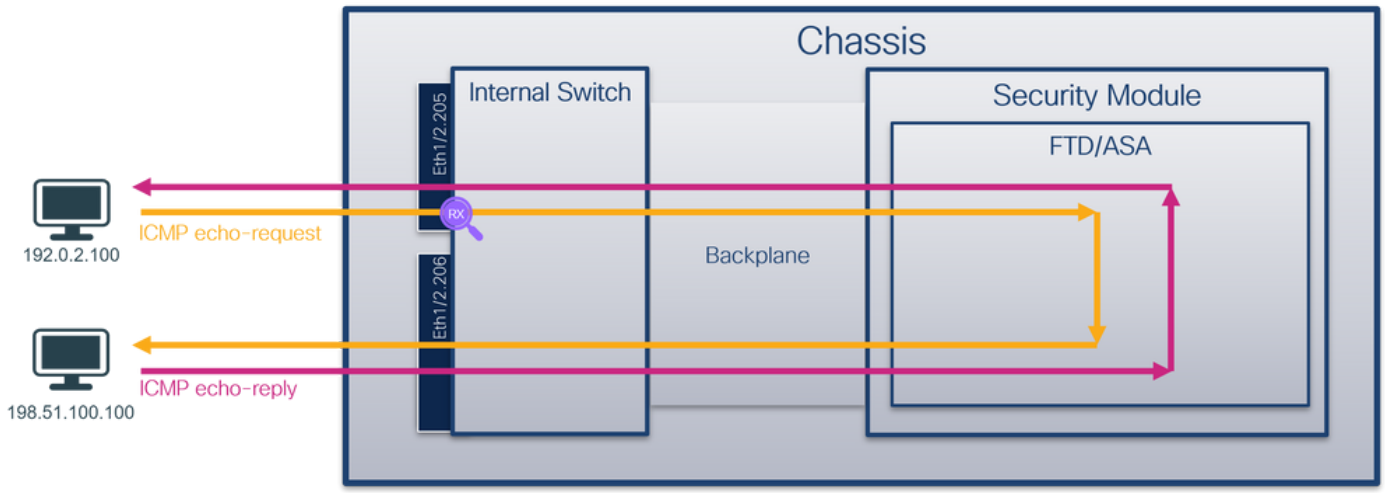
タスクの要約を次の表に示します。

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

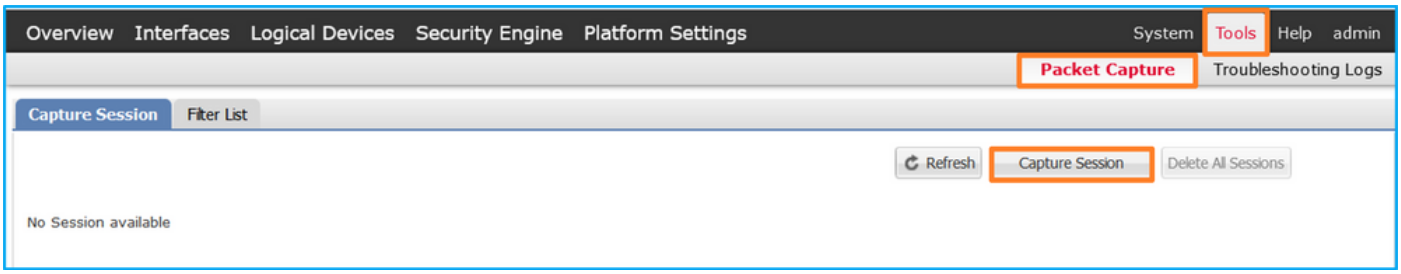


コンフィギュレーション

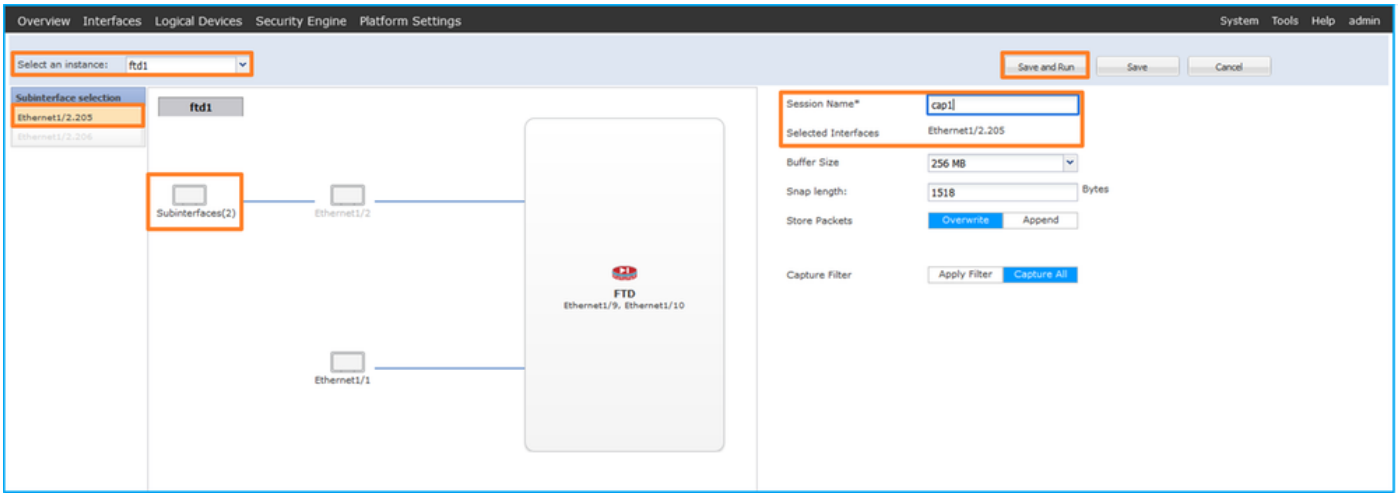
FCM（必須）

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。



3. ポートチャ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

```
       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   Eth1/3(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 #
```

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

```
<#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 #
```

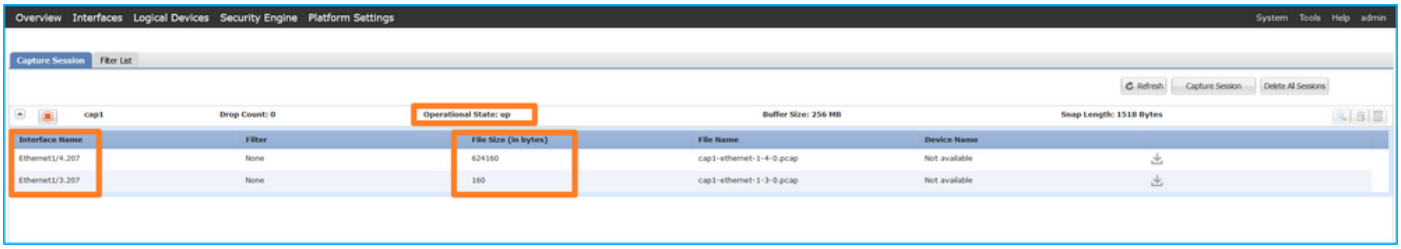
検証

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

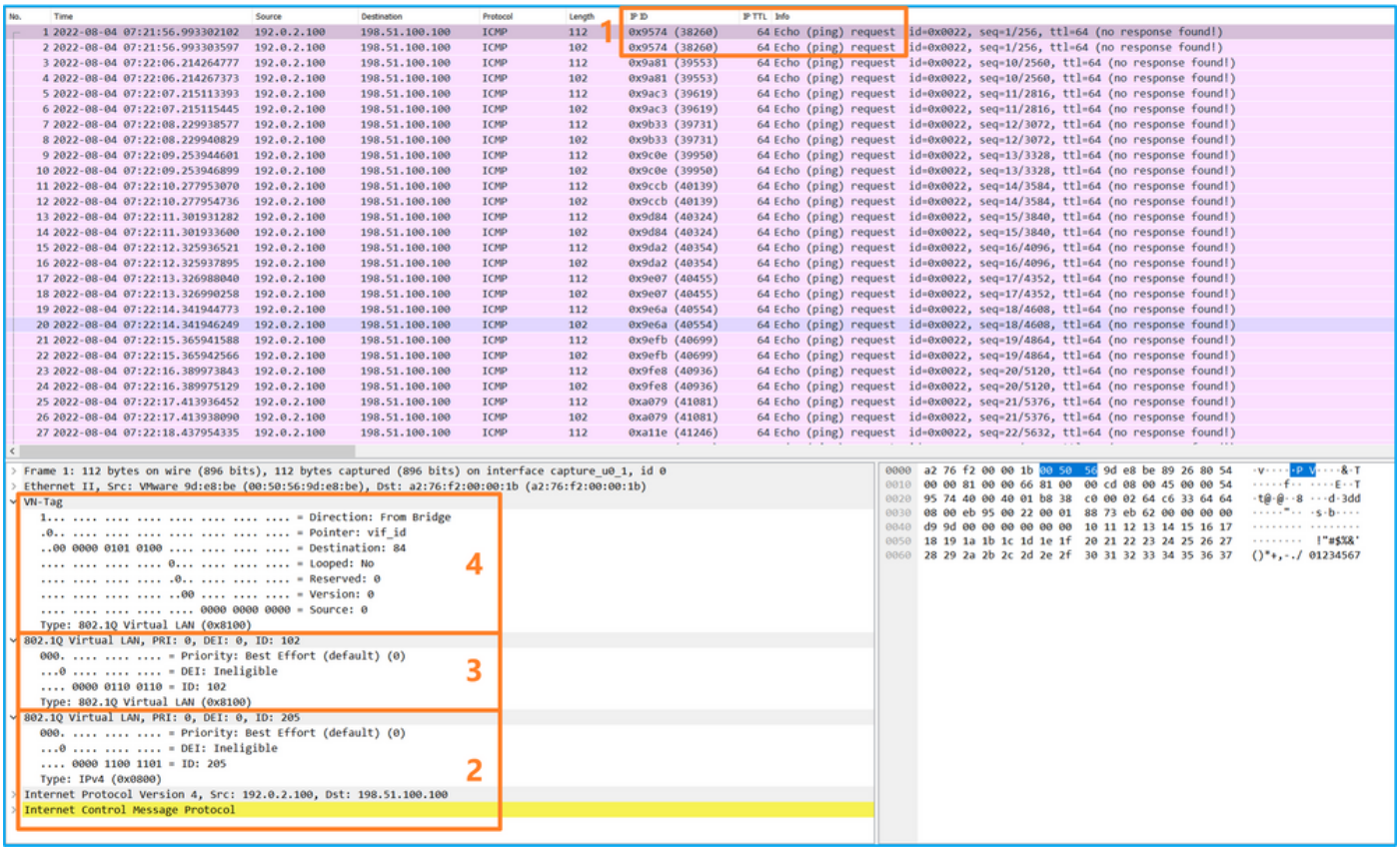
キャプチャファイルの収集

「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

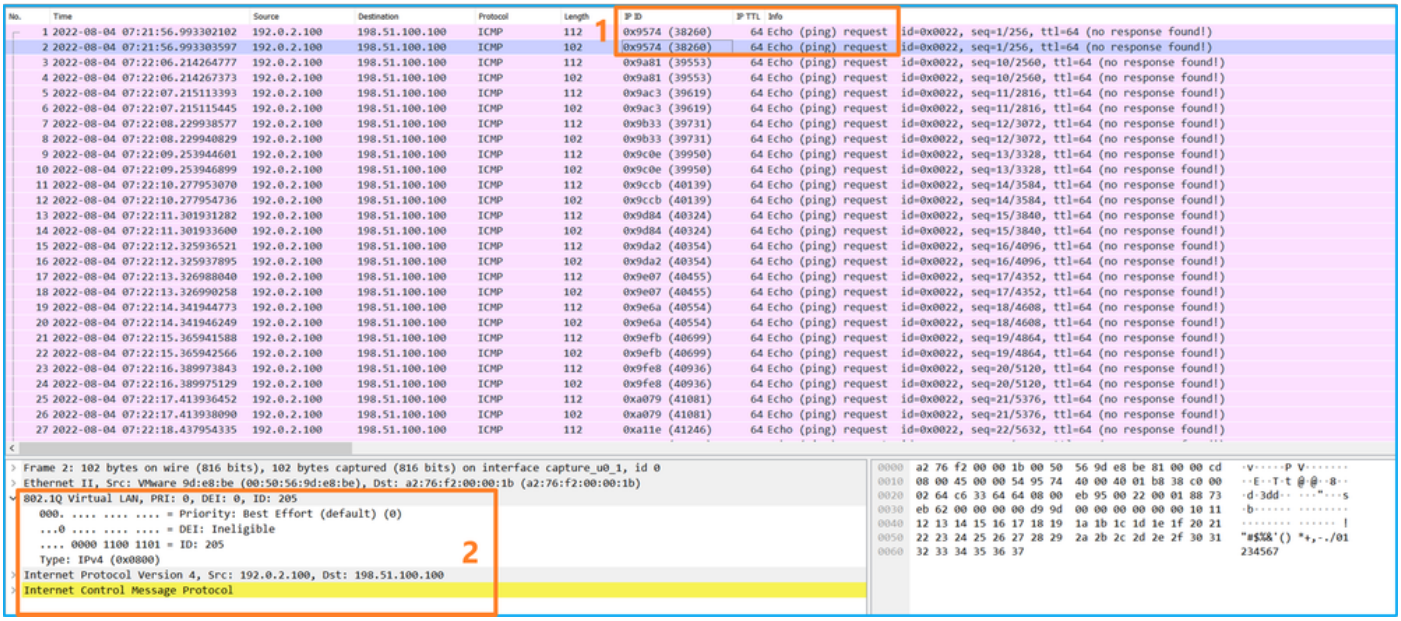
パケットキャプチャファイルリーダーアプリケーションを使用して、キャプチャファイルを開きます。最初のパケットを選択し、キーポイントを確認します。

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。



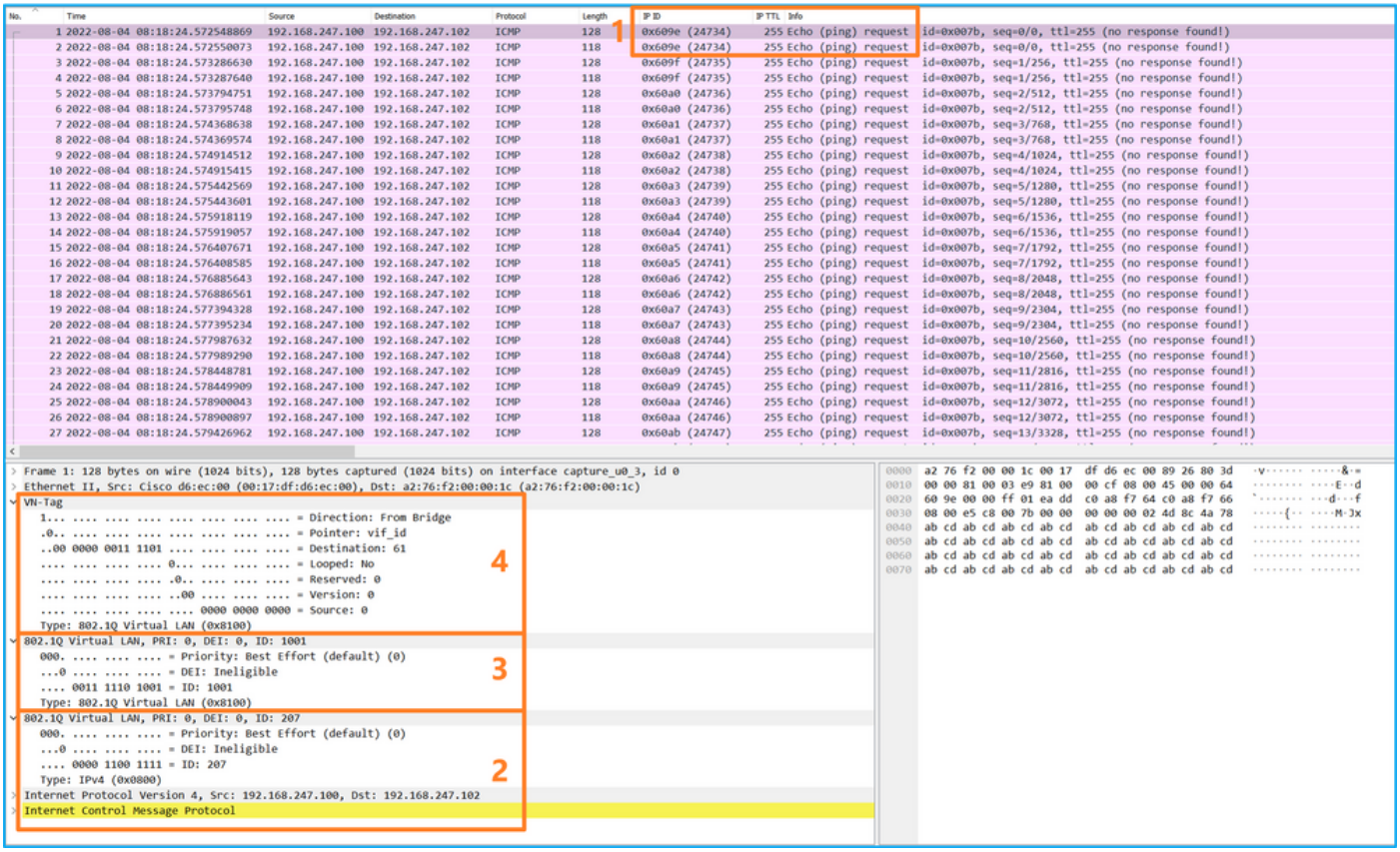
2番目のパケットを選択し、キーポイントを確認します。

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。



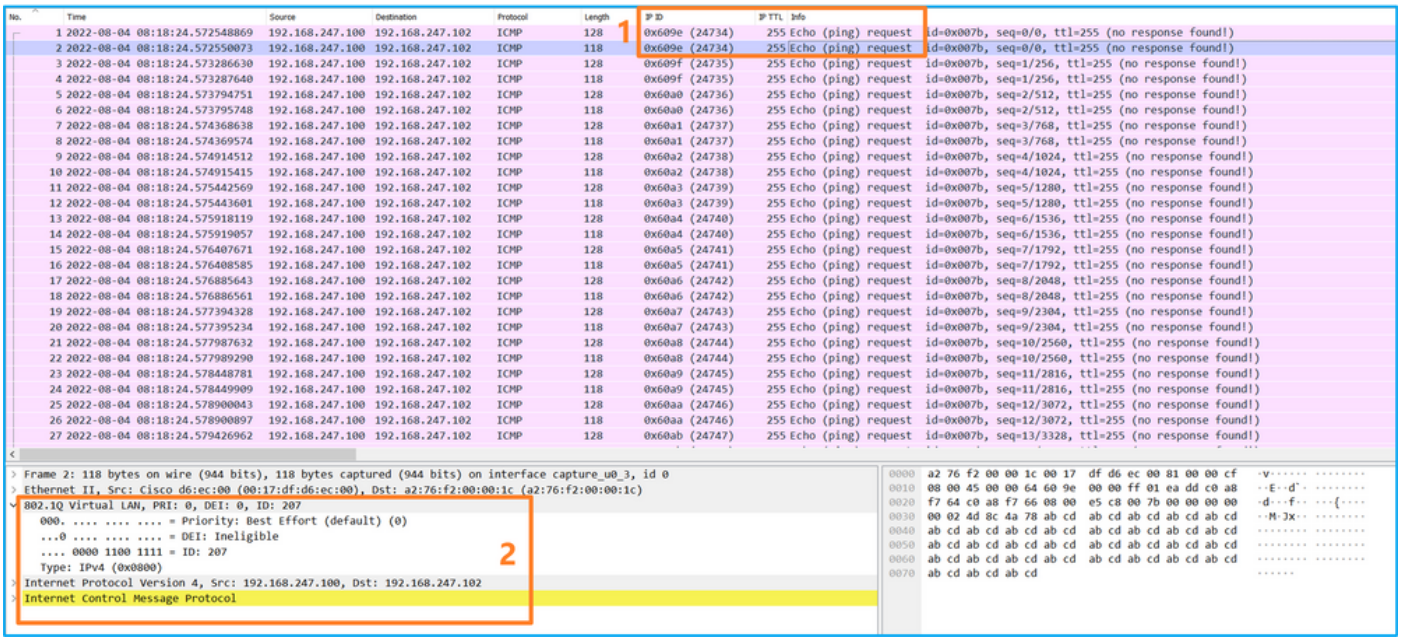
次に、Portchannel1.207のキャプチャファイルを開きます。最初のパケットを選択し、キーポイントを確認します

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。



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。



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。

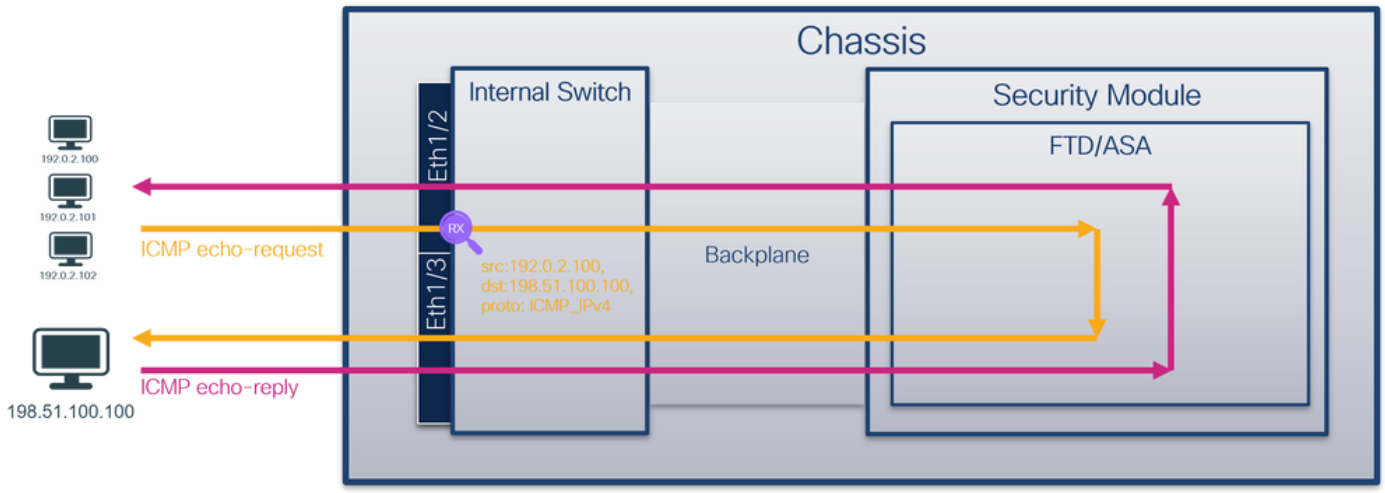
タスク	キャプチャポイント	キャプチャされたパケットの内部ポートVLAN	方向	キャプチャされたトラフィック
サブインターフェイスEthernet1/2.205でのパケットキャプチャの設定と確認	Ethernet1/2.205	102	入力のみ	ホスト192.0.2.100からホスト198.51.100.100へのICMPエコー要求
メンバーインターフェイスEthernet1/3および	Ethernet1/3	1001	入力のみ	192.168.207.100からホスト192.168.207.102へのICMPエコ

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



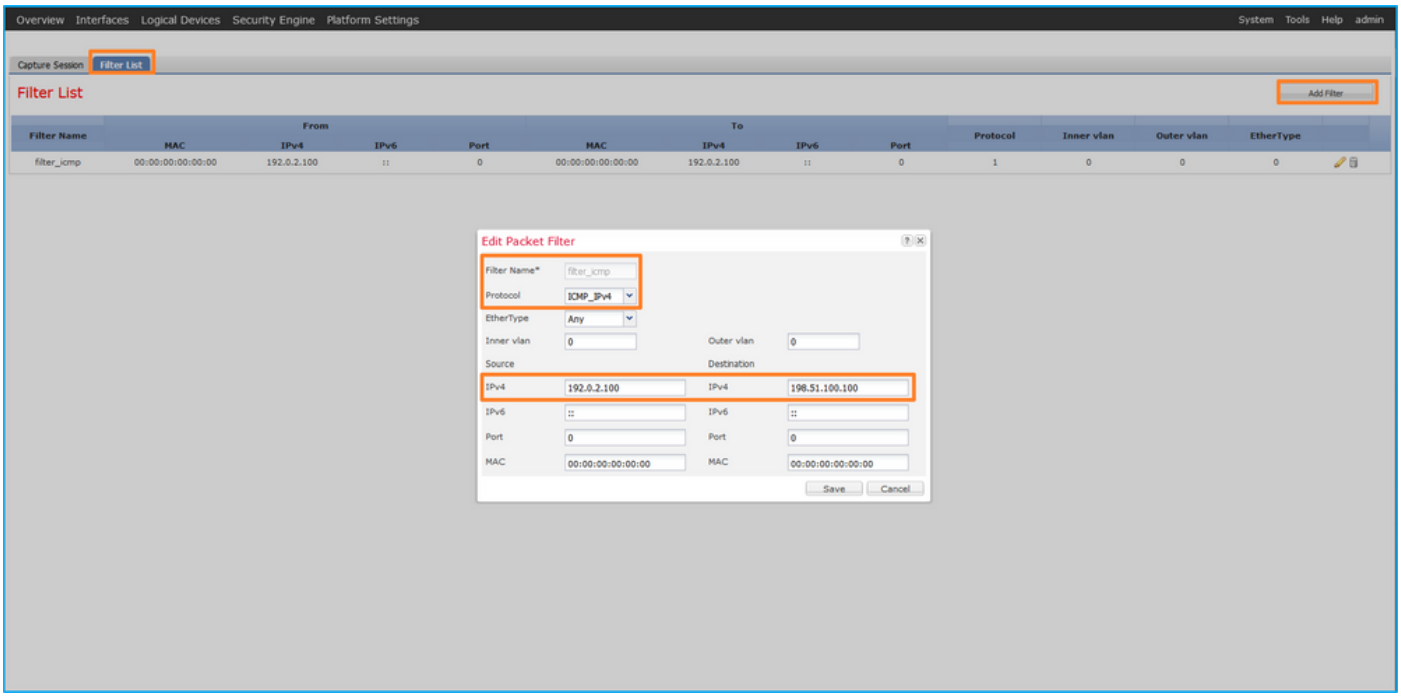
コンフィギュレーション

FCM (必須)

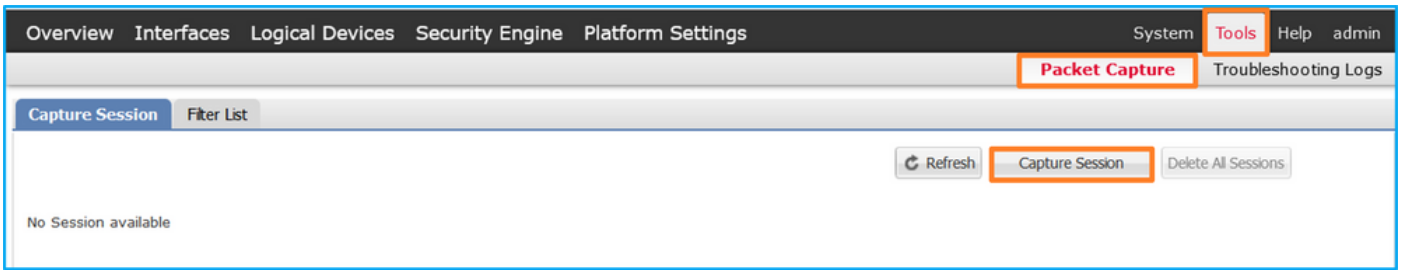
ホスト192.0.2.100からホスト198.51.100.100へのICMPエコー要求パケットのキャプチャフィルタを設定し、インターフェイスEthernet1/2のパケットキャプチャに適用するには、FCMで次の手順を実行します。

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。

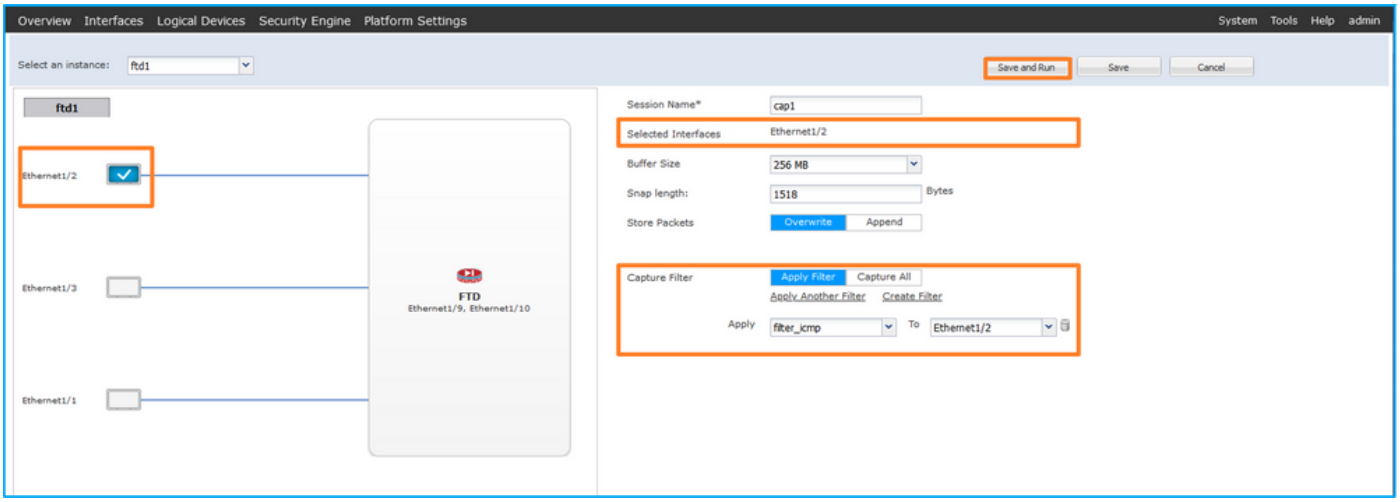
2. フィルタ名、プロトコル、送信元IPv4、宛先IPv4を指定し、Save:をクリックします。



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。

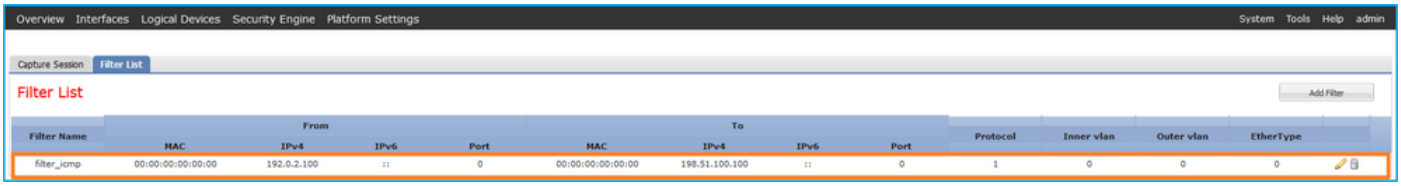
```
<#root>

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 #
```

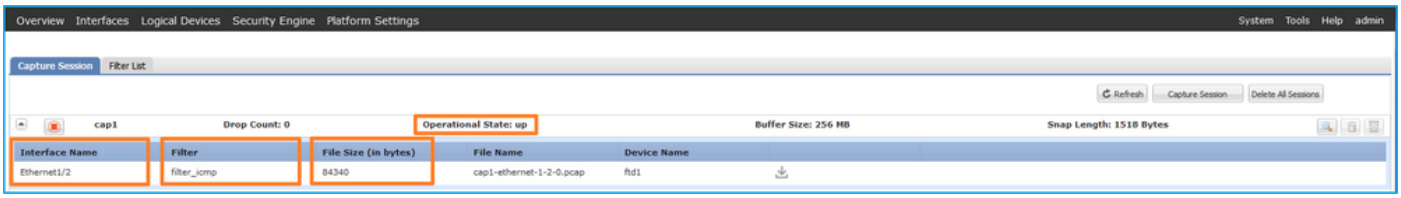
検証

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。



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。



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

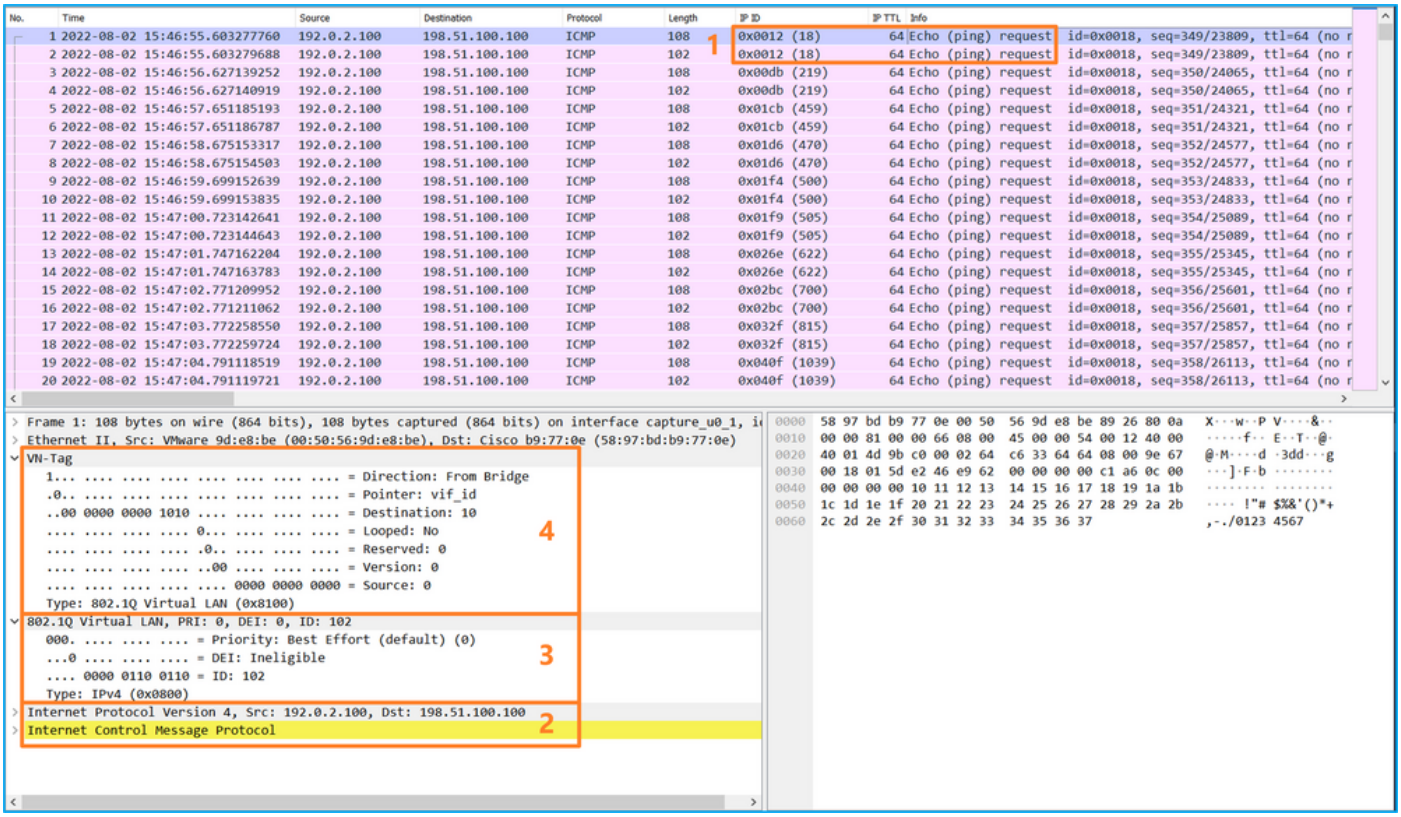
「Firepower 4100/9300内部スイッチキャプチャファイルの収集」セクションの手順を実行します。

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

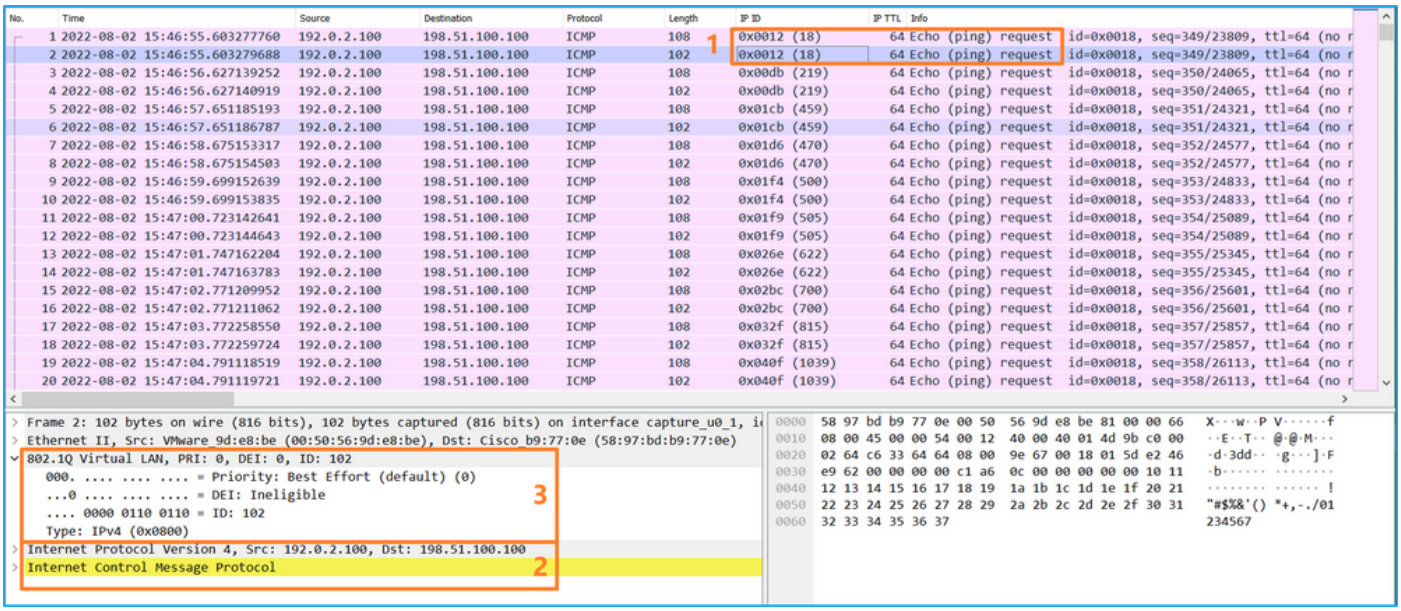
1. ICMPエコー要求パケットだけがキャプチャされます。各パケットは2回取得されて表示され

ます。
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。



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。



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。

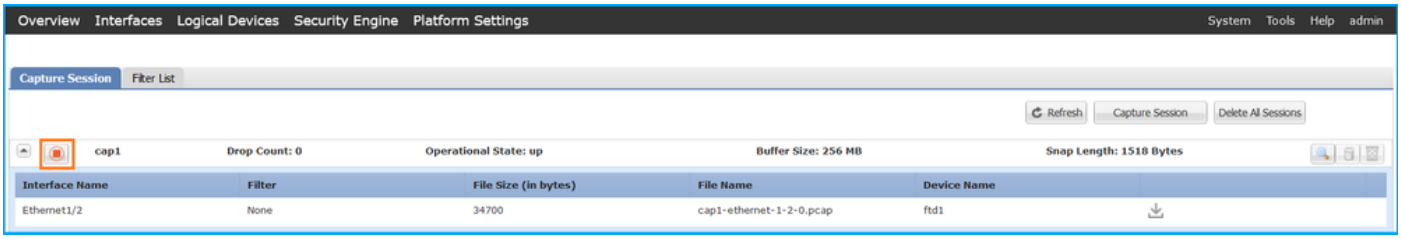
タスク	キャプチャポイント	キャプチャされたパケットの内部ポートVLAN	方向	ユーザフィルタ	キャプチャされたトラフィック
前面インターフェイスEthernet1/2のフィルタを使用したパケットキャプチャの設定と確認	イーサネット1/2	102	入力のみ	プロトコル：ICMP Source:192.0.2.100 Destination:198.51.100.100	ホスト192.0.2.100からホスト198.51.100.100へのICMPエコー要求

Firepower 4100/9300内部スイッチキャプチャファイルの収集

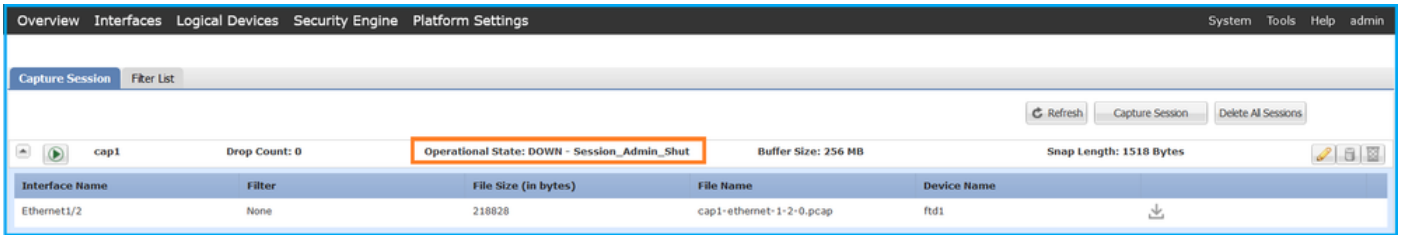
FCM（必須）

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。

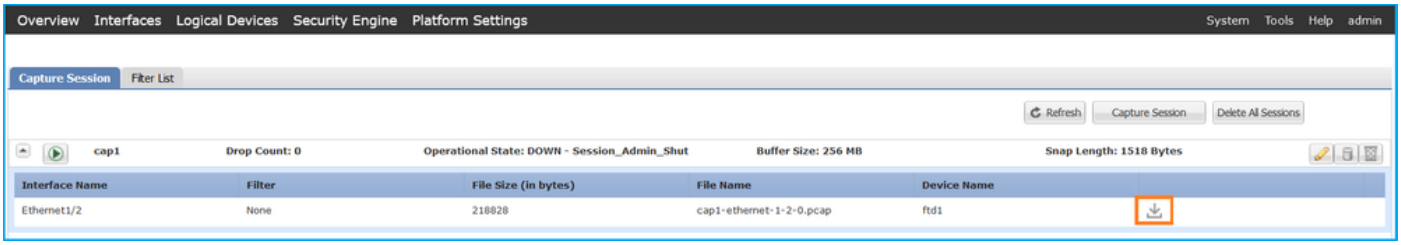
1. Disable Sessionボタンをクリックして、アクティブなキャプチャを停止します。



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://ftpuser@10.10.10.1/cap1-ethernet-1-2-0.pca

Password:
```

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

内部スイッチのパケット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、廃棄カウント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
```

2. イーサネットフレームのEtherTypeを指定します。デフォルトのEtherTypeはIPです。ethernet-typeオプションの値は、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。

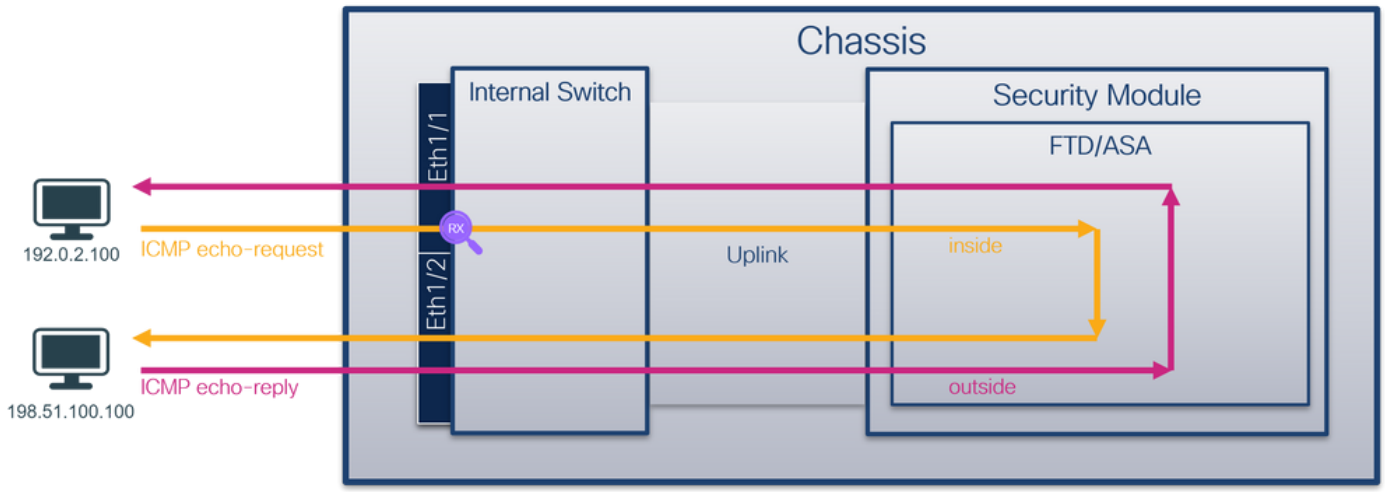
これらのシナリオでは、Secure Firewall 3100/4200内部スイッチのキャプチャの一般的な使用例を取り上げています。

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

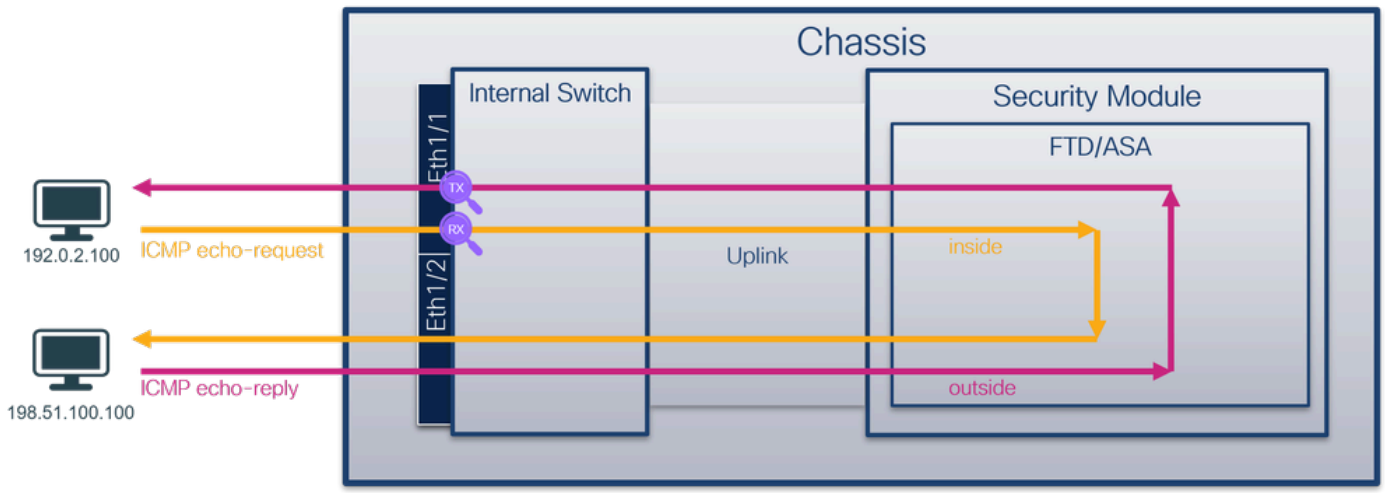
FTDまたはASA CLIを使用して、インターフェイスEthernet1/1またはPortchannel1インターフェイスのパケットキャプチャを設定および確認します。どちらのインターフェイスもnameifはinsideです。

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

Total Physical breakout ports involved in Packet Capture: 0

79 packets captured on disk using switch capture


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

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。

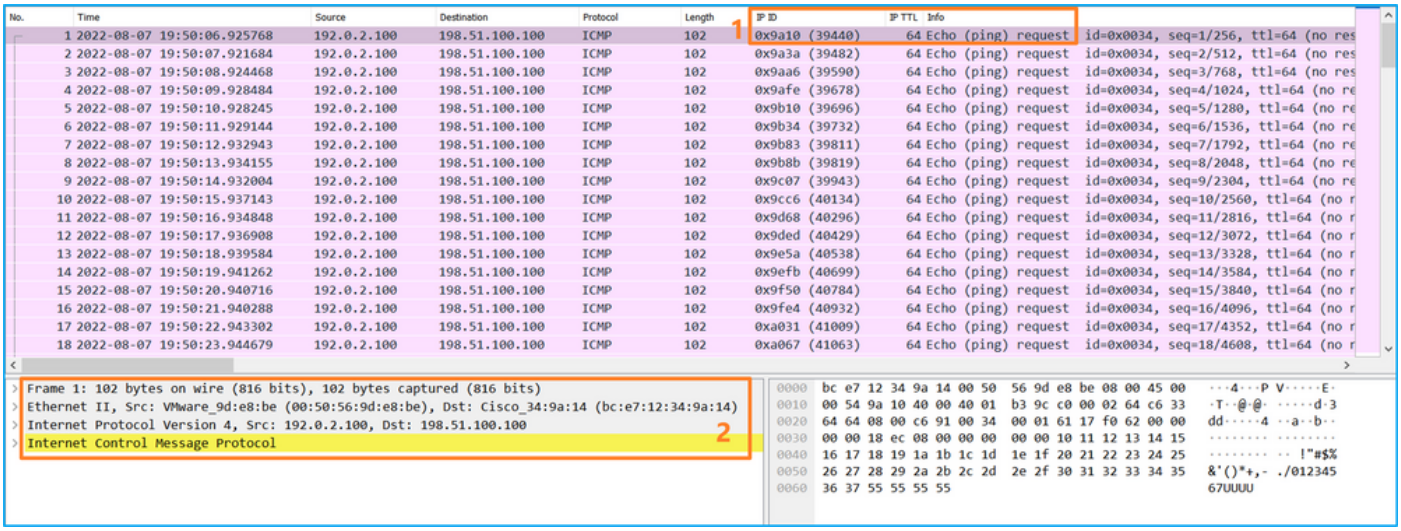
キャプチャファイルの収集

「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

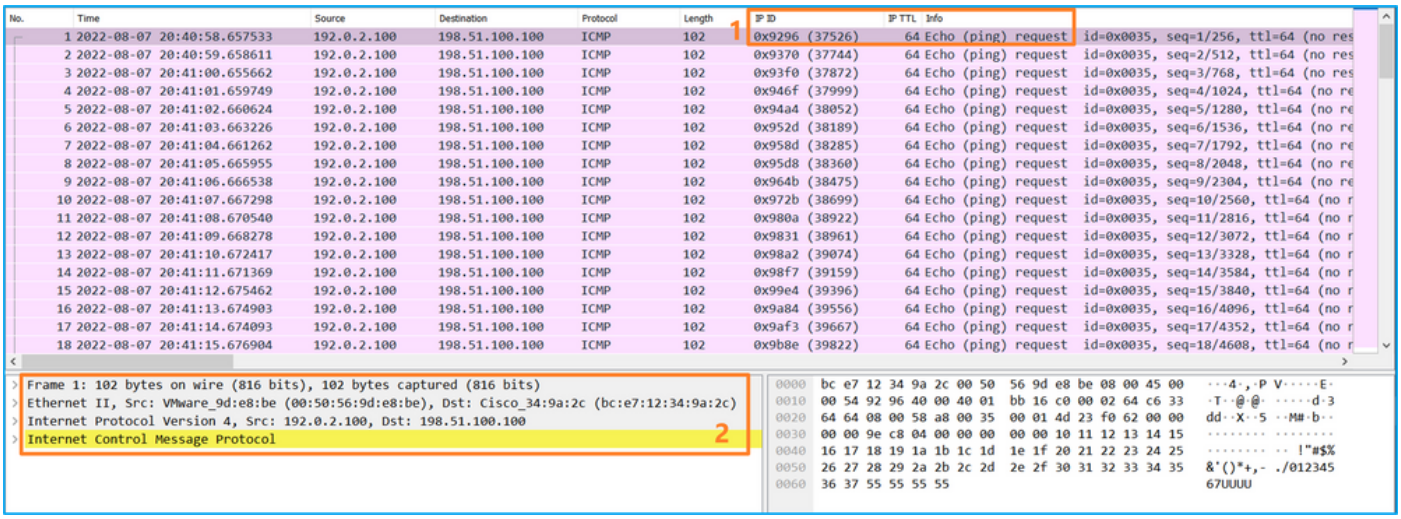
パケットキャプチャファイルリーダーアプリケーションを使用して、Ethernet1/1のキャプチャファイルを開きます。この例では、Secure Firewall 3100でのパケットキャプチャが分析されます。最初のパケットを選択し、キーポイントを確認します。

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。



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。



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

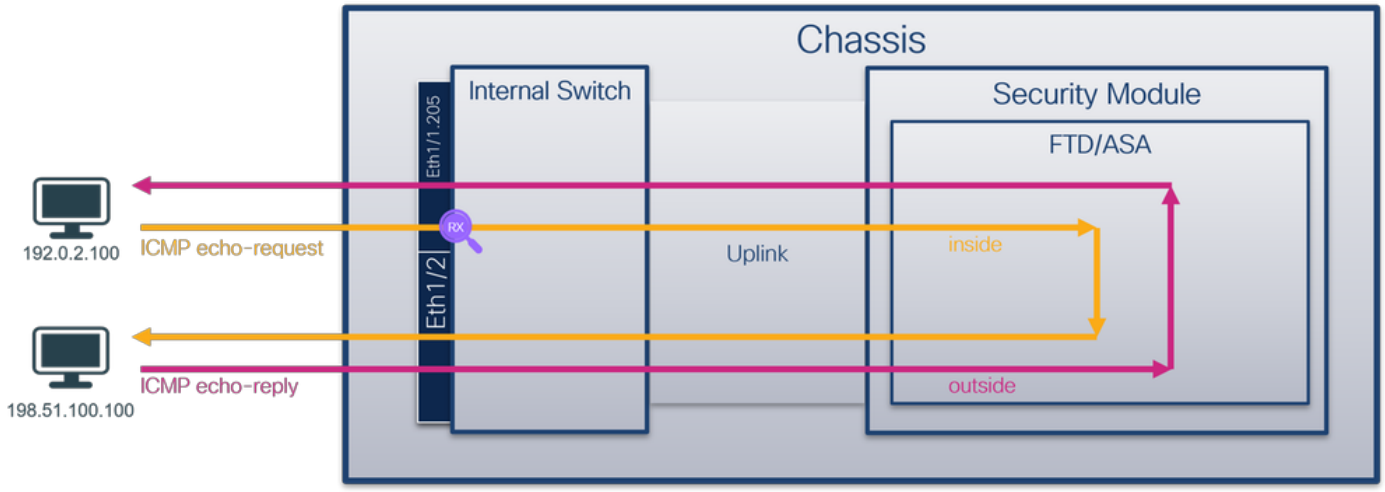
* 3100とは異なり、セキュアファイアウォール4200は双方向（入力および出力）キャプチャをサポートします。

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

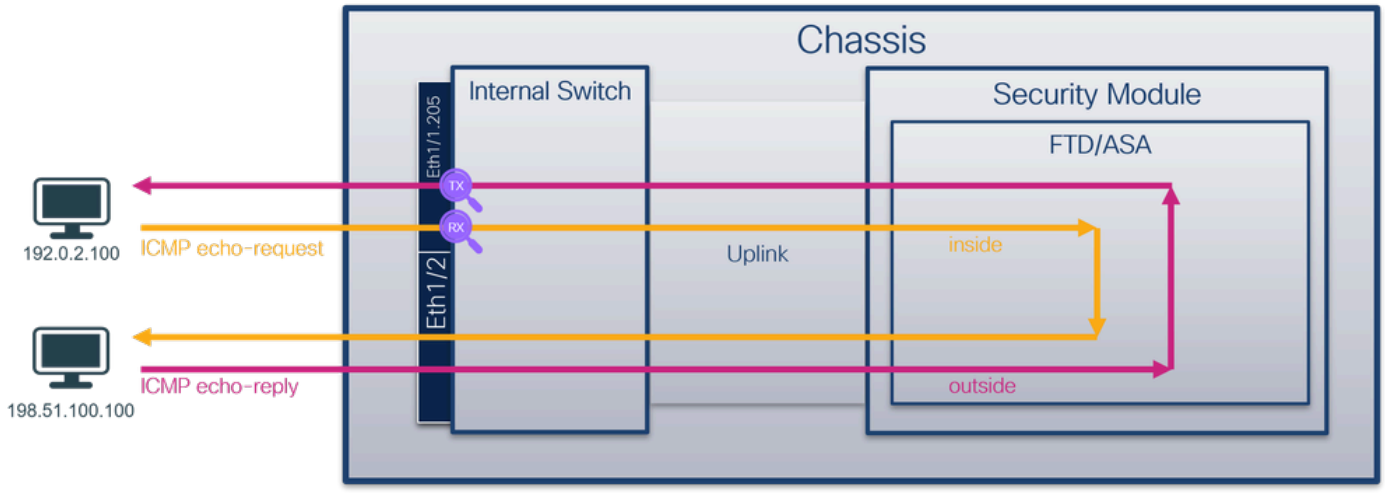
FTDまたはASA CLIを使用して、サブインターフェイスEthernet1/1.205またはPortchannel1.205上のパケットキャプチャを設定および確認します。どちらのサブインターフェイスもnameifはinsideです。

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-       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、このコマンドを管理コンテキストで実行します。

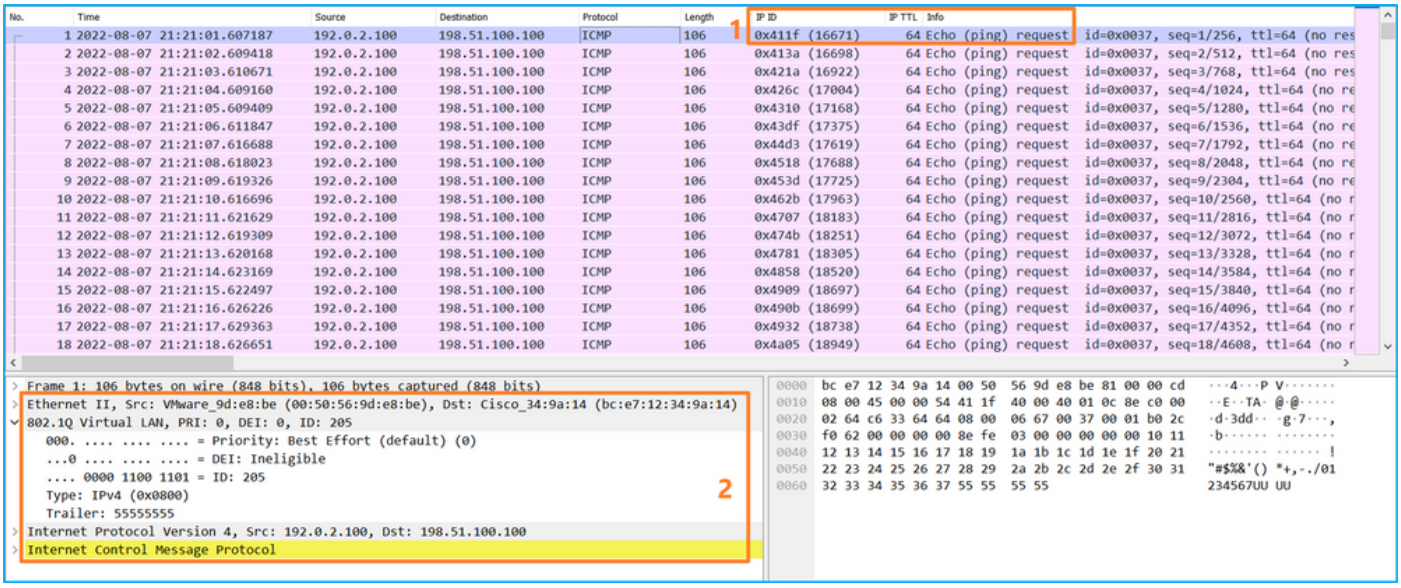
キャプチャファイルの収集

「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

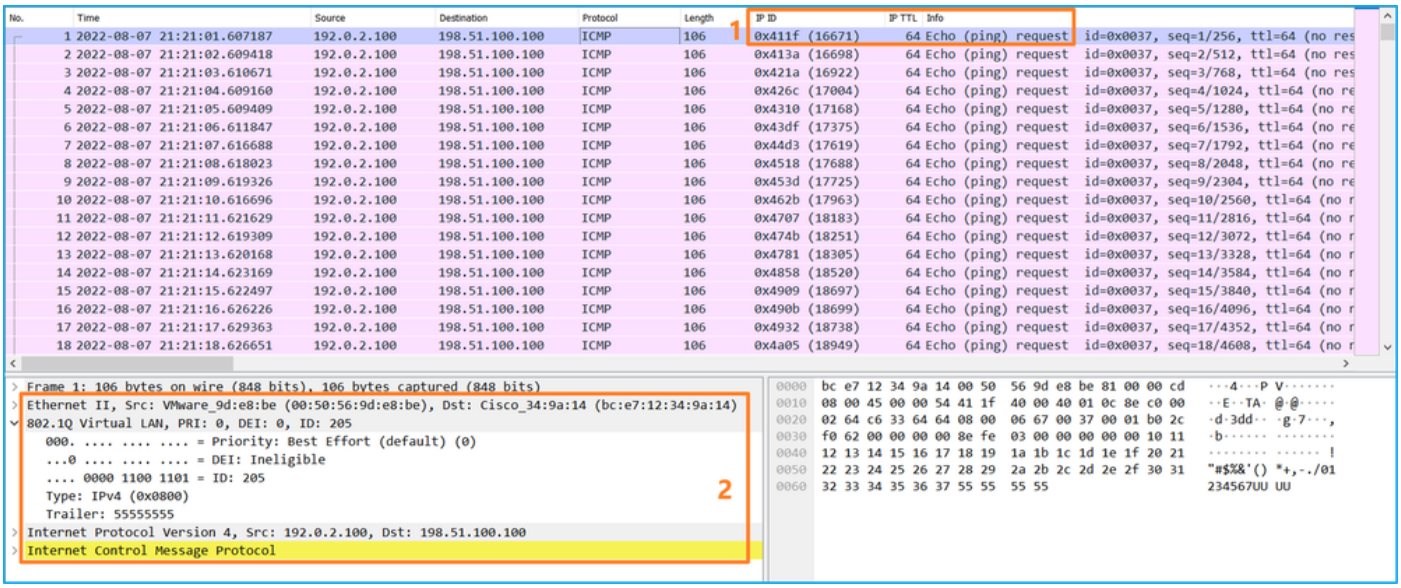
パケットキャプチャファイルリーダーアプリケーションを使用して、Ethernet1/1.205のキャプチャファイルを開きます。この例では、Secure Firewall 3100でのパケットキャプチャが分析されます。最初のパケットを選択し、キーポイントを確認します。

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。



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。

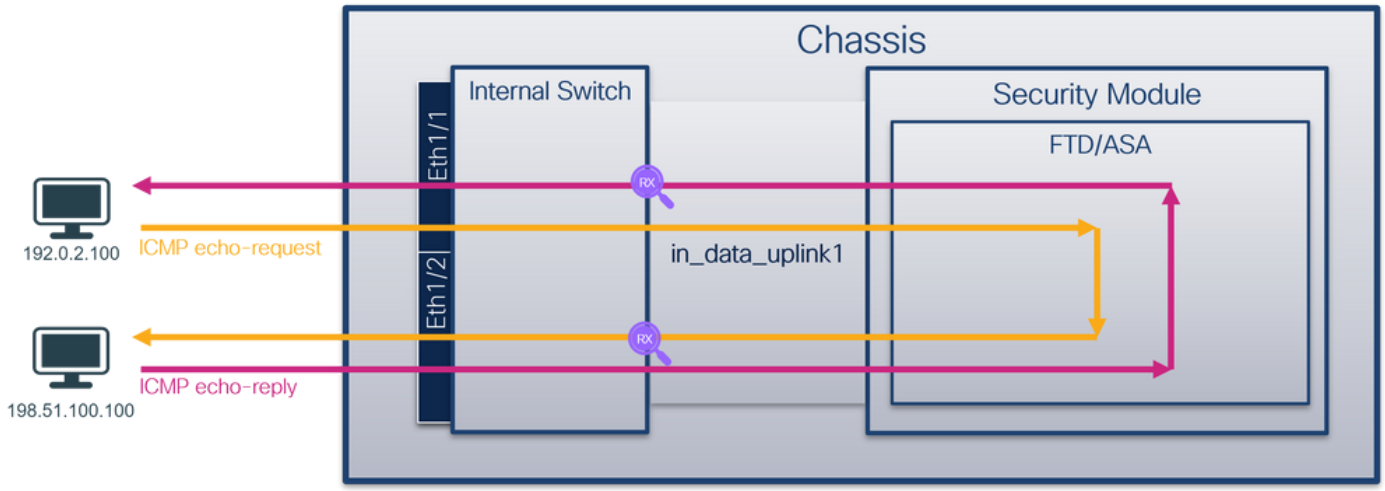
- in_data_uplink1およびin_data_uplink2（4245のみ）：これらのインターフェイスは、アプリケーションを内部スイッチに接続します。4245の場合、パケットは2つのアップリンクインターフェイス間でロードバランスされます。
- in_mgmt_uplink1およびin_mgmt_uplink2 – これらのインターフェイスは、FMCとFTD間の管理インターフェイス（またはsftunnelとも呼ばれる）へのSSHなどの管理接続のための専用パケットパスを提供します。セキュアファイアウォール4200は、2つの管理インターフェイスをサポートしています。

タスク 1

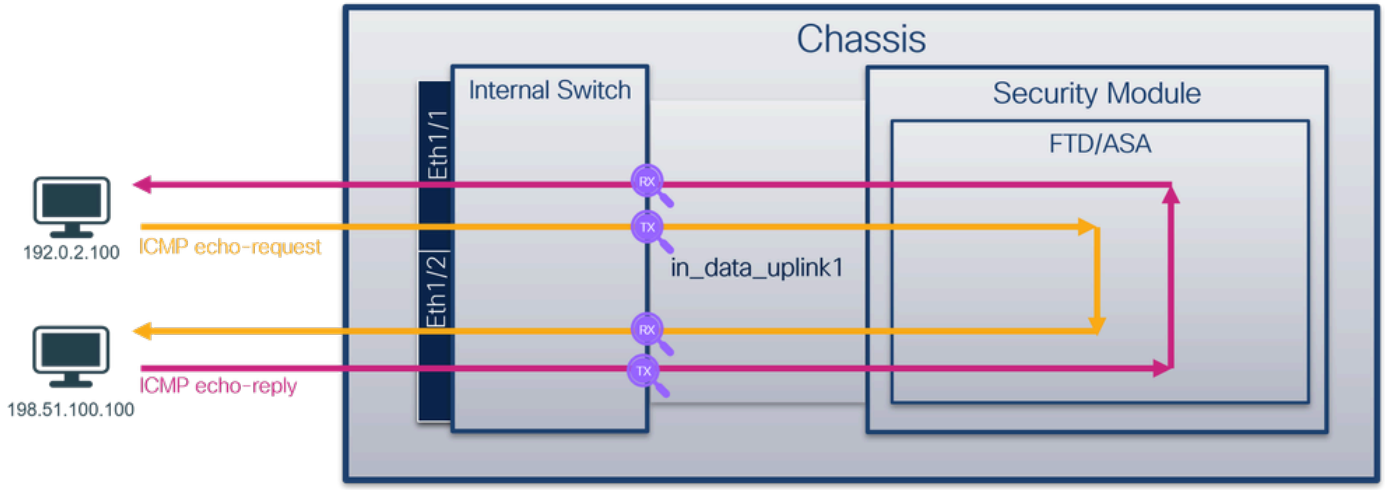
FTDまたはASA CLIを使用して、アップリンクインターフェイスin_data_uplink1上のパケットキャプチャを設定および確認します。

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
```

```
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。

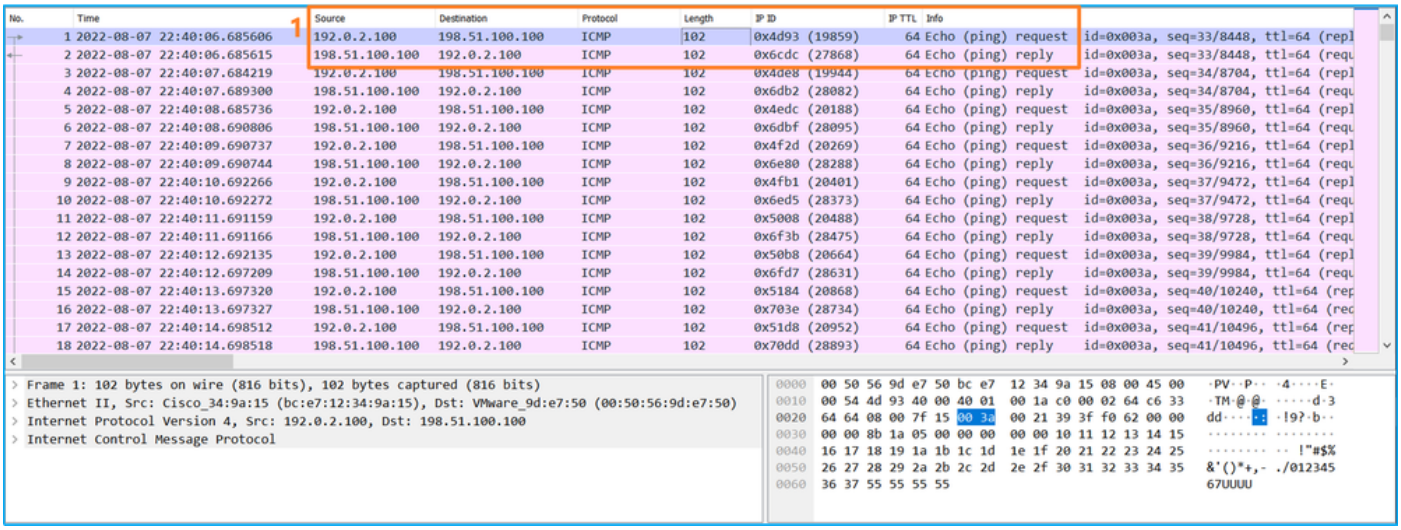
キャプチャファイルの収集

「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、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。



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

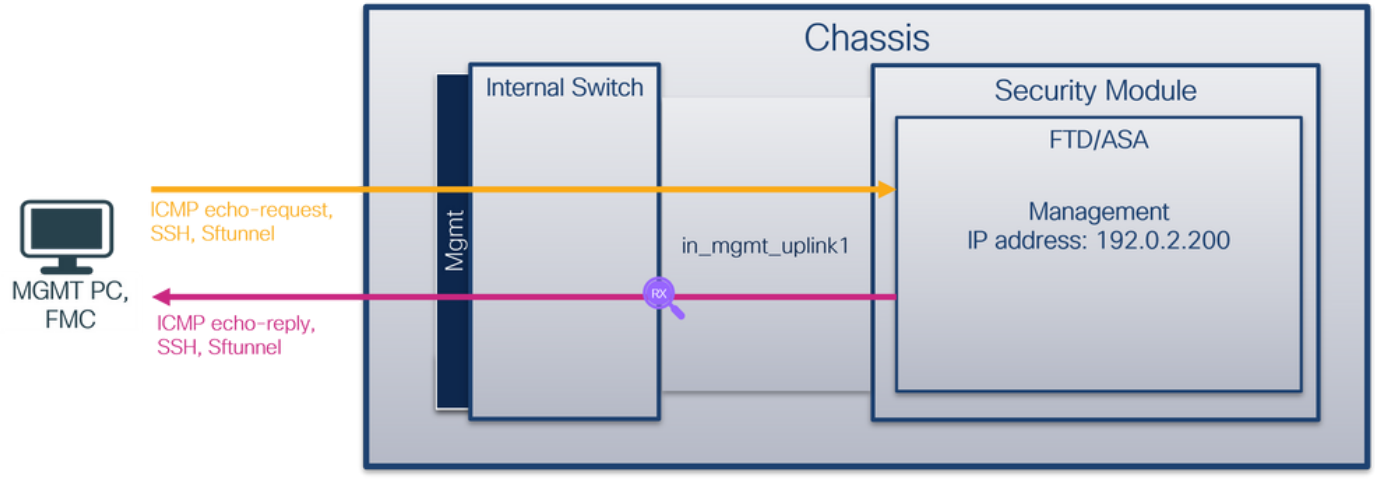
* 3100とは異なり、セキュアファイアウォール4200は双方向（入力および出力）キャプチャをサポートします。

タスク 2

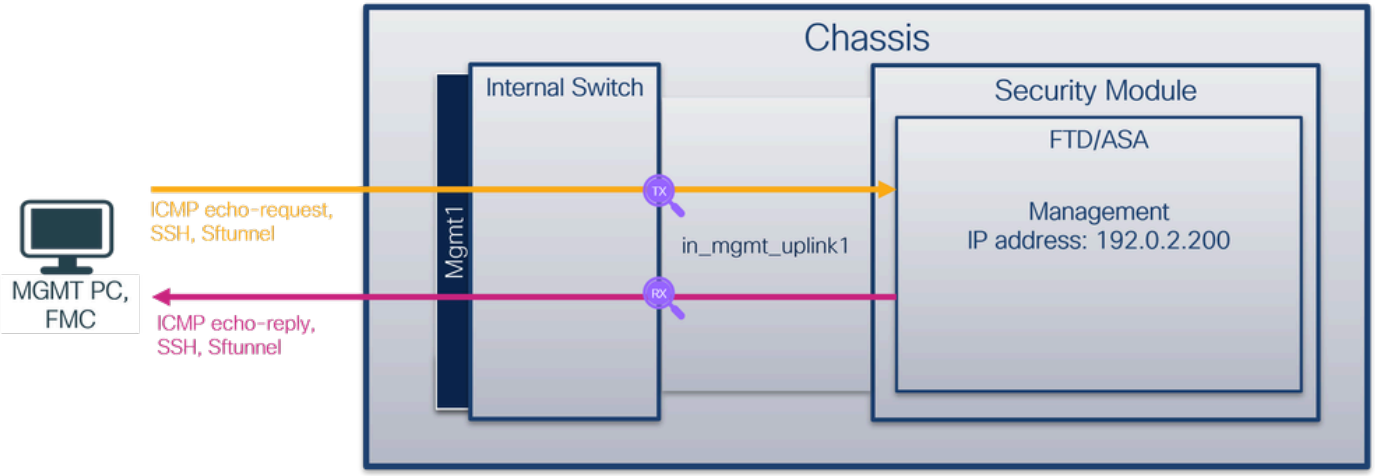
FTDまたはASA CLIを使用して、アップリンクインターフェイスin_mgmt_uplink1上のパケットキャプチャを設定および確認します。管理プレーン接続のパケットだけがキャプチャされます。

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コマンドシェルの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。

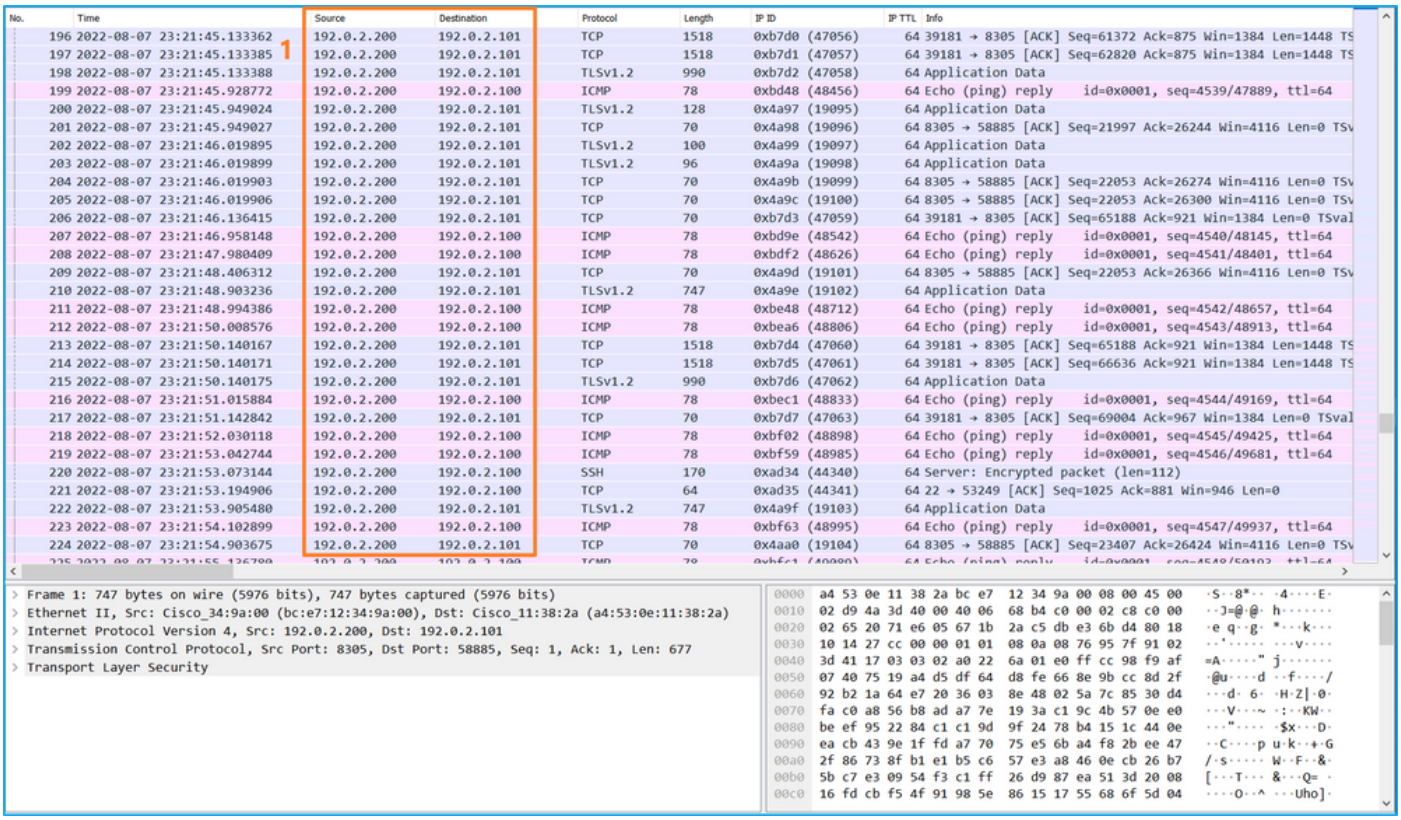
キャプチャファイルの収集

「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。



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
管理アップリンクインターフェイスでのパケットキャプチャの設定と確認	in_mgmt_uplink1	なし	入力のみ* （管理インターフェイスから内部スイッチ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:              capsw-1-1



Protocol:          1


  Ivlan:             0
  Ovlan:             0


Src Ip:            198.51.100.100


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

Total Physical breakout ports involved in Packet Capture: 0

0 packets captured on disk using switch capture

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

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

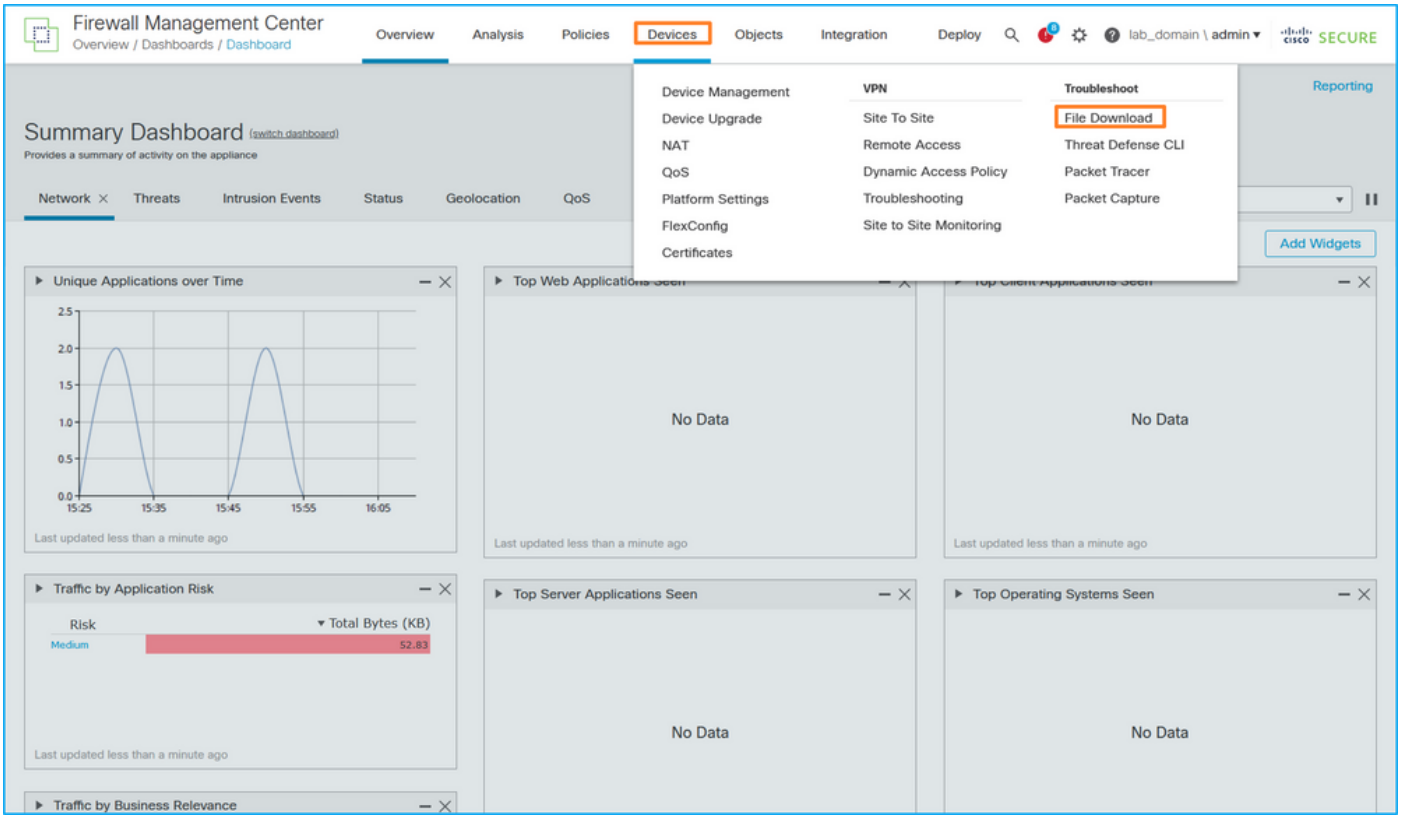
ls -l /ngfw/var/common/sess*

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

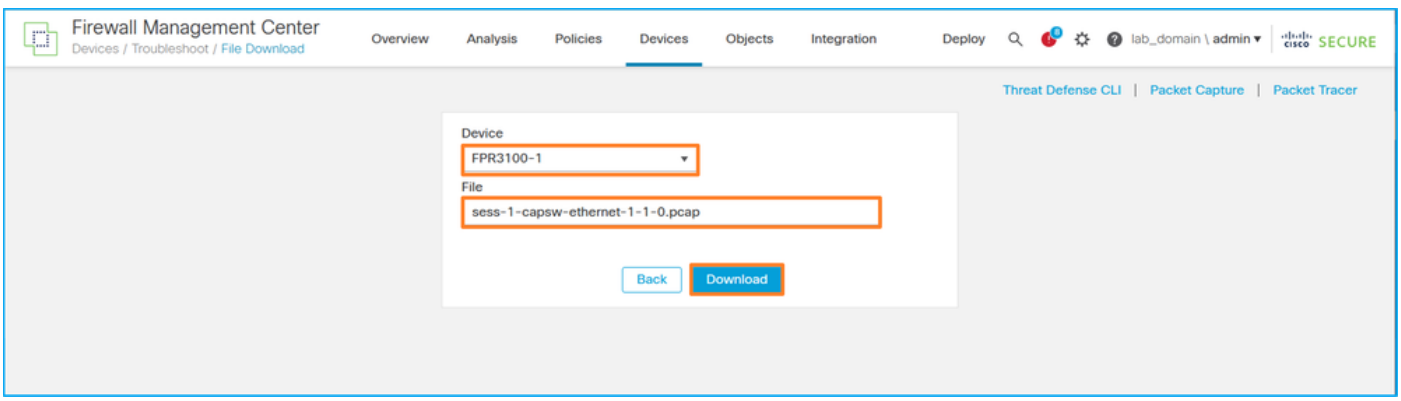
/ngfw/var/common/sess-1-capsw-ethernet-1-1-0.pcap

-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。



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。



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タが増加します。

関連情報

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

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