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
<u>はじめに</u>
<u>前提条件</u>
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>システムアーキテクチャの概要</u>
<u>内部スイッチの動作の概要</u>
<u>パケットフローとキャプチャポイント</u>
<u>Firepower 4100/9300の設定と検証</u>
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
<u>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</u>
<u>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</u>
<u>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</u> <u>ットキャプチャ</u>
<u>パケット キャプチャ フィルタ</u>
<u>Firepower 4100/9300内部スイッチキャプチャファイルの収集</u>
<u>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</u>
<u>セキュアファイアウォール3100/4200の設定と検証</u>
<u>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</u>
<u>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</u> <u>ットキャプチャ</u>
<u>内部インターフェイスでのパケットキャプチャ</u>
<u>パケット キャプチャ フィルタ</u>
<u>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</u>
<u>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</u>

<u>関連情報</u>

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(<u>https://www.wireshark.org/download.html</u>)

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	サトる ュィュの め し	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0/1

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。

- 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
- 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。

- 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
- 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。

Overview I	nterfaces	Logical Devices	Security Engine	Platform Settings			Sy	stem	Tools	Help	admin
							Packet Captu	ire	Trouble	eshooti	ng Logs
Capture Sessi	on Filter Lis	st									
					C Refresh	C	Capture Session	Delet	e All Sessic	ons	
No Session avail	able										

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。

Overview Interfaces Logical Devices Security Engine Platform Settings		System Tools Help admin
Select an instance: ftd1		Save and Run Save Cancel
ftd1	Session Name* Cap1 Selected Interfaces Ethernet1/2	
Ethernet1/2	Buffer Size 256 MB V	
Ethernet1/3	Shap length: 1518 Direction of the state of	2
Ethernet1/1 FTD Ethernet1/9, Ethernet1/10	Capture Filter Apply Filter Capture All	
Ethernet1/5 (Portchannel1)		
Ebernet1/4 (Porthannels)		

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。

Overview Interfaces Logical Devices Security Engine Platform Settings		System Tools Help admin
Select an instance: ftd1 v		Save and Run Save Cancel
ftd1	Session Name" Cap1 Selected Interfaces Ethernet1/5, Ethernet1/4	
Ethernet1/2	Buffer Size 256 MB	•
Ethernet1/3	Snap length: 1518 Bytes Store Packets Overwrite Append	
Ethernet1/1 Ethernet1/10	Capture Filter Apply Filter Capture All	
Ethernet1/5 Cortchannel1		
Ethernet1/4 (Portchannel1)		

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 Versi	on Startup	Version D	eploy Ty
ftd	ftd1							
1	Enat	bled Or	line	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 I - Indiv s - Suspe S - Swite U - Up (M - Not	P vidual H ended r ched R port-chan in use. M	P - Up in po I - Hot-stan - Module-r - Routed mel) lin-links no	rt-channel (m dby (LACP onl emoved t met	nembers) y)	
Group	Port- Channel	Туре	Protocol	Member Ports	;	
1	Pol(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
```

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。

Overview	Interfaces	Logical Devices	Security Engine	Platform Settings				System	Tools He	slp admin	
Capture Ses	Capture Session Fiter List										
							C Refresh Capture Sessio	Delete Al Ses	sions		
	cap1	Drop Coun	t: 0	Operational State: up	Buffer Size: 256 M	в	Snap Length: 1518 Byte	is .			
Interface Na	ame	Filter		File Size (in bytes)	File Name	Device Name					
Ethernet1/2		None		28632	cap1-ethernet-1-2-0.pcap	ftd1	1				

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

Overview Interfaces Li	ogical Devices Security Engine Platform S	Settings						System Tools Help admin		
Capture Session FRer Lit										
							C Refresh Capture Session	Delete All Sessions		
🔺 🔳 cap1	Drop Count: 0	Operation	nal State: up		Buffer Size: 256 MB		Snap Length: 1518 Bytes			
Interface Name	Filter		File Size (in bytes)	File N	ame	Device Name				
Ethernet1/S	None		160	cap1-e	thernet-1-5-0.pcap	ftd1	-)]			
Ethernet1/4	None	L	85000	cap1-e	thernet-1-4-0.pcap	ftd1	*			

FXOSのCLI

scope packet-captureでキャプチャの詳細を確認します。

<#root>

firepower#

scope packet-capture

firepower /packet-capture #

show session cap1

Traffic Monitoring Session:

Packet Capture Session Name: cap1

Session: 1

Admin State: Enabled

Oper State: Up

```
Oper State Reason: Active
    Config Success: Yes
    Config Fail Reason:
    Append Flag: Overwrite
    Session Mem Usage: 256 MB
    Session Pcap Snap Len: 1518 Bytes
    Error Code: 0
   Drop Count: 0
Physical ports involved in Packet Capture:
    Slot Id: 1
   Port Id: 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。
- 内部スイッチは、入力インターフェイスEthernet1/2を識別する追加のポートVLANタグ 102を挿入します。
- 4. 内部スイッチは、追加のVNタグを挿入します。

No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info	
Г	1 2022-07-13 06:23:58.285080930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (40428)	64 Echo (ping) reques	t id=0x001a, seq=7/1792, ttl=64 (no response found!)
	2 2022-07-13 06:23:58.285082858	192.0.2.100	198.51.100.100	ICMP	102	0x9dec (40428)	64 Echo (ping) reques	t id=0x001a, seq=7/1792, ttl=64 (no response found!)
	3 2022-07-13 06:23:59.309048886	192.0.2.100	198.51.100.100	ICMP	108	0x9ed0 (40656)	64 Echo (ping) reques	t id=0x001a, seq=8/2048, ttl=64 (no response found!)
	4 2022-07-13 06:23:59.309193731	192.0.2.100	198.51.100.100	ICMP	102	0x9ed0 (40656)	64 Echo (ping) reques	t id=0x001a, seq=8/2048, ttl=64 (no response found!)
	5 2022-07-13 06:24:00.333054190	192.0.2.100	198.51.100.100	ICMP	108	0x9f20 (40736)	64 Echo (ping) reques	t id=0x001a, seq=9/2304, ttl=64 (no response found!)
	6 2022-07-13 06:24:00.333056014	192.0.2.100	198.51.100.100	ICMP	102	0x9f20 (40736)	64 Echo (ping) reques	t id=0x001a, seq=9/2304, ttl=64 (no response found!)
	7 2022-07-13 06:24:01.357173530	192.0.2.100	198.51.100.100	ICMP	108	0x9f2d (40749)	64 Echo (ping) reques	t id=0x001a, seq=10/2560, ttl=64 (no response found!)
	8 2022-07-13 06:24:01.357174708	192.0.2.100	198.51.100.100	ICMP	102	0x9f2d (40749)	64 Echo (ping) reques	t id=0x001a, seq=10/2560, ttl=64 (no response found!)
	9 2022-07-13 06:24:02.381073741	192.0.2.100	198.51.100.100	ICMP	108	0x9f88 (40840)	64 Echo (ping) reques	t id=0x001a, seq=11/2816, ttl=64 (no response found!)
	10 2022-07-13 06:24:02.381074999	192.0.2.100	198.51.100.100	ICMP	102	0x9f88 (40840)	64 Echo (ping) reques	t id=0x001a, seq=11/2816, ttl=64 (no response found!)
	11 2022-07-13 06:24:03.405199041	192.0.2.100	198.51.100.100	ICMP	108	0xa077 (41079)	64 Echo (ping) reques	t id=0x001a, seq=12/3072, ttl=64 (no response found!)
	12 2022-07-13 06:24:03.405200261	192.0.2.100	198.51.100.100	ICMP	102	0xa077 (41079)	64 Echo (ping) reques	t id=0x001a, seq=12/3072, ttl=64 (no response found!)
	13 2022-07-13 06:24:04.429155683	192.0.2.100	198.51.100.100	ICMP	108	0xa10f (41231)	64 Echo (ping) reques	t id=0x001a, seq=13/3328, ttl=64 (no response found!)
	14 2022-07-13 06:24:04.429156831	192.0.2.100	198.51.100.100	ICMP	102	0xa10f (41231)	64 Echo (ping) reques	t id=0x001a, seq=13/3328, ttl=64 (no response found!)
	15 2022-07-13 06:24:05.453156612	192.0.2.100	198.51.100.100	ICMP	108	0xa16a (41322)	64 Echo (ping) reques	t id=0x001a, seq=14/3584, ttl=64 (no response found!)
	16 2022-07-13 06:24:05.453158052	192.0.2.100	198.51.100.100	ICMP	102	0xa16a (41322)	64 Echo (ping) reques	t id=0x001a, seq=14/3584, ttl=64 (no response found!)
	17 2022-07-13 06:24:06.477127687	192.0.2.100	198.51.100.100	ICMP	108	0xa1e9 (41449)	64 Echo (ping) reques	t id=0x001a, seq=15/3840, ttl=64 (no response found!)
	18 2022-07-13 06:24:06.477129899	192.0.2.100	198.51.100.100	ICMP	102	0xa1e9 (41449)	64 Echo (ping) reques	t id=0x001a, seq=15/3840, ttl=64 (no response found!)
	19 2022-07-13 06:24:07.501291314	192.0.2.100	198.51.100.100	ICMP	108	0xa1f6 (41462)	64 Echo (ping) reques	t id=0x001a, seq=16/4096, ttl=64 (no response found!)
	20 2022-07-13 06:24:07.501293041	192.0.2.100	198.51.100.100	ICMP	102	0xa1f6 (41462)	64 Echo (ping) reques	t id=0x001a, seq=16/4096, ttl=64 (no response found!)
	21 2022-07-13 06:24:08.525089956	192.0.2.100	198.51.100.100	ICMP	108	0xa257 (41559)	64 Echo (ping) reques	t id=0x001a, seq=17/4352, ttl=64 (no response found!)
	22 2022-07-13 06:24:08.525092088	192.0.2.100	198.51.100.100	ICMP	102	0xa257 (41559)	64 Echo (ping) reques	t id=0x001a, seq=17/4352, ttl=64 (no response found!)
	23 2022-07-13 06:24:09.549236500	192.0.2.100	198.51.100.100	ICMP	108	0xa2a9 (41641)	64 Echo (ping) reques	t id=0x001a, seq=18/4608, ttl=64 (no response found!)
	24 2022-07-13 06:24:09.549238564	192.0.2.100	198.51.100.100	ICMP	102	0xa2a9 (41641)	64 Echo (ping) reques	t id=0x001a, seq=18/4608, ttl=64 (no response found!)
	25 2022-07-13 06:24:10.573110146	192.0.2.100	198.51.100.100	ICMP	108	0xa345 (41797)	64 Echo (ping) reques	t id=0x001a, seq=19/4864, ttl=64 (no response found!)
	26 2022-07-13 06:24:10.573112504	192.0.2.100	198.51.100.100	ICMP	102	0xa345 (41797)	64 Echo (ping) reques	t id=0x001a, seq=19/4864, ttl=64 (no response found!)
	27 2022-07-13 06:24:11.597086027	192.0.2.100	198.51.100.100	ICMP	108	0xa349 (41801)	64 Echo (ping) reques	t id=0x001a, seq=20/5120, ttl=64 (no response found!)
	28 2022-07-13 06:24:11.597088170	192.0.2.100	198.51.100.100	ICMP	102	0xa349 (41801)	64 Echo (ping) reques	t id=0x001a, seq=20/5120, ttl=64 (no response found!)
	29 2022-07-13 06:24:12.621061022	192.0.2.100	198.51.100.100	ICMP	108	0xa3dc (41948)	64 Echo (ping) reques	t id=0x001a, seq=21/5376, ttl=64 (no response found!)
¢.								
>	Frame 1: 108 bytes on wire (864 bit	ts), 108 bytes (aptured (864 bits)	on interface	capture u	0 1. id 0		0000 58 97 bd b9 77 0e 00 50 56 9d e8 be 89 26 80 0a X ··· W ·· P V ··· · &··
5	Ethernet II. Src: VMware 9d:e8:be ((00:50:56:9d:e8	be). Dst: Cisco b9	77:00 (58:97	bd:b9:77:	(Be)		0010 00 00 81 00 00 66 08 00 45 00 00 54 9d ec 40 00 ·····f·· E··T··@·
	VN-Tag							0020 40 01 af c0 c0 00 02 64 c6 33 64 64 08 00 4e a2 @·····d ·3dd··N·
	1	= Direc	tion: From Bridge	_				0030 00 1a 00 07 f4 64 ce 62 00 00 00 00 20 a2 07 00d.b
	.0	Point	er: vif id					0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b
		= Desti	nation: 10					0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ···· !"# \$%&'()*+
		= Loope	d: No	A				0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,/0123 4567
		= Reser	ved: 0	4				
		= Versi	on: 0					
	0000 00	00 0000 = Sourc	01.0					
	Type: 802 10 Virtual LAN (0x8100)						
J,	802.10 Virtual LAN, PRI: 0, DEI: 0.	ID: 102						
1	and = Priority	Rest Effort (de	fault) (0)	_				
	a - DEI: Inali	gible	ruure) (0)	2				
	0000 0110 0110 - TD: 102	BIDIE		2				
	Type: TPu4 (0y0800)							
	Internet Protocol Version 4 Sect 1	192 8 2 188 Det	102 51 100 100	_				
	Internet Control Message Destoral		. 190.91.100.100	2				
1	internet control Message Protocol			4				

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。

No.	Time	Source	Destination	Protocol	Length	1P 1D	JP TTL Info	
F	1 2022-07-13 06:23:58.285080930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (40428)	64 Echo (ping) request	id=0x001a, seq=7/1792, ttl=64 (no response found!)
	2 2022-07-13 06:23:58.285082858	192.0.2.100	198.51.100.100	ICMP	102	0x9dec (40428)	64 Echo (ping) request	id=0x001a, seq=7/1792, ttl=64 (no response found!)
	3 2022-07-13 06:23:59.309048886	192.0.2.100	198.51.100.100	ICMP	108	0x9ed0 (40656)	64 Echo (ping) request	id=0x001a, seq=8/2048, ttl=64 (no response found!)
	4 2022-07-13 06:23:59.309193731	192.0.2.100	198.51.100.100	ICMP	102	0x9ed0 (40656)	64 Echo (ping) request	id=0x001a, seq=8/2048, ttl=64 (no response found!)
	5 2022-07-13 06:24:00.333054190	192.0.2.100	198.51.100.100	ICMP	108	0x9f20 (40736)	64 Echo (ping) request	id=0x001a, seq=9/2304, ttl=64 (no response found!)
	6 2022-07-13 06:24:00.333056014	192.0.2.100	198.51.100.100	ICMP	102	0x9f20 (40736)	64 Echo (ping) request	id=0x001a, seq=9/2304, ttl=64 (no response found!)
	7 2022-07-13 06:24:01.357173530	192.0.2.100	198.51.100.100	ICMP	108	0x9f2d (40749)	64 Echo (ping) request	id=0x001a, seq=10/2560, ttl=64 (no response found!)
	8 2022-07-13 06:24:01.357174708	192.0.2.100	198.51.100.100	ICMP	102	0x9f2d (40749)	64 Echo (ping) request	id=0x001a, seq=10/2560, ttl=64 (no response found!)
	9 2022-07-13 06:24:02.381073741	192.0.2.100	198.51.100.100	ICMP	108	0x9f88 (40840)	64 Echo (ping) request	id=0x001a, seq=11/2816, ttl=64 (no response found!)
	10 2022-07-13 06:24:02.381074999	192.0.2.100	198.51.100.100	ICMP	102	0x9f88 (40840)	64 Echo (ping) request	id=0x001a, seq=11/2816, ttl=64 (no response found!)
	11 2022-07-13 06:24:03.405199041	192.0.2.100	198.51.100.100	ICMP	108	0xa077 (41079)	64 Echo (ping) request	id=0x001a, seq=12/3072, ttl=64 (no response found!)
	12 2022-07-13 06:24:03.405200261	192.0.2.100	198.51.100.100	ICMP	102	0xa077 (41079)	64 Echo (ping) request	id=0x001a, seq=12/3072, ttl=64 (no response found!)
	13 2022-07-13 06:24:04.429155683	192.0.2.100	198.51.100.100	ICMP	108	0xa10f (41231)	64 Echo (ping) request	id=0x001a, seq=13/3328, ttl=64 (no response found!)
	14 2022-07-13 06:24:04.429156831	192.0.2.100	198.51.100.100	ICMP	102	0xa10f (41231)	64 Echo (ping) request	id=0x001a, seq=13/3328, ttl=64 (no response found!)
	15 2022-07-13 06:24:05.453156612	192.0.2.100	198.51.100.100	ICMP	108	0xa16a (41322)	64 Echo (ping) request	id=0x001a, seq=14/3584, ttl=64 (no response found!)
	16 2022-07-13 06:24:05.453158052	192.0.2.100	198.51.100.100	ICMP	102	0xa16a (41322)	64 Echo (ping) request	id=0x001a, seq=14/3584, ttl=64 (no response found!)
	17 2022-07-13 06:24:06.477127687	192.0.2.100	198.51.100.100	ICMP	108	0xa1e9 (41449)	64 Echo (ping) request	id=0x001a, seq=15/3840, ttl=64 (no response found!)
	18 2022-07-13 06:24:06.477129899	192.0.2.100	198.51.100.100	ICMP	102	0xa1e9 (41449)	64 Echo (ping) request	id=0x001a, seq=15/3840, ttl=64 (no response found!)
	19 2022-07-13 06:24:07.501291314	192.0.2.100	198.51.100.100	ICMP	108	0xa1f6 (41462)	64 Echo (ping) request	id=0x001a, seq=16/4096, ttl=64 (no response found!)
	20 2022-07-13 06:24:07.501293041	192.0.2.100	198.51.100.100	ICMP	102	0xa1f6 (41462)	64 Echo (ping) request	id=0x001a, seq=16/4096, ttl=64 (no response found!)
	21 2022-07-13 06:24:08.525089956	192.0.2.100	198.51.100.100	ICMP	108	0xa257 (41559)	64 Echo (ping) request	id=0x001a, seq=17/4352, ttl=64 (no response found!)
	22 2022-07-13 06:24:08.525092088	192.0.2.100	198.51.100.100	ICMP	102	0xa257 (41559)	64 Echo (ping) request	id=0x001a, seq=17/4352, ttl=64 (no response found!)
	23 2022-07-13 06:24:09.549236500	192.0.2.100	198.51.100.100	ICMP	108	0xa2a9 (41641)	64 Echo (ping) request	id=0x001a, seq=18/4608, ttl=64 (no response found!)
	24 2022-07-13 06:24:09.549238564	192.0.2.100	198.51.100.100	ICMP	102	0xa2a9 (41641)	64 Echo (ping) request	id=0x001a, seq=18/4608, ttl=64 (no response found!)
	25 2022-07-13 06:24:10.573110146	192.0.2.100	198.51.100.100	ICMP	108	0xa345 (41797)	64 Echo (ping) request	id=0x001a, seq=19/4864, ttl=64 (no response found!)
	26 2022-07-13 06:24:10.573112504	192.0.2.100	198.51.100.100	ICMP	102	0xa345 (41797)	64 Echo (ping) request	id=0x001a, seq=19/4864, ttl=64 (no response found!)
	27 2022-07-13 06:24:11.597086027	192.0.2.100	198.51.100.100	ICMP	108	0xa349 (41801)	64 Echo (ping) request	id=0x001a, seq=20/5120, ttl=64 (no response found!)
	28 2022-07-13 06:24:11.597088170	192.0.2.100	198.51.100.100	ICMP	102	0xa349 (41801)	64 Echo (ping) request	id=0x001a, seq=20/5120, ttl=64 (no response found!)
	29 2022-07-13 06:24:12.621061022	192.0.2.100	198.51.100.100	ICMP	108	0xa3dc (41948)	64 Echo (ping) request	id=0x001a, seq=21/5376, ttl=64 (no response found!)
<								
> F	rame 2: 102 bytes on wire (816 bit	s), 102 bytes o	aptured (816 bits)	on interface	capture u	0 1. id 0		0000 58 97 bd b9 77 0e 00 50 56 9d e8 be 81 00 00 66 Xw.P Vf
> 6	thernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:	be), Dst: Cisco b9:	77:0e (58:97:	bd:b9:77:	Be)		0010 08 00 45 00 00 54 9d ec 40 00 40 01 af c0 c0 00 ··E··T··@·@····
1	302.10 Virtual LAN, PRI: 0, DEI: 0.	ID: 102						0020 02 64 c6 33 64 64 08 00 4e a2 00 1a 00 07 f4 64 ·d·3dd·· N·····d
11	000 = Priority:	Best Effort (de	fault) (0)					0030 ce 62 00 00 00 00 20 a2 07 00 00 00 00 00 10 11 ·b·····
	0 = DEI: Inelia	gible		2				0040 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21
	0000 0110 0110 = ID: 102			-				0050 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 "#\$X&"() "+,/01
	Type: IPv4 (0x0800)							0000 32 33 34 35 36 37 234567
> 1	Internet Protocol Version 4. Src: 1	92.0.2.100, Dst	: 198.51.100.100					
> 1	Internet Control Message Protocol			2				
6								

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

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

No.	Time	Source	Destination	Protocol	Length	IP ID		IP TTL Info		1			^
-	1 2022-08-05 23:07:31.865872877	192.0.2.100	198.51.100.100	ICMP	108	0x322e ((12846)	64 Echo (ping) request	id=0x002d,	seq=245/62720,	ttl=64 (r	nc
	2 2022-08-05 23:07:31.865875131	192.0.2.100	198.51.100.100	ICMP	102	0x322e ((12846)	64 Echo (ping) request	id=0x002d,	seq=245/62720,	ttl=64 (r	nc
	3 2022-08-05 23:07:32.867144598	192.0.2.100	198.51.100.100	ICMP	108	0x32b9 ((12985)	64 Echo (ping) request	id=0x002d,	seq=246/62976,	ttl=64 (r	nc
	4 2022-08-05 23:07:32.867145852	192.0.2.100	198.51.100.100	ICMP	102	0x32b9 ((12985)	64 Echo (ping) request	id=0x002d,	seq=246/62976,	ttl=64 (r	nc
	5 2022-08-05 23:07:33.881902485	192.0.2.100	198.51.100.100	ICMP	108	0x32d8 ((13016)	64 Echo (ping) request	id=0x002d,	seq=247/63232,	ttl=64 (r	nc
	6 2022-08-05 23:07:33.881904191	192.0.2.100	198.51.100.100	ICMP	102	0x32d8 ((13016)	64 Echo (ping) request	id=0x002d,	seq=247/63232,	ttl=64 (r	nc
	7 2022-08-05 23:07:34.883049425	192.0.2.100	198.51.100.100	ICMP	108	Øx3373 ((13171)	64 Echo (ping) request	id=0x002d,	seq=248/63488,	ttl=64 (r	nc
	8 2022-08-05 23:07:34.883051649	192.0.2.100	198.51.100.100	ICMP	102	0x3373 ((13171)	64 Echo (ping) request	id=0x002d,	seq=248/63488,	ttl=64 (r	nc
	9 2022-08-05 23:07:35.883478016	192.0.2.100	198.51.100.100	ICMP	108	0x3427 ((13351)	64 Echo (ping) request	id=0x002d,	seq=249/63744,	ttl=64 (r	nc
	10 2022-08-05 23:07:35.883479190	192.0.2.100	198.51.100.100	ICMP	102	0x3427 ((13351)	64 Echo (ping) request	id=0x002d,	seq=249/63744,	ttl=64 (r	nc
	11 2022-08-05 23:07:36.889741625	192.0.2.100	198.51.100.100	ICMP	108	0x34de ((13534)	64 Echo (ping) request	id=0x002d,	seq=250/64000,	ttl=64 (r	nc
	12 2022-08-05 23:07:36.889742853	192.0.2.100	198.51.100.100	ICMP	102	0x34de ((13534)	64 Echo (ping) request	id=0x002d,	seq=250/64000,	ttl=64 (r	nc
	13 2022-08-05 23:07:37.913770117	192.0.2.100	198.51.100.100	ICMP	108	0x354c ((13644)	64 Echo (ping) request	id=0x002d,	seq=251/64256,	ttl=64 (r	nc
	14 2022-08-05 23:07:37.913772219	192.0.2.100	198.51.100.100	ICMP	102	0x354c ((13644)	64 Echo (ping) request	id=0x002d,	seq=251/64256,	ttl=64 (r	nc
	15 2022-08-05 23:07:38.937829879	192.0.2.100	198.51.100.100	ICMP	108	0x3602 ((13826)	64 Echo (ping) request	id=0x002d,	seq=252/64512,	ttl=64 (r	nc
	16 2022-08-05 23:07:38.937831215	192.0.2.100	198.51.100.100	ICMP	102	0x3602 ((13826)	64 Echo (ping) request	id=0x002d,	seq=252/64512,	ttl=64 (r	nc
	17 2022-08-05 23:07:39.961786128	192.0.2.100	198.51.100.100	ICMP	108	0x36ed ((14061)	64 Echo (ping) request	id=0x002d,	seq=253/64768,	ttl=64 (r	nc
	18 2022-08-05 23:07:39.961787284	192.0.2.100	198.51.100.100	ICMP	102	0x36ed ((14061)	64 Echo (ping) request	id=0x002d,	seq=253/64768,	ttl=64 (r	nc
	19 2022-08-05 23:07:40.985773090	192.0.2.100	198.51.100.100	ICMP	108	0x37d5 ((14293)	64 Echo (ping) request	id=0x002d,	seq=254/65024,	ttl=64 (r	nc v
<												3	>
>	Frame 1: 108 bytes on wire (864 bits), 108 bytes ca	ptured (864 bits) on	interface	e capture_u0_3,	ic 0000	a2 76	f2 00 00 25 00 50	56 9d e8	be 89 26 80	54 · v · · · % · P	v&.т	
>	Ethernet II, Src: VMware_9d:e8:be (0	0:50:56:9d:e8:b	e), Dst: a2:76:f2:00	:00:25 (a2	2:76:f2:00:00:2	5) 0010	00 00	81 00 03 e9 08 00	45 00 00	54 32 2e 40	00	ET2.@·	
	VN-Tag					0020	40 01	1b 7f c0 00 02 64	c6 33 64	64 08 00 1e	d6 @·····d	- 3dd	
	1	= Directi	ion: From Bridge			0030	00 2d	00 f5 a6 a2 ed 62	00 00 00	00 7a 2f 0b	00 ·-···b	····z/··	
н.	.0	= Pointer	<pre>vif_id</pre>			0040	00 00	00 00 10 11 12 13	14 15 16	17 18 19 1a	10 ·····	d%0.1/1*.	
н.	00 0000 0101 0100	= Destina	ation: 84			0050	10 10 20 2d	10 17 20 21 22 23	24 25 26	27 28 29 28	- /0123	\$%& ()"+ 4567	
н.	0	= Looped:	No 4			0000	20 20	20 21 30 31 32 33	54 55 50	57	,/0125	4307	
н.	0	= Reserve	ed: 0										
н.	00	= Version	n: 0										
н.	0000 0000	0000 = Source:	0										
IL	Type: 802.10 Virtual LAN (0x8100)												
	802.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 1001											
	000 Be	est Effort (defa	ault) (0)										
н.	0 = DEI: Ineligi	ible	2										
	0011 1110 1001 = ID: 1001		5										
	Type: IPv4 (0x0800)												
П	Internet Protocol Version 4, Src: 19	2.0.2.100, Dst:	198.51.100.100										
	Internet Control Message Protocol		2										

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。

				Burney of	t a state			10 M H					_	
N	0. Time	Source	Destination	Protocol	Length	PD 0×2220 (1)	1046	PTTL Into	nonuost	id-ovoord	600-245 /62720	++1-64 (100	
	- 12022-08-05 23:07:31.8058/28/7	192.0.2.100	198.51.100.100	TCHP	108	0x322e (1	(846)	64 Echo (ping)	request	1d=0x002d,	seq=245/62/20,	111=04 ((nc	
	2 2022-08-05 23:07:31.8058/5131	192.0.2.100	198.51.100.100	ICMP	102	0x322e (1	(846)	64 Echo (ping)	request	1d=0x002d,	seq=245/62/20,	ttl=64 (Inc	
	3 2022-08-05 23:07:32.867144598	192.0.2.100	198.51.100.100	ICMP	108	0x32b9 (1	2985)	64 Echo (ping)	request	1d=0x002d,	seq=246/62976,	tt1=64 ((nc	
	4 2022-08-05 23:07:32.867145852	192.0.2.100	198.51.100.100	ICMP	102	0x32b9 (1	2985)	64 Echo (ping)	request	id=0x002d,	seq=246/62976,	ttl=64 ((nc	
	5 2022-08-05 23:07:33.881902485	192.0.2.100	198.51.100.100	ICMP	108	0x32d8 (1	3016)	64 Echo (ping)	request	id=0x002d,	seq=247/63232,	ttl=64 ((nc	
	6 2022-08-05 23:07:33.881904191	192.0.2.100	198.51.100.100	ICMP	102	0x32d8 (1	3016)	64 Echo (ping)	request	id=0x002d,	seq=247/63232,	ttl=64 ((nc	
	7 2022-08-05 23:07:34.883049425	192.0.2.100	198.51.100.100	ICMP	108	0x3373 (1	3171)	64 Echo (ping)	request	id=0x002d,	seq=248/63488,	ttl=64 ((nc	
	8 2022-08-05 23:07:34.883051649	192.0.2.100	198.51.100.100	ICMP	102	0x3373 (1	3171)	64 Echo (ping)	request	id=0x002d,	seq=248/63488,	ttl=64 ((nc	
	9 2022-08-05 23:07:35.883478016	192.0.2.100	198.51.100.100	ICMP	108	0x3427 (1	3351)	64 Echo (ping)	request	id=0x002d,	seq=249/63744,	ttl=64 ((nc	
	10 2022-08-05 23:07:35.883479190	192.0.2.100	198.51.100.100	ICMP	102	0x3427 (1	3351)	64 Echo (ping)	request	id=0x002d,	seq=249/63744,	ttl=64 ((nc	
	11 2022-08-05 23:07:36.889741625	192.0.2.100	198.51.100.100	ICMP	108	0x34de (1	3534)	64 Echo (ping)	request	id=0x002d,	seq=250/64000,	ttl=64 ((nc	
	12 2022-08-05 23:07:36.889742853	192.0.2.100	198.51.100.100	ICMP	102	0x34de (1	3534)	64 Echo (ping)	request	id=0x002d,	seq=250/64000,	ttl=64 ((nc	
	13 2022-08-05 23:07:37.913770117	192.0.2.100	198.51.100.100	ICMP	108	0x354c (1	3644)	64 Echo (ping)	request	id=0x002d,	seq=251/64256,	ttl=64 ((nc	
	14 2022-08-05 23:07:37.913772219	192.0.2.100	198.51.100.100	ICMP	102	0x354c (1	3644)	64 Echo (ping)	request	id=0x002d,	seq=251/64256,	ttl=64 ((nc	
	15 2022-08-05 23:07:38.937829879	192.0.2.100	198.51.100.100	ICMP	108	0x3602 (1	3826)	64 Echo (ping)	request	id=0x002d,	seq=252/64512,	ttl=64 ((nc	
	16 2022-08-05 23:07:38.937831215	192.0.2.100	198.51.100.100	ICMP	102	0x3602 (1	3826)	64 Echo (ping)	request	id=0x002d,	seq=252/64512,	ttl=64 ((nc	
	17 2022-08-05 23:07:39,961786128	192.0.2.100	198,51,100,100	ICMP	108	0x36ed (1	1061)	64 Echo (ping)	request	id=0x002d.	seg=253/64768,	ttl=64 ((nc	
	18 2022-08-05 23:07:39.961787284	192.0.2.100	198,51,100,100	ICMP	102	0x36ed (1	1061)	64 Echo (ping)	request	id=0x002d.	seg=253/64768,	tt1=64 ((nc	
	19 2022-08-05 23:07:40.985773090	192.0.2.100	198,51,100,100	ICMP	108	0x37d5 (1	1293)	64 Echo (ping)	request	id=0x002d.	seg=254/65024,	tt1=64 ((nc	~
<								(1-0)		, , , , , , , , , , , , , , , , , , , ,			>	
E,	Frame 2: 102 bytes on wire (816 hits)). 102 hytes cant	ured (816 hits) or	interface ca	anture uB 3	i) 0000	2 76 f2	00 00 25 00 50	56 9d e8	be 81 00 03	09 · V · · · Ž · P	v		
	Ethernet II. Src: VMware 9d:e8:he (0	0:50:56:0d:e8:be)	Dst: a2:76:f2:00	1.00.25 (a2.7/	5.f2.00.00.7	5) 0010	8 00 45	00 00 54 32 2e	40 00 40	01 1b 7f c0	00 ··E··T2.			
Ĵ	802 10 Virtual LAN DRI: A DEL: A	ID: 1001	, oser azironizio	(02170		0020	2 64 c6	33 64 64 08 00	1e d6 00	2d 00 f5 a6	a2 ·d·3dd··			
	and = Priority: Re	st Effort (defau	1+) (0)			0030	d 62 00	00 00 00 7a 2f	0b 00 00	00 00 00 10	11 ·b····z/			
	a = DET: Ineligi	ble	2			0040	2 13 14	15 16 17 18 19	1a 1b 1c	1d 1e 1f 20	21	····· 1		
	0011 1110 1001 - TD: 1001	DIC	2			0050	22 23 24	25 26 27 28 29	2a 2b 2c	2d 2e 2f 30	31 "#\$%&'()	*+,/01		
	Tupo: 1044 (0x0000)					0060	32 33 34	35 36 37			234567			
	Internet Protocol Version 4 Spc: 10	2 0 2 100 Det. 1	09 51 100 100											
	Internet Protocol Version 4, SFC: 19.	2.0.2.100, DSC: 1	2											
11	Internet Control Message Protocol		-											
Ľ														

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		要求
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		

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。

Overview Interfaces Logical Devices Security Engine Platform Settings	System	Tools Help admin
	Packet Capture	Troubleshooting Logs
Capture Session Fitter List		
C Refresh	Capture Session Delet	e All Sessions
No Session available		

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。

Overview Interfaces Logical Devices Security Engine	Platform Settings		System Tools Help admin
Select an instance: ftd1 v			Save and Run Save Cancel
ftd1		Session Name*	capi
		Selected Interfaces	None
Ethemet1/2		Buffer Size	256 MB 👻
		Snap length:	1518 Bytes
		Store Packets	Overwrite Append
		Capture On	Al Backplane Ports
Ethernet1/3	ED	Cashura Elber	ftd Ethernet1/9
	Ethernet1/9, Ethernet1/10	Capture Hiter	Ethernet1/10 Al Backplane Ports
		L 1	
Ethernet1/1			

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 S	tate Oper State	Running Version	Startup	Version Deploy Ty
ftd	ftdl					
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。

Overview Interfa	ces Logical Devices Security Engine	Platform Settings				System Tools Help admin						
Capture Session	apture Session Fiker List											
					Capture Session	Delete Al Sessions						
ap1	Drop Count: 0	Operational State: up	Buffer Size: 256 MB		Snap Length: 1518 Bytes							
Interface Name	Filter	File Size (in bytes)	File Name	Device Name								
Ethernet1/10	None	194352	cap1-ethernet-1-10-0.pcap	ftd1	$\underline{+}$							
Ethernet1/9	None	286368	cap1-ethernet-1-9-0.pcap	ftd1	\pm							

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: O Drop Count: O

Physical ports involved in Packet Capture:

Slot Id: 1

Port Id: 10

```
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/capl-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。

No. Time	Source	Destination	Protocol	Length	PD	IP TTL Info							
1 2022-07-14 20:20:36.	513854256 192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64 Echo ((ping) req	quest	id=0x0001,	seq=15/3840,	ttl=64	(no response found!)	
2 2022-07-14 20:20:36.	513857289 192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64 Echo ((ping) req	quest	id=0x0001,	seq=15/3840,	ttl=64	(reply in 3)	
3 2022-07-14 20:20:36.	514117394 198.51.100.10	0 192.0.2.100	ICMP	108	0xcc2c (52268)	64 Echo ((ping) rep	ply	id=0x0001,	seq=15/3840,	ttl=64	(request in 2)	
4 2022-07-14 20:20:36.	514119312 198.51.100.10	0 192.0.2.100	ICMP	108	Øxcc2c (52268)	64 Echo ((ping) rep	ply	id=0x0001,	seq=15/3840,	ttl=64		
5 2022-07-14 20:20:37.	37723822 192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040)	64 Echo ((ping) req	quest	id=0x0001,	seq=16/4096,	ttl=64	(no response found1)	
6 2022-07-14 20:20:37.	37726588 192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040)	64 Echo ((ping) req	quest	id=0x0001,	seq=16/4096,	ttl=64	(reply in 7)	
7 2022-07-14 20:20:37.5	38846165 198.51.100.10	0 192.0.2.100	ICMP	108	0xcc9b (52379)	64 Echo ((ping) rep	oly	id=0x0001,	seq=16/4096,	ttl=64	(request in 6)	
8 2022-07-14 20:20:37.5	38048311 198.51.100.10	0 192.0.2.100	ICMP	108	0xcc9b (52379)	64 Echo ((ping) rep	ply	id=0x0001,	seq=16/4096,	ttl=64		
9 2022-07-14 20:20:38.	561776064 192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64 Echo ((ping) req	quest	id=0x0001,	seq=17/4352,	ttl=64	(no response found!)	
10 2022-07-14 20:20:38.	61778310 192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64 Echo ((ping) req	quest	id=0x0001,	seq=17/4352,	ttl=64	(reply in 11)	
11 2022-07-14 20:20:38.	62048288 198.51.100.10	0 192.0.2.100	ICMP	108	0xccc4 (52420)	64 Echo ((ping) rep	ply	id=0x0001,	seq=17/4352,	ttl=64	(request in 10)	
12 2022-07-14 20:20:38.	62050333 198.51.100.10	0 192.0.2.100	ICMP	108	0xccc4 (52420)	64 Echo ((ping) rep	ply	id=0x0001,	seq=17/4352,	ttl=64		
13 2022-07-14 20:20:39.	85677043 192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366)	64 Echo ((ping) req	quest	id=0x0001,	seq=18/4608,	tt1=64	(no response found!)	
14 2022-07-14 20:20:39.	85678455 192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366)	64 Echo ((ping) req	quest	id=0x0001,	seg=18/4608,	tt1=64	(reply in 15)	
15 2022-07-14 20:20:39.	85936554 198.51.100.10	0 192.0.2.100	ICMP	108	0xcd8d (52621)	64 Echo ((ping) rep	olv	id=0x0001,	seg=18/4608.	tt1=64	(request in 14)	
16 2022-07-14 20:20:39.	\$85937900 198.51.100.10	0 192.0.2.100	ICMP	108	0xcd8d (52621)	64 Echo ((ping) rep	ply	id=0x0001,	seg=18/4608,	tt1=64		
17 2022-07-14 20:20:40.0	509884884 192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (23419)	64 Echo ((ping) req	quest	id=0x0001,	seq=19/4864,	tt1=64	(no response found!)	
18 2022-07-14 20:20:40.0	09807618 192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (23419)	64 Echo ((ping) req	quest	id=0x0001,	seg=19/4864,	tt1=64	(reply in 19)	
19 2022-07-14 20:20:40.0	510179685 198.51.100.10	0 192.0.2.100	ICMP	108	0xcd8f (52623)	64 Echo ((ping) rep	ply	id=0x0001,	seq=19/4864,	ttl=64	(request in 18)	
20 2022-07-14 20:20:40.0	510181944 198.51.100.10	0 192.0.2.100	ICMP	108	0xcd8f (52623)	64 Echo ((ping) rep	ply	id=0x0001,	seg=19/4864,	ttl=64		
21 2022-07-14 20:20:41.0	33805153 192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64 Echo ((ping) req	quest	id=0x0001,	seq=20/5120,	ttl=64	(no response found!)	
22 2022-07-14 20:20:41.0	33806997 192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64 Echo ((ping) req	quest	id=0x0001,	seq=20/5120,	ttl=64	(reply in 23)	
23 2022-07-14 20:20:41.0	34084102 198.51.100.10	0 192.0.2.100	ICMP	108	0xce36 (52790)	64 Echo ((ping) rep	ply	id=0x0001,	seq=20/5120,	ttl=64	(request in 22)	
24 2022-07-14 20:20:41.0	34085368 198.51.100.10	0 192.0.2.100	ICMP	108	0xce36 (52790)	64 Echo ((ping) rep	ply	id=0x0001,	seq=20/5120,	ttl=64		
25 2022-07-14 20:20:42.0	557709898 192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64 Echo ((ping) req	quest	id=0x0001,	seq=21/5376,	tt1=64	(no response found!)	
26 2022-07-14 20:20:42.0	557711660 192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64 Echo ((ping) req	quest	id=0x0001,	seq=21/5376,	tt1=64	(reply in 27)	
27 2022-07-14 20:20:42.0	557980675 198.51.100.10	0 192.0.2.100	ICMP	108	0xce49 (52809)	64 Echo ((ping) rep	ply	id=0x0001,	seq=21/5376,	tt1=64	(request in 26)	
28 2022-07-14 20:20:42.0	557981971 198.51.100.10	0 192.0.2.100	ICMP	108	0xce49 (52809)	64 Echo ((ping) rep	ply	id=0x0001,	seq=21/5376,	tt1=64		
29 2022-07-14 20:20:43.0	581736697 192.0.2.100	198.51.100.100	ICMP	108	0x5c52 (23634)	64 Echo ((ping) req	quest	id=0x0001,	seq=22/5632,	tt1=64	(no response found!)	
<													
h forme is 100 butes on win	· (Off bits) 100 butss	continued (OCA bits)	n intenfore a		0 14 0				000 00 50	56 0d o7 50 5	0 07 b	1 ho 77 34 90 36 00 00	DV DV AND R
> Frame 1: 108 bytes on wir	e (864 Dits), 108 Dytes	captured (864 Dits) (on interface c	apture_ue	8, 10 0				010 00 00	50 90 e7 50 50 91 00 00 67 0	8 97 00	5 00 00 54 50 00 40 00	PV PA W- Q
> Ethernet II, Src: Cisco b	a://i2d (58:a/ibdiba://i	2d), Dst: VMWare_9d:	27150 (0015015	619016715	(0)				020 40 01	f4 1c c0 00 07 0	2 64 6	33 64 64 88 88 22 68	@d .3dd"h
VN-Tag	- Dise	tion. To Doldas						0	030 00 01	00 0f 89 7a d	0 62 0	00 00 00 b3 d7 09 00	z.b
0	= Direc	tion: To Bridge						0	040 00 00	00 00 10 11 1	2 13 14	1 15 16 17 18 19 1a 1b	
	- Dorti	er: vit_id						0	050 1c 1d	1e 1f 20 21 2	2 23 24	1 25 26 27 28 29 2a 2b	···· !"# \$%8'()"+
		that ton: 0						0	060 2c 2d	2e 2f 30 31 3	2 33 34	1 35 36 37	,/0123 4567
	= Loope	iu: No	41										
	- Heser	ved: 0											
	0000 0000 1010 - Cours	ton: 0											
Turney 002 40 Wintwol L	. 0000 0000 1010 = Sourc	e; 10											
Type: 802.10 VIPtual L	44 (6X8166)		_										
M 802.10 VIFCUAI LAN, PRI:	o, DEI: 0, 1D: 103	fault) (a)											
000	The Teoligible	Haure) (0)											
	ver. merigible		3										
Turnet Thut (0+0000)	10. 103												
Internet Protocol Version	4 5001 102 0 2 100 00	** 100 51 100 100	_										
Internet Control Massage	4, SIC: 192.0.2.100, US	. 198.51.100.100	2										
internet control Message	Protocol .												

3番目と4番目のパケットを選択し、キーポイントを確認します。

- 1. 各ICMPエコー応答がキャプチャされて2回表示されます。
- 2. 元のパケットヘッダーにはVLANタグが付いていません。
- 3. 内部スイッチは、出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。

- 12022-07-14 2022:07-14 202:07-14	
+ 2 2022-07-14 20:20:36.51387289 192.0.2.100 196.51.100.100 1C/P 108 0x:5000 (22028) 64 Echo (ping) reply id=0x0001, seq=15/3404, ttl=64 (request in 2) 4 2022-07-14 20:20:36.514119312 198.51.100.100 192.0.2.100 IC/P 108 0x:C2C (52268) 64 Echo (ping) reply id=0x0001, seq=15/3404, ttl=64 (request in 2) 5 2022-07-14 20:20:36.514119312 198.51.100.100 192.0.2.100 IC/P 108 0x:C2C (52268) 64 Echo (ping) reply id=0x0001, seq=15/3404, ttl=64 (request in 2) 5 2022-07-14 20:20:37.5372582 192.0.2.100 198.51.100.100 IC/P 108 0x:5a00 (23040) 64 Echo (ping) request id=0x0001, seq=15/3404, ttl=64 (request in 2) 6 2022-07-14 20:20:37.5372658 198.51.100.100 192.0.2.100 IC/P 108 0x:Sa00 (23040) 64 Echo (ping) reply id=0x0001, seq=15/3404, ttl=64 (reply in 7) 7 2022-07-14 20:20:37.538048311 198.51.100.100 192.0.2.100 IC/P 108 0x:Sa00 (2322) 64 Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (reply in 7) 1040x0001, seq=16/4096, ttl=64 (reply in 7) 10202-07-14 20:20:38.56176640 198.51.100.100 192.0.2.100 IC/P 108 0x:Sab7 (2322) 64 Echo (ping) reply id=0x0	
s 32022-07-14 20:20:36.51111394 198.51.100.100 192.0.2.100 ICMP 108 0xcc2c (52268) 64 Echo (ping) reply id=0x0001, seq=15/3404, ttl=64 (request in 2) 4 2022-07-14 20:20:37.53772382 195.51.100.100 198.51.100.100 ICMP 108 0xcc2c (52268) 64 Echo (ping) reply id=0x0001, seq=15/3404, ttl=64 5 2022-07-14 20:20:37.53772382 192.0.2.100 198.51.100.100 ICMP 108 0xcc2c (52268) 64 Echo (ping) reply id=0x0001, seq=15/3404, ttl=64 7 2022-07-14 20:20:37.53772368 192.0.2.100 108 10.01 10.00 10.00 0xcc9 652390 64 Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 6) 8 2022-07-14 20:20:37.538040511 198.51.100.100 10.00	
4 2022-07-14 20:20:36.54119312 198.51.100.100 102.0.2.100 100 100 0 <td></td>	
5 2022-07-14 20:20:37.53772582 192.0.2.100 198.51.100.100 ICMP 108 0x5a00 (23040) 64 Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (no response found)) 6 2022-07-14 20:20:37.5372658 192.0.2.100 198.51.100.100 ICMP 108 0x5a00 (23040) 64 Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (request in 6) 7 2022-07-14 20:20:37.538046155 198.51.100.100 192.0.2.100 ICMP 108 0x5a00 (23040) 64 Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (request in 6) 8 2022-07-14 20:20:37.538046155 198.51.100.100 120.0.2.100 ICMP 108 0x5ab0 (23279) 64 Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 6) 9 2022-07-14 20:20:37.538046151 198.51.100.100 120.0.2.100 188.51.100.100 ICMP 108 0x5ab7 (2322) 64 Echo (ping) request id=0x001, seq=16/4096, ttl=64 (no response found]) 10 202-07-14 20:20:38.56170641 192.0.2.100 188.51.100.100 ICMP 108 0x5ab7 (2322) 64 Echo (ping) request id=0x001, seq=16/4096, ttl=64 (reqlest in 1) 10 202-07-14 20:20:38.56170641 195.51.100.100 ICMP 108 0x5ab7 (2322) 64 Echo (ping) request id=0x001, seq=17/4352, ttl=64 (reqlest in 10) 12 202-07-14 20:20:38.56205033 196.51.100.100 1	
6 2022-07-14 20:20:37.53726588 192.0.2.100 198.51.100.100 ICMP 108 0x5a00 (23040) 64 Echo (ping) request id=0x0001, seq=16/4096, tt]=64 (reqly in 7) 7 2022-07-14 20:20:37.53084311 198.51.100.100 192.0.2.100 ICMP 108 0xccob (5237) 64 Echo (ping) request id=0x0001, seq=16/4096, tt]=64 (request in 6) 8 2022-07-14 20:20:37.53084311 198.51.100.100 192.0.2.100 ICMP 108 0xccob (5237) 64 Echo (ping) request id=0x0001, seq=16/4096, tt]=64 9 2022-07-14 20:20:38.561778016 192.0.2.100 108 192.0.2.100 ICMP 108 0xccob (5237) 64 Echo (ping) request id=0x0001, seq=17/4352, tt]=64 (request in 6) 10 2022-07-14 20:20:38.561778310 192.0.2.100 198.51.100.100 ICMP 108 0x5ab7 (23223) 64 Echo (ping) request id=0x0001, seq=17/4352, tt]=64 (request in 10) 11 2022-07-14 20:20:38.562048288 198.51.100.100 120.0.2.100 10MP 108 0x5ccd (5240) 64 Echo (ping) request id=0x0001, seq=17/4352, tt]=64 (request in 10) 12 2022-07-14 20:20:38.562048288 198.51.100.100 120.0.2.100 ICMP 108 0x5ccd (5240) 64 Echo (ping) request id=0x0001, seq=17/4352, tt]=64 (request in 10) 12 2022-07-14 20:20:38.56204828 198.51.100.100 ICMP 108<	
7 2022-07-14 20:20:37,538048115 198.51.100.100 192.0.2.100 ICMP 108 0xcc9b (52379) 64 Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 6) 8 2022-07-14 20:20:37,538048311 198.51.100.100 192.0.2.100 ICMP 108 0xcc9b (52379) 64 Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 6) 9 2022-07-14 20:20:38.56177664 192.0.2.100 198.51.100.100 ICMP 108 0xcc9b (52379) 64 Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (no response found1) 10 2022-07-14 20:20:38.561776310 192.0.2.100 198.51.100.100 ICMP 108 0xcc16 (2240) 64 Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (no response found1) 11 2022-07-14 20:20:38.5607833 198.51.100.100 104P 108 0xccc4 (5240) 64 Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (reply in 11) 12 2022-07-14 20:20:38.56205033 198.51.100.100 192.0.2.100 ICMP 108 0xccc4 (5240) 64 Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (no response found1) 12 2022-07-14 20:20:38.56205033 198.51.100.100 192.0.2.100 ICMP 108 0xccc4 (5240) 64 Echo (ping) reply id=0x0001, seq=18/408, ttl=64 (reply in 11) 12 202-07-14 20:20:38.56205033 198.51.1	
8 2022-07-14 20:20:37.538048311 198.51.100.100 192.0.2.100 ICMP 108 0xcc9b (52379) 64 Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 9 2022-07-14 20:20:38.561778064 192.0.2.100 198.51.100.100 ICMP 108 0x5ab7 (23223) 64 Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 10 2022-07-14 20:20:38.56177810 192.0.2.100 198.51.100.100 ICMP 108 0x5ab7 (23223) 64 Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (no response found!) 11 2022-07-14 20:20:38.562048288 198.51.100.100 192.0.2.100 ICMP 108 0x5ab7 (23223) 64 Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (reply in 11) 12 2022-07-14 20:20:38.562048288 198.51.100.100 192.0.2.100 ICMP 108 0x5ab7 (23224) 64 Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (reply in 11) 12 2022-07-14 20:20:38.562048288 198.51.100.100 192.0.2.100 ICMP 108 0x5cd4 (52420) 64 Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 10) 12 2022-07-14 20:20:38.56207833 198.51.100.100 ICMP 108 0x5cd4 (52420) 64 Echo (ping) reply id=0x0001, seq=18/408, ttl=64 (no response found!) 12 2022-07-14 20:20:39.585677043 <td< td=""><td></td></td<>	
9 2022-07-14 20:20:38.561776064 192.0.2.100 198.51.100.100 ICMP 108 0x5ab7 (23223) 64 Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (no response found!) 10 2022-07-14 20:20:38.561778310 192.0.2.100 198.51.100.100 ICMP 108 0x5ab7 (23223) 64 Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (reply in 11) 11 2022-07-14 20:20:38.56204288 198.51.100.100 192.0.2.100 ICMP 108 0xccc4 (52420) 64 Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (request in 10) 12 2022-07-14 20:20:38.56204288 198.51.100.100 192.0.2.100 ICMP 108 0xccc4 (52420) 64 Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 10) 12 2022-07-14 20:20:39.58567043 192.0.2.100 IDM ICMP 108 0xccc4 (52420) 64 Echo (ping) reply id=0x0001, seq=18/4608, ttl=64 (no response found!) 14 2022-07-14 20:20:39.58567043 192.0.2.100 ISS.51.100.100 ICMP 108 0x5b46 (23366) 64 Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (reply in 15)	
10 2022-07-14 20:20:38.561778310 192.0.2.100 108.51.100.100 ICMP 108 0x5ab7 (23223) 64 Echo (ping) request i d-0x0001, seq=17/4352, ttl=64 (reply in 11) 11 2022-07-14 20:20:38.562048288 198.51.100.100 192.0.2.100 ICMP 108 0xccc4 (52420) 64 Echo (ping) request i d-0x0001, seq=17/4352, ttl=64 (reply in 11) 12 2022-07-14 20:20:38.562045033 196.51.100.100 192.0.2.100 ICMP 108 0xccc4 (52420) 64 Echo (ping) reply id-0x0001, seq=17/4352, ttl=64 (reply in 12) 13 2022-07-14 20:20:38.562045033 195.51.100.100 192.0.2.100 ICMP 108 0xccc4 (52420) 64 Echo (ping) reply id-0x0001, seq=18/4052, ttl=64 (reply in 12) 13 2022-07-14 20:20:39.585670453 192.0.2.100 108.51.100.100 ICMP 108 0x5b64 (23366) 64 Echo (ping) request id-0x0001, seq=18/4089, ttl=64 (no response found1) 14 2022-07-14 20:20:39.585670453 192.0.2.100 198.51.100.100 ICMP 108 0x5b64 (23366) 64 Echo (ping) request id-0x0001, seq=18/4089, ttl=64 (no response found1) 14 2022-07-14 20:20:39.585670453 192.0.2.100 198.51.100.100 ICMP 108 0x5b64 (23366) 64 Echo (ping) request id-0x0001, seq=18/4089, ttl=64 (no response found1) 114 202-07-14 20:20:39.585670453 104.4008, ttl=64 (reply in 15)	
11 2022-07-14 20:20:38.562048288 198.51.100.100 192.0.2.100 ICMP 108 0xccc4 (52420) 64 Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 10) 12 2022-07-14 20:20:38.562048288 198.51.100.100 192.0.2.100 ICMP 108 0xccc4 (52420) 64 Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 10) 12 2022-07-14 20:20:39.58657043 192.0.2.100 198.51.100.100 ICMP 108 0x5b46 (23366) 64 Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (no response found]) 14 2022-07-14 20:20:39.586570455 192.0.2.100 198.51.100.100 ICMP 108 0x5b46 (23366) 64 Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (reply in 15)	
12 2022-07-14 20:20:38.562050333 198.51.100.100 192.0.2.100 ICMP 108 0xccc4 (52420) 64 Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 13 2022-07-14 20:20:39.5567043 192.0.2.100 109.151.100.100 ICMP 108 0xccc4 (52420) 64 Echo (ping) reply id=0x0001, seq=18/4608, ttl=64 14 2022-07-14 20:20:39.55670453 192.0.2.100 198.51.100.100 ICMP 108 0x5bd6 (23366) 64 Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (no response found!) 14 2022-07-14 20:20:39.55670453 192.0.2.100 198.51.100.100 ICMP 108 0x5bd6 (23366) 64 Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (reply in 15)	
13 2022-07-14 20:20:39.585677043 192.0.2.100 198.51.100.100 ICMP 108 0x5b46 (23366) 64 Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (no response foundl) 14 2022-07-14 20:20:39.585678455 192.0.2.100 198.51.100.100 ICMP 108 0x5b46 (23366) 64 Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (no response foundl)	
14 2022-07-14 20:20:39.585678455 192.0.2.100 198.51.100.100 ICMP 108 0x5b46 (23366) 64 Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (reply in 15)	
15 2022-07-14 20:20:39.585936554 198.51.100.100 192.0.2.100 ICMP 108 0xcd8d (52621) 64 Echo (ping) reply id=0x0001, seg=18/4608, ttl=64 (request in 14)	
16 2022-07-14 20:20:39.585937900 198.51,100.100 192.0.2.100 ICMP 108 0xcd8d (52621) 64 Echo (ping) reply id=0x0001, sec=18/4608, ttl=64	
12 2022-07-14 20:20:40.600804804 102.0.2.100 108.51.100.100 ICMP 108 0x5h7b (23410) 64 Echo (ning) request id=0x0001, son=19/4864, ttl=64 (no response found))	
18 202-07-14 20:20:40.609807618 192.0.2.100 198.51.100.100 ICMP 108 0x5676 (23410) 64 Fcbo (ning) request id=0x0001.seq=10/4864.ttl=64 (reply in 19)	
19 2022-07-14 20:20:40.610170685 108.51.100.100.100.102.0.2.100 ICMP 108 0xcd8f (5262) 64 Echo (ning) renty id=0x0001 cm id=0x00001 cm id=0x000001 cm id=0x00001 cm id=0x000001 cm id=0x000000 cm id=0x0000000 cm id=0x000000 cm id=0x00000000 cm id=0x00000000000000000000000000000000000	
20 202-07-14 20120140 (10181044 198.51.100.100 192.0.2.100 ICMP 108 0xcd6 (55/62) 64 Echo (ninp) reps) id=0x0001, separa/(4864, tt)=64	
212027, 2142023 , 21420323 , 2120323 , 212032 , 21203 , 2	
22 2022 - 07-14 20:20:41 633806007 102 0.2 100 109 51 100 100 10 10 10 100 100 100 100 100	
22 202-07-42 20141 63408410 198 51 100 100 100 4 2 100 (Fey an 20)	
22 2012 01 42 2014 2014 2014 2014 2014 2	
25202-07-42 2012014205204026 1200-11000052000 1200-11000 1200052100 100 120000000 1200-1100000000 1200-1100000000 1200-1100000000 1200-11000000000 1200-11000000000 1200-11000000000 1200-11000000000 1200-11000000000 1200-11000000000 1200-110000000000	
25 2022-07-14 20:40 (42):40 (50):405050 152:02:100 150:51:100:100 1101 1100 0 AUG (25):50 04 EURO (PARG) (EQUEST 10400004) Seque21/500 (10 (ES)0050 (10011) 120:01011)	
$20 2022^{+}0^{-}42 20 \cdot 20^{+}a^{-}20 \cdot 20^{+}a^{-}21 \cdot 50^{-}100 = 196 \cdot 31 \cdot 100 \cdot 100 = 100 = 0 \cdot 300 \cdot 10 (2530) = 0 + 0 \cdot 100 \cdot 100 \cdot 100 \cdot 100 + 0 \cdot 100 \cdot$	
27 2022-07-34 20.20.42.05790073 196.53.100.100 192.05.100 10.0 17.00 0XCH2 (52007) 04 ECH0 (PHK) TEPJY 10-0X004, 504-21/576, 41-64	
20 2022-07-14 20:00/42:00/3013/1 190:01100 192:02:100 1100 100 00 000 100 00 000 00 00 000 000 00000 000000	
29 2022-07-14 20:20:43.081/30097 192.0.2.100 198.51.100.100 10 10 10 10 0X3C32 (23034) 04 ECHO (ping) request 10-0x0001, seq=227/3032, tt1-b4 (no response found)	
C	
Frame 3: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0	X · · · w · · & · ·
> Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: Whware 9d:e8:be (00:50:56:9d:e8:be) 0010 00 0a 81 00 00 66 08 00 45 00 00 54 cc 2c 00 00	έτο Εττ Ττ ,ττ
VN-Tag 0020 40 01 c1 80 c6 33 64 64 c0 00 02 64 00 00 2a 68 @····	dd ···d··*h
0 = Direction: To Bridge	1-p
.0	
.00 0000 0000 = Destination: 0	# \$88 ()"+
0000 2. 20 20 21 30 31 32 35 34 35 30 57 j=1/0	25 4307
Type: 802.10 Virtual LAN (0x8100)	
V 802.10 Virtual LAN, PRI: 0, DEI: 0, ID: 102	
000 = Priority: Best Effort (default) (0)	
0000 0110 0110 = ID: 102	
Type: IPv4 (0x0800)	
3 Internet Protocol Version 4, Src: 198,51,100,100, Dst: 192,0,2,100	
Internet Control Message Protocol	

説明

バックプレーンインターフェイス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 プレイン ターン 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。





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。

Overview Interfaces Logical Devices Security Engine Platform Settings	System	Tools Help admin
	Packet Capture	Troubleshooting Logs
Capture Session Filter List		
C Refresh	Capture Session Dele	te All Sessions
No Session available		

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。

Overview Interfaces Logical Devices Security Engine Platform Settings		System Tools Help admin
Select an instance: ftd1		Save and Run Save Cancel
ftd1	Session Name*	cap1
	Selected Interfaces	None
Ethernet1/2	Buffer Size	256 MB 👻
	Snap length:	1518 Bytes
	Store Packets	Overwrite Append
	Capture On	ftd
Ethernet1/3	Application Port	Ethernet1/2
Ethernet1/9, Eth	Application Capture Direction	ion All Packets Egress Packet
	Capture Filter	Apply Filter Capture All
Ethernet1/1		

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	0per	State	Running	Version	Startup	Version	Deploy	Ту
ftd	ftdl												
1	Enat	oled	0n1	ine		7.2	2.0.82	7.2.0.8	32	Native	No		

```
2. キャプチャセッションを作成します。
```

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

検証

FCM(必須)

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

Overvie	w Interfaces	Logical Devices	Security Engine	Platform S	Settings				5	System	Tools	Help	admin
Capture	Session Filter Li	st											
								C Refresh Capt	ure Session	Delete All S	Sessions		
•	cap1	Drop Count	t: 0	Operation	nal State: up	Buffer Size: 256 MB		Snap Length: 1518	Bytes				
Interfac	e Name	Filter		F	File Size (in bytes)	File Name	Device Name						
Ethernet	1/2 - Ethernet1/10	None		5	576	cap1-vethemet-1175.pcap	ftd1		\mathbb{A}				
Ethernet	1/2 - Ethernet1/9	None		4	\$360	cap1-vethemet-1036.pcap	ftd1		4				

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: O Drop Count: O

Application ports involved in Packet Capture:

slot Id: 1

Link Name: 112

Port Name: Ethernet1/2

App Name: ftd Sub Interface: 0 Application Instance Identifier: ftd1 Application ports resolved to: Name: vnic1 Eq Slot Id: 1 Eq Port Id: 9 Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1036.pcap Pcapsize: 53640 bytes Vlan: 102 Filter: Name: vnic2 Eq Slot Id: 1 Eq Port Id: 10 Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1175.pcap Pcapsize: 1824 bytes Vlan: 102 Filter:

キャプチャファイルの収集

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

ファイル分析のキャプチャ

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

最初と2番目のパケットを選択し、キーポイントを確認します。

- 1. 各ICMPエコー応答がキャプチャされて2回表示されます。
- 2. 元のパケットヘッダーにはVLANタグが付いていません。
- 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。

No. Time	Source	Destination	Protocol	Length	PD	IP TTL Info	
1 2022-08-01 10:03:22.231237959	198,51,100,100	192.0.2.100	TCMP	108 4	9x42f8 (17144)	64 Echo (ning) renly	id=0x0012, seg=1/256, ttl=64
2 2022-08-01 10:03:22.231239747	198,51,100,100	192.0.2.100	ICMP	108	9x42f8 (17144)	64 Echo (ping) reply	id=0x0012, seg=1/256, tt]=64
3 2022-08-01 10:03:23.232244769	198.51.100.100	192.0.2.100	ICMP	108	0X4305 (1/351)	64 ECHO (DINK) PEDIV	id=0x0012, seg=2/512, ttl=64
4 2022-08-01 10:03:23.232247753	198.51.100.100	192.0.2.100	ICMP	108	0x43b3 (17331)	64 Echo (ping) reply	id=0x0012, seq=2/512, ttl=64
5 2022-08-01 10:03:24.234703981	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64 Echo (ping) reply	id=0x0012, seq=3/768, ttl=64
6 2022-08-01 10:03:24.234706751	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64 Echo (ping) reply	id=0x0012, seq=3/768, ttl=64
7 2022-08-01 10:03:25.258672449	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64 Echo (ping) reply	id=0x0012, seq=4/1024, ttl=64
8 2022-08-01 10:03:25.258674861	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64 Echo (ping) reply	id=0x0012, seq=4/1024, ttl=64
9 2022-08-01 10:03:26.282663169	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64 Echo (ping) reply	id=0x0012, seq=5/1280, ttl=64
10 2022-08-01 10:03:26.282666183	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64 Echo (ping) reply	id=0x0012, seq=5/1280, ttl=64
11 2022-08-01 10:03:27.306671694	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64 Echo (ping) reply	id=0x0012, seq=6/1536, ttl=64
12 2022-08-01 10:03:27.306674378	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64 Echo (ping) reply	id=0x0012, seq=6/1536, ttl=64
13 2022-08-01 10:03:28.330664677	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64 Echo (ping) reply	id=0x0012, seq=7/1792, ttl=64
14 2022-08-01 10:03:28.330667153	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64 Echo (ping) reply	id=0x0012, seq=7/1792, ttl=64
15 2022-08-01 10:03:29.354795931	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64 Echo (ping) reply	id=0x0012, seq=8/2048, ttl=64
16 2022-08-01 10:03:29.354936706	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64 Echo (ping) reply	id=0x0012, seq=8/2048, ttl=64
17 2022-08-01 10:03:30.378795204	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64 Echo (ping) reply	id=0x0012, seq=9/2304, ttl=64
18 2022-08-01 10:03:30.378798172	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64 Echo (ping) reply	id=0x0012, seq=9/2304, ttl=64
19 2022-08-01 10:03:31.402772217	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18842)	64 Echo (ping) reply	1d=0x0012, seq=10/2560, ttl=64
20 2022-08-01 10:03:31.402774775	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18842)	64 Echo (ping) reply	1d=0x0012, seq=10/2560, tt1=64
21 2022-08-01 10:03:32.426693254	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64 Echo (ping) reply	1d=0x0012, seq=11/2816, tt1=64
د .							
> Frame 1: 108 bytes on wire (864 bits	s), 108 bytes ca	ptured (864 bits) o	n interface ca	oture u0 i	8. id 0		000 00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00 ·PV···X· ··w··&··
> Ethernet II, Src: Cisco b9:77:0e (5)	8:97:bd:b9:77:0e). Dst: VMware 9d:e	8:be (00:50:56	:9d:e8:be)		0010 00 0a 81 00 00 66 08 00 45 00 00 54 42 f8 00 00 ·····f··E··TB···
VN-Tag			_		·		0020 40 01 4a b5 c6 33 64 64 c0 00 02 64 00 00 90 04 @·J··3dd ···d····
0	= Directi	ion: To Bridge					0030 00 12 00 01 dd a4 e7 62 00 00 00 00 e3 0d 09 00bb
.0	= Pointer	: vif_id					0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b
00 0000 0000 0000	= Destina	tion: 0					10 10 10 11 120 21 22 23 24 25 26 27 28 29 24 20 ····· ! # \$A& ()**
···· ··· ··· ··· ··· 0··· ···	= Looped:	NO 🖌					2. 20 20 21 30 31 32 33 34 33 30 37
0	= Reserve	d: 0	· I · · ·				
	· · · · · · · · · Version	1: 0					
0000 000	0 1010 = Source:	10					
Type: 802.10 Virtual LAN (0x8100)			_				
802.10 VIPTUAI LAN, PKI: 0, DEI: 0,	10: 102						
000 Priority: 8	est Effort (defa	uit) (0)					
0000 0110 0110 - TD: 102	1016						
Type: TPv4 (0x0800)							
Internet Protocol Version 4, Src: 19	98.51.100.100. D	st: 192.0.2.100					
Internet Control Message Protocol							

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。

Overview Interfaces Logical Devices Security Engine Platform Settings	System	Tools Help admin
	Packet Capture	Troubleshooting Logs
Capture Session Fitter List		
C Refresh	Capture Session Dele	te All Sessions
No Session available		

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。

Overview I	nterfaces Logical Devices Security Engine	Natform Settings					System Tools H	lelp admin
Select an insta	nce: ftd1 💌					Save and Run	Save	Cancel
ftd1			Session Name*	cap1				
			Selected Interfaces	None	_			
Ethernet1/2			Buffer Size	256 MB	•			
			Snap length:	1518	Bytes			
			Store Packets	Overwrite Append]			
			Capture On	ftd 🗸	3			
Ethernet1/3			Application Port	Ethernet1/2	1			
	Sector Se	Ethernet1/9, Ethernet1/10	Application Capture Direction	All Packets Egress Packet				
			Capture Filter	Apply Filter Capture All				
Ethernet1/1								

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 , show app-in	/ssa# nstance						
App Name	Identifier Slot ID	Admin State	Oper State	Running Version	Startup	Version	Deploy Ty
ftd	ftdl						
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。

Overview Interfaces L	ogical Devices Security Engine Pla	tform Settings				System 1	iools He	ılp admin
Capture Session Filter List								
						Refresh	Capture Se	De
a Cap1	Drop Count: 0	Operational State: up	Buffer Size: 256 MB		Snap Length: 1518 Bytes			
Interface Name	Filter	File Size (in bytes)	File Name	Device Name				
Ethernet1/2	None	95040	cap1-ethernet-1-2-0.pcap	ftd1	*			
Ethernet1/2 - Ethernet1/10	None	368	cap1-vethernet-1175.pcap	ftd1	*			
Ethernet1/2 - Ethernet1/9	None	13040	cap1-vethernet-1036.pcap	ftd1	*			

FXOS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: O
Drop Count: O
```

Physical ports involved in Packet Capture:

Slot Id: 1

Port Id: 2

```
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。
- 内部スイッチは、入力インターフェイスEthernet1/2を識別する追加のポートVLANタグ 102を挿入します。
- 4. 内部スイッチは、追加のVNタグを挿入します。

No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info		
-	1 2022-08-01 11:33:19.070693081	192.0.2.100	198.51.100.100	ICMP	108 1	0xc009 (491	51) 64 Echo (ping	g) request	id=0x0013, seq=1/256, ttl=64 (no response found!)
	2 2022-08-01 11:33:19.070695347	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (491	 64 Echo (ping 	g) request	id=0x0013, seq=1/256, ttl=64 (no response found!)
	3 2022-08-01 11:33:19.071217121	192.0.2.100	198.51.100.100	ICMP	102	8XC889 (49)	51) 64 ECRO (p1ng	g) request	id=0x0013, seq=1/256, ttl=64 (no response found!)
	4 2022-08-01 11:33:19.071218458	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (491	51) 64 Echo (ping	g) request	id=0x0013, seq=1/256, ttl=64 (no response found!)
	5 2022-08-01 11:33:20.072036625	192.0.2.100	198,51,100,100	ICMP	108	OxcOae (49)	26) 64 Echo (pine	g) request	id=0x0013, seg=2/512, ttl=64 (no response found!)
	6 2022-08-01 11:33:20.072038399	192.0.2.100	198,51,100,100	ICMP	102	OxcBae (49)	26) 64 Echo (pine	g) request	id=0x0013, seq=2/512, ttl=64 (no response found!)
	7 2022-08-01 11:33:21 073266030	192.0.2.100	198.51.100.100	TCMP	108	8xc167 (495	(11) 64 Echo (ping	g) request	id=0x0013, seq=3/768, ttl=64 (no response found!)
	0 2022 00 01 11:33:21:07 5200030	102.0.2.100	100 51 100 100	TCMD	100	Oxc167 (49)	(ping	g) request	id-avaala can-3/760 ttl-64 (no response found))
	8 2022-08-01 11:33:21.0/320832/	192.0.2.100	190.51.100.100	TCHP	102	0xc107 (49:	(1) 64 Echo (ping	g) request	id=0x0013, seq=3/708, cc1=04 (no response round))
	9 2022-08-01 11:33:22.074576640	192.0.2.100	198.51.100.100	ICMP	108	0xc1/5 (495	(5) 64 Echo (ping	g) request	1d=0x0013, seq=4/1024, ttl=64 (no response found)
	10 2022-08-01 11:33:22.0/45/8010	192.0.2.100	198.51.100.100	TCMP	102	0xc1/5 (495	(5) 64 Echo (ping	g) request	1d=0x0013, seq=4/1024, ttl=64 (no response found)
	11 2022-08-01 11:33:23.075779089	192.0.2.100	198.51.100.100	ICMP	108	0xc208 (496	72) 64 Echo (ping	g) request	1d=0x0013, seq=5/1280, ttl=64 (no response found!)
	12 2022-08-01 11:33:23.075781513	192.0.2.100	198.51.100.100	ICMP	102	0xc208 (496	72) 64 Echo (ping	g) request	id=0x0013, seq=5/1280, ttl=64 (no response found!)
	13 2022-08-01 11:33:24.081839490	192.0.2.100	198.51.100.100	ICMP	108	0xc211 (496	31) 64 Echo (ping	g) request	id=0x0013, seq=6/1536, ttl=64 (no response found!)
	14 2022-08-01 11:33:24.081841386	192.0.2.100	198.51.100.100	ICMP	102	0xc211 (496	31) 64 Echo (ping	g) request	id=0x0013, seq=6/1536, ttl=64 (no response found!)
	15 2022-08-01 11:33:25.105806249	192.0.2.100	198.51.100.100	ICMP	108	Øxc2e2 (498	90) 64 Echo (ping	g) request	id=0x0013, seq=7/1792, ttl=64 (no response found!)
	16 2022-08-01 11:33:25.105807895	192.0.2.100	198.51.100.100	ICMP	102	Øxc2e2 (498	90) 64 Echo (ping	g) request	id=0x0013, seq=7/1792, ttl=64 (no response found!)
	17 2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	ICMP	108	0xc3b4 (501	00) 64 Echo (ping	g) request	id=0x0013, seq=8/2048, ttl=64 (no response found!)
	18 2022-08-01 11:33:26.129838114	192.0.2.100	198,51,100,100	ICMP	102	0xc3b4 (501	(0) 64 Echo (ping)	g) request	id=0x0013, seg=8/2048, ttl=64 (no response found!)
	19 2022-08-01 11:33:27,153828653	192.0.2.100	198,51,100,100	ICMP	108	0xc476 (50)	() 64 Echo (pine	g) request	id=0x0013, seg=9/2304, ttl=64 (no response found!)
	20 2022-08-01 11:33:27,153830201	192.0.2.100	198,51,100,100	ICMP	102	0xc476 (502	04) 64 Echo (pine	g) request	id=0x0013, seg=9/2304, ttl=64 (no response found!)
	21 2022-08-01 11:33:28.177847175	192.0.2.100	198,51,100,100	TCMP	108	8xc516 (58	(4) 64 Echo (nine	g) request	id=0x0013, seq=10/2560, ttl=64 (no response found!)
	22 2022-08-01 11:33:28 177849075	192.0.2.100	198.51.100.100	TCMP	102	8xc516 (58	(4) 64 Echo (ping	g) request	id=0x0013, seq=10/2560, ttl=64 (no response found!)
	22 2022-00-01 11:33:20 201904760	192.0.2.100	199.51.100.100	TCMP	102	BYC578 (504	(2) 64 Echo (ping	g) request	id=0x0013, seq=11/2016, ttl=64 (no response found1)
	24 2022 00 01 11:33:29 201004700	102.0.2.100	100 51 100 100	TCMD	100	0xc570 (50.	(2) 64 Echo (ping	g) request	id-0x0013, seq-11/2016, ttl-64 (no response found)
	24 2022-08-01 11:55:29.201600488	192.0.2.100	198.51.100.100	TCHP	102	0xc5/8 (50:	(f) G4 Echo (ping	g) request	id-outpoint, seq-12/2010, (C1=64 (no response found))
	25 2022-08-01 11:33:30.225834/05	192.0.2.100	198.51.100.100	TCHP	108	0xc585 (50:	(1 Color (ping	g) request	id-0x0013, seq=12/3072, tt1=64 (no response found!)
	26 2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (503	55) 64 Echo (ping	g) request	1d=0x0013, seq=12/30/2, tt1=64 (no response found))
	27 2022-08-01 11:33:31.249828955	192.0.2.100	198.51.100.100	ICMP	108	0xc618 (50)	12) 64 Echo (ping	g) request	1d=0x0013, seq=13/3328, ttl=64 (no response found!)
	28 2022-08-01 11:33:31.249831121	192.0.2.100	198.51.100.100	ICMP	102	0xc618 (50)	12) 64 Echo (ping	g) request	1d=0x0013, seq=13/3328, ttl=64 (no response found!)
	29 2022-08-01 11:33:32.273867960	192.0.2.100	198.51.100.100	ICMP	108	0xc64f (50)	57) 64 Echo (ping	g) request	1d=0x0013, seq=14/3584, ttl=64 (no response found!)
<									
> 1	Frame 1: 108 bytes on wire (864 bit:	s), 108 bytes cap	otured (864 bits) o	n interface ca	pture_u0_	1, id 0		000	0 58 97 bd b9 77 0e 00 50 56 9d e8 be 89 26 80 0a X···w··P V····&··
>	Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:b	e), Dst: Cisco b9:7	7:0e (58:97:bd	:b9:77:0e)		001	0 00 00 81 00 00 66 08 00 45 00 00 54 c0 09 40 00 ·····f··E··T··@·
V 1	VN-Tag							002	10 40 01 8d a3 c0 00 02 64 c6 33 64 64 08 00 8d 7c @·····d ·3dd···
Ľ	1	= Directi	on: From Bridge					003	0 00 13 00 01 f2 b9 e7 62 00 00 00 00 cb 7f 06 00bb
	.0	= Pointer	: vif id					084	0 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b
		= Destina	tion: 10					005	0 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ···· !"# \$%&'()"+
		= Looped:	No					006	0 2c 2d 2e 2t 30 31 32 33 34 35 36 37 ,/0123 4567
		= Reserve	d: 0						
		= Version	1.0						
	0000 000	0 0000 = Source:							
	Type: 802 10 Victual LAN (0x8100)	o ocoo - source.	•						
	POD 10 Vintual LAN DOT: A DET: A	TD: 102							
	and _ Delegiture P	art Effort (dofo	ult) (0)						
	000 Priority: 8	ible	01()(0)						
	DEI: Inelig	1016							
	0000 0110 0110 = 1D: 102								
L b	Type: (PV4 (0x0800)		***	_					
2	Internet Protocol Version 4, Src: 1	92.0.2.100, Dst:	198.51.100.100						
2	Internet Control Message Protocol								

2番目のパケットを選択し、キーポイントを確認します。

- 1. ICMPエコー要求パケットだけがキャプチャされます。各パケットは2回取得されて表示され ます。
- 2. 元のパケットヘッダーにはVLANタグが付いていません。
- 3. 内部スイッチは、入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。

	io. Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info		
L	1 2022-08-01 11:33:19.070693081	192.0.2.100	198.51.100.100	ICMP	108 1	0xc009 (49161)	64 Echo (ping	request	id=0x0013, seq=1/256, ttl=64 (no response found!)
L	2 2022-08-01 11:33:19.070695347	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping	request	id=0x0013, seq=1/256, ttl=64 (no response found!)
I	3 2022-08-01 11:33:19.071217121	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping	request	id=0x0013, seq=1/256, ttl=64 (no response found!)
L	4 2022-08-01 11:33:19.071218458	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping	() request	id=0x0013, seq=1/256, ttl=64 (no response found!)
L	5 2022-08-01 11:33:20.072036625	192.0.2.100	198.51.100.100	ICMP	108	0xc0ae (49326)	64 Echo (ping) request	id=0x0013, seg=2/512, ttl=64 (no response found!)
L	6 2022-08-01 11:33:20.072038399	192.0.2.100	198,51,100,100	ICMP	102	0xc0ae (49326)	64 Echo (ping	t) request	id=0x0013, seg=2/512, ttl=64 (no response found!)
L	7 2022-08-01 11:33:21.073266030	192.0.2.100	198,51,100,100	ICMP	108	0xc167 (49511)	64 Echo (ping) request	id=0x0013, seg=3/768, ttl=64 (no response found!)
L	8 2022-08-01 11:33:21.073268327	192.0.2.100	198,51,100,100	ICMP	102	Øxc167 (49511)	64 Echo (ping) request	id=0x0013, seg=3/768, ttl=64 (no response found!)
L	9 2022-08-01 11:33:22.074576640	192.0.2.100	198, 51, 100, 100	TCMP	108	Øxc175 (49525)	64 Echo (pine) request	id=0x0013, seg=4/1024, ttl=64 (no response found1)
L	10 2022-08-01 11:33:22.074578010	192.0.2.100	198,51,100,100	TCMP	102	0xc175 (49525)	64 Echo (pine) request	id=0x0013, seq=4/1024, ttl=64 (no response found1)
L	11 2022 00 01 11:33:23 075770000	102 0 2 100	109 51 100 100	TCMD	109	0x(209 (49672)	64 Echo (ping) request	id=0x0013, seq=5/1200, ttl=64 (no response found1)
L	12 2022-08-01 11:33:23:07 5775085	102 0 2 100	100 51 100 100	TCMD	100	0xc208 (49072)	64 Echo (ping) request	id=0x0013, seq=5/1200, ttl=64 (no response found1)
L	12 2022-08-01 11:33:23:07 5781515	102.0.2.100	100 51 100 100	TCMD	102	0xc208 (49072)	64 Echo (ping	() request	id=0x0013, seq=5/1220, tt1=04 (no response found1)
L	13 2022-08-01 11:33:24.081839490	102.0.2.100	100 51 100 100	TCMP	100	0xc211 (49081)	64 Echo (ping	() request	id=0x0013, seq=0/1530, tt1=04 (no response found1)
L	14 2022-08-01 11:33:24.081841380	192.0.2.100	198.51.100.100	ICHP	102	0xc211 (49081)	oa Echo (ping	() request	id exects, seq=0/1530, ttl=04 (no response round)
L	15 2022-08-01 11:33:25.105806249	192.0.2.100	198.51.100.100	ICMP	108	0xc2e2 (49890)	64 Echo (ping	() request	1d=0x0013, seq=//1/92, ttl=64 (no response found)
L	16 2022-08-01 11:33:25.105807895	192.0.2.100	198.51.100.100	ICMP	102	0xc2e2 (49890)	64 Echo (ping	() request	1d=0x0013, seq=//1/92, tt1=64 (no response found)
L	17 2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	ICMP	108	0xc304 (50100)	64 Echo (ping	() request	1d=0x0013, seq=8/2048, tt1=64 (no response found!)
L	18 2022-08-01 11:33:26.129838114	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100)	64 Echo (ping	;) request	1d=0x0013, seq=8/2048, ttl=64 (no response found!)
L	19 2022-08-01 11:33:27.153828653	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294)	64 Echo (ping	request	id=0x0013, seq=9/2304, ttl=64 (no response found!)
L	20 2022-08-01 11:33:27.153830201	192.0.2.100	198.51.100.100	ICMP	102	0xc476 (50294)	64 Echo (ping	request	id=0x0013, seq=9/2304, ttl=64 (no response found!)
L	21 2022-08-01 11:33:28.177847175	192.0.2.100	198.51.100.100	ICMP	108	0xc516 (50454)	64 Echo (ping	request	id=0x0013, seq=10/2560, ttl=64 (no response found!)
L	22 2022-08-01 11:33:28.177849075	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (50454)	64 Echo (ping	request	id=0x0013, seq=10/2560, ttl=64 (no response found!)
L	23 2022-08-01 11:33:29.201804760	192.0.2.100	198.51.100.100	ICMP	108	0xc578 (50552)	64 Echo (ping	request	id=0x0013, seq=11/2816, ttl=64 (no response found!)
L	24 2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	102	0xc578 (50552)	64 Echo (ping	request	id=0x0013, seq=11/2816, ttl=64 (no response found!)
L	25 2022-08-01 11:33:30.225834765	192.0.2.100	198.51.100.100	ICMP	108	0xc585 (50565)	64 Echo (ping	request	id=0x0013, seq=12/3072, ttl=64 (no response found!)
L	26 2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (50565)	64 Echo (ping	request	id=0x0013, seq=12/3072, ttl=64 (no response found!)
L	27 2022-08-01 11:33:31.249828955	192.0.2.100	198.51.100.100	ICMP	108	0xc618 (50712)	64 Echo (ping	request	id=0x0013, seq=13/3328, ttl=64 (no response found!)
L	28 2022-08-01 11:33:31.249831121	192.0.2.100	198.51.100.100	ICMP	102	0xc618 (50712)	64 Echo (ping	request	id=0x0013, seq=13/3328, ttl=64 (no response found!)
L	29 2022-08-01 11:33:32.273867960	192.0.2.100	198.51.100.100	ICMP	108	0xc64f (50767)	64 Echo (ping) request	id=0x0013, seg=14/3584, ttl=64 (no response found!)
F	Frame 2: 102 bytes on wire (816 bit	(s), 102 hytes ca	ntured (816 bits) or	interface ca	nture uB	1. id 0			58 97 bd b9 77 8e 89 58 56 9d e8 be 81 88 88 66 X w P V f
L	Ethernet II. Src: Wware 9d:e8:be	00:50:56:9d:e8:b	e). Dst: Cisco b9:7	7:0e (58:97:bd	:h9:77:0e)		001	0 08 00 45 00 00 54 c0 09 40 00 40 01 8d a3 c0 00 ··E··T·· @·@····
	802.10 Virtual LAN, PRT: 0, DET: 0	TD: 102	C/1 0501 01500 0517			·		002	0 02 64 c6 33 64 64 08 00 8d 7c 00 13 00 01 f2 b9 ·d·3dd···
L	and - Deioeitu:	Bast Effort (daf:	(a) (a)	_				003	e7 62 00 00 00 00 cb 7f 06 00 00 00 00 00 10 11 .b
L	- OFT Teels	aible	uic) (0)					004	0 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21
L		gible	-					005	0 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 "#\$%&"() *+,/01
L	Tupor Thut (0x0000)							006	0 32 33 34 35 36 37 234567
L	Type: 1994 (0x0800)	0.0 0 0 000 0 000	100 51 100 100	_					
L	Internet Protocol Version 4, Src: :	192.0.2.100, DST:	198.51.100.100						
L	Internet Control Message Protocol								
I									

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。
- 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。

No. Time Source	Destination	Protocol	Length	PD	PTTL Pro	I de anna constante del es
1 2022-08-01 11:33:19:0/1512098 198.51.	100.100 192.0.2.100	ICHP	108	0x4127 (20263)	64 Echo (ping) reply	10=0x0013, Seq=1/256, tt1=64
2 2022-08-01 11:33:19.0/1514882 198.51.	100.100 192.0.2.100	ICMP	108	0x4127 (20263)	64 Echo (ping) reply	1d=0x0013, seq=1/256, tt1=64
3 2022-08-01 11:33:20.072677302 198.51.	100.100 192.0.2.100	ICMP	108	0,4110 (20475)	64 ECHO (ping) reply	1d=0x0013, seq=2/512, tt1=64
4 2022-08-01 11:33:20.072679384 198.51.	100.100 192.0.2.100	ICMP	108	0x411D (20475)	64 Echo (ping) reply	1d=0x0013, seq=2/512, ttl=64
5 2022-08-01 11:33:21.073913640 198.51.	100.100 192.0.2.100	ICMP	108	0x50ac (20652)	64 Echo (ping) reply	1d=0x0013, seq=3/768, tt1=64
6 2022-08-01 11:33:21.073915690 198.51.	100.100 192.0.2.100	ICMP	108	0x50ac (20652)	64 Echo (ping) reply	id=0x0013, seq=3/768, ttl=64
7 2022-08-01 11:33:22.075239381 198.51.	100.100 192.0.2.100	ICMP	108	0x513e (20798)	64 Echo (ping) reply	id=0x0013, seq=4/1024, ttl=64
8 2022-08-01 11:33:22.075241491 198.51.	100.100 192.0.2.100	ICMP	108	0x513e (20798)	64 Echo (ping) reply	id=0x0013, seq=4/1024, ttl=64
9 2022-08-01 11:33:23.076447152 198.51.	100.100 192.0.2.100	ICMP	108	0x51c9 (20937)	64 Echo (ping) reply	id=0x0013, seq=5/1280, ttl=64
10 2022-08-01 11:33:23.076449303 198.51.	100.100 192.0.2.100	ICMP	108	0x51c9 (20937)	64 Echo (ping) reply	id=0x0013, seq=5/1280, ttl=64
11 2022-08-01 11:33:24.082407896 198.51.	100.100 192.0.2.100	ICMP	108	0x528e (21134)	64 Echo (ping) reply	id=0x0013, seq=6/1536, ttl=64
12 2022-08-01 11:33:24.082410099 198.51.	100.100 192.0.2.100	ICMP	108	0x528e (21134)	64 Echo (ping) reply	id=0x0013, seq=6/1536, ttl=64
13 2022-08-01 11:33:25.106382424 198.51.	100.100 192.0.2.100	ICMP	108	0x52af (21167)	64 Echo (ping) reply	id=0x0013, seq=7/1792, ttl=64
14 2022-08-01 11:33:25.106384549 198.51.	100.100 192.0.2.100	ICMP	108	0x52af (21167)	64 Echo (ping) reply	id=0x0013, seq=7/1792, ttl=64
15 2022-08-01 11:33:26.130437851 198.51.	100.100 192.0.2.100	ICMP	108	0x53a6 (21414)	64 Echo (ping) reply	id=0x0013, seq=8/2048, ttl=64
16 2022-08-01 11:33:26.130440320 198.51.	100.100 192.0.2.100	ICMP	108	0x53a6 (21414)	64 Echo (ping) reply	id=0x0013, seq=8/2048, ttl=64
17 2022-08-01 11:33:27.154398212 198.51.	100.100 192.0.2.100	ICMP	108	0x5446 (21574)	64 Echo (ping) reply	id=0x0013, seq=9/2304, ttl=64
18 2022-08-01 11:33:27.154400198 198.51.	100.100 192.0.2.100	ICMP	108	0x5446 (21574)	64 Echo (ping) reply	id=0x0013, seg=9/2304, ttl=64
19 2022-08-01 11:33:28.178469866 198.51.	100.100 192.0.2.100	ICMP	108	0x5493 (21651)	64 Echo (ping) reply	id=0x0013, seq=10/2560, ttl=64
20 2022-08-01 11:33:28.178471810 198.51.	100.100 192.0.2.100	ICMP	108	0x5493 (21651)	64 Echo (ping) reply	id=0x0013, seg=10/2560, ttl=64
21 2022-08-01 11:33:29,202395869 198,51.	100.100 192.0.2.100	ICMP	108	0x54f4 (21748)	64 Echo (ping) reply	id=0x0013, seg=11/2816, ttl=64
22 2022-08-01 11:33:29,202398067 198,51.	100,100 192,0,2,100	ICMP	108	0x54f4 (21748)	64 Echo (ping) reply	id=0x0013, seg=11/2816, ttl=64
23 2022-08-01 11:33:30,226398735 198,51.	100,100 192,0,2,100	ICMP	108	0x5526 (21798)	64 Echo (ping) reply	id=0x0013, seg=12/3072, ttl=64
24 2022-08-01 11:33:30.226401017 198.51.	100,100 192,0,2,100	ICMP	108	0x5526 (21798)	64 Echo (ping) reply	id=0x0013, seg=12/3072, ttl=64
25 2022-08-01 11:33:31.250387808 198.51.	100.100 192.0.2.100	TCMP	108	0x55f2 (22002)	64 Echo (ping) reply	id=0x0013, seg=13/3328, ttl=64
26 2022-08-01 11:33:31.250389971 198.51.	100.100 192.0.2.100	TCMP	108	8x55f2 (22882)	64 Echo (ning) renly	id=8x8813, seg=13/3328, tt1=64
27 2022-08-01 11:33:32 274416011 198-51	100,100, 192,0,2,100	TCMP	108	8x5668 (22112)	64 Echo (ping) reply	id=0x0013, seq=14/3584, tt1=64
28 2022-00-01 11:33:32 274419229 108 51	100 100 102 0 2 100	TCMP	108	av5660 (22112)	64 Echo (ping) reply	id=0x0013, seq=14/3504, tt1=64
20 2022-00-01 11:33:32.27444.0223 190.51	100.100 102.0.2.100	TCMD	109	0x5607 (22242)	64 Echo (ping) reply	id=0x0013, seq=15/3840, tt1=64
<pre></pre>	100.100 192.0.2.100	ACOP.	100	000007 (22247)	ou cono (pring) repry	10-080015, 364-15/3040, ((1-04
France A: 100 butes on view (064 bits) 100	huter conturned (064 bits)	an Interface o		0.14.0		2000 00 50 55 0d e0 he 50 07 hd ho 77 0e 00 25 00 00
Therest IV foce fiere building (604 bits), 108	bytes captured (864 bits)	on incertace c	apture_uo_	0, 10 0		0010 00 90 90 90 90 00 97 00 09 77 00 09 20 00 00 PV X W W W
> Ethernet 11, Src: CISCO 09:77:00 (58:97:00:	(09:77:00), DSC: VMware 90:	68:06 (00:50:5	5:90:08:00	:)		0020 40 01 30 86 c6 33 64 64 c0 00 02 64 00 00 95 7c 0 33ddd
vivi- lag	- Blasskins, Xe Baldes					0030 00 13 00 01 f2 b9 e7 62 00 00 00 cb 7f 06 00b
0	= Direction: To Bridge					0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b
	= Pointer: Vit_10					0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ···· !"# \$%&"()"+
	= Destination: 0					0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,/0123 4567
	= Looped: No	4				
	= Reserved: 0					
	= Version: 0					
0000 1010	= Source: 10					
Type: 802.1Q Virtual LAN (0x8100)		_				
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102	2					
000 = Priority: Best Eff	ort (default) (0)	<u>_</u>				
0 = DEI: Ineligible		31				
0000 0110 0110 = ID: 102		-				
Type: IPv4 (0x0800)						
Internet Protocol Version 4, Src: 198.51.10	00.100, Dst: 192.0.2.100	2				
> Internet Control Message Protocol		2				

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	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
Ethernet1/2でのキャプチ ャの設定と確認	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 一要求

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)

o

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。

Overview Interfaces Logical Devices Security Engine Platform Settings	System	Tools Help admin
	Packet Capture	Troubleshooting Logs
Capture Session Fiter List		
C Refresh	Capture Session Dele	te All Sessions
No Session available		

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

Overview Interfaces L	Logical Devices Security	r Engine Platform Settings				System Tools Help admin
Select an instance: ftd1	*				Save and Run Save	Cancel
Subinterface selection Ethernet1/2.205 Ethernet1/2.204	ftd1	Ethernet1/2		Session Name* Selected Interfaces Buffer Size Snap length: Store Packets	Cap1] Ethernet1/2.205 256 MB 1518 Bytes Overwarke Append	
		Ethernet1/1	ED FD Ethernet1/9. Ethernet1/10	Capture Filter	Apply Filter Capture Al	

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 <u>CSCvq33119</u>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

firepo	ower/	/ssa #										
show a	app-ir	nstance										
App Na	ame	Identi	fier Slo	t ID /	Admin Stat	e Oper	State	Running	Version	Startup \	/ersion	Deploy Ty
ftd		ftd1										
ftd	1	ftd2	Enabled 1	Onli E	ine Enabled	7.2 Onlin	.0.82 e	7.2.0.8 7.2.0.82	2	Containe 7.2.0.82	er No	R Container
2.	ポー	トチャ	ネルイン	゚ターフェ	イスの場	合は、	そのメンノ	バーインタ	ーフェイ	イスを識別	りします	۲.
<#roo	ot>											
firepo	ower#											
connec	et fxo	os										
<outpu firepo</outpu 	ut ski ower(1	ipped> fxos)#										
show p	port-c	channel	summary									
Flags	: D - I - S - U - M -	- Down - Indiv - Suspe - Switc - Up (p - Not i	P idual H nded r hed R ort-chan n use. M	- Up in - Hot-st - Module - Routed nel) in-links	port-chan candby (LA e-removed d not met	nel (me CP only	mbers))					
Group	Port- Chanr	 - 1el	Туре	Protoco	ol Member	Ports						
1	Po1(\$	3U)	Eth	LACP	Eth1/3	(P)	Eth1/3(P)			_		
3.	+ †]	プチャ	セッショ	ンを作成	えします。							

<#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。

Overview	Interfaces	Logical Devices Secu	urity Engine Platform Settings								System Tools	Help admin
Capture Ses	sion Fiter List											
									C Re	capture Session	Delete Al Session	á .
•	cap1	Drop (Count: 0	Operatio	onal State: up	Buffer Size:	256 MB		Snap Length: 1518 By	tes		
	_	-				 						(inclusion)
Interface No	ime		Filter		File Size (in bytes)	File Name	1	Device Name				
Ethernet1/2.	205		None		233992	cap1-ethemet-1-2-0.pcap		ftd1		土		
	_											

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。

Overview Interfaces Logical	Devices Security Engine Platform Settings					System Tools He	dp admin
Capture Session Filter List							
					Capture Session	Delete Al Sessions	
a 🔳 capt	Drop Count: 0	Operational State: up	Buffer Size: 256 MB		Snap Length: 1518 Bytes		1812
Interface Name	Filter	File Size (in bytes)	File Name	Device Name			
Ethernet1/4.207	None	624160	cap1-ethernet-1-4-0.pcap	Not available	*		
Ethernet1/3.207	None	160	cap1-ethernet-1-3-0.pcap	Not available	*		

FXOS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: O

```
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。
- 内部スイッチは、入力インターフェイスEthernet1/2を識別する追加のポートVLANタグ 102を挿入します。
- 4. 内部スイッチは、追加のVNタグを挿入します。

No.	Time	Source	Destination	Protocol	Length	PD	PTTL Info		
	1 2022-08-04 07:21:56.993302102	192.0.2.100	198,51,100,100	TCMP	112	8x9574 (38268)	64 Echo (ning) reque	st id	exx0022, seg=1/256, ttl=64 (no response foundl)
	2 2822-88-84 87:21:56.993383597	192.0.2.100	198, 51, 100, 100	TCMP	102	8x9574 (38268)	64 Echo (ning) reque	st id	anyonic segurities the formation of the segurity and the segurities of the seguritie
	2 2022 00 04 07:22:06 214264777	102 0 2 100	100 51 100 100	TCMD	112	0x0391 (30552)	64 Echo (ping) reque	id id	l-0x0022, seq=10/3560, t+1=64 (no response found1)
	4 2022 00 04 07:22:00.214204/77	102.0.2.100	100 51 100 100	TCMD	102	0x9301 (39553)	64 Echo (ping) reque	ist id	1-0x0022, seq=10/2500, ((1-04 (no response found))
	4 2022-08-04 07:22:00.214207373	192.0.2.100	198.51.100.100	TCHD	112	0x9881 (39555)	64 Echo (ping) reque	est id	-0x0022, seq=10/2000, ((1=04 (no response found))
	5 2022-08-04 07:22:07.215115395	192.0.2.100	198.51.100.100	TCHP	112	6X39C3 (33013)	64 Echo (ping) reque	ist 10	-oxoozz, seq=11/2016, ttl=04 (no response found)
	6 2022-08-04 07:22:07.215115445	192.0.2.100	198.51.100.100	ICMP	102	0x9ac3 (39619)	64 Echo (ping) reque	est 10	1=0x0022, seq=11/2816, ttl=64 (no response found))
	7 2022-08-04 07:22:08.229938577	192.0.2.100	198.51.100.100	ICMP	112	0x9b33 (39731)	64 Echo (ping) reque	est id	<pre>websile="form: seq=12/3072">= form: seq=12/3072</pre> , ttl=64 (no response found!)
	8 2022-08-04 07:22:08.229940829	192.0.2.100	198.51.100.100	ICMP	102	0x9b33 (39731)	64 Echo (ping) reque	est id	<pre>weight and the second sec</pre>
	9 2022-08-04 07:22:09.253944601	192.0.2.100	198.51.100.100	ICMP	112	0x9c0e (39950)	64 Echo (ping) reque	est id	i=0x0022, seq=13/3328, ttl=64 (no response found!)
	10 2022-08-04 07:22:09.253946899	192.0.2.100	198.51.100.100	ICMP	102	0x9c0e (39950)	64 Echo (ping) reque	est id	i=0x0022, seq=13/3328, ttl=64 (no response found!)
	11 2022-08-04 07:22:10.277953070	192.0.2.100	198.51.100.100	ICMP	112	0x9ccb (40139)	64 Echo (ping) reque	est id	l=0x0022, seq=14/3584, ttl=64 (no response found!)
	12 2022-08-04 07:22:10.277954736	192.0.2.100	198.51.100.100	ICMP	102	0x9ccb (40139)	64 Echo (ping) reque	est id	=0x0022, seq=14/3584, ttl=64 (no response found!)
	13 2022-08-04 07:22:11.301931282	192.0.2.100	198.51.100.100	ICMP	112	0x9d84 (40324)	64 Echo (ping) reque	st id	=0x0022, seq=15/3840, ttl=64 (no response found!)
	14 2022-08-04 07:22:11.301933600	192.0.2.100	198.51.100.100	ICMP	102	0x9d84 (40324)	64 Echo (ping) reque	st id	=0x0022, seg=15/3840, ttl=64 (no response found!)
	15 2022-08-04 07:22:12.325936521	192.0.2.100	198,51,100,100	ICMP	112	0x9da2 (40354)	64 Echo (ping) reque	st id	=0x0022, seg=16/4096, ttl=64 (no response found!)
	16 2022-08-04 07:22:12.325937895	192.0.2.100	198.51.100.100	ICMP	102	0x9da2 (40354)	64 Echo (ping) reque	est id	=0x0022, seg=16/4096, ttl=64 (no response found!)
	17 2022-08-04 07:22:13.326988040	192.0.2.100	198,51,100,100	TCMP	112	0x9e07 (48455)	64 Echo (ning) reque	est id	=0x0022, seg=17/4352, ttl=64 (no response found))
	19 2022-09-04 07:22:13 226000259	192 0 2 100	100 51 100 100	TCMP	102	0x0007 (40455)	64 Echo (ning) reque	et id	-0x0022 sec=17/4352 ++1=64 (no response found))
	10 2022-00-04 07:22:15:520550250	192.0.2.100	100 51 100 100	TCMP	112	0x9063 (40554)	64 Echo (ping) reque	at id	Lavaar found)
-	19 2022-00-04 07:22:14:341944775	102.0.2.100	100 51 100 100	TCHP	102	0x960a (40554)	of Echo (ping) reque	ist id	l-0x0022, seq-10/4000, ttl-64 (no response found)
	20 2022-08-04 07:22:14.341946249	192.0.2.100	198.51.100.100	TCHP	102	0x900a (40554)	64 Echo (ping) reque	ist 10	-0x0022, seq=18/4008, ttl=04 (no response found!)
	21 2022-08-04 07:22:15.365941588	192.0.2.100	198.51.100.100	ICMP	112	0X90TD (40699)	64 Ecno (ping) reque	ist 10	1=0x0022, seq=19/4864, tt1=64 (no response round)
	22 2022-08-04 07:22:15.365942566	192.0.2.100	198.51.100.100	ICMP	102	0x9etb (40699)	64 Echo (ping) reque	ist 1d	<pre>1=0x0022, seq=19/4864, ttl=64 (no response found!)</pre>
	23 2022-08-04 07:22:16.389973843	192.0.2.100	198.51.100.100	ICMP	112	0x91e8 (40936)	64 Echo (ping) reque	ist 1d	1=0x0022, seq=20/5120, tt1=64 (no response found!)
	24 2022-08-04 07:22:16.389975129	192.0.2.100	198.51.100.100	ICMP	102	0x9fe8 (40936)	64 Echo (ping) reque	est id	#0x0022, seq#20/5120, ttl#64 (no response found!)
	25 2022-08-04 07:22:17.413936452	192.0.2.100	198.51.100.100	ICMP	112	0xa079 (41081)	64 Echo (ping) reque	est id	l=0x0022, seq=21/5376, ttl=64 (no response found!)
	26 2022-08-04 07:22:17.413938090	192.0.2.100	198.51.100.100	ICMP	102	0xa079 (41081)	64 Echo (ping) reque	est id	l=0x0022, seq=21/5376, ttl=64 (no response found!)
	27 2022-08-04 07:22:18.437954335	192.0.2.100	198.51.100.100	ICMP	112	0xa11e (41246)	64 Echo (ping) reque	est id	<pre>l=0x0022, seq=22/5632, ttl=64 (no response found!)</pre>
έII									
	Frame 1, 112 butes on vine (006 bit	A12 hotes co.	ntured (006 bits)	on intenface c	neture un	1 14 0		0000	22 76 62 00 00 1h 00 50 56 0d og ho 90 26 90 54
1	There is in the one of the one of the one of the of	(a), 112 bytes ta	a) Detty april 2015)	on incertace c	apture_uo	1, 10 0		0010	00 00 91 00 00 10 00 00 00 00 90 90 00 00 00 00 00 00 00
í.	Ethernet 11, Src: VHware Suiesibe (00:50:56:90:68:0	e), USC: az:/6:T2:	00:00:10 (az:/	5:12:00:00	5:10)		0020	95 74 49 99 49 91 b8 38 c9 99 92 64 c6 33 64 64 t0-0-3dd
1	vn-Tag	- Disecti	and from Boldes					0030	08 00 eb 95 00 22 00 01 88 73 eb 62 00 00 00 00
	1	= Directi	ion: From Bridge					0040	d9 9d 00 00 00 00 00 00 10 11 12 13 14 15 16 17
	.0	= Pointer	": v1t_1d					0050	18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 !"#\$%8"
		= Destina	ition: 84					0060	28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ()*+,/ 01234567
	0	= Looped:	No	4 1					
	0	= Reserve	ed: 0						
	00	= Version	n: 0						
	0000 000	00 0000 = Source:	0						
L	Type: 802.1Q Virtual LAN (0x8100)							
V 0	802.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 102							
	000 = Priority:	Best Effort (defa	ult) (0)	-					
	0 = DEI: Ineli	gible		21					
	0000 0110 0110 = ID: 102	0							
	Type: 802.10 Virtual LAN (0x8100)							
J.	902 10 Victual LAN DET: 0 DET: 0	10: 205							
	and priority and a priority	Rest Effort (defa	(a) (thus						
	- DET TRAIL	aible	(0)						
	0000 1100 1101 - UC: 200	Erore							
	6666 1166 1161 = 10: 265			2					
	Type: 1PV4 (0x0800)			-					
2	Internet Protocol Version 4, Src: 1	192.0.2.100, Dst:	198.51.100.100						
2	Internet Control Message Protocol								
								_	

2番目のパケットを選択し、キーポイントを確認します。

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

No. Time Source	Destination Proto	col Length	₽ D	IP TTL Info	
1 2022-08-04 07:21:56.993302102 192.0.2.100	198.51.100.100 ICM	P 112	0x9574 (38260)	64 Echo (ping) request	id=0x0022, seq=1/256, ttl=64 (no response found!)
2 2022-08-04 07:21:56.993303597 192.0.2.100	198.51.100.100 ICM	P 102	0x9574 (38260)	64 Echo (ping) request	id=0x0022, seq=1/256, ttl=64 (no response found!)
3 2022-08-04 07:22:06.214264777 192.0.2.100	198.51.100.100 ICM	P 112	0x9a81 (39553)	64 Echo (ping) request	id=0x0022, seq=10/2560, ttl=64 (no response found!)
4 2022-08-04 07:22:06.214267373 192.0.2.100	198.51.100.100 ICM	P 102	0x9a81 (39553)	64 Echo (ping) request	id=0x0022, seq=10/2560, ttl=64 (no response found!)
5 2022-08-04 07:22:07.215113393 192.0.2.100	198.51.100.100 ICM	P 112	0x9ac3 (39619)	64 Echo (ping) request	id=0x0022, seq=11/2816, ttl=64 (no response found!)
6 2022-08-04 07:22:07.215115445 192.0.2.100	198.51.100.100 ICM	P 102	0x9ac3 (39619)	64 Echo (ping) request	id=0x0022, seq=11/2816, ttl=64 (no response found!)
7 2022-08-04 07:22:08.229938577 192.0.2.100	198.51.100.100 ICM	P 112	0x9b33 (39731)	64 Echo (ping) request	id=0x0022, seq=12/3072, ttl=64 (no response found!)
8 2022-08-04 07:22:08.229940829 192.0.2.100	198.51.100.100 ICM	P 102	0x9b33 (39731)	64 Echo (ping) request	id=0x0022, seq=12/3072, ttl=64 (no response found!)
9 2022-08-04 07:22:09.253944601 192.0.2.100	198.51.100.100 ICM	P 112	0x9c0e (39950)	64 Echo (ping) request	id=0x0022, seq=13/3328, ttl=64 (no response found!)
10 2022-08-04 07:22:09.253946899 192.0.2.100	198.51.100.100 ICM	P 102	0x9c0e (39950)	64 Echo (ping) request	id=0x0022, seq=13/3328, ttl=64 (no response found!)
11 2022-08-04 07:22:10.277953070 192.0.2.100	198.51.100.100 ICM	P 112	0x9ccb (40139)	64 Echo (ping) request	id=0x0022, seq=14/3584, ttl=64 (no response found!)
12 2022-08-04 07:22:10.277954736 192.0.2.100	198.51.100.100 ICM	P 102	0x9ccb (40139)	64 Echo (ping) request	id=0x0022, seq=14/3584, ttl=64 (no response found!)
13 2022-08-04 07:22:11.301931282 192.0.2.100	198.51.100.100 ICM	P 112	0x9d84 (40324)	64 Echo (ping) request	id=0x0022, seq=15/3840, ttl=64 (no response found!)
14 2022-08-04 07:22:11.301933600 192.0.2.100	198.51.100.100 ICM	P 102	0x9d84 (40324)	64 Echo (ping) request	id=0x0022, seq=15/3840, ttl=64 (no response found!)
15 2022-08-04 07:22:12.325936521 192.0.2.100	198.51.100.100 ICM	P 112	0x9da2 (40354)	64 Echo (ping) request	id=0x0022, seq=16/4096, ttl=64 (no response found!)
16 2022-08-04 07:22:12.325937895 192.0.2.100	198.51.100.100 ICM	P 102	0x9da2 (40354)	64 Echo (ping) request	id=0x0022, seg=16/4096, ttl=64 (no response found!)
17 2022-08-04 07:22:13.326988040 192.0.2.100	198.51.100.100 ICM	P 112	0x9e07 (40455)	64 Echo (ping) request	id=0x0022, seq=17/4352, ttl=64 (no response found!)
18 2022-08-04 07:22:13.326990258 192.0.2.100	198.51.100.100 ICM	P 102	0x9e07 (40455)	64 Echo (ping) request	id=0x0022, seq=17/4352, ttl=64 (no response found!)
19 2022-08-04 07:22:14.341944773 192.0.2.100	198.51.100.100 ICM	P 112	0x9e6a (40554)	64 Echo (ping) request	id=0x0022, seq=18/4608, ttl=64 (no response found!)
20 2022-08-04 07:22:14.341946249 192.0.2.100	198.51.100.100 ICM	P 102	0x9e6a (40554)	64 Echo (ping) request	id=0x0022, seq=18/4608, ttl=64 (no response found!)
21 2022-08-04 07:22:15.365941588 192.0.2.100	198.51.100.100 ICM	P 112	0x9efb (40699)	64 Echo (ping) request	id=0x0022, seq=19/4864, ttl=64 (no response found!)
22 2022-08-04 07:22:15.365942566 192.0.2.100	198.51.100.100 ICM	P 102	0x9efb (40699)	64 Echo (ping) request	id=0x0022, seq=19/4864, ttl=64 (no response found!)
23 2022-08-04 07:22:16.389973843 192.0.2.100	198.51.100.100 ICM	P 112	0x9fe8 (40936)	64 Echo (ping) request	id=0x0022, seq=20/5120, ttl=64 (no response found!)
24 2022-08-04 07:22:16.389975129 192.0.2.100	198.51.100.100 ICM	P 102	0x9fe8 (40936)	64 Echo (ping) request	id=0x0022, seq=20/5120, ttl=64 (no response found!)
25 2022-08-04 07:22:17.413936452 192.0.2.100	198.51.100.100 ICM	P 112	0xa079 (41081)	64 Echo (ping) request	id=0x0022, seq=21/5376, ttl=64 (no response found!)
26 2022-08-04 07:22:17.413938090 192.0.2.100	198.51.100.100 ICM	P 102	0xa079 (41081)	64 Echo (ping) request	id=0x0022, seg=21/5376, ttl=64 (no response found!)
27 2022-08-04 07:22:18.437954335 192.0.2.100	198.51.100.100 ICM	P 112	0xa11e (41246)	64 Echo (ping) request	id=0x0022, seg=22/5632, ttl=64 (no response found!)
<			1 1		
Ename 2: 102 hutes on wire (016 hits) 102 hutes can	turned (016 hits) on in	terface canture u0	1 14 0		an an 76 fo an an th an sa se od an ha na an an an
Ethernet TT_Src: Whare Od:e8:he (00:50:56:0d:e8:he) Det: a2:76:f2:00:00	th (a2:76:f2:00:00	_1, 10 0		10 08 00 45 00 00 54 95 74 40 00 40 01 b8 38 c0 00
902 10 Victual LAN DRT: 0 DET: 0 TD: 205	J, DSC: 02170112100100	10 (02.70112.00100	0110)	00	20 02 64 c6 33 64 64 08 00 eb 95 00 22 00 01 88 73 ·d·3dd·····"···s
- Deigeity: Best Effort (defau	(1+) (0)			00	30 eb 62 00 00 00 00 d9 9d 00 00 00 00 00 00 10 11 ·b·····
a = DET: Inaligible				00	40 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21
0000 1100 1101 - TD: 205				00	50 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 "#\$%&'() *+,/01
Tune: TDu4 (0x0000)	2			00	60 32 33 34 35 36 37 234567
Internet Destacel Vension 4, Sect 103, 0, 3, 100, Date					
internet Protocol version 4, SPC: 192.0.2.100, DSC: .	1100 5 1 1000 1000				
Internet Control Message Protocol	198.51.100.100				

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。

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info		
Γ.	1 2022-08-04 08:18:24.572548869	192.168.247.100	192.168.247.102	ICMP	128	0x609e (24734)	255 Echo (ping) re	equest	id=0x007b, seq=0/0, ttl=255 (no response found!)
	2 2022-08-04 08:18:24.572550073	192.168.247.100	192.168.247.102	ICMP	118	0x609e (24734)	255 Echo (ping) re	equest	id=0x007b, seq=0/0, ttl=255 (no response found!)
	3 2022-08-04 08:18:24.573286630	192.168.247.100	192.168.247.102	ICMP	128	0x609f (24735)	255 Echo (ping) re	equest	id=0x007b, seq=1/256, ttl=255 (no response found!)
	4 2022-08-04 08:18:24.573287640	192.168.247.100	192.168.247.102	ICMP	118	0x609f (24735)	255 Echo (ping) re	equest	id=0x007b, seq=1/256, ttl=255 (no response found!)
	5 2022-08-04 08:18:24.573794751	192.168.247.100	192.168.247.102	ICMP	128	0x60a0 (24736)	255 Echo (ping) re	equest	id=0x007b, seq=2/512, ttl=255 (no response found!)
	6 2022-08-04 08:18:24.573795748	192.168.247.100	192.168.247.102	ICMP	118	0x60a0 (24736)	255 Echo (ping) re	equest	id=0x007b, seq=2/512, ttl=255 (no response found!)
	7 2022-08-04 08:18:24.574368638	192.168.247.100	192.168.247.102	ICMP	128	0x60a1 (24737)	255 Echo (ping) re	equest	id=0x007b, seq=3/768, ttl=255 (no response found!)
	8 2022-08-04 08:18:24.574369574	192.168.247.100	192.168.247.102	ICMP	118	0x60a1 (24737)	255 Echo (ping) re	equest	id=0x007b, seq=3/768, ttl=255 (no response found!)
	9 2022-08-04 08:18:24.574914512	192.168.247.100	192.168.247.102	ICMP	128	0x60a2 (24738)	255 Echo (ping) re	equest	id=0x007b, seq=4/1024, ttl=255 (no response found!)
	10 2022-08-04 08:18:24.574915415	192.168.247.100	192.168.247.102	ICMP	118	0x60a2 (24738)	255 Echo (ping) re	equest	id=0x007b, seq=4/1024, ttl=255 (no response found!)
	11 2022-08-04 08:18:24.575442569	192.168.247.100	192.168.247.102	ICMP	128	0x60a3 (24739)	255 Echo (ping) re	equest	id=0x007b, seq=5/1280, ttl=255 (no response found!)
	12 2022-08-04 08:18:24.575443601	192.168.247.100	192.168.247.102	ICMP	118	0x60a3 (24739)	255 Echo (ping) re	equest	id=0x007b, seq=5/1280, ttl=255 (no response found!)
	13 2022-08-04 08:18:24.575918119	192.168.247.100	192.168.247.102	ICMP	128	0x60a4 (24740)	255 Echo (ping) re	equest	id=0x007b, seq=6/1536, ttl=255 (no response found!)
	14 2022-08-04 08:18:24.575919057	192.168.247.100	192.168.247.102	ICMP	118	0x60a4 (24740)	255 Echo (ping) re	equest	id=0x007b, seq=6/1536, ttl=255 (no response found!)
	15 2022-08-04 08:18:24.576407671	192.168.247.100	192.168.247.102	ICMP	128	0x60a5 (24741)	255 Echo (ping) re	equest	id=0x007b, seq=7/1792, ttl=255 (no response found!)
	16 2022-08-04 08:18:24.576408585	192.168.247.100	192.168.247.102	ICMP	118	0x60a5 (24741)	255 Echo (ping) re	equest	id=0x007b, seq=7/1792, ttl=255 (no response found!)
	17 2022-08-04 08:18:24.576885643	192.168.247.100	192.168.247.102	ICMP	128	0x60a6 (24742)	255 Echo (ping) re	equest	id=0x007b, seq=8/2048, ttl=255 (no response found!)
	18 2022-08-04 08:18:24.576886561	192.168.247.100	192.168.247.102	ICMP	118	0x60a6 (24742)	255 Echo (ping) re	equest	1d=0x007b, seq=8/2048, ttl=255 (no response found!)
	19 2022-08-04 08:18:24.577394328	192.168.247.100	192.168.247.102	ICMP	128	0x60a7 (24743)	255 Echo (ping) re	equest	id=0x007b, seq=9/2304, ttl=255 (no response found!)
	20 2022-08-04 08:18:24.577395234	192.168.247.100	192.168.247.102	ICMP	118	0x60a7 (24743)	255 Echo (ping) re	equest	1d=0x007b, seq=9/2304, ttl=255 (no response found!)
	21 2022-08-04 08:18:24.577987632	192.168.247.100	192.168.247.102	ICMP	128	0x60a8 (24744)	255 Echo (ping) re	equest	1d=0x007b, seq=10/2560, ttl=255 (no response found!)
	22 2022-08-04 08:18:24.57/989290	192.168.247.100	192.168.247.102	ICMP	118	0x60a8 (24/44)	255 Echo (ping) re	equest	1d=0x007b, seq=10/2560, ttl=255 (no response found!)
	23 2022-08-04 08:18:24.5/8448/81	192.168.247.100	192.168.247.102	TCHP	128	0x60a9 (24745)	255 Echo (ping) Pe	equest	1d=0x007b, seq=11/2016, ttl=255 (no response found!)
	24 2022-08-04 08:18:24.578449909	192.108.247.100	192.108.247.102	TCMP	110	0x00a9 (24745)	255 Echo (ping) re	equest	id=0x007b, seq=11/2010, ttl=255 (no response found!)
	25 2022-08-04 08:18:24.578900043	192.168.247.100	192.168.247.102	TCHP	128	0x60aa (24746)	255 Echo (ping) Pe	equest	id=0x007b, seq=12/3072, ttl=255 (no response found!)
	20 2022-00-04 00:10:24.570900097	192.108.247.100	192.108.247.102	TCMP	110	0x00aa (24740)	255 Echo (ping) re	equest	id=0x007b, seq=12/3072, ttl=255 (no response foundl)
	27 2022-00-04 08:10:24.579420902	192.100.247.100	192.100.247.102	ICHP	120	000000 (24/4/)	255 ECHO (prng) 14	equest	10-6x06/0, seq=15/5526, CC1=255 (no response round)
<									
> F	rame 1: 128 bytes on wire (1024 bits), 128 bytes capt	tured (1024 bits) or	n interface ca	pture_u0_	3, id 0		0000	a2 76 f2 00 00 1c 00 17 df d6 ec 00 89 26 80 3d · v · · · · · & · ·
> E	thernet II, Src: Cisco d6:ec:00 (00:	17:df:d6:ec:00),	Dst: a2:76:f2:00:0	ð:1c (a2:76:f2	:00:00:10	:)		0010	00 00 81 00 03 e9 81 00 00 cf 08 00 45 00 00 64
ΥV	N-Tag							0020	
	1	= Direction	: From Bridge					0040	ab cd
	.0	= Pointer:	vit_id					0050	ab cd
		= Destinati	on: 61	A				0060	ab cd
		= Looped: N	0	41				0070	ab cd
	0	···· = Reserved:	0						
		= Version:	0						
	Turne: 902 10 Virtual LAN (0x9100)	oooo = source: o							
J 8	02 10 Virtual IAN DRI' A DET A T	D: 1001		_					
	and = Priority: Ret	t Effort (defaul	t) (0)	-					
	B DET: Ineligi	ale	(0)</td <td>21</td> <td></td> <td></td> <td></td> <td></td> <td></td>	21					
	0011 1110 1001 = ID: 1001	PAC .		2					
	Type: 802.10 Virtual LAN (0x8100)								
V 8	02.10 Virtual LAN, PRI: 0, DEI: 0, I	D: 207							
Ĩ	000 = Priority: Be	st Effort (defaul	t) (0)						
	0 = DEI: Ineligit	ole							
	0000 1100 1111 = ID: 207			2					
	Type: IPv4 (0x0800)			4					
> 1	nternet Protocol Version 4, Src: 192	.168.247.100, Dst	: 192.168.247.102						
> 1	nternet Control Message Protocol								

2番目のパケットを選択し、キーポイントを確認します。

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

No.	Time	Source	Destination	Protocol	Length	19 ID	JP TTL Info		
E.	1 2022-08-04 08:18:24.572548869	192.168.247.100	192.168.247.102	ICMP	128	0x609e (24734)	255 Echo (ping) requ	uest i	ld=0x007b, seq=0/0, ttl=255 (no response found!)
	2 2022-08-04 08:18:24.572550073	192.168.247.100	192.168.247.102	ICMP	118	0x609e (24734)	255 Echo (ping) requ	uest i	id=0x007b, seq=0/0, ttl=255 (no response found!)
	3 2022-08-04 08:18:24.573286630	192.168.247.100	192.168.247.102	ICMP	128	0x609f (24735)	255 Echo (ping) requ	uest i	id=0x007b, seq=1/256, ttl=255 (no response found!)
	4 2022-08-04 08:18:24.573287640	192.168.247.100	192.168.247.102	ICMP	118	0x609f (24735)	255 Echo (ping) requ	uest i	id=0x007b, seq=1/256, ttl=255 (no response found!)
	5 2022-08-04 08:18:24.573794751	192.168.247.100	192.168.247.102	ICMP	128	0x60a0 (24736)	255 Echo (ping) requ	uest i	id=0x007b, seq=2/512, ttl=255 (no response found!)
	6 2022-08-04 08:18:24.573795748	192.168.247.100	192.168.247.102	ICMP	118	0x60a0 (24736)	255 Echo (ping) requ	uest i	id=0x007b, seq=2/512, ttl=255 (no response found!)
	7 2022-08-04 08:18:24.574368638	192.168.247.100	192.168.247.102	ICMP	128	0x60a1 (24737)	255 Echo (ping) requ	uest i	id=0x007b, seq=3/768, ttl=255 (no response found!)
	8 2022-08-04 08:18:24.574369574	192.168.247.100	192.168.247.102	ICMP	118	0x60a1 (24737)	255 Echo (ping) requ	uest i	id=0x007b, seq=3/768, ttl=255 (no response found!)
	9 2022-08-04 08:18:24.574914512	192.168.247.100	192.168.247.102	ICMP	128	0x60a2 (24738)	255 Echo (ping) requ	uest i	id=0x007b, seq=4/1024, ttl=255 (no response found!)
	10 2022-08-04 08:18:24.574915415	192.168.247.100	192.168.247.102	ICMP	118	0x60a2 (24738)	255 Echo (ping) requ	uest i	id=0x007b, seq=4/1024, ttl=255 (no response found!)
	11 2022-08-04 08:18:24.575442569	192.168.247.100	192.168.247.102	ICMP	128	0x60a3 (24739)	255 Echo (ping) requ	uest i	id=0x007b, seq=5/1280, ttl=255 (no response found!)
	12 2022-08-04 08:18:24.575443601	192.168.247.100	192.168.247.102	ICMP	118	0x60a3 (24739)	255 Echo (ping) requ	uest i	id=0x007b, seq=5/1280, ttl=255 (no response found!)
	13 2022-08-04 08:18:24.575918119	192.168.247.100	192.168.247.102	ICMP	128	0x60a4 (24740)	255 Echo (ping) requ	uest i	id=0x007b, seq=6/1536, ttl=255 (no response found!)
	14 2022-08-04 08:18:24.575919057	192.168.247.100	192.168.247.102	ICMP	118	0x60a4 (24740)	255 Echo (ping) requ	uest i	id=0x007b, seq=6/1536, ttl=255 (no response found!)
	15 2022-08-04 08:18:24.576407671	192.168.247.100	192.168.247.102	ICMP	128	0x60a5 (24741)	255 Echo (ping) requ	uest i	id=0x007b, seq=7/1792, ttl=255 (no response found!)
	16 2022-08-04 08:18:24.576408585	192.168.247.100	192.168.247.102	ICMP	118	0x60a5 (24741)	255 Echo (ping) requ	uest i	id=0x007b, seq=7/1792, ttl=255 (no response found!)
	17 2022-08-04 08:18:24.576885643	192.168.247.100	192.168.247.102	ICMP	128	0x60a6 (24742)	255 Echo (ping) requ	uest i	id=0x007b, seq=8/2048, ttl=255 (no response found!)
	18 2022-08-04 08:18:24.576886561	192.168.247.100	192.168.247.102	ICMP	118	0x60a6 (24742)	255 Echo (ping) requ	uest i	id=0x007b, seq=8/2048, ttl=255 (no response found!)
	19 2022-08-04 08:18:24.577394328	192.168.247.100	192.168.247.102	ICMP	128	0x60a7 (24743)	255 Echo (ping) requ	uest i	id=0x007b, seq=9/2304, ttl=255 (no response found!)
	20 2022-08-04 08:18:24.577395234	192.168.247.100	192.168.247.102	ICMP	118	0x60a7 (24743)	255 Echo (ping) requ	uest i	id=0x007b, seq=9/2304, ttl=255 (no response found!)
	21 2022-08-04 08:18:24.577987632	192.168.247.100	192.168.247.102	ICMP	128	0x60a8 (24744)	255 Echo (ping) requ	uest i	id=0x007b, seq=10/2560, ttl=255 (no response found!)
	22 2022-08-04 08:18:24.577989290	192.168.247.100	192.168.247.102	ICMP	118	0x60a8 (24744)	255 Echo (ping) requ	uest i	id=0x007b, seq=10/2560, ttl=255 (no response found!)
	23 2022-08-04 08:18:24.578448781	192.168.247.100	192.168.247.102	ICMP	128	0x60a9 (24745)	255 Echo (ping) requ	uest i	id=0x007b, seq=11/2816, ttl=255 (no response found!)
	24 2022-08-04 08:18:24.578449909	192.168.247.100	192.168.247.102	ICMP	118	0x60a9 (24745)	255 Echo (ping) requ	uest i	id=0x007b, seq=11/2816, ttl=255 (no response found!)
	25 2022-08-04 08:18:24.578900043	192.168.247.100	192.168.247.102	ICMP	128	0x60aa (24746)	255 Echo (ping) requ	uest i	id=0x007b, seq=12/3072, ttl=255 (no response found!)
	26 2022-08-04 08:18:24.578900897	192.168.247.100	192.168.247.102	ICMP	118	0x60aa (24746)	255 Echo (ping) requ	uest i	id=0x007b, seq=12/3072, ttl=255 (no response found!)
	27 2022-08-04 08:18:24.579426962	192.168.247.100	192.168.247.102	ICMP	128	0x60ab (24747)	255 Echo (ping) requ	uest i	id=0x007b, seq=13/3328, ttl=255 (no response found!)
<									
5.6	Frame 2: 118 bytes on wire (944 bits)	118 bytes cant	uned (944 hits) on	interface cant	ure u8 3.	id 0		0000 4	a2 76 f2 00 00 1c 00 17 df d6 ec 00 81 00 00 cf
S I	Ethernet II. Src: Cisco d6:ec:00 (00:	17:df:d6:ec:00).	Dst: a2:76:f2:00:0	1:1c (a2:76:f2	:00:00:10	-)		0010	08 00 45 00 00 64 60 9e 00 00 ff 01 ea dd c0 a8 ··E··d`· ·····
5	R02.10 Virtual LAN, PRI: 0, DFI: 0, I	D: 207	0.000 000000000000000000000000000000000			.,		0020 f	f7 64 c0 a8 f7 66 08 00 e5 c8 00 7b 00 00 00 00 ·d···f·· ···{···
1	000	st Effort (defaul	t) (0)	_				0030 0	ee e2 4d 8c 4a 78 ab cd ab cd ab cd ab cd ab cd ab cdM.Jx
		ble						0040 a	ab cd
	0000 1100 1111 = ID: 207			2				0050 a	ab cd
	Type: IPv4 (0x0800)			4				0060 a	ab cd
Ъİ	Internet Protocol Version 4, Src: 192	.168,247,100, Ds	: 192,168,247,102					0070 4	ab cd ab cd ab cd
	Internet Control Message Protocol								
ĽĽ									
-									

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 一要求
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、	イーサネット		一要求
Portchannel1サブインタ	1/4		
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			

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。

Overview Inter	faces Logical Devices Se	ecurity Engine Platf	orm Settings									System Tools	Help admin
Capture Session	Filter List												_
Filter List												Ad	id Filter
	_	From	_	_	_	То	_	-					
Filter Name	MAC	IPv4	IPv6	Port	MAC	IPv4	IPv6	Port	Protocol	Inner vlan	Outer vian	EtherType	
filter_icmp	00:00:00:00:00:00	192.0.2.100	п	0	00:00:00:00:00:00	192.0.2.100	п	0	1	0	0	0	/8
				Edit Packe	t Filter								
				Filter Name*	filter_icmp								
				Protocol	ICMP_IPv4 ¥								
				EtherType	Any 👻								
				Inner vlan	0	Outer vlan	0						
				Source		Destination							
				IPv4	192.0.2.100	IPv4	198.51.100.100						
				IPv6	::	IPv6	:						
				Port	0	Port	0						
				MAC	00:00:00:00:00:00	MAC	00:00:00:00:00						
							Save	Cancel					

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。

Overview Interfaces Logical Devices Security Engine Platform Settings	System	Tools Help admin
	Packet Capture	Troubleshooting Logs
Capture Session Fiter List		
C Refresh	Capture Session Dele	te All Sessions
No Session available		

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。

Overview Interfaces Logical Devices Security Engine Platform Settings	System Tools Help admin
Select an instance: ftd1 v	Seve and Run Seve Cancel
ftd1	Session Name* Cap1
Rherset/2	Buffer Size 256 MB Snap length: 1518 Bytes Store Packets Overwrite Append
Ethernet1/3 FTD FTD Ethernet1/9. Ethernet1/10	Capture Filter Apply Capture All Apply Create Filter Apply filter_icmp To Ethernet1/2
EthernetI/1	

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 / show app-ir	'ssa# nstance						
App Name	Identifier Slot I	D Admin	State Oper State	Running Version	Startup	Version	Deploy Ty
ftd	ftdl						
1	Enabled	Online	7.2.0.82	7.2.0.82	Native	No	

2. <u>https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml</u>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。

Overview I	nterfaces	Logical Devices	Security Engine	Platform Settings					System T	ools Help	admin
Capture Sess	ion Filter L	lst									
								C Refresh Capture S	Session Delete All S	essions	
•	cap1		Drop Count: 0		Operational State: up		Buffer Size: 256 MB	Snap Length: 1518 Bytes			8
Interface Na	me	Filter		File Size (in bytes)	File Name	Device Name					
Ethernet1/2		filter_icmp		84340	cap1-ethernet-1-2-0.pcap	ftd1	*				

FXOSのCLI

scope packet-captureでキャプチャの詳細を確認します。

<#root>

firepower#

scope packet-capture

firepower /packet-capture #

show 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
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。

	a Time	Saurea	Dectionting	Protocol	Length	10.10	ID TTI MA		-
14	1 2022 00 02 15:46:55 602277760	102 0 2 100	109 51 100 100	TCMD	Length 109	P 10	64 Echo (pipg) poquest	id=0x0010 con=240/22000 ttl=64 (no r	
	2 2022-08-02 15:46:55 603277700	102.0.2.100	108 51 100 100	TCMP	103	0x0012 (18)	64 Echo (ping) request	id=0x0018, Seq=349/23809, tt1=04 (no r	
	2 2022-08-02 15:40:55:005275088	102.0.2.100	198.51.100.100	TCMP	102 -	exeedb (210)	64 Echo (ping) request	id=0x0018, Seq=349/23809, tt1=04 (no r	
	A 2022-08-02 15:40:50:02/159252	192.0.2.100	198.51.100.100	TCMP	103	exeedb (219)	64 Echo (ping) request	id=0x0018, Seq=350/24005, tt1=04 (no r	
		192.0.2.100	198.51.100.100	TCMP	102	0x0000 (219)	64 Echo (ping) request	id=0x0018, Seq=350/24005, tt1=04 (no r	
	5 2022-08-02 15:40:57.051185195	192.0.2.100	198.51.100.100	TCMP	100	0x01cb (459)	64 Echo (ping) request	id=0x0018, Seq=351/24321, tt1=04 (no r	
	0 2022-08-02 15:40:57.051180787	192.0.2.100	198.51.100.100	TCMP	102	0x01c0 (459)	64 Echo (ping) request	id=0x0018, Seq=351/24321, tt1=04 (no r	
	/ 2022-08-02 15:40:58.0/515551/	192.0.2.100	198.51.100.100	TCMP	100	0x01d6 (470)	64 Echo (ping) request	id=0x0010, seq=352/24577, tt1=64 (no r	
	8 2022-08-02 15:40:58.0/5154505	192.0.2.100	198.51.100.100	TCHP	102	0x0100 (470)	64 Echo (ping) request	id=0x0010, seq=352/24377, tt1=64 (no r	
	9 2022-08-02 15:40:59.099152039	192.0.2.100	198.51.100.100	TCHP	108	0x01f4 (500)	64 Echo (ping) request	id=0x0010, seq=353/24833, tt1=64 (no r	
	10 2022-08-02 15:40:59.099153835	192.0.2.100	198.51.100.100	TCHP	102	0x0114 (500)	64 Echo (ping) request	1d=0x0018, Seq=353/24833, tt1=64 (no r	
	11 2022-08-02 15:47:00.723142641	192.0.2.100	198.51.100.100	TCMP	108	0x0119 (505)	64 Echo (ping) request	1d=0x0018, Seq=354/25089, tt1=64 (no r	
	12 2022-08-02 15:47:00.723144643	192.0.2.100	198.51.100.100	TCMP	102	0x0119 (505)	64 Echo (ping) request	1d=0x0018, seq=354/25089, tt1=64 (no r	
	13 2022-08-02 15:47:01.747162204	192.0.2.100	198.51.100.100	TCMP	108	0x026e (622)	64 Echo (ping) request	1d=0x0018, seq=355/25345, tt1=64 (no r	
	14 2022-08-02 15:47:01.747163783	192.0.2.100	198.51.100.100	TCMP	102	0x026e (622)	64 Echo (ping) request	1d=0x0018, seq=355/25345, tt1=64 (no r	
	15 2022-08-02 15:47:02.771209952	192.0.2.100	198.51.100.100	TCMP	108	0x020c (700)	64 Echo (ping) request	1d=0x0018, seq=356/25601, tt1=64 (no r	
	16 2022-08-02 15:47:02.771211062	192.0.2.100	198.51.100.100	TCMP	102	0x020c (700)	64 Echo (ping) request	1d=0x0018, seq=356/25601, tt1=64 (no r	
	1/ 2022-08-02 15:4/:03.//2258550	192.0.2.100	198.51.100.100	TCMP	108	0x032f (815)	64 Echo (ping) request	1d=0x0018, seq=35//2585/, tt1=64 (no r	
	18 2022-08-02 15:47:03.772259724	192.0.2.100	198.51.100.100	ICMP	102	0X032T (815)	64 Echo (ping) request	1d=0x0018, seq=35//2585/, tt1=64 (no r	
	19 2022-08-02 15:47:04.791118519	192.0.2.100	198.51.100.100	ICMP	108	0x040f (1039)	64 Echo (ping) request	1d=0x0018, seq=358/26113, tt1=64 (no r	
	20 2022-08-02 15:47:04.791119721	192.0.2.100	198.51.100.100	ICMP	102	0x040† (1039)	64 Echo (ping) request	1d=0x0018, seq=358/26113, ttl=64 (no r	~
<								>	_
>	Frame 1: 108 bytes on wire (864 bit	ts), 108 bytes c	aptured (864 bits) (on interfac	e capture_u0_	1, it 0000 58 9	97 bd b9 77 0e 00 50 56 9d e	8 be 89 26 80 0a X ··· W ·· P V ··· · & ·	
>	Ethernet II, Src: VMware 9d:e8:be	(00:50:56:9d:e8:	be), Dst: Cisco b9:7	77:0e (58:9	7:bd:b9:77:0e) 0010 00	00 81 00 00 66 08 00 45 00 0	0 54 00 12 40 00 ····· t·· E·· t·· @·	
Ň	VN-Tag					0020 40	01 40 90 00 00 02 64 06 33 0	4 64 68 66 96 67 @··································	
	1	= Direct	ion: From Bridge			0030 00	18 01 50 02 46 09 62 00 00 0	6 17 18 19 1a 1b	
	.0	= Pointe	er: vif_id			0050 1c	1d 1e 1f 20 21 22 23 24 25 2	6 27 28 29 2a 2b ···· !"# \$%&'()"+	
	00 0000 0000 1010	= Destin	ation: 10			0060 2c	2d 2e 2f 30 31 32 33 34 35 3	6 37/0123 4567	
	0	= Looped	1: No 4					,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
		= Reserv	red: Ø						
	00	= Versio	on: 0						
	0000 00	00 0000 = Source	: 0						
	Type: 802.1Q Virtual LAN (0x8100)							
×	802.1Q Virtual LAN, PRI: 0, DEI: 0	, ID: 102							
	000 = Priority:	Best Effort (def	ault) (0)						
	0 = DEI: Ineli	gible	5						
	0000 0110 0110 = ID: 102								
	Type: IPv4 (0x0800)								
>	Internet Protocol Version 4, Src: :	192.0.2.100, Dst	: 198.51.100.100						
>	Internet Control Message Protocol		4						
<						>			

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。

No	p. Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info		^
C	1 2022-08-02 15:46:55.603277760	192.0.2.100	198.51.100.100	ICMP	108 1	0x0012 (18)	64 Echo (ping) reques	t id=0x0018, seq=349/2380	9, ttl=64 (no r
	2 2022-08-02 15:46:55.603279688	192.0.2.100	198.51.100.100	ICMP	102	0x0012 (18)	64 Echo (ping) reques	t id=0x0018, seq=349/2380	9, ttl=64 (no r
	3 2022-08-02 15:46:56.627139252	192.0.2.100	198.51.100.100	ICMP	108	0x00db (219)	64 Echo (ping) reques	t id=0x0018, seq=350/2406	5, ttl=64 (no r
	4 2022-08-02 15:46:56.627140919	192.0.2.100	198.51.100.100	ICMP	102	0x00db (219)	64 Echo (ping) reques	t id=0x0018, seq=350/2406	5, ttl=64 (no r
	5 2022-08-02 15:46:57.651185193	192.0.2.100	198.51.100.100	ICMP	108	0x01cb (459)	64 Echo (ping) reques	t id=0x0018, seq=351/2432	1, ttl=64 (no r
	6 2022-08-02 15:46:57.651186787	192.0.2.100	198.51.100.100	ICMP	102	0x01cb (459)	64 Echo (ping) reques	t id=0x0018, seq=351/2432	1, ttl=64 (no r
	7 2022-08-02 15:46:58.675153317	192.0.2.100	198.51.100.100	ICMP	108	0x01d6 (470)	64 Echo (ping) reques	t id=0x0018, seq=352/2457	7, ttl=64 (no r
	8 2022-08-02 15:46:58.675154503	192.0.2.100	198.51.100.100	ICMP	102	0x01d6 (470)	64 Echo (ping) reques	t id=0x0018, seq=352/2457	7, ttl=64 (no r
	9 2022-08-02 15:46:59.699152639	192.0.2.100	198.51.100.100	ICMP	108	0x01f4 (500)	64 Echo (ping) reques	t id=0x0018, seq=353/2483	3, ttl=64 (no r
	10 2022-08-02 15:46:59.699153835	192.0.2.100	198.51.100.100	ICMP	102	0x01f4 (500)	64 Echo (ping) reques	t id=0x0018, seq=353/2483	3, ttl=64 (no r
	11 2022-08-02 15:47:00.723142641	192.0.2.100	198.51.100.100	ICMP	108	0x01f9 (505)	64 Echo (ping) reques	t id=0x0018, seq=354/2508	9, ttl=64 (no r
	12 2022-08-02 15:47:00.723144643	192.0.2.100	198.51.100.100	ICMP	102	0x01f9 (505)	64 Echo (ping) reques	t id=0x0018, seq=354/2508	9, ttl=64 (no r
	13 2022-08-02 15:47:01.747162204	192.0.2.100	198.51.100.100	ICMP	108	0x026e (622)	64 Echo (ping) reques	t id=0x0018, seq=355/2534	5, ttl=64 (no r
	14 2022-08-02 15:47:01.747163783	192.0.2.100	198.51.100.100	ICMP	102	0x026e (622)	64 Echo (ping) reques	t id=0x0018, seq=355/2534	5, ttl=64 (no r
	15 2022-08-02 15:47:02.771209952	192.0.2.100	198.51.100.100	ICMP	108	0x02bc (700)	64 Echo (ping) reques	t id=0x0018, seq=356/2560	1, ttl=64 (no r
	16 2022-08-02 15:47:02.771211062	192.0.2.100	198.51.100.100	ICMP	102	0x02bc (700)	64 Echo (ping) reques	t id=0x0018, seq=356/2560	1, ttl=64 (no r
	17 2022-08-02 15:47:03.772258550	192.0.2.100	198.51.100.100	ICMP	108	0x032f (815)	64 Echo (ping) reques	t id=0x0018, seq=357/2585	7, ttl=64 (no r
	18 2022-08-02 15:47:03.772259724	192.0.2.100	198.51.100.100	ICMP	102	0x032f (815)	64 Echo (ping) reques	t id=0x0018, seq=357/2585	7, ttl=64 (no r
	19 2022-08-02 15:47:04.791118519	192.0.2.100	198.51.100.100	ICMP	108	0x040f (1039)	64 Echo (ping) reques	t id=0x0018, seq=358/2611	3, ttl=64 (no r
	20 2022-08-02 15:47:04.791119721	192.0.2.100	198.51.100.100	ICMP	102	0x040f (1039)	64 Echo (ping) reques	t id=0x0018, seq=358/2611	3, ttl=64 (no r 🗸
<									>
>	Frame 2: 102 bytes on wire (816 bit	s), 102 bytes ca	ptured (816 bits) or	interface ca	pture u0 1	, i 0000 58 97	bd b9 77 0e 00 50 56 9d	e8 be 81 00 00 66 X····w	1P. Vf
>	Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:b	e), Dst: Cisco b9:77	:0e (58:97:bo	:b9:77:0e)	0010 08 00	45 00 00 54 00 12 40 00	40 01 4d 9b c0 00 ··E··	T·· @·@·M···
~	802.10 Virtual LAN, PRI: 0, DEI: 0,	ID: 102				0020 02 64	c6 33 64 64 08 00 9e 67	00 18 01 5d e2 46 ·d·3d	ld·· ·g···]·F
	000 = Priority: 1	Best Effort (defa	ault) (0)			0030 e9 62	00 00 00 00 c1 a6 0c 00	00 00 00 00 10 11 ·b···	
	0 = DEI: Inelig	gible	3			0040 12 13	14 15 16 17 18 19 1a 1b	1c 1d 1e 1f 20 21	
	0000 0110 0110 = ID: 102		-			0050 22 23	24 25 26 27 28 29 2a 2b	2c 2d 2e 2f 30 31 "#\$%8	() *+,/01
	Type: IPv4 (0x0800)					0000 32 33	34 35 36 37	23456	1
>	Internet Protocol Version 4, Src: 1	92.0.2.100, Dst:	198.51.100.100						
>	Internet Control Message Protocol		2						
1									

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	キプャイト	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。

Overview	Interfaces	Logical Devices	Security Engine	Platforn	n Settings				s	iystem	Tools	Help	admin
Capture Ses	ision Filter Lis	t											
								C Refresh Captu	re Session	Delete Al	Sessions		
	cap1	Drop Coun	t: 0	Operat	ional State: up	Buffer Size: 256 MB		Snap Length: 151	8 Bytes			٩.	6. I 🖸 I
Interface Na	ame	Filter			File Size (in bytes)	File Name	Device Name						
Ethernet1/2		None			34700	cap1-ethernet-1-2-0.pcap	ftd1		<u>*</u>				

2. 動作状態がDOWN - Session_Admin_Shut:

Overview	Interfaces	Logical Devices	Security Engine	Platform Settings					System	Tools	Help	admin
Capture Sess	sion Filter Lis	t										
								Capture Capture	Session Delete	All Sessions		
	cap1	Drop Count	: 0	Operational State: DOWN - Sessie	on_Admin_Shut	Buffer Size: 256 MB		Snap Length: 1518	lytes		0	8 🛛
Interface Na	me	Filter		File Size (in bytes)	F	File Name	Device Name					
Ethernet1/2		None		218828	c	cap1-ethemet-1-2-0.pcap	ftd1	2	Ł			

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。

Overview	Interfaces	Logical Devices	Security Engine	Platform Settings				System Tools	Help	admin
Capture Ses	sion Filter Lis	t								
							Capture Session	Delete All Session	15	
	cap1	Drop Count	: 0	Operational State: DOWN - Session_Admin_Shu	Buffer Size: 256 MB		Snap Length: 1518 Bytes		1	8 🖾
Interface N	ame	Filter		File Size (in bytes)	File Name	Device Name				
Ethernet1/2		None		218828	cap1-ethemet-1-2-0.pcap	ftd1	土			

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。

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 Capture packets on a specific interface 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 packet capture stop Trace the captured packets trace Capture packets based on a particular type 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	interfa	ce M	Management	t1/2		
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	interfa	ce M	Management	t1/1		

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>

```
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	
ір	
ipinip	
ipsec	
mac	Mac-address filter
nos	
ospf	
рср	
pim	
pptp	
sctp	
snp	
spi	SPI value
tcp	
udp	
<cr></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>

>

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/packetcapture/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 port Physical port:	s involved in Packet Capture: 1
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 Filt	er Info
Name:	capsw-1-1
Protocol:	0
Ivlan:	0
Ovlan•	205
	205
Src Ip:	0.0.0
Dest Ip:	0.0.0.0
Src Ipv6:	::
Dest Ipv6:	::
Src MAC:	00:00:00:00:00
Dest MAC:	00:00:00:00:00
Src Port:	0
Dest Port:	0
Ethertype:	0
Total Physical brea	ukout ports involved in Packet Capture: 0
0 packet captured o	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 0.0.0.0 Src Ip: 0.0.0.0 Dest Ip: Src Ipv6: :: Dest Ipv6: :: 00:00:00:00:00:00 Src MAC: 00:00:00:00:00:00 Dest MAC: Src Port: 0 0 Dest Port: 0 Ethertype: 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 Management1/1	outside diagnostic	0 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。

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 de	etail
Packet Capture info	
Name:	capsw
Session:	1
Admin State:	enabled
Oper State:	up
Oper State Reason:	Active
Config Success: Config Fail Reason: Append Flag: Session Mem Usage: Session Pcap Snap I Error Code: Drop Count:	yes : overwrite 256 Len: 1518 0 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 Filte Name:	r Info capsw-1-1

0
0
0
0.0.0.0
0.0.0.0
::
::
00:00:00:00:00:00
00:00:00:00:00:00
0
0
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

Session:

Name:	capsw

Admin State: enabled

1

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 0.0.0.0 Src Ip: Dest Ip: 0.0.0.0 Src Ipv6: :: Dest Ipv6: :: Src MAC: 00:00:00:00:00:00 00:00:00:00:00:00 Dest MAC: Src Port: 0 Dest Port: 0 0 Ethertype: 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						
lotal 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 Filte	r Info						
Name: Protocol:	capsw-1-4 O						
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						
Dest MAC:							
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 Filte	r Info						
Name:	capsw-1-3						
Protocol:							
ivian: Ovlan:							
Src In:	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: I - Ir s - Su S - Sw U - Up M - No	: D - Down ndividual H uspended r vitched R o (port-chan ot in use. M	P - Hot-st - Module - Routed nel) lin-links	- Up in po andby (LAC -removed not met	rt-channel (m P only)	embers)	
Group	Port- Channel	Туре	Protocol	Member Ports		
1	Pol(U)	Eth	LACP	Eth1/3(P)	Eth1/4(P)	

LACP KeepAlive Timer: Channel PeerKeepAliveTimerFast 1 Pol(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。

No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info		^
E	1 2022-08-07 19:50:06.925768	192.0.2.100	198.51.100.100	ICMP	102	0x9a10 (39440)	64 Echo (ping) request	id=0x0034, seq=1/256, ttl=64 (no re	5
	2 2022-08-07 19:50:07.921684	192.0.2.100	198.51.100.100	ICMP	102	0x9a3a (39482)	64 Echo (ping) request	id=0x0034, seq=2/512, ttl=64 (no re-	5
	3 2022-08-07 19:50:08.924468	192.0.2.100	198.51.100.100	ICMP	102	0x9aa6 (39590)	64 Echo (ping) request	id=0x0034, seq=3/768, ttl=64 (no res	5
	4 2022-08-07 19:50:09.928484	192.0.2.100	198.51.100.100	ICMP	102	0x9afe (39678)	64 Echo (ping) request	id=0x0034, seq=4/1024, ttl=64 (no re	e
	5 2022-08-07 19:50:10.928245	192.0.2.100	198.51.100.100	ICMP	102	0x9b10 (39696)	64 Echo (ping) request	id=0x0034, seq=5/1280, ttl=64 (no re	e
	6 2022-08-07 19:50:11.929144	192.0.2.100	198.51.100.100	ICMP	102	0x9b34 (39732)	64 Echo (ping) request	id=0x0034, seq=6/1536, ttl=64 (no re	e
	7 2022-08-07 19:50:12.932943	192.0.2.100	198.51.100.100	ICMP	102	0x9b83 (39811)	64 Echo (ping) request	id=0x0034, seq=7/1792, ttl=64 (no re	e
	8 2022-08-07 19:50:13.934155	192.0.2.100	198.51.100.100	ICMP	102	0x9b8b (39819)	64 Echo (ping) request	id=0x0034, seq=8/2048, ttl=64 (no re	e
	9 2022-08-07 19:50:14.932004	192.0.2.100	198.51.100.100	ICMP	102	0x9c07 (39943)	64 Echo (ping) request	id=0x0034, seq=9/2304, ttl=64 (no re	e
	10 2022-08-07 19:50:15.937143	192.0.2.100	198.51.100.100	ICMP	102	0x9cc6 (40134)	64 Echo (ping) request	id=0x0034, seq=10/2560, ttl=64 (no)	r
	11 2022-08-07 19:50:16.934848	192.0.2.100	198.51.100.100	ICMP	102	0x9d68 (40296)	64 Echo (ping) request	id=0x0034, seq=11/2816, ttl=64 (no)	r
	12 2022-08-07 19:50:17.936908	192.0.2.100	198.51.100.100	ICMP	102	0x9ded (40429)	64 Echo (ping) request	id=0x0034, seq=12/3072, ttl=64 (no)	r
	13 2022-08-07 19:50:18.939584	192.0.2.100	198.51.100.100	ICMP	102	0x9e5a (40538)	64 Echo (ping) request	id=0x0034, seq=13/3328, ttl=64 (no)	r
	14 2022-08-07 19:50:19.941262	192.0.2.100	198.51.100.100	ICMP	102	0x9efb (40699)	64 Echo (ping) request	id=0x0034, seq=14/3584, ttl=64 (no)	r
	15 2022-08-07 19:50:20.940716	192.0.2.100	198.51.100.100	ICMP	102	0x9f50 (40784)	64 Echo (ping) request	id=0x0034, seq=15/3840, ttl=64 (no)	r
	16 2022-08-07 19:50:21.940288	192.0.2.100	198.51.100.100	ICMP	102	0x9fe4 (40932)	64 Echo (ping) request	id=0x0034, seq=16/4096, ttl=64 (no)	r
	17 2022-08-07 19:50:22.943302	192.0.2.100	198.51.100.100	ICMP	102	0xa031 (41009)	64 Echo (ping) request	id=0x0034, seq=17/4352, ttl=64 (no)	r
	18 2022-08-07 19:50:23.944679	192.0.2.100	198.51.100.100	ICMP	102	0xa067 (41063)	64 Echo (ping) request	id=0x0034, seq=18/4608, ttl=64 (no)	r v
<								>	
5	Frame 1: 102 bytes on wire (816 bits	s), 102 hytes can	tured (816 bits)			0000 bc e7 12	34 9a 14 00 50 56 9d e8	be 08 00 45 00 ····4···P V·····E·	
Ś	Ethernet II. Src: VMware 9d:e8:be (0:50:56:9d:e8:be). Dst: Cisco 34:9a	:14 (hc:e7:12)	34:9a:14)	0010 00 54 9a	10 40 00 40 01 b3 9c c0	00 02 64 c6 33 ·T··@·@· ····d·3	
Ś	Internet Protocol Version 4. Src: 19	2.0.2.100. Dst:	198.51.100.100			0020 64 64 08	00 c6 91 00 34 00 01 61	17 f0 62 00 00 dd ····· 4 ··a··b··	
Ś	Internet Control Message Protocol	210121200, 0301	19019111001100		2	0030 00 00 18	ec 08 00 00 00 00 00 10	11 12 13 14 15	
						0040 16 17 18	19 1a 1b 1c 1d 1e 1f 20	21 22 23 24 25 !"#\$%	
						0050 26 27 28	29 2a 2b 2c 2d 2e 2f 30	31 32 33 34 35 &'()*+,/012345	
						0060 36 37 55	55 55 55	670000	

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

1. ICMPエコー要求パケットだけがキャプチャされます。

2. 元のパケットヘッダーにはVLANタグが付いていません。

No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info	^
_	1 2022-08-07 20:40:58.657533	192.0.2.100	198.51.100.100	ICMP	102	0x9296 (37526)	64 Echo (ping) request	id=0x0035, seq=1/256, ttl=64 (no res
	2 2022-08-07 20:40:59.658611	192.0.2.100	198.51.100.100	ICMP	102	0x9370 (37744)	64 Echo (ping) request	id=0x0035, seq=2/512, ttl=64 (no res
	3 2022-08-07 20:41:00.655662	192.0.2.100	198.51.100.100	ICMP	102	0x93f0 (37872)	64 Echo (ping) request	id=0x0035, seq=3/768, ttl=64 (no res
	4 2022-08-07 20:41:01.659749	192.0.2.100	198.51.100.100	ICMP	102	0x946f (37999)	64 Echo (ping) request	id=0x0035, seq=4/1024, ttl=64 (no re
	5 2022-08-07 20:41:02.660624	192.0.2.100	198.51.100.100	ICMP	102	0x94a4 (38052)	64 Echo (ping) request	id=0x0035, seq=5/1280, ttl=64 (no r€
	6 2022-08-07 20:41:03.663226	192.0.2.100	198.51.100.100	ICMP	102	0x952d (38189)	64 Echo (ping) request	id=0x0035, seq=6/1536, ttl=64 (no r€
	7 2022-08-07 20:41:04.661262	192.0.2.100	198.51.100.100	ICMP	102	0x958d (38285)	64 Echo (ping) request	id=0x0035, seq=7/1792, ttl=64 (no re
	8 2022-08-07 20:41:05.665955	192.0.2.100	198.51.100.100	ICMP	102	0x95d8 (38360)	64 Echo (ping) request	id=0x0035, seq=8/2048, ttl=64 (no re
	9 2022-08-07 20:41:06.666538	192.0.2.100	198.51.100.100	ICMP	102	0x964b (38475)	64 Echo (ping) request	id=0x0035, seq=9/2304, ttl=64 (no re
	10 2022-08-07 20:41:07.667298	192.0.2.100	198.51.100.100	ICMP	102	0x972b (38699)	64 Echo (ping) request	id=0x0035, seq=10/2560, ttl=64 (no r
	11 2022-08-07 20:41:08.670540	192.0.2.100	198.51.100.100	ICMP	102	0x980a (38922)	64 Echo (ping) request	id=0x0035, seq=11/2816, ttl=64 (no r
	12 2022-08-07 20:41:09.668278	192.0.2.100	198.51.100.100	ICMP	102	0x9831 (38961)	64 Echo (ping) request	id=0x0035, seq=12/3072, ttl=64 (no r
	13 2022-08-07 20:41:10.672417	192.0.2.100	198.51.100.100	ICMP	102	0x98a2 (39074)	64 Echo (ping) request	id=0x0035, seq=13/3328, ttl=64 (no r
	14 2022-08-07 20:41:11.671369	192.0.2.100	198.51.100.100	ICMP	102	0x98f7 (39159)	64 Echo (ping) request	id=0x0035, seq=14/3584, ttl=64 (no r
	15 2022-08-07 20:41:12.675462	192.0.2.100	198.51.100.100	ICMP	102	0x99e4 (39396)	64 Echo (ping) request	id=0x0035, seq=15/3840, ttl=64 (no r
	16 2022-08-07 20:41:13.674903	192.0.2.100	198.51.100.100	ICMP	102	0x9a84 (39556)	64 Echo (ping) request	id=0x0035, seq=16/4096, ttl=64 (no r
	17 2022-08-07 20:41:14.674093	192.0.2.100	198.51.100.100	ICMP	102	0x9af3 (39667)	64 Echo (ping) request	id=0x0035, seq=17/4352, ttl=64 (no r
	18 2022-08-07 20:41:15.676904	192.0.2.100	198.51.100.100	ICMP	102	Øx9b8e (39822)	64 Echo (ping) request	id=0x0035, seq=18/4608, ttl=64 (no r v
<								>
> Er	rame 1: 102 bytes on wire (816 bits)	, 102 bytes capt	ured (816 bits)			0000 bc e7 12	34 9a 2c 00 50 56 9d e8	be 08 00 45 00 ···4·, P V····E·
> E1	thernet II, Src: VMware 9d:e8:be (00	:50:56:9d:e8:be)	, Dst: Cisco 34:9a:	2c (bc:e7:12:	34:9a:2c)	0010 00 54 92	96 40 00 40 01 bb 16 c0	00 02 64 c6 33 ·T··@·@· ·····d·3
> Ir	nternet Protocol Version 4, Src: 192	2.0.2.100, Dst: 1	98.51.100.100		-	0020 64 64 08	00 58 a8 00 35 00 01 4d	23 f0 62 00 00 dd · · X · · 5 · · M# · b · ·
	nternet Control Message Protocol				2	0030 00 00 9e	c8 04 00 00 00 00 00 10	11 12 13 14 15
	÷					0040 16 17 18	19 1a 1b 1c 1d 1e 1f 20	21 22 23 24 25!"#\$%
						0050 26 27 28	29 2a 2b 2c 2d 2e 2f 30	31 32 33 34 35 & ()*+,/012345
						0060 36 37 55	55 55 55	670000

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

<#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

1

Physical port:

- Slot Id:
- 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: Ivlan:	0 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 Fi	lter Info
Name:	capsw-1-4
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
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 Fi	lter Info
Name:	capsw-1-3
Protocol:	0
IVIAII.	0
Ovlan:	205
Src Ip:	0.0.0.0
Dest Ip:	0.0.0.0
Src Ipv6:	::
Dest Ipv6:	::
STC MAL: Dest MAC:	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 _____ Pol(U) Eth LACP Eth1/3(P) Eth1/4(P) 1 LACP KeepAlive Timer: _____ Channel PeerKeepAliveTimerFast _____ Po1(U) 1 False

Cluster LACP Status:

	Channe1	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。

No.	Time	Source	Destination	Protocol	Length	IP ID		IP TTL Info						^
-	1 2022-08-07 21:21:01.607187	192.0.2.100	198.51.100.100	ICMP	106	0x411f	(16671)	64 Echo (ping)	request	id=0x0037,	seq=1/256,	ttl=64 (r	no res	
	2 2022-08-07 21:21:02.609418	192.0.2.100	198.51.100.100	ICMP	106	0x413a	(16698)	64 Echo (ping)	request	id=0x0037,	seq=2/512,	ttl=64 (r	no res	
	3 2022-08-07 21:21:03.610671	192.0.2.100	198.51.100.100	ICMP	106	0x421a	(16922)	64 Echo (ping)	request	id=0x0037,	seq=3/768,	ttl=64 (r	no res	
	4 2022-08-07 21:21:04.609160	192.0.2.100	198.51.100.100	ICMP	106	0x426c	(17004)	64 Echo (ping)	request	id=0x0037,	seq=4/1024,	tt1=64 ((no re	
	5 2022-08-07 21:21:05.609409	192.0.2.100	198.51.100.100	ICMP	106	0x4310	(17168)	64 Echo (ping)	request	id=0x0037,	seq=5/1280,	ttl=64 ((no re	
	6 2022-08-07 21:21:06.611847	192.0.2.100	198.51.100.100	ICMP	106	0x43df	(17375)	64 Echo (ping)	request	id=0x0037,	seq=6/1536,	ttl=64 ((no re	
	7 2022-08-07 21:21:07.616688	192.0.2.100	198.51.100.100	ICMP	106	0x44d3	(17619)	64 Echo (ping)	request	id=0x0037,	seq=7/1792,	ttl=64 ((no re	
	8 2022-08-07 21:21:08.618023	192.0.2.100	198.51.100.100	ICMP	106	0x4518	(17688)	64 Echo (ping)	request	id=0x0037,	seq=8/2048,	ttl=64 ((no re	
	9 2022-08-07 21:21:09.619326	192.0.2.100	198.51.100.100	ICMP	106	0x453d	(17725)	64 Echo (ping)	request	id=0x0037,	seq=9/2304,	ttl=64 ((no re	
	10 2022-08-07 21:21:10.616696	192.0.2.100	198.51.100.100	ICMP	106	0x462b	(17963)	64 Echo (ping)	request	id=0x0037,	seq=10/2560	, ttl=64	(no r	
	11 2022-08-07 21:21:11.621629	192.0.2.100	198.51.100.100	ICMP	106	0x4707	(18183)	64 Echo (ping)	request	id=0x0037,	seq=11/2816	, ttl=64	(no r	
	12 2022-08-07 21:21:12.619309	192.0.2.100	198.51.100.100	ICMP	106	0x474b	(18251)	64 Echo (ping)	request	id=0x0037,	seq=12/3072	, ttl=64	(no r	
	13 2022-08-07 21:21:13.620168	192.0.2.100	198.51.100.100	ICMP	106	0x4781	(18305)	64 Echo (ping)	request	id=0x0037,	seq=13/3328	, ttl=64	(no r	
	14 2022-08-07 21:21:14.623169	192.0.2.100	198.51.100.100	ICMP	106	0x4858	(18520)	64 Echo (ping)	request	id=0x0037,	seq=14/3584	, ttl=64	(no r	
	15 2022-08-07 21:21:15.622497	192.0.2.100	198.51.100.100	ICMP	106	0x4909	(18697)	64 Echo (ping)	request	id=0x0037,	seq=15/3840	, ttl=64	(no r	
	16 2022-08-07 21:21:16.626226	192.0.2.100	198.51.100.100	ICMP	106	0x490b	(18699)	64 Echo (ping)	request	id=0x0037,	seq=16/4096	, ttl=64	(no r	
	17 2022-08-07 21:21:17.629363	192.0.2.100	198.51.100.100	ICMP	106	0x4932	(18738)	64 Echo (ping)	request	id=0x0037,	seq=17/4352	, ttl=64	(no r	
	18 2022-08-07 21:21:18.626651	192.0.2.100	198.51.100.100	ICMP	106	0x4a05	(18949)	64 Echo (ping)	request	id=0x0037,	seq=18/4608	, ttl=64	(no r	~
<													>	
> 1	Frame 1: 106 bytes on wire (848 bits), 106 bytes car	otured (848 bits)			0000	bc e7 1	2 34 9a 14 00 50	56 9d e8	be 81 00 00	cd4	• P V • • • •		
> 1	Ethernet II, Src: VMware_9d:e8:be (0	0:50:56:9d:e8:be	e), Dst: Cisco_34:9a	a:14 (bc:e7	:12:34:9a:14)	0010	08 00 4	5 00 00 54 41 1f	40 00 40	01 0c 8e c0	00 ··E··T	A- @-@		
~ 8	802.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 205				0020	02 64 c	6 33 64 64 08 00	06 67 00	37 00 01 b0	2c · d · 3dd	··· ·g·7·	··,	
L F	000 B	est Effort (defa	ult) (0)			0030	f0 62 0	0 00 00 00 8e fe	03 00 00	00 00 00 10	11 ·b····			
	0 = DEI: Inelig:	ible				0040	12 13 1	4 15 16 17 18 19	1a 1b 1c	1d 1e 1f 20	21			
	0000 1100 1101 = ID: 205				-	0050	22 23 2	4 25 26 27 28 29	2a 2b 2c	2d 2e 2f 30	31 "#\$%&"	() *+,,	/01	
	Type: IPv4 (0x0800)				2	0000	32 33 3	4 35 36 37 55 55	55 55		234567	00 00		
	Trailer: 55555555													
> 1	Internet Protocol Version 4, Src: 19	2.0.2.100, Dst:	198.51.100.100											
> 1	Internet Control Message Protocol													

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

1. ICMPエコー要求パケットだけがキャプチャされます。

2. 元のパケットヘッダーにはVLANタグ205が付いています。

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info	^
_	1 2022-08-07 21:21:01.607187	192.0.2.100	198.51.100.100	ICMP	106	0x411f (16671)	64 Echo (ping) request	id=0x0037, seq=1/256, ttl=64 (no res
	2 2022-08-07 21:21:02.609418	192.0.2.100	198.51.100.100	ICMP	106	0x413a (16698)	64 Echo (ping) request	id=0x0037, seq=2/512, ttl=64 (no res
	3 2022-08-07 21:21:03.610671	192.0.2.100	198.51.100.100	ICMP	106	0x421a (16922)	64 Echo (ping) request	id=0x0037, seq=3/768, ttl=64 (no res
	4 2022-08-07 21:21:04.609160	192.0.2.100	198.51.100.100	ICMP	106	0x426c (17004)	64 Echo (ping) request	id=0x0037, seq=4/1024, ttl=64 (no r€
	5 2022-08-07 21:21:05.609409	192.0.2.100	198.51.100.100	ICMP	106	0x4310 (17168)	64 Echo (ping) request	id=0x0037, seq=5/1280, ttl=64 (no re
	6 2022-08-07 21:21:06.611847	192.0.2.100	198.51.100.100	ICMP	106	0x43df (17375)	64 Echo (ping) request	id=0x0037, seq=6/1536, ttl=64 (no re
	7 2022-08-07 21:21:07.616688	192.0.2.100	198.51.100.100	ICMP	106	0x44d3 (17619)	64 Echo (ping) request	id=0x0037, seq=7/1792, ttl=64 (no re
	8 2022-08-07 21:21:08.618023	192.0.2.100	198.51.100.100	ICMP	106	0x4518 (17688)	64 Echo (ping) request	id=0x0037, seq=8/2048, ttl=64 (no re
	9 2022-08-07 21:21:09.619326	192.0.2.100	198.51.100.100	ICMP	106	0x453d (17725)	64 Echo (ping) request	id=0x0037, seq=9/2304, ttl=64 (no re
	10 2022-08-07 21:21:10.616696	192.0.2.100	198.51.100.100	ICMP	106	0x462b (17963)	64 Echo (ping) request	id=0x0037, seq=10/2560, ttl=64 (no r
	11 2022-08-07 21:21:11.621629	192.0.2.100	198.51.100.100	ICMP	106	0x4707 (18183)	64 Echo (ping) request	id=0x0037, seq=11/2816, ttl=64 (no r
	12 2022-08-07 21:21:12.619309	192.0.2.100	198.51.100.100	ICMP	106	0x474b (18251)	64 Echo (ping) request	id=0x0037, seq=12/3072, ttl=64 (no r
	13 2022-08-07 21:21:13.620168	192.0.2.100	198.51.100.100	ICMP	106	0x4781 (18305)	64 Echo (ping) request	id=0x0037, seq=13/3328, ttl=64 (no r
	14 2022-08-07 21:21:14.623169	192.0.2.100	198.51.100.100	ICMP	106	0x4858 (18520)	64 Echo (ping) request	id=0x0037, seq=14/3584, ttl=64 (no r
	15 2022-08-07 21:21:15.622497	192.0.2.100	198.51.100.100	ICMP	106	0x4909 (18697)	64 Echo (ping) request	id=0x0037, seq=15/3840, ttl=64 (no r
	16 2022-08-07 21:21:16.626226	192.0.2.100	198.51.100.100	ICMP	106	0x490b (18699)	64 Echo (ping) request	id=0x0037, seq=16/4096, ttl=64 (no r
	17 2022-08-07 21:21:17.629363	192.0.2.100	198.51.100.100	ICMP	106	0x4932 (18738)	64 Echo (ping) request	id=0x0037, seq=17/4352, ttl=64 (no r
	18 2022-08-07 21:21:18.626651	192.0.2.100	198.51.100.100	ICMP	106	0x4a05 (18949)	64 Echo (ping) request	id=0x0037, seq=18/4608, ttl=64 (no r 🗸
<								>
> En	ame 1: 106 bytes on wire (848 bits)	. 106 bytes capt	ured (848 bits)			0000 bc e7 1	2 34 9a 14 00 50 56 9d e8	be 81 00 00 cd ···4···P V·····
> Et	hernet II, Src: VMware 9d:e8:be (00	:50:56:9d:e8:be)	, Dst: Cisco 34:9a:	14 (bc:e7:12:3	34:9a:14)	0010 08 00 4	5 00 00 54 41 1f 40 00 40	01 0c 8e c0 00 ··E··TA·@·@·····
~ 80	2.1Q Virtual LAN, PRI: 0, DEI: 0, I	D: 205	-			0020 02 64 c	6 33 64 64 08 00 06 67 00	37 00 01 b0 2c ·d·3dd·· ·g·7···,
	000 Beiority: Be	st Effort (defaul	t) (0)			0030 f0 62 0	00 00 00 00 8e fe 03 00 00	00 00 00 10 11 ·b·····
	0 = DEI: Ineligi	ble				0040 12 13 1	4 15 16 17 18 19 1a 1b 1c	1d 1e 1f 20 21
	0000 1100 1101 = ID: 205				-	0050 22 23 2	4 25 26 27 28 29 2a 2b 2c	2d 2e 2t 30 31 "#\$%&"() "+,/01
	Type: IPv4 (0x0800)				2	0000 32 33 3	4 35 36 37 55 55 55 55	23456700 00
	Trailer: 5555555							
> In	ternet Protocol Version 4, Src: 192	.0.2.100, Dst: 1	98.51.100.100					
> In	ternet Control Message Protocol							

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 7704 Pcapsize: 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 0 Ethertype: Total Physical breakout ports involved in Packet Capture: 0

66 packets captured on disk using switch capture

Reading of capture file from disk is not supported

この場合、キャプチャは内部ID 18のインターフェイス(セキュアファイアウォール3130の in_data_uplink1インターフェイス)で作成されます。FXOSのlocal-mgmtコマンドシェルでshow portmanager switch statusコマンドを実行すると、インターフェイスIDが表示されます。

<#root>

>

...

connect fxos

firewall#

connect local-mgmt

firewall(local-mgmt)#

show portmanager switch status

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

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

キャプチャファイルの収集

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

ファイル分析のキャプチャ

パケットキャプチャファイルリーダーアプリケーションを使用して、インターフェイス in_data_uplink1のキャプチャファイルを開きます。この例では、Secure Firewall 3100でのパケッ トキャプチャが分析されます。

キーポイントを確認します。この場合、ICMPエコー要求およびエコー応答パケットがキャプチャ されます。これらは、アプリケーションから内部スイッチに送信されるパケットです。

No.	Time	• [Source	Destination	Protocol	Length	IP ID			IP 1	TL Info												^
	1 2022-08-07 22:40:06.685606	ч	192.0.2.100	198.51.100.100	ICMP	102	0x4	193	(19859)		64 Ech	10 (p	oing)	reque	st	id=0	x003a	a, s	eq=33/844	8, tt	tl=64	(repl	
4	2 2022-08-07 22:40:06.685615		198.51.100.100	192.0.2.100	ICMP	102	0x6	dc	(27868)		64 Ech	10 (1	oing)	reply	1	id=0	x003a	a, s	eq=33/844	8, tt	tl=64	(requ	
	3 2022-08-07 22:40:07.684219		192.0.2.100	198.51.100.100	ICMP	102	0x4	168	(19944)		64 ECI	10 (p	oing)	reque	st	id=0	x003a	a, s	eq=34/870	4, tt	tl=64	(repl	
	4 2022-08-07 22:40:07.689300		198.51.100.100	192.0.2.100	ICMP	102	0x6	ib2	(28082)		64 Ech	10 (1	oing)	reply	1	id=0	x003a	a, s	eq=34/870	4, tt	cl=64	(requ	
	5 2022-08-07 22:40:08.685736		192.0.2.100	198.51.100.100	ICMP	102	0x4	edc	(20188)		64 Ech	10 (1	oing)	reque	st	id=0	x003a	a, s	eq=35/896	ð, tt	cl=64	(repl	
	6 2022-08-07 22:40:08.690806		198.51.100.100	192.0.2.100	ICMP	102	0x6	fdt	(28095)		64 Ech	10 (1	oing)	reply	1	id=0	x003a	a, s	eq=35/896	ð, tt	cl=64	(requ	
	7 2022-08-07 22:40:09.690737		192.0.2.100	198.51.100.100	ICMP	102	0x4	F2d	(20269)		64 Ech	10 (1	oing)	reque	st	id=0	x003a	a, s	eq=36/921	6, tt	cl=64	(repl	
	8 2022-08-07 22:40:09.690744		198.51.100.100	192.0.2.100	ICMP	102	0x6	80	(28288)		64 Ech	10 (1	oing)	reply	1	id=0	x003a	a, s	eq=36/921	6, tt	cl=64	(requ	
	9 2022-08-07 22:40:10.692266		192.0.2.100	198.51.100.100	ICMP	102	0x4	fb1	(20401)		64 Ech	10 (1	oing)	reque	st	id=0	x003a	a, s	eq=37/947	2, tt	tl=64	(repl	
	10 2022-08-07 22:40:10.692272		198.51.100.100	192.0.2.100	ICMP	102	0x6	ed5	(28373)		64 Ech	10 (1	oing)	reply	1	id=0	x003a	a, s	eq=37/947	2, tt	cl=64	(requ	
	11 2022-08-07 22:40:11.691159		192.0.2.100	198.51.100.100	ICMP	102	0x50	806	(20488)		64 Ech	10 (1	oing)	reque	st	id=0	x003a	a, s	eq=38/972	8, tt	cl=64	(repl	
	12 2022-08-07 22:40:11.691166		198.51.100.100	192.0.2.100	ICMP	102	0x6	F3b	(28475)		64 Ech	10 (1	oing)	reply	1	id=0	x003a	a, s	eq=38/972	8, tt	cl=64	(requ	
	13 2022-08-07 22:40:12.692135		192.0.2.100	198.51.100.100	ICMP	102	0x50	8d6	(20664)		64 Ech	10 (1	oing)	reque	st	id=0	x003a	a, s	eq=39/998	4, tt	cl=64	(repl	
	14 2022-08-07 22:40:12.697209		198.51.100.100	192.0.2.100	ICMP	102	0x6	fd7	(28631)		64 Ech	10 (1	oing)	reply	1	id=0	x003a	a, s	eq=39/998	4, tt	tl=64	(requ	
	15 2022-08-07 22:40:13.697320		192.0.2.100	198.51.100.100	ICMP	102	0x5	184	(20868)		64 Ech	10 (1	oing)	reque	st	id=0	x003a	a, s	eq=40/102	40, t	ttl=64	(rep	
	16 2022-08-07 22:40:13.697327		198.51.100.100	192.0.2.100	ICMP	102	0x70	33e	(28734)		64 Ech	10 (1	oing)	reply	1	id=0	x003a	a, s	eq=40/102	40, t	ttl=64	(rec	
	17 2022-08-07 22:40:14.698512		192.0.2.100	198.51.100.100	ICMP	102	0x5	1d8	(20952)		64 Ech	10 (1	oing)	reque	st	id=0	x003a	a, s	eq=41/104	96, t	ttl=64	(rep	
	18 2022-08-07 22:40:14.698518		198.51.100.100	192.0.2.100	ICMP	102	0x70	bb6	(28893)		64 Ech	10 (1	oing)	reply	1	id=0	x003a	a, s	eq=41/104	96, t	ttl=64	(rec	~
<																						>	
>	Frame 1: 102 bytes on wire (816 bits	s),	102 bytes captu	red (816 bits)				0000	00 50 5	6 9d	e7 5	0 bc	e7	12 34	9a :	15 0	3 00	45 0	0 ·PV··	P · · ·	-4	E٠	_
>	Ethernet II, Src: Cisco_34:9a:15 (be	c:e	7:12:34:9a:15),	Dst: VMware_9d:e7:5	0 (00:50:56:9	d:e7:50)		0010	00 54 4	ld 93	40 0	0 40	01	00 la	CØ (90 OS	2 64	c6 3	3 ·TM-@	·@· /	· · · · · d	- 3	
>	Internet Protocol Version 4, Src: 19	92.	0.2.100, Dst: 19	8.51.100.100			(020	64 64 0	8 06	7f 1	5 00	3a	00 21	39	3f fe	62	00 C	00 dd · · ·	1 1 1	·197-b		
>	Internet Control Message Protocol						6	9030	00 00 8	3b 1a	05 0	0 00	00	00 00	10	11 13	2 13	14 1	5				
								9040	16 17 1	8 19	1a 1	b 1c	1d	1e 1f	20	21 2	2 23	24 2	5			\$%	
								1050	26 27 2	28 29	2a 2	0 2C	20	ze zt	30	51 32	2 33	34 3	5 & ()*	+,- ·	./0123	45	
									30 37 5	00 55	55 53	2							67000	U			

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: Config Fail Reason Append Flag: Session Mem Usage: Session Pcap Snap Error Code: Drop Count:	yes : overwrite 256 Len: 1518 0 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: 1	37248
Filter:	capsw-1-19
Packet Capture Filte	r Info
Name:	capsw-1-19
Protocol:	0
Ivlan:	0
Ovlan:	0
Src Ip:	0.0.0
Dest Ip:	0.0.0.0
Src ipvo:	
Src MAC:	
Dest MAC.	00.00.00.00.00
Src Port:	0
Dest Port:	0
Ethertype:	0
Total Physical break	out ports involved in Packet Capture: 0

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	lln	256	Full	None	link-lln
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	Ň/A	Reset
0/28	n/a	Down	n/a	Full	Ň/A	Reset
0/29	1000_BaseX	Down	1G	Full	None	Link-Down
0/30	n/a	Down	n/a	Full	N/A	Reset
0/31	n/a	Down	n/a	Full	N/A	Reset
0/32	n/a	Down	n/a	Full	N/A	Reset
0/33	1000_BaseX	Down	1G	Full	None	Link-Down
0/34	n/a	Down	n/a	Full	N/A	Reset
0/35	n/a	Down	n/a	Full	N/A	Reset
0/36	n/a	Down	n/a	Full	N/A	Reset

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

キャプチャファイルの収集

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

ファイル分析のキャプチャ

パケットキャプチャファイルリーダーアプリケーションを使用して、in_mgmt_uplink1インターフ ェイスのキャプチャファイルを開きます。この例では、Secure Firewall 3100でのパケットキャプ チャが分析されます。

キーポイントを確認します。この例では、管理IPアドレス192.0.2.200からのパケットだけが表示 されています。例としては、SSH、Sftunnel、またはICMPエコー応答パケットがあります。これ らは、内部スイッチを介してアプリケーション管理インターフェイスからネットワークに送信さ れるパケットです。

No. Time		Source	Destination	Protocol	Length	IP ID		IP TTL Info
196 2022-08-07	23:21:45.133362	192.0.2.200	192.0.2.101	TCP	1518	0xb7d0	(47056)	64 39181 → 8305 [ACK] Seq=61372 Ack=875 Win=1384 Len=1448 TS
197 2022-08-07	23:21:45.133385	192.0.2.200	192.0.2.101	TCP	1518	Øxb7d1	(47057)	64 39181 → 8305 [ACK] Seq=62820 Ack=875 Win=1384 Len=1448 TS
198 2022-08-07	23:21:45.133388	192.0.2.200	192.0.2.101	TLSv1.2	990	Øxb7d2	(47058)	64 Application Data
199 2022-08-07	23:21:45.928772	192.0.2.200	192.0.2.100	ICMP	78	Øxbd48	(48456)	64 Echo (ping) reply id=0x0001, seq=4539/47889, ttl=64
200 2022-08-07	23:21:45.949024	192.0.2.200	192.0.2.101	TLSv1.2	128	0x4a97	(19095)	64 Application Data
201 2022-08-07	23:21:45.949027	192.0.2.200	192.0.2.101	TCP	70	0x4a98	(19096)	64 8305 → 58885 [ACK] Seq=21997 Ack=26244 Win=4116 Len=0 TSv
202 2022-08-07	23:21:46.019895	192.0.2.200	192.0.2.101	TLSv1.2	100	0x4a99	(19097)	64 Application Data
203 2022-08-07	23:21:46.019899	192.0.2.200	192.0.2.101	TLSv1.2	96	0x4a9a	(19098)	64 Application Data
204 2022-08-07	23:21:46.019903	192.0.2.200	192.0.2.101	TCP	70	0x4a9b	(19099)	64 8305 → 58885 [ACK] Seq=22053 Ack=26274 Win=4116 Len=0 TSv
205 2022-08-07	23:21:46.019906	192.0.2.200	192.0.2.101	TCP	70	0x4a9c	(19100)	64 8305 → 58885 [ACK] Seq=22053 Ack=26300 Win=4116 Len=0 TSv
206 2022-08-07	23:21:46.136415	192.0.2.200	192.0.2.101	TCP	70	Øxb7d3	(47059)	64 39181 → 8305 [ACK] Seq=65188 Ack=921 Win=1384 Len=0 TSval
207 2022-08-07	23:21:46.958148	192.0.2.200	192.0.2.100	ICMP	78	Øxbd9e	(48542)	64 Echo (ping) reply id=0x0001, seq=4540/48145, ttl=64
208 2022-08-07	23:21:47.980409	192.0.2.200	192.0.2.100	ICMP	78	Øxbdf2	(48626)	64 Echo (ping) reply id=0x0001, seq=4541/48401, ttl=64
209 2022-08-07	23:21:48.406312	192.0.2.200	192.0.2.101	TCP	70	0x4a9d	(19101)	64 8305 → 58885 [ACK] Seq=22053 Ack=26366 Win=4116 Len=0 TSv
210 2022-08-07	23:21:48.903236	192.0.2.200	192.0.2.101	TLSv1.2	747	0x4a9e	(19102)	64 Application Data
211 2022-08-07	23:21:48.994386	192.0.2.200	192.0.2.100	ICMP	78	Øxbe48	(48712)	64 Echo (ping) reply id=0x0001, seq=4542/48657, ttl=64
212 2022-08-07	23:21:50.008576	192.0.2.200	192.0.2.100	ICMP	78	Øxbea6	(48806)	64 Echo (ping) reply id=0x0001, seq=4543/48913, ttl=64
213 2022-08-07	23:21:50.140167	192.0.2.200	192.0.2.101	TCP	1518	Øxb7d4	(47060)	64 39181 → 8305 [ACK] Seq=65188 Ack=921 Win=1384 Len=1448 TS
214 2022-08-07	23:21:50.140171	192.0.2.200	192.0.2.101	TCP	1518	Øxb7d5	(47061)	64 39181 → 8305 [ACK] Seq=66636 Ack=921 Win=1384 Len=1448 TS
215 2022-08-07	23:21:50.140175	192.0.2.200	192.0.2.101	TLSv1.2	990	Øxb7d6	(47062)	64 Application Data
216 2022-08-07	23:21:51.015884	192.0.2.200	192.0.2.100	ICMP	78	Øxbec1	(48833)	64 Echo (ping) reply id=0x0001, seq=4544/49169, ttl=64
217 2022-08-07	23:21:51.142842	192.0.2.200	192.0.2.101	TCP	70	Øxb7d7	(47063)	64 39181 → 8305 [ACK] Seq=69004 Ack=967 Win=1384 Len=0 TSval
218 2022-08-07	23:21:52.030118	192.0.2.200	192.0.2.100	ICMP	78	0xbf02	(48898)	64 Echo (ping) reply id=0x0001, seq=4545/49425, ttl=64
219 2022-08-07	23:21:53.042744	192.0.2.200	192.0.2.100	ICMP	78	Øxbf59	(48985)	64 Echo (ping) reply id=0x0001, seq=4546/49681, ttl=64
220 2022-08-07	23:21:53.073144	192.0.2.200	192.0.2.100	SSH	170	Øxad34	(44340)	64 Server: Encrypted packet (len=112)
221 2022-08-07	23:21:53.194906	192.0.2.200	192.0.2.100	TCP	64	Øxad35	(44341)	64 22 → 53249 [ACK] Seq=1025 Ack=881 Win=946 Len=0
222 2022-08-07	23:21:53.905480	192.0.2.200	192.0.2.101	TLSv1.2	747	0x4a9f	(19103)	64 Application Data
223 2022-08-07	23:21:54.102899	192.0.2.200	192.0.2.100	ICMP	78	0xbf63	(48995)	64 Echo (ping) reply id=0x0001, seq=4547/49937, ttl=64
224 2022-08-07	23:21:54.903675	192.0.2.200	192.0.2.101	TCP	70	0x4aa0	(19104)	64 8305 → 58885 [ACK] Seq=23407 Ack=26424 Win=4116 Len=0 TSv
175 2022 00 07	12:11:55 126700	103 0 3 300	103 0 3 100	TCMD	70	avhfc1	(10000)	Aa-[++ CO102/0424-000 100000-bi v[non (nnin) 0423 43
Ename 1: 747 byte	as on wine (5076 hits) 747 butos car	tured (5076 bi	tc)			a4 53 (an 11 32 3a he n7 12 34 9a 00 02 00 45 00 .S. 2*4E.
Ethernet II Sport	Cisco 34:02:00 (hc:	67.12.34.02.00)	Det: Cisco 11	·38·22 (24·53·00·11	.38.22)	0010	02 d9	4a 3d 40 00 40 06 68 b4 c0 00 02 c8 c0 00 ···3=@·@· h·····
> Internet Protocol	Version A Sect 103	0 2 200 Det: 1	02 0 2 101	130120 (04133100111		0020	02 65	20 71 e6 05 67 1b 2a c5 db e3 6b d4 80 18 ·e g·g· *···k···
> Transmission Cont	trol Protocol Src Pr	nt: 8305 Det De	nt: 59995 Son	1 Ack: 1 Lon: 6	77	0030	10 14	27 cc 00 00 01 01 08 0a 08 76 95 7f 91 02
> Transport Laver	Security		i ci 50005, 5cq	· .,		0040	3d 41 3	17 03 03 02 a0 22 6a 01 e0 ff cc 98 f9 af =A·····" j·····
in an sport cuyer .	Jeeur rey					0050	07 40	75 19 a4 d5 df 64 d8 fe 66 8e 9b cc 8d 2f - @u····d ··f····/
						0060	92 b2 :	1a 64 e7 20 36 03 8e 48 02 5a 7c 85 30 d4 ····d· 6· ·H·Z 0·
						0070	fa c0 a	a8 56 b8 ad a7 7e 19 3a c1 9c 4b 57 0e e0 ···V···~ ·:·KW··
						0080	be ef s	95 22 84 C1 C1 90 91 24 78 04 15 1C 44 00
						0090	ea co 4	45 96 11 TU a7 70 75 65 67 a3 a0 46 6a ch 36 h7 / .e PU K ++ 6
						aaha	5h c7	a a a f a c 1 ff 26 d a 87 a a 51 3d 20 08 [T 2
						0000	16 fd	ch f5 4f 91 98 56 86 15 17 55 68 6f 5d 840
						0000		

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 Management1/1	outside diagnostic	0 0

2. ARPまたはICMPのキャプチャセッションを作成します。

>

capture capsw switch interface inside ethernet-type arp

<#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 O 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
Port Id: Pcapfile: Pcapsize:	1 /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.p 0

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
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

O 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>

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
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

Config Success:

yes

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 inf	ō
Name:	capsw
Session:	1
Admin State:	disabled
Oper State:	down
Oper State Reaso	on: Session_Admin_Shut

Config Fail Reason: Append Flag: overwrite Session Mem Usage: 256 Session Pcap Snap Len: 1518 Error Code: 0 0 Drop Count: 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 0 Ivlan: 0vlan: 0 Src Ip: 0.0.0.0 0.0.0.0 Dest Ip: Src Ipv6: :: Dest Ipv6: :: Src MAC: 00:00:00:00:00:00 00:00:00:00:00:00 Dest MAC: Src Port: 0 0 Dest Port: 0 Ethertype: 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 0 Drop Count: 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 139826 Pcapsize: 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: :: 00:00:00:00:00:00 Src MAC: Dest MAC: 00:00:00:00:00:00 Src Port: 0 0 Dest Port: 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 -1 /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。

Firewall Management Center Devices / Troubleshoot / File Download	Analysis Policies	Devices Objects	Integration D	eploy Q 🧬 🌣 🕜 lab_domain \ admin 🔻 👘 🕏 SECURE
				Threat Defense CLI Packet Capture Packet Tracer
	Device FPR3100-1 v File sess-1-capsw-ethernet-1-1-0.pcap			
		Back Download		

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 ア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

- <u>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</u>
- <u>Cisco Secure Firewall 3100スタートアップガイド</u>
- <u>Cisco Firepower 4100/9300 FXOS コマンド リファレンス</u>

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。