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

内容

概要 前提条件 要件 使用するコンポーネント 背景説明 システムアーキテクチャの概要 内部スイッチの動作の概要 パケットフローとキャプチャポイント Firepower 4100/9300の設定と確認 物理インターフェイスまたはポートチャ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> アプリケーションおよびアプリケーションポートでのパケットキャプチャ 物理インターフェイスまたはポートチャネルインターフェイスのサブインターフェイスでのパケ ットキャプチャ パケット キャプチャ フィルタ Firepower 4100/9300内部スイッチキャプチャファイルの収集 内部スイッチパケットキャプチャのガイドライン、制限事項、およびベストプラクティス Secure Firewall 3100の設定と検証 物理インターフェイスまたはポートチャネルインターフェイスでのパケットキャプチャ 物理インターフェイスまたはポートチャ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>ットキャプ</u>チャ 内部インターフェイスでのパケットキャプチャ パケット キャプチャ フィルタ Secure Firewall 3100内部スイッチキャプチャファイルの収集 内部スイッチパケットキャプチャのガイドライン、制限事項、およびベストプラクティス 関連情報

概要

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

前提条件

要件

製品に関する基本的な知識、キャプチャ分析。

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

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

- Secure Firewall 31xx
- Firepower 41xx
- Firepower 93xx
- Cisco Secure eXtensible Operating System(FXOS)2.12.0.x
- Cisco Secure Firewall Threat Defense(FTD)7.2.0.x
- Cisco Secure Firewall Management Center(FMC)7.2.0.x
- Cisco Secure Firewall Device Manager(FDM)7.2.0.x
- ・適応型セキュリティアプライアンス(ASA)9.18(1)x
- Adaptive Security Appliance Device Manager(ASDM)7.18.1.x
- Wireshark 3.6.7(<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Secure Firewall 3100のアーキテクチャを次の図のように視覚化できます。



シャーシには次のコンポーネントが含まれます。

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

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

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

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

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

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

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

> show interface detail | grep Interface Interface Internal-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(ポート** VLANタグ)と仮想ネットワークタグ(VN-tag)を使用します。

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

```
firepower# connect fxos
•••
firepower(fxos) # show run int e1/2
!Command: show running-config interface Ethernet1/2
!Time: Tue Jul 12 22:32:11 2022
version 5.0(3)N2(4.120)
interface Ethernet1/2
description U: Uplink
no lldp transmit
no lldp receive
no cdp enable
switchport mode dot1q-tunnel
 switchport trunk native vlan 102
speed 1000
duplex full
udld disable
no shutdown
```

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

ポートVLANタグとVNタグはアプリケーションと共有されます。アプリケーションは、それぞれ の出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。

Secure Firewall 3100

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

ポートVLANタグはアプリケーションと共有されます。アプリケーションは、それぞれの出力イ 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で受信されると、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特定し、ポートのVLANタグを削除して、パケ ットをネットワークに転送します。

パケットフローとキャプチャポイント

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

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



キャプチャポイントは次のとおりです。

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

4. データプレーンインターフェイス出力キャプチャポイント

 5. 内部スイッチバックプレーンまたはアップリンク入力キャプチャポイント。バックプレーン またはアップリンクインターフェイスは、内部スイッチをアプリケーションに接続します。
 内部スイッチは、入力インターフェイスキャプチャのみをサポートします。つまり、ネットワー クまたはASA/FTDアプリケーションから受信したパケットだけをキャプチャできます。出力パケ ットキャプチャはサポートされていません。

の設定と検証 Firepower 4100/9300

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

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

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

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

トポロジ、パケットフロー、およびキャプチャポイント



			Chassis										
			Internal Switch			Security Module							
		Po1				FTD/ASA							
		R											
192.0.2.100	ICMP echo-request	Eth1/1		Backplane									
198.51.100.100	ICMP echo-reply												

コンフィギュレーション

FCM

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

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

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

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 v		Save and Run Save Cancel
ftd1	Session Name* Cap1 Selected Interfaces Ethernet1/2	
Ethernet/2	Buffer Size 256 MB 👻 Snap length: 1518 Bytes	
Ethernet1/3	Store Packets Overwrite Append	
Ethernet1/1 FTD Ethernet1/10	Capture Filter Apply Filter Capture All	
Ehenet1/5 [Portchannel1]		
Ebenet1/4 (Portchannel1)		

3. ポートチャネルインターフェイスの場合は、すべての物理メンバーインターフェイスを選択 し、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 V		Save and Run Save Cancel
ftd1	Session Name* cap1 Selected Interfaces Ethernet1/5, Ethernet1/4	
Ethernet1/2	Buffer Size 256 MB V	-
Ethernet1/3	Shap length: 1518 bytes Store Packets Overwrite Append	
Ethernet1/1 Ethernet1/0, Ethernet1/10	Capture Filter Apply Filter Cepture All	
Ethernet1/5 (Portchannel1)		
Ethernet1/4 (Portchannel1)		

FXOS CLI

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

1. アプリケーションのタイプと識別子を特定します。

firepower# firepower App Name Deploy Typ	scope ssa /ssa # show Identifier e Turbo Mod	app-instance Slot ID Ac e Profile Name	lmin State Ope e Cluster Stat	r State e Cluster	Running Vers Role	ion Startup Version					
ftd	ftd1	1 Er	nabled Onl	ine La Nama	7.2.0.82	7.2.0.82					
Native 2. ポー	^{NO} トチャネル	インターフェ	イスの場合は、	そのメンバ	バーインターフ	ェイスを特定します。					
firepower# <output sk<br="">firepower(Flags: D I - S - S - U - M -</output>	<pre>firepower# connect fxos <output skipped=""> firepower(fxos)# show port-channel summary Flags: D - Down P - Up in port-channel (members)</output></pre>										
Group Port Chann	 - Тур el	e Protocol	Member Port	s							
1 Pol(3. + 7	su) Eth プチャセッ	LACP ションを作成	Eth1/4(P) します。	Eth1/5(P)							
firepower# firepower firepower firepower firepower firepower firepower firepower firepower	scope pack /packet-cap /packet-cap /packet-cap /packet-cap /packet-cap /packet-cap /packet-cap	et-capture ture # create ture/session/m ture/session/m ture/session/m ture/session* ture/session* ture/session	<pre>session cap1 # create phy-; bhy-port* # se bhy-port* # se bhy-port* # up # enable # commit #</pre>	port Eth1/2 t app ftd t app-identi	fier ftd1						

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

firepower#	scope packet-capture							
firepower	<pre>/packet-capture # create session c</pre>	ap1						
firepower	<pre>/packet-capture/session* # create</pre>	phy	-po	rt E	th1/	4		
firepower	<pre>/packet-capture/session/phy-port*</pre>	# se	et	app	ftđ			
firepower	<pre>/packet-capture/session/phy-port*</pre>	# se	et	app-	iden	tifie	r ftð	11
firepower	<pre>/packet-capture/session/phy-port*</pre>	# uj	p					
firepower	<pre>/packet-capture/session* # create</pre>	phy	-po	rt E	th1/	5		
firepower	<pre>/packet-capture/session/phy-port*</pre>	# se	et	app	ftđ			
firepower	<pre>/packet-capture/session/phy-port*</pre>	# se	et	app-	iden	tifie	r ftð	11
firepower	<pre>/packet-capture/session/phy-port*</pre>	# uj	p					
firepower	<pre>/packet-capture/session* # enable</pre>							
firepower	<pre>/packet-capture/session* # commit</pre>							
firepower	/packet-capture/session #							
確認								

FCM

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

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

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	Settings			s	ystem Tools Help admin
Capture Session Filter List						
					C Refresh Capture Session	Delete All Sessions
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/S	None	160	cap1-ethernet-1-5-0.pcap	ftd1	*	
Ethernet1/4	None	85000	cap1-ethernet-1-4-0.pcap	ftd1	*	

FXOS CLI

scope packet-captureでキャプチャの詳細を確認します。

```
firepower# scope packet-capture
firepower /packet-capture # show session cap1
Traffic Monitoring Session:
    Packet Capture Session Name: cap1
    Session: 1
    Admin State: Enabled
    Oper State: Up
    Oper State Reason: Active
    Config Success: Yes
    Config Fail Reason:
    Append Flag: Overwrite
    Session Mem Usage: 256 MB
```

```
Session Pcap Snap Len: 1518 Bytes
  Error Code: 0
  Drop Count: 0
Physical ports involved in Packet Capture:
   Slot Id: 1
   Port Id: 2
   Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap
   Pcapsize: 75136 bytes
  Filter:
  Sub Interface: 0
   Application Instance Identifier: ftd1
   Application Name: ftd
メンバーインターフェイスEthernet1/4およびEthernet1/5を持つポートチャネル1:
firepower# scope packet-capture
firepower /packet-capture # show session cap1
Traffic Monitoring Session:
   Packet Capture Session Name: cap1
  Session: 1
   Admin State: Enabled
   Oper State: Up
   Oper State Reason: Active
  Config Success: Yes
  Config Fail Reason:
  Append Flag: Overwrite
  Session Mem Usage: 256 MB
  Session Pcap Snap Len: 1518 Bytes
  Error Code: 0
  Drop Count: 0
Physical ports involved in Packet Capture:
  Slot Id: 1
   Port Id: 4
   Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-4-0.pcap
   Pcapsize: 310276 bytes
  Filter:
  Sub Interface: 0
   Application Instance Identifier: ftd1
   Application Name: ftd
  Slot Id: 1
   Port Id: 5
   Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-5-0.pcap
   Pcapsize: 160 bytes
  Filter:
  Sub Interface: 0
   Application Instance Identifier: ftd1
   Application Name: ftd
キャプチャファイルの収集
```

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

ファイル分析のキャプチャ

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

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

示されます。

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

No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info	
E.	1 2022-07-13 06:23:58,285080930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (40428)	64 Echo (ping) reque	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) reque	st 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) reque	it 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) reque	it 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) reque	it 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) reque	it 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) reque	it 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) reque	st 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) reque	st 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) reque	it 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) reque	it 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) reque	it 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) reque	it 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) reque	it 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) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	<pre>it id=0x001a, seq=16/4096, ttl=64 (no response found!)</pre>
	20 2022-07-13 06:24:07.501293041	192.0.2.100	198.51.100.100	ICMP	102	0xa1f6 (41462)	64 Echo (ping) reque	it 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) reque	it 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) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	<pre>st id=0x001a, seq=19/4864, ttl=64 (no response found!)</pre>
	27 2022-07-13 06:24:11.597086027	192.0.2.100	198.51.100.100	ICMP	108	0xa349 (41801)	64 Echo (ping) reque	<pre>it id=0x001a, seq=20/5120, ttl=64 (no response found!)</pre>
	28 2022-07-13 06:24:11.597088170	192.0.2.100	198.51.100.100	ICMP	102	0xa349 (41801)	64 Echo (ping) reque	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) reque	st id=0x001a, seq=21/5376, ttl=64 (no response found!)
έ.								
	Frame 1: 100 butes on wine (064 bit	(c) 100 butos	conturned (964 hits)	on inte	nfaco contuno u	0 1 id 0		anna 58 07 hd ha 77 an an 50 56 ad ng ha 80 26 80 As Y P. V &
1	Thereat II Sect Whene OdieBabe	op. Fo. Fo. od. op.	captured (864 Dits)	on ince	rrace capture_u	001, 10 0		0010 38 97 00 09 77 00 00 30 30 90 08 00 89 20 80 00 X ······························
í,	Echernet II, Sic: whware suceside (00:00:00:00:00:00	:De), DSC: CISCO D9	:77:00 (56:97:00:09:77:	0e)		0020 40 01 af c0 c0 00 00 c0 45 00 c0 54 50 c0 54 50 c0 40 00
1	vn-tag	- Dines	tion, From Baidao					0030 00 1a 00 07 f4 64 ce 62 00 00 00 00 20 a2 07 00d.b
			cion: From Bridge					0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b
		- Docti	er: vir_iu					0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ···· !"# \$%&'()*+
			nation: 10					0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,/0123 4567
			ut No	4				
	0		ved: 0					
	Turnet 002 10 Wintwal LAN (0x0100	00 0000 = Sourc	e: 0					
L.	17pe: 802.10 VIPtual LAN (0X8100	10: 103		_				
	and - Deiopitul	Doct Effort (do	(a)					
	- 057, Teoli	sible	aure) (0)	b				
	0000 0110 0110 - TO: 102	Erore		2				
11	Tupo: TDu4 (0x0000)							
L.	Internet Protocol Version 4, Spc: 1	03 0 3 100 Dr	+ 100 51 100 100	_				
1	Internet Protocol Version 4, SFC: 1	52.0.2.100, DS	. 190.31.100.100	2				
1	internet control Message Protocol			6				
				_				

2番目のパケットを選択し、キーポイントを確認します。

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

Ma	Time	Secret	Destination	Protocol	Length	10.10	NO TTO Info	1
-	1 2022-07-13 06:23:58 285080030	102 0 2 100	108 51 100 100	TCMP	108	Ovodor (A0A28)	64 Echo (ning) request	id=9x991a seg=7/1792 ttl=64 (no response foundl)
F	2 2022-07-13 06:23:50.205000550	102.0.2.100	109 51 100 100	TCMD	100	0x9dec (40428)	64 Echo (ping) request	id-0x001a, seq=7/1792, ttl=64 (no response found1)
	3 2022-07-13 06:23:50 200048986	102 0 2 100	108 51 100 100	TCMP	109	0x0ad0 (40656)	64 Echo (ping) request	id=0x001a, seq=9/3049 tt]=64 (no response found1)
	4 2022-07-13 06:23:59:50 200103731	102 0 2 100	100 51 100 100	TCMD	100	0x9ed0 (40050)	64 Echo (ping) request	(d-0x001a, seq=0/2040, ttl=64 (no response found1)
	4 2022-07-13 00.23.39.309193731 E 2022 07 13 06.24.00 2330E4100	102.0.2.100	100 51 100 100	TCMD	102	0x9600 (40030)	64 Echo (ping) request	id-0x001a, seq=0/2046, (C1=04 (no response found))
	6 2022-07-13 06:24:00.333054190	192.0.2.100	100 51 100 100	TCMD	100	0x9120 (40730)	64 Echo (ping) request	id-0x001a, seq=9/2304, ttl=64 (no response found1)
	7 2022-07-13 06:24:00.555050014	192.0.2.100	100 51 100 100	TCMP	102	0x9120 (40750)	64 Echo (ping) request	id=0x001a, seq=9/2560, ttl=64 (no response found!)
	/ 2022-07-13 00:24:01.33/1/3330	192.0.2.100	198.51.100.100	TCMP	100	0x9120 (40749)	64 Echo (ping) request	id-0x001a, seq=10/2500, (C1=04 (no response found))
	0 2022-07-13 06:24:01.337174708	102.0.2.100	100 51 100 100	TCMD	102	0x9120 (40749)	64 Echo (ping) request	id=0x001a, seq=10/2500, (C1=04 (no response found1)
	9 2022-07-13 00:24:02.3810/3/41	192.0.2.100	198.51.100.100	ICHP	103	0x9188 (40840)	64 Echo (ping) request	id=0x001a, seq=11/2016, ttl=64 (no response foundl)
	10 2022-07-13 00:24:02.381074999	192.0.2.100	198,51,100,100	ICHP	102	0x9188 (40840)	64 Echo (ping) request	id-0x001a, seq=11/2010, ((1=04 (no response found))
	12 2022-07-13 00:24:03.405199041	192.0.2.100	198.51.100.100	TCMP	108	0xa077 (41079)	64 Echo (ping) request	id=0x001a, seq=12/30/2, tt1=64 (no response found!)
	12 2022-07-13 00:24:03.403200201	192.0.2.100	198.51.100.100	TCHP	102	0xa077 (41079)	64 Echo (ping) request	id-0x001a, seq=12/3072, tt1=04 (no response found!)
	13 2022-07-13 00:24:04.429155085	192.0.2.100	198.51.100.100	TCHP	108	0xa10f (41231)	64 Echo (ping) request	id-0x001a, seq=13/3528, tt1=64 (no response found!)
	16 2022-07-13 00:24:04.429130831	192.0.2.100	198.51.100.100	TCMP	102	0x3101 (41231)	64 Echo (ping) request	id-0x001a, seq=13/3528, tt1=64 (no response found)
	15 2022-07-15 00:24:05.453150012	192.0.2.100	198.51.100.100	TCHP	100	0xa16a (41322)	64 Echo (ping) request	id-0x001a, seq=14/3504, ttl=64 (no response found)
	10 2022-07-13 00:24:05.453158052	192.0.2.100	198.51.100.100	ICHP	102	0x3103 (41322)	64 Echo (ping) request	id=0x001a, seq=14/3584, (C1=04 (no response found1)
	19 2022-07-13 06:24:06.47712/08/	102.0.2.100	198,51,100,100	ICHP	103	0x3109 (41449)	64 Echo (ping) request	id=0x001a, seq=15/3840, tt1=64 (no response found1)
	10 2022-07-13 00.24.00.477125055	102.0.2.100	198.51.100.100	TCHP	102	0x3165 (41445)	64 Echo (ping) request	id=0x001a, seq=15/3040, ttl=04 (no response found!)
	20 2022-07-13 06:24:07.501291314	192.0.2.100	198.51.100.100	TCMP	100	0x0116 (41462)	64 Echo (ping) request	id-0x001a, seq=16/4096, tt1=64 (no response found!)
	20 2022-07-13 00:24:07.301293041	192.0.2.100	198.51.100.100	TCMP	102	0x3110 (41402)	64 Echo (ping) request	id=0x001a, seq=10/4050, tt1=64 (no response found1)
	22 2022-07-13 00.24.00.525005950	102.0.2.100	100 51 100 100	TCMD	100	0x3257 (41559)	64 Echo (ping) request	id-0x001a, seq=17/4352, ttl=64 (no response found1)
	22 2022-07-13 00.24.00.52.092000	102.0.2.100	100 51 100 100	TCMD	102	0x0237 (41533)	64 Echo (ping) request	id-0x0010, seq=17/4532, ttl=64 (no perpose found))
	24 2022-07-13 06:24:09.549230300	192.0.2.100	198.51.100.100	ICMP	100	0x3239 (41041)	64 Echo (ping) request	id=0x001a, seq=10/4000, (t1=04 (no response found1)
	25 2022-07-13 06:24:09:549230304	192.0.2.100	198.51.100.100	TCMP	102	0x3245 (41041)	64 Echo (ping) request	id=0x001a, seq=10/4066, tt1=64 (no response found1)
	26 2022-07-13 06:24:10:573110504	102 0 2 100	100 51 100 100	TCMD	100	0x0345 (41797)	64 Echo (ping) request	(d-0x001a, seq=10/4064, ttl=64 (no response found1)
	27 2022-07-13 06:24:10:575112504	192 0 2 100	100 51 100 100	TCMP	102	0x0349 (41991)	64 Echo (ping) request	id-0x001a, seq=19/4004, cc1-04 (no response found1)
	28 2022-07-13 06:24:11 597088170	192.0.2.100	198.51.100.100	TCMP	102	0x3349 (41801)	64 Echo (ping) request	id=0x001a, seq=20/5120, tt1=64 (no response found1)
	20 2022-07-13 06:24:11.557000170	102.0.2.100	109 51 100 100	TCMP	109	0xa3dc (41042)	64 Echo (ping) request	id=0x001a, seq=21/5326, ttl=64 (no response found1)
1	29 2022-07-15 00.24.12.021001022	192.0.2.100	190.91.100.100	ACTIP	100	exasur (arsae)	ou ceno (pring) requese	id-oxobia, seq-21/55/0, cci-od (io response roundry
<								
>	Frame 2: 102 bytes on wire (816 bit	s), 102 bytes o	aptured (816 bits) o	on interface	capture_u	0_1, id 0		3000 58 97 bd b9 77 0e 00 50 56 9d e8 be 81 00 00 66 X ··· W ·· P V ····· f
2	Ethernet II, Src: VMware_9d:e8:be (00:50:56:9d:e8:	:be), Dst: Cisco b9:7	7:0e (58:97:	bd:b9:77:	0e)		3010 08 00 45 00 00 54 9d ec 40 00 40 01 at c0 c0 00 ··E··T· g·g·····
~ 1	802.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 102						3020 02 64 66 53 64 64 08 00 40 a2 00 1a 00 07 74 64 - 0-500 · N·····0
н	000 E Priority: E	est Effort (de	fault) (0)					12 13 14 15 16 17 18 19 1a th 1c 1d 1a 1f 28 21
т	0 = DEI: Inelig	ible		5				2050 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 "#\$%8"() *+/01
	0000 0110 0110 = ID: 102							3060 32 33 34 35 36 37 234567
Ŀ	Type: IPv4 (0x0800)			_				
2	Internet Protocol Version 4, Src: 1	92.0.2.100, Dst	: 198.51.100.100					
2	Internet Control Message Protocol			2				
-								

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

-										
No.	Time	Source	Destination	Protocol	Length	IP ID		IP TTL Info		^
-	1 2022-08-05 23:07:31.865872877	192.0.2.100	198.51.100.100	ICMP	108	Øx322e (1	2846)	64 Echo (ping) request	id=0x002d, seq=245/62720, ttl=64 (nc
	2 2022-08-05 23:07:31.865875131	192.0.2.100	198.51.100.100	ICMP	102	Øx322e (1	2846)	64 Echo (ping) request	id=0x002d, seq=245/62720, ttl=64 (nc
	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	id=0x002d, seq=246/62976, ttl=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	4061)	64 Echo (ping) request	id=0x002d, seq=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	4061)	64 Echo (ping) request	id=0x002d, seq=253/64768, ttl=64 (nc
Π.	19 2022-08-05 23:07:40.985773090	192.0.2.100	198.51.100.100	ICMP	108	0x37d5 (1	4293)	64 Echo (ping) request	id=0x002d, seq=254/65024, ttl=64 (nc ~
<										>
>	Frame 1: 108 bytes on wire (864 bits), 108 bytes capt	ured (864 bits) on	n interface	e capture_u0_3,	i 0000	a2 76	f2 00 00 25 00 50 56 9d e8	be 89 26 80 54 ·v···%·P V····&·T	
>	Ethernet II, Src: VMware_9d:e8:be (0	0:50:56:9d:e8:be)	, Dst: a2:76:f2:00	00:25 (a)	2:76:f2:00:00:2	5) 0010	00 00	81 00 03 e9 08 00 45 00 00	54 32 2e 40 00 ····· E··T2.@·	
I	VN-Tag					0020	40 01	1b 7f c0 00 02 64 c6 33 64	64 08 00 1e d6 @·····d ·3dd····	
н	1	= Direction	n: From Bridge			0030	00 2d (00 f5 a6 a2 ed 62 00 00 00	00 7a 2f 0b 00 ·····b ····z/··	
ш	.0	= Pointer:	vif_id			0040	00 00	00 00 10 11 12 13 14 15 16	17 18 19 1a 1b	
ш	00 0000 0101 0100	= Destinat:	ion: 84			0050	1C 10 1	1e 1f 20 21 22 23 24 25 26	27 28 29 28 20 1 # \$48 ()*+	
ш	0	= Looped: 1	No 4			0000	20 20 .	20 21 30 31 32 33 34 33 30	5/ ,/0125 430/	
ш	0	= Reserved	: 0							
ш	00	= Version:	0							
ш	0000 0000	0 0000 = Source: 0	9							
I L	Type: 802.10 Virtual LAN (0x8100)									
1	802.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 1001								
н	000 Be	est Effort (defau	lt) (0)							
ш	0 = DEI: Ineligi	ible	2							
ш	0011 1110 1001 = ID: 1001		5							
١L	Type: IPv4 (0x0800)									
H	Internet Protocol Version 4, Src: 19	2.0.2.100, Dst: 1	98.51.100.100 👆							
H	Internet Control Message Protocol		2							
Ľ										

2番目のパケットを選択し、キーポイントを確認します。

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

No.	Time	Source	Destination	Protocol	Length	IP ID		IP TT	'L Info							^
E	1 2022-08-05 23:07:31.865872877	192.0.2.100	198.51.100.100	ICMP	108	Øx322e	(12846)	6	64 Echo	(ping)	request	id=0x002d,	seq=245/62720,	ttl=64	(nc	
	2 2022-08-05 23:07:31.865875131	192.0.2.100	198.51.100.100	ICMP	102	Øx322e	(12846)	6	64 Echo	(ping)	request	id=0x002d,	seq=245/62720,	ttl=64	(nc	
	3 2022-08-05 23:07:32.867144598	192.0.2.100	198.51.100.100	ICMP	108	0x32b9	(12985)	6	64 Echo	(ping)	request	id=0x002d,	seq=246/62976,	ttl=64	(nc	
	4 2022-08-05 23:07:32.867145852	192.0.2.100	198.51.100.100	ICMP	102	0x32b9	(12985)	6	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	(13016)	6	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	(13016)	6	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	Øx3373	(13171)	6	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	Øx3373	(13171)	6	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	(13351)	6	4 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	(13351)	6	4 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	(13534)	6	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	(13534)	6	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	(13644)	6	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	(13644)	6	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	(13826)	6	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	(13826)	6	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	(14061)	6	64 Echo	(ping)	request	id=0x002d,	seq=253/64768,	ttl=64	(nc	
	18 2022-08-05 23:07:39.961787284	192.0.2.100	198.51.100.100	ICMP	102	0x36ed	(14061)	6	64 Echo	(ping)	request	id=0x002d,	seq=253/64768,	ttl=64	(nc	
	19 2022-08-05 23:07:40.985773090	192.0.2.100	198.51.100.100	ICMP	108	0x37d5	(14293)	6	64 Echo	(ping)	request	id=0x002d,	seq=254/65024,	ttl=64	(nc	~
<															>	
>	Frame 2: 102 bytes on wire (816 bits)	, 102 bytes capt	ured (816 bits) on	interface capt	ure u0 3.	i 0000	a2 76	f2 00	00 25 0	80 50	56 9d e8	be 81 00 03	e9 ·v···%·P	v		_
>	Ethernet II, Src: VMware 9d:e8:be (00	:50:56:9d:e8:be)	, Dst: a2:76:f2:00	:00:25 (a2:76:f	2:00:00:2	(5) 0010	08 00	45 00	00 54	32 2e	40 00 40	01 1b 7f ce	00 ··E··T2.	@·@·····		
Ł	802.10 Virtual LAN, PRI: 0, DEI: 0, 1	ID: 1001				0020	02 64	c6 33	64 64 0	88 60	1e d6 00	2d 00 f5 a6	a2 ·d·3dd··			
н	000 Be Priority: Be	st Effort (defaul	t) (0)			0030	ed 62	00 00	00 00	7a 2f	0b 00 00	00 00 00 10	11 ·b····z/			
н	0 = DEI: Ineligi	ble	3			0040	12 13	14 15	16 17	18 19	1a 1b 1c	1d 1e 1f 20	21			
н	0011 1110 1001 = ID: 1001		~ ~ 1			0050	22 23	24 25	26 27	28 29	2a 2b 2c	2d 2e 2f 30	31 "#\$%&'()	*+,/01		
	Type: IPv4 (0x0800)					0060	32 33	34 35	36 37				234567			
۱ŀ	Internet Protocol Version 4, Src: 192	2.0.2.100, Dst: 1	98,51,100,100													
H	Internet Control Message Protocol	,	2													
I L																

説明

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

•ポートVLANタグの挿入後。

• VNタグの挿入後。

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

タスクの要約を次の表に示します。

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

バックプレーンインターフェイスでのパケットキャプチャ

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

トポロジ、パケットフロー、およびキャプチャポイント



コンフィギュレーション

FCM

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

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

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

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

Overview Interfaces Logical Devices Security Engine Platform Settings	System loois Help admin
Select an instance: ftd1 v	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 Al Backplane Ports
Ethernet1/3 FID	Capture Efter Etter
Ethernet1/9, Ethernet1/10	Ethernet1/10 Al Backplane Ports
Ethernet1/1	

FXOS CLI

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

1. アプリケーションのタイプと識別子を特定します。

firepower#	scope s	ssa					
firepower	/ssa# s	now app-instan	ce				
App Name	Identii	fier Slot ID	Admin Stat	te Oper St	ate	Running Version	Startup Version
Deploy Typ	e Turbo	Mode Profile	Name Cluster	State	Cluster R	ple	
						-	
ftd	ftd1	1	Enabled	Online		7.2.0.82	7.2.0.82
Native	No		Not App	plicable	None		
2. キャ	プチャt	ェッションを作	乍成します。				

firepower	<pre>/packet-capture/session* # create phy-port Eth1/9</pre>
firepower	<pre>/packet-capture/session/phy-port* # set app ftd</pre>
firepower	<pre>/packet-capture/session/phy-port* # set app-identifier ftd1</pre>
firepower	/packet-capture/session/phy-port* # up
firepower	<pre>/packet-capture/session* # create phy-port Eth1/10</pre>
firepower	<pre>/packet-capture/session/phy-port* # set app ftd</pre>
firepower	<pre>/packet-capture/session/phy-port* # set app-identifier ftd1</pre>
firepower	/packet-capture/session/phy-port* # up
firepower	/packet-capture/session* # enable
firepower	/packet-capture/session* # commit
firepower	/packet-capture/session #
確認	

FCM

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

Overview Interfa	aces Logical Devices Security Engine	Platform Settings			Syste	m Tools Help admin
Capture Session	iker List					
					Capture Session Delet	e Al Sessions
🔺 🧵 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		
Ethernet1/10	None	194352	cap1-ethernet-1-10-0.pcap	ftd1	\pm	
Ethernet1/9	None	286368	cap1-ethernet-1-9-0.pcap	ftd1	*	

FXOS CLI

scope packet-captureでキャプチャの詳細を確認します。

```
firepower# scope packet-capture
firepower /packet-capture # show session cap1
Traffic Monitoring Session:
   Packet Capture Session Name: cap1
  Session: 1
  Admin State: Enabled
   Oper State: Up
   Oper State Reason: Active
   Config Success: Yes
  Config Fail Reason:
  Append Flag: Overwrite
  Session Mem Usage: 256 MB
  Session Pcap Snap Len: 1518 Bytes
  Error Code: 0
  Drop Count: 0
Physical ports involved in Packet Capture:
  Slot Id: 1
   Port Id: 10
   Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-10-0.pcap
   Pcapsize: 1017424 bytes
  Filter:
   Sub Interface: 0
   Application Instance Identifier: ftd1
   Application Name: ftd
```

```
Slot Id: 1
```

```
Port Id: 9
Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-9-0.pcap
Pcapsize: 1557432 bytes
Filter:
Sub Interface: 0
Application Instance Identifier: ftd1
Application Name: ftd
キャプチャファイルの収集
```

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

ファイル分析のキャプチャ

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

最初と2番目のパケットを選択し、キーポイントを確認します。

- 1. 各ICMPエコー要求パケットがキャプチャされ、2回表示されます。
- 2. 元のパケットヘッダーにはVLANタグが付いていません。
- 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			
F	1 2022-07-14 20:20:36.513854256	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928	64 Echo	(ping) rea	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) rea	quest	id=0x0001, seq=15/3840, ttl=64 (reply in 3)
	3 2022-07-14 20:20:36.514117394	198.51.100.100	192.0.2.100	ICMP	108	0xcc2c (52264	64 Echo	(ping) rep	ply	id=0x0001, seq=15/3840, ttl=64 (request in 2)
	4 2022-07-14 20:20:36.514119312	198.51.100.100	192.0.2.100	ICMP	108	Øxcc2c (52264	64 Echo	(ping) rep	ply	id=0x0001, seq=15/3840, ttl=64
	5 2022-07-14 20:20:37.537723822	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (2304)	64 Echo	(ping) rea	quest	id=0x0001, seq=16/4096, ttl=64 (no response found!)
	6 2022-07-14 20:20:37.537726588	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040	64 Echo	(ping) rea	quest	id=0x0001, seq=16/4096, ttl=64 (reply in 7)
	7 2022-07-14 20:20:37.538046165	198.51.100.100	192.0.2.100	ICMP	108	Øxcc9b (52379	64 Echo	(ping) rep	oly	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) 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) red	quest	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) red	quest	id=0x0001, seq=17/4352, ttl=64 (reply in 11)
	11 2022-07-14 20:20:38.562048288	198.51.100.100	192.0.2.100	ICMP	108	0xccc4 (52426) 64 Echo	(ping) rep	ply	id=0x0001, seq=17/4352, ttl=64 (request in 10)
	12 2022-07-14 20:20:38.562050333	198.51.100.100	192.0.2.100	ICMP	108	0xccc4 (52420) 64 Echo	(ping) rep	ply	id=0x0001, seq=17/4352, ttl=64
	13 2022-07-14 20:20:39.585677043	192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366) 64 Echo	(ping) red	quest	id=0x0001, seq=18/4608, ttl=64 (no response found!)
	14 2022-07-14 20:20:39.585678455	192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366	64 Echo	(ping) red	quest	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	Øxcd8d (5262)) 64 Echo	(ping) rep	ply	id=0x0001, seq=18/4608, ttl=64 (request in 14)
	16 2022-07-14 20:20:39.585937900	198.51.100.100	192.0.2.100	ICMP	108	Øxcd8d (5262)) 64 Echo	(ping) rep	ply	id=0x0001, seq=18/4608, ttl=64
	17 2022-07-14 20:20:40.609804804	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (23419) 64 Echo	(ping) red	quest	id=0x0001, seq=19/4864, ttl=64 (no response found!)
	18 2022-07-14 20:20:40.609807618	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (23419) 64 Echo	(ping) red	quest	id=0x0001, seq=19/4864, ttl=64 (reply in 19)
	19 2022-07-14 20:20:40.610179685	198.51.100.100	192.0.2.100	ICMP	108	0xcd8f (5262)) 64 Echo	(ping) rep	ply	id=0x0001, seq=19/4864, ttl=64 (request in 18)
	20 2022-07-14 20:20:40.610181944	198.51.100.100	192.0.2.100	ICMP	108	0xcd8f (5262)) 64 Echo	(ping) rep	ply	id=0x0001, seq=19/4864, ttl=64
	21 2022-07-14 20:20:41.633805153	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (2342)) 64 Echo	(ping) red	quest	id=0x0001, seq=20/5120, ttl=64 (no response found!)
	22 2022-07-14 20:20:41.633806997	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (2342)	e) 64 Echo	(ping) red	quest	id=0x0001, seq=20/5120, ttl=64 (reply in 23)
	23 2022-07-14 20:20:41.634084102	198.51.100.100	192.0.2.100	ICMP	108	0xce36 (52796) 64 Echo	(ping) rep	ply	id=0x0001, seq=20/5120, ttl=64 (request in 22)
	24 2022-07-14 20:20:41.634085368	198.51.100.100	192.0.2.100	ICMP	108	0xce36 (52796) 64 Echo	(ping) rep	ply	id=0x0001, seq=20/5120, ttl=64
	25 2022-07-14 20:20:42.657709898	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23530) 64 Echo	(ping) red	quest	id=0x0001, seq=21/5376, ttl=64 (no response found!)
	26 2022-07-14 20:20:42.657711660	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23530) 64 Echo	(ping) red	quest	id=0x0001, seq=21/5376, ttl=64 (reply in 27)
	27 2022-07-14 20:20:42.657980675	198.51.100.100	192.0.2.100	ICMP	108	0xce49 (52809) 64 Echo	(ping) rep	ply	id=0x0001, seq=21/5376, ttl=64 (request in 26)
	28 2022-07-14 20:20:42.657981971	198.51.100.100	192.0.2.100	ICMP	108	0xce49 (5280) 64 Echo	(ping) rep	ply	id=0x0001, seq=21/5376, ttl=64
	29 2022-07-14 20:20:43.681736697	192.0.2.100	198.51.100.100	ICMP	108	0x5c52 (23634) 64 Echo	(ping) red	quest	id=0x0001, seq=22/5632, ttl=64 (no response found!)
¢.										
~	Frame 1: 100 butes on wine (064 bi	te) 100 botos c	antured (064 hits)	on intenface (anture u					ann an sa sa sa ad ar sa sa ar bd ba rr od sa os an an
(Ethacoat II Sec: Cisco b0:77:3d (co, 07. hd. ho. 77. 7	d) Det: Whate of	·07-50 (00-50-5	apcure_u	50)				010 00 00 00 00 00 07 00 08 07 00 09 77 20 09 20 00 00 PV PX PA PA
Ĵ,	Echernee II, Sici cisco_09.77.20 (56.97.00.09.77.2	uj, osc. viware_su	.00.30.	o.su.er.	50)			0	40 01 f4 1c c0 00 02 64 c6 33 64 64 08 00 22 68 @d .3dd"h
1	AN- Lag	= Direct	tion: To Bridge						0	030 00 01 00 0f 89 7a d0 62 00 00 00 00 b3 d7 09 00z.b
	A	- Doint	and wiff id						0	040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b
		- Dosti	er: VII_IO						0	050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ···· !"# \$%&'()*+
		- Loopor	di Mo						0	060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,/0123 4567
1		- Roson	and a	4						
		- Voncia	Neu. 0							
1	0000 00	00 1010 - Source	on. 0							
	Tunoi 903 10 Vintual IAN (0x9100	1010 = 3001C	c, 10							
J	1992 10 Victual LAN DRI: A DET: A	10: 103		_						
	- Deioeitu	Doct Effort (do	fault) (0)							
	a per mali	gible	1001() (0)	2						
1	0000 0110 0111 - TD: 103	Prove		2						
1	Turne: TPu4 (0x0000)									
J	Internet Protocol Version A. Spc:	192 8 2 188 Det	198 51 100 100	_						
1	Internet Control Message Protocol		. 1991911100.100	2						
1	and a second of the stage of otocor			-						
_										

No.	Time	Source	Destination	Protocol	Length	IP ID		IP TTL Info							
E	1 2022-07-14 20:20:36.513854256	192.0.2.100	198.51.100.100	ICMP	108	0x5990	(22928)	64 Echo	(ping)	request	id=0x0001	seq=15/3840,	ttl=64	(no response found!)	
	2 2022-07-14 20:20:36.513857289	192.0.2.100	198.51.100.100	ICMP	108	0x5990	(22928)	64 Echo	(ping)	request	id=0x0001	seq=15/3840,	ttl=64	(reply in 3)	
-	3 2022-07-14 20:20:36.514117394	198.51.100.10	9 192.0.2.100	ICMP	108	Øxcc2c	(52268)	64 Echo	(ping)	reply	id=0x0001	seq=15/3840,	ttl=64	(request in 2)	
	4 2022-07-14 20:20:36.514119312	198.51.100.10	0 192.0.2.100	ICMP	108	0xcc2c	(52268)	64 Echo	(ping)	reply	id=0x0001	seq=15/3840,	ttl=64		
	5 2022-07-14 20:20:37.537723822	192.0.2.100	198.51.100.100	ICMP	108	0x5a00	(23040)	64 Echo	(ping)	request	id=0x0001	seq=16/4096,	ttl=64	(no response found!)	
	6 2022-07-14 20:20:37.537726588	192.0.2.100	198.51.100.100	ICMP	108	0x5a00	(23040)	64 Echo	(ping)	request	id=0x0001	seq=16/4096,	ttl=64	(reply in 7)	
	7 2022-07-14 20:20:37.538046165	198.51.100.100	0 192.0.2.100	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	0 192.0.2.100	ICMP	108	0xcc9b	(52379)	64 Echo	(ping)	reply	id=0x0001	seq=16/4096,	ttl=64		
	9 2022-07-14 20:20:38.561776064	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7	(23223)	64 Echo	(ping)	request	id=0x0001	seq=17/4352,	ttl=64	(no response found!)	
	10 2022-07-14 20:20:38.561778310	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7	(23223)	64 Echo	(ping)	request	id=0x0001	seq=17/4352,	ttl=64	(reply in 11)	
	11 2022-07-14 20:20:38.562048288	198.51.100.10	0 192.0.2.100	ICMP	108	0xccc4	(52420)	64 Echo	(ping)	reply	id=0x0001	seq=17/4352,	ttl=64	(request in 10)	
	12 2022-07-14 20:20:38.562050333	198.51.100.10	0 192.0.2.100	ICMP	108	Øxccc4	(52420)	64 Echo	(ping)	reply	id=0x0001	seq=17/4352,	ttl=64		
	13 2022-07-14 20:20:39.585677043	192.0.2.100	198.51.100.100	ICMP	108	0x5b46	(23366)	64 Echo	(ping)	request	id=0x0001	seq=18/4608,	ttl=64	(no response found!)	
	14 2022-07-14 20:20:39.585678455	192.0.2.100	198.51.100.100	ICMP	108	0x5b46	(23366)	64 Echo	(ping)	request	id=0x0001	seq=18/4608,	ttl=64	(reply in 15)	
	15 2022-07-14 20:20:39.585936554	198.51.100.100	0 192.0.2.100	ICMP	108	0xcd8d	(52621)	64 Echo	(ping)	reply	id=0x0001	seq=18/4608,	ttl=64	(request in 14)	
	16 2022-07-14 20:20:39.585937900	198.51.100.100	9 192.0.2.100	ICMP	108	0xcd8d	(52621)	64 Echo	(ping)	reply	id=0x0001	seq=18/4608,	ttl=64		
	17 2022-07-14 20:20:40.609804804	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b	(23419)	64 Echo	(ping)	request	id=0x0001	seq=19/4864,	ttl=64	(no response found!)	
	18 2022-07-14 20:20:40.609807618	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b	(23419)	64 Echo	(ping)	request	id=0x0001	seq=19/4864,	ttl=64	(reply in 19)	
	19 2022-07-14 20:20:40.610179685	198.51.100.10	0 192.0.2.100	ICMP	108	0xcd8f	(52623)	64 Echo	(ping)	reply	id=0x0001	seq=19/4864,	ttl=64	(request in 18)	
	20 2022-07-14 20:20:40.610181944	198.51.100.10	0 192.0.2.100	ICMP	108	0xcd8f	(52623)	64 Echo	(ping)	reply	id=0x0001	seq=19/4864,	ttl=64		
	21 2022-07-14 20:20:41.633805153	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e	(23422)	64 Echo	(ping)	request	id=0x0001	seq=20/5120,	tt1=64	(no response found!)	
	22 2022-07-14 20:20:41.633806997	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e	(23422)	64 Echo	(ping)	request	id=0x0001	seq=20/5120,	tt1=64	(reply in 23)	
	23 2022-07-14 20:20:41.634084102	198.51.100.100	0 192.0.2.100	ICMP	108	0xce36	(52790)	64 Echo	(ping)	reply	id=0x0001	seq=20/5120,	tt1=64	(request in 22)	
	24 2022-07-14 20:20:41.634085368	198.51.100.100	0 192.0.2.100	ICMP	108	0xce36	(52790)	64 Echo	(ping)	reply	id=0x0001	seq=20/5120,	tt1=64		
	25 2022-07-14 20:20:42.657709898	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0	(23536)	64 Echo	(ping)	request	id=0x0001	seq=21/5376,	tt1=64	(no response found!)	
	26 2022-07-14 20:20:42.657711660	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0	(23536)	64 Echo	(ping)	request	1d=0x0001	seq=21/5376,	tt1=64	(reply in 27)	
	27 2022-07-14 20:20:42.657980675	198.51.100.100	3 192.0.2.100	ICMP	108	0xce49	(52809)	64 Echo	(ping)	reply	1d=0x0001	seq=21/5376,	ttl=64	(request in 26)	
	28 2022-07-14 20:20:42.657981971	198.51.100.100	3 192.0.2.100	ICMP	108	Øxce49	(52809)	64 Echo	(ping)	reply	1d=0x0001	seq=21/5376,	tt1=64	(
	29 2022-07-14 20:20:43.681736697	192.0.2.100	198.51.100.100	ICMP	108	0X5C52	(23634)	64 Echo	(ping)	request	1d=0x0001	seq=22/5632,	tt1=64	(no response tound1)	
<															
>	Frame 2: 108 bytes on wire (864 bit	s), 108 bytes (captured (864 bits)) on int	terface capture_u	0_8, id (3			6	000 00 50	56 9d e7 50 5	897 bo	d b9 77 2d 89 26 00 00	·PV ··PX · ··w ··& ··
>	Ethernet II, Src: Cisco b9:77:2d (5	8:97:bd:b9:77:	2d), Dst: VMware 9d	d:e7:50	(00:50:56:9d:e7:	50)				6	0010 00 0a	81 00 00 67 0	8 00 45	5 00 00 54 59 90 40 00	····g·· E··TY·@·
4	VN-Tag									6	0020 40 01	f4 1c c0 00 0	2 64 ce	5 33 64 64 08 00 22 68	@·····d ·3dd··"h
	0	= Direc	tion: To Bridge								030 00 01	00 01 89 7a d	0 62 0	0 00 00 00 b3 d7 09 00	·····z·b
	.0	= Point	er: vif_id								0040 00 00	10 16 20 21 2	2 13 14	4 15 16 17 18 19 1a 10	1"# 678'/*+
		= Desti	nation: 0								1050 1C 10	2e 2f 30 31 3	2 23 24	4 25 26 27 26 25 28 20	
	···· ··· ··· ··· ··· 0 ····	= Loope	d: No	4											,
	0	= Reser	ved: 0												
		= Versi	on: 0												
	0000 000	90 1010 = Sourc	e: 10												
	Type: 802.1Q Virtual LAN (0x8100))													
М	802.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 103													
11	000 E Priority: E	Best Effort (de	fault) (0)												
11	0 = DEI: Inelig	gible		3											
11	0000 0110 0111 = ID: 103			-											
L	Type: IPv4 (0x0800)		. 100 51 100 100												
P	Internet Protocol Version 4, Src: 1	92.0.2.100, DS	t: 198.51.100.100	2											
2	Internet control Message Protocol			4											
Ц				_											

3番目と4番目のパケットを選択し、キーポイントを確認します。

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

2

Type: IPv4 (0x0800) Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100 Internet Control Message Protocol

- 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。

No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info						
Γ.	1 2022-07-14 20:20:36.513854256	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928) 64 Echo (ping)	request	id=0x000	1, 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	8x5998 (22928	64 Ecbo (ning)	request	id=0x000	1, seq=15/3840,	ttl=64	(reply in 3)	
+	3 2022-07-14 20:20:36.514117394	198.51.100.100	192.0.2.100	ICMP	108	0xcc2c (52268) 64 Echo (ping)	reply	id=0x000	1, seq=15/3840,	ttl=64	(request in 2)	
	4 2022-07-14 20:20:36.514119312	198.51.100.100	192.0.2.100	ICMP	108	0xcc2c (52268) 64 Echo (ping)	reply	id=0x000	1, seq=15/3840,	ttl=64		
	5 2022-07-14 20:20:37.537723822	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040) 64 Echo (ping)	request	id=0x000	1, seq=16/4096,	ttl=64	(no response found!)	
	6 2022-07-14 20:20:37.537726588	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040) 64 Echo (ping)	request	id=0x000	1, seq=16/4096,	tt1=64	(reply in 7)	
	7 2022-07-14 20:20:37.538046165	198.51.100.100	192.0.2.100	ICMP	108	Øxcc9b (52379) 64 Echo (ping)	reply	id=0x000	1, seq=16/4096,	tt1=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=0x000	1, seq=16/4096,	tt1=64		
	9 2022-07-14 20:20:38.561776064	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223) 64 Echo (ping)	request	id=0x000	1, seq=17/4352,	tt1=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	1d=0x000	1, seq=17/4352,	tt1=64	(reply in 11)	
	11 2022-07-14 20:20:38.562048288	198.51.100.100	192.0.2.100	ICMP	108	0xccc4 (52420) 64 Echo (ping)	reply	1d=0x000	1, seq=17/4352,	tt1=64	(request in 10)	
	12 2022-07-14 20:20:38.562050333	198.51.100.100	192.0.2.100	ICMP	108	0xccc4 (52420) 64 Echo (ping)	reply	1d=0x000	1, seq=17/4352,	tt1=64		
	13 2022-07-14 20:20:39.585677043	192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366) 64 Echo (ping)	request	1d=0x000	1, seq=18/4608,	tt1=64	(no response found!)	
	14 2022-07-14 20:20:39.585678455	192.0.2.100	198.51.100.100	ICMP	108	0x5046 (23366) 64 Echo (ping)	request	1d=0x000	1, seq=18/4608,	tt1=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	1d=0x000	1, seq=18/4608,	tt1=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)	repty	10=0x000	1, seq=18/4608,	tt1=64	(an annance found))	
	1/ 2022-0/-14 20:20:40.609804804	192.0.2.100	198.51.100.100	ICMP	108	0x50/0 (23419) 64 Echo (ping)	request	10=0x000	1, seq=19/4864,	tt1=64	(no response tound1)	
	18 2022-07-14 20:20:40.009807018	192.0.2.100	198.51.100.100	TCMP	108	0x50/0 (23419) 64 Echo (ping)	request	10=0x000	1, seq=19/4804,	tt1=04	(reply in 19)	
	19 2022-07-14 20:20:40.0101/9085	198.51.100.100	192.0.2.100	TCMP	108	0xcuat (52623) 64 Echo (ping)	reply	10=0x000	1, seq=19/4804,	ttl=04	(request in is)	
	20 2022-07-14 20:20:40.010181944	103 0 3 100	100 51 100 100	TCMP	100	0xcuar (32023) 64 Echo (ping)	repry	id-0x000	1, seq=19/4804,	ttl-64	(no recentre found))	
	22 2022-07-14 20:20:41.055805155	192.0.2.100	100 51 100 100	TCMP	100	0x507e (23422) 64 Echo (ping)	request	id=0x000	1, seq=20/5120,	++1-64	(no response round)	
	22 2022-07-14 20:20:41.033800997	102.51.100 100	193.51.100.100	TCMP	100	0X5076 (25422 0X6036 (53700	64 Echo (ping)	request	id-exee	1, seq=20/5120,	++1=64	(request in 22)	
	24 2022-07-14 20:20:41.634085368	108 51 100 100	192.0.2.100	TCMP	108	0xce36 (52790	64 Echo (ping)	reply	id-evee	1 seq=20/5120	tt1=64	(request in zz)	
	25 2022-07-14 20:20:41:054005500	192.0.2.100	198.51.100.100	TCMP	108	avshfa (23536	64 Echo (ping)	request	id-evee	1, seq=20/5120,	tt1=64	(no response found!)	
	26 2022-07-14 20:20:42.657711660	192.0.2.100	198.51.100.100	TCMP	108	exshfe (23536	64 Echo (ping)	request	id=0x000	 seq=21/5376. 	tt1=64	(renly in 27)	
	27 2022-07-14 20:20:42.657980675	198,51,100,100	192.0.2.100	TCMP	108	8xce49 (52889	64 Echo (ping)	renly	id=0x000	1. seg=21/5376.	tt1=64	(request in 26)	
	28 2022-07-14 20:20:42.657981971	198,51,100,100	192.0.2.100	ICMP	108	0xce49 (52809	64 Echo (ping)	reply	id=0x000	1. seg=21/5376.	tt1=64	(request in roy	
	29 2022-07-14 20:20:43.681736697	192.0.2.100	198,51,100,100	ICMP	108	0x5c52 (23634	64 Echo (ping)	request	id=0x000	 seq=22/5632. 	tt1=64	(no response found!)	
	ES LOLL OF 14 LOLLOF451001150051	1511011100	1.00001100		100	CHISCOL (LISODA	, or coup (brug)	. educat		, ocq,		(in tesponse round)	
<u> </u>										a sc ad la be s	0.07 b		Phil 14
2	Frame 3: 108 bytes on wire (864 bit	s), 108 bytes c	aptured (864 bits)	on interface	capture_u0	_8, 1d 0			0000 00 5	0 56 90 e8 be 5	8 97 0	d b9 77 0e 89 26 00 00	·PV···X···W··&··
2	Ethernet II, Src: Cisco D9:77:0e (5	8:97:00:09:77:0	e), Dst: VMware_9d:	e8:De (00:50:	56:9d:e8:0	e)			0010 00 0		4 64 (1	9 99 92 64 99 99 23 68	@3ddd*h
1	vn-tag	0 and	dans To Daldas						0030 00 0	1 00 0f 89 7a d	0 62 0	e ee ee ee b3 d7 e9 ee	ez.b
T	0	= Direct	tion: To Bridge						0040 00 0	0 00 00 10 11 1	2 13 1	4 15 16 17 18 19 1a 1b	
T		- Pointe	er: VIT_10						0050 1c 1	d 1e 1f 20 21 2	2 23 24	4 25 26 27 28 29 2a 2b	···· !"# \$%&'()*+
T		= Destin	acion: 0						0060 2c 2	d 2e 2f 30 31 3	2 33 34	4 35 36 37	,/0123 4567
T			india a	4									
T		- Vorsio	neu. o										
T			01:0										
1	Type: 902 10 Victual LAN (0v9100))											
J	1992 10 Victual LAN DRI: 0 DEI: 0	10: 102		_									
1	and - Deigeitur	To: 102	(a)										
T	000 = Priority: 1	mible	aur() (0)	2									
1	0000 0110 0110 - TO: 102	Prove		2									
1	Tunoi Thuế (0x0200)												

説明

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

タスクの要約を次の表に示します。

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

アプリケーションおよびアプリケーションポートでのパケットキャプチャ

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

主に2つの使用例があります。

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

このセクションでは、両方の使用例について説明します。

タスク1

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

トポロジ、パケットフロー、およびキャプチャポイント



コンフィギュレーション

FCM

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

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

Overview	Interfaces	Logical Devices	Security Engine	Platform Settings		System	Tools Help admin
						Packet Capture	Troubleshooting Logs
Capture See	sion Fiter Li	st					
					C Refresh	Capture Session Dele	te All Sessions
No Session a	vailable						

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

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	
Ethernet1/2		Buffer Size	256 MB	
		Snap length:	1518 Bytes	
		Store Packets	Overwrite Append	
		Capture On	ftd	
Ethernet1/3	ED	Application Port	Ethernet1/2	
	Ethernet1/9, Ethernet1/10	Application Capture Direction	All Packets Egress Packet	
		Capture Filter	Apply Filter Capture All	
Ethernet1/1				

FXOS CLI

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

実行します。

1. アプリケーションのタイプと識別子を特定します。

firepower	# scope sa	sa									
firepower	/ssa# sl	now app-inst	ance								
App Name	Identif	ier Slot ID	Admin Stat	te Oper State	Running Versi	on Startup Version					
Deploy Ty	Deploy Type Turbo Mode Profile Name Cluster State Cluster Role										
ftd	ftd1	1	Enabled	Online	7.2.0.82	7.2.0.82					
Native	No		Not App	plicable None							
2 = +	ヮプチャヤ	ッションを	作成します。								
	, , , , , , , , , , , , , , , , , , ,										

firepower	# scope packet-capture	
firepower	<pre>/packet-capture # create session cap1</pre>	
firepower	<pre>/packet-capture/session* # create app</pre>	-port 1 112 Ethernet1/2 ftd
firepower	/packet-capture/session/app-port* # s	et app-identifier ftd1
firepower	/packet-capture/session/app-port* # s	et filter ""
firepower	/packet-capture/session/app-port* # s	et subinterface 0
firepower	/packet-capture/session/app-port* # u	D
firepower	/packet-capture/session* # commit	
firepower	/packet-capture/session #	
確認		

FCM

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

Overvie	w Interfaces	Logical Devices Se	ecurity Engine P	Platform Settings			System	n Tools Help admin
Capture	Session Fiter Li	t						
							Capture Session Delete	e Al Sessions
•	cap1	Drop Count: 0		Operational State: up	Buffer Size: 256 M	4B	Snap Length: 1518 Bytes	
Interfac	e Name	Filter		File Size (in bytes)	File Name	Device Name		
Ethernet	1/2 - Ethernet1/10	None		576	cap1-vethernet-1175.pcap	ftd1	.⊻	
Ethernet	I/2 - Ethernet1/9	None		4360	cap1-vethemet-1036.pcap	ftd1	⊻	

FXOS CLI

scope packet-captureでキャプチャの詳細を確認します。

firepower# scope packet-capture
firepower /packet-capture # show session cap1
Traffic Monitoring Session:
 Packet Capture Session Name: cap1
 Session: 1
 Admin State: Enabled
 Oper State: Up
 Oper State Reason: Active
 Config Success: Yes
 Config Fail Reason:
 Append Flag: Overwrite
 Session Mem Usage: 256 MB

```
Session Pcap Snap Len: 1518 Bytes
  Error Code: 0
  Drop Count: 0
Application ports involved in Packet Capture:
   Slot Id: 1
   Link Name: 112
   Port Name: Ethernet1/2
  App Name: ftd
   Sub Interface: 0
   Application Instance Identifier: ftd1
Application ports resolved to:
   Name: vnic1
   Eq Slot Id: 1
   Eq Port Id: 9
   Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1036.pcap
   Pcapsize: 53640 bytes
  Vlan: 102
  Filter:
  Name: vnic2
   Eq Slot Id: 1
   Eq Port Id: 10
   Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1175.pcap
   Pcapsize: 1824 bytes
  Vlan: 102
  Filter:
キャプチャファイルの収集
```

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

ファイル分析のキャプチャ

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

最初と2番目のパケットを選択し、キーポイントを確認します。

- 1. 各ICMPエコー応答はキャプチャされ、2回表示されます。
- 2. 元のパケットヘッダーにはVLANタグが付いていません。
- 3. 内部スイッチは、出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 -	9x42f8 (17144)	64 Echo (ping) rep	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	0x42f8 (17144)	64 Echo (ping) rep	ly id=0x0012, seg=1/256, tt1=64
3 2022-08-01 10:03:23.232244769	198.51.100.100	192.0.2.100	ICMP	108	0X4303 (17331)	64 ECHO (DINK) PED	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) rep	ly 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) rep	ly 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) rep	ly 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) rep	ly 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) rep	ly 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) rep	ly 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) rep	ly 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) rep	ly 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) rep	ly 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) rep	ly 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) rep	ly 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) rep	ly 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) rep	ly 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) rep	ly 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) rep	ly 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 (18042)	64 Echo (ping) rep	ly id=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 (18042)	64 Echo (ping) rep	ly id=0x0012, seq=10/2560, ttl=64
21 2022-08-01 10:03:32.426693254	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64 Echo (ping) rep	ly id=0x0012, seq=11/2816, ttl=64
22 2022-08-01 10:03:32.426695691	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64 Echo (ping) rep	ly id=0x0012, seq=11/2816, ttl=64
<pre>< Frame 1: 108 bytes on wire (864 bit Ethernet II, Src: Cisco b9:77:8e (5 Wh-Tag 0 0 0 0 0 0 0 0.</pre>	s), 108 bytes ca 8:97:bd:b9:77:00 = Direct	ptured (864 bits)), Dst: VMware 9d: ion: To Bridge e: vif (d	on interface (e8:be (00:50:	capture_ui 56:9d:e8:1	0_8, id 0 be)		0000 00 50 56 9d e8 58 97 bd b7 78 89 26 00 00
	= Pointe = Destin = Looped = Reserve = Version 00 1010 = Source	r: vif_id ation: 0 : No ed: 0 n: 0 : 10	4				0050 lc ld le lf 20 21 22 23 24 25 26 27 28 29 2a 2b !*# \$\$\$\$()*+ 0050 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,/0123 4567
802.10 Virtual LAN, PRI: 0. DET: 0.	ID: 102		_				
000 = Priority:	Best Effort (def	ault) (0)					
0 = DEI: Ineli	gible		2				
0000 0110 0110 = ID: 102	Prove		2				
Type: TPv4 (0x0000)							
Internet Protocol Version 4. Src: 1	98.51.100.100.0	st: 192.0.2.100					
Internet Control Message Protocol			21				
incernet control nessage riotocol			~				
L							
No. Time	Source	Destination	Protocol	Lendth	PD	IP TTL Info	
No. Time 1 2022-08-01 10:03:22,231237959	Source 198.51.100.100	Destination 192.0.2.100	Protocol	Length	PD 0x42f8 (17144)	PTTL Mo 64 Echo (ping) reply	id-9x0012, seg=1/256, ttl=64
No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231239747	Source 198.51.100.100 198.51.100.100	Destination 192.0.2.100 192.0.2.100	Protocol ICMP ICMP	Length 108	PD 0x42f8 (17144) 0x42f8 (17144)	PTTL Mo 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64
No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.2312379747 3 2022-08-01 10:03:23.232244769	Source 198.51.100.100 198.51.100.100 198.51.100.100	Destination 192.0.2.100 192.0.2.100 192.0.2.100	Protocol ICMP ICMP ICMP	Length 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x4303 (1/331)	PTTL №6 64 Echo (ping) reply 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, tt1=64 id=0x0012, seq=1/256, tt1=64 id=0x0012, seq=2/512, tt1=64
No. Teme 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:23.232244769 4 2022-08-01 10:03:23.232244753	Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Protocol ICMP ICMP ICMP ICMP	Length 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x4303 (17331) 0x4303 (17331)	PTTL 100 64 Echo (ping) reply 64 Echo (ping) reply 04 Echo (ping) reply 64 Echo (ping) reply	id-0x0012, seq=1/256, ttl=64 id-0x0012, seq=1/256, ttl=64 id-0x0012, seq=2/512, ttl=64 id-0x0012, seq=2/512, ttl=64
Ime Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:23.23224769 4 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:24.232470598 5 2022-08-01 10:03:24.232470598	Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Protocol ICMP ICMP ICMP ICMP ICMP	Length 108 108 108 108 108	₽ D 0x42f8 (17144) 0x42f8 (17144) 0x4303 (17331) 0x4303 (17331) 0x445e (17502)	PTTL 140 64 Echo (ping) reply 64 Echo (ping) reply 64 Echo (ping) reply 64 Echo (ping) reply 64 Echo (ping) reply	id-0x0012, seq=1/256, ttl=64 id-0x0012, seq=1/256, ttl=64 id-0x0012, seq=2/512, ttl=64 id-0x0012, seq=2/512, ttl=64 id-0x0012, seq=3/568, ttl=64
No. Time 1 2022-08-01 10:03:22.231237959 2 3022-08-01 10:03:23.232239747 3 2022-08-01 10:03:23.232247753 4 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:23.232247753 6 2022-08-01 10:03:23.232247753 6 2022-08-01 10:03:23.232247753	Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Protocol ICMP ICMP ICMP ICMP ICMP	Length 108 1 108 1 108 1 08 108 1 08 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x4303 (17331) 0x445e (17502) 0x445e (17502)	PTTL Mo 64 Echo (ping) reply 64 Echo (ping) reply 64 Echo (ping) reply 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64
Tme 1 2022-08-01 10:03:22.231237959 2 0022-08-01 10:03:22.231239747 3 2022-08-01 10:03:23.23224759 4 2022-08-01 10:03:23.23224759 5 2022-08-01 10:03:24.234703981 6 2022-08-01 10:03:24.234705751 7 2022-08-01 10:03:25.258572489	Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Protocol ICNP ICNP ICNP ICNP ICNP ICNP ICNP	Length 108 108 108 108 108 108 108	₽ D 0x42f8 (17144) 0x42f8 (17144) 0x4303 (17331) 0x4353 (17331) 0x445e (17502) 0x445e (17502) 0x4454 (17508)	PTTL 3% 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, tt1=64 id=0x0012, seq=1/256, tt1=64 id=0x0012, seq=2/512, tt1=64 id=0x0012, seq=2/512, tt1=64 id=0x0012, seq=3/766, tt1=64 id=0x0012, seq=3/766, tt1=64
Ime Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:23.232244769 4 2022-08-01 10:03:23.232244769 5 2022-08-01 10:03:24.234709811 6 2022-08-01 10:03:24.2347096751 7 2022-08-01 10:03:25.2586724601 8 2022-08-01 10:03:25.258672461	Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Protocol ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP	Length 108 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x4305 (17331) 0x4305 (17331) 0x445e (17502) 0x4454 (17508) 0x4464 (17508)	PTTL bb 64 Echo (ping) reply 64 Echo (ping) reply	id-0x0012, seq=1/256, ttl=64 id-0x0012, seq=1/256, ttl=64 id-0x0012, seq=2/512, ttl=64 id-0x0012, seq=2/512, ttl=64 id-0x0012, seq=3/768, ttl=64 id-0x0012, seq=3/768, ttl=64 id-0x0012, seq=4/1024, ttl=64
No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:23.23224759 4 2022-08-01 10:03:23.23224759 5 2022-08-01 10:03:23.23224759 6 2022-08-01 10:03:23.23224759 7 2022-08-01 10:03:24.234706791 7 2022-08-01 10:03:25.258672449 8 2022-08-01 10:03:25.2586724461 9 2022-08-01 10:03:25.2586724461	Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 1 108 1 108 1 08 1 08 1 08 1 08 1 0	PD 0x42f8 (17144) 10x42f8 (17144) 0x4305 (1731) 0x4355 (1752) 0x4456 (17502) 0x4456 (17508) 0x4464 (17508) 0x4463 (17603)	PTTL Mo 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/766, ttl=64 id=0x0012, seq=3/766, ttl=64 id=0x0012, seq=3/1024, ttl=64 id=0x0012, seq=3/1024, ttl=64 id=0x0012, seq=3/1024, ttl=64
Ime Time 1 2022-08-01 10:03:22,231237959 2 2022-08-01 10:03:22,231239747 3 2022-08-01 10:03:23,23224759 4 2022-08-01 10:03:23,23224759 5 2022-08-01 10:03:23,23224759 7 2022-08-01 10:03:24,234703981 6 2022-08-01 10:03:25,25867249 8 2022-08-01 10:03:25,2586724651 9 2022-08-01 10:03:26,282663169 10 2022-08-01 10:03:26,282665169	Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Protocol ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP	Length 108 108 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x43f8 (17144) 0x4303 (17331) 0x4352 (17502) 0x4454 (17502) 0x4464 (17508) 0x4464 (17508) 0x4463 (17603)	PTTL b6 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=5/1280, ttl=64
No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.231239747 4 2022-08-01 10:03:23.23224775 5 2022-08-01 10:03:23.23224775 6 2022-08-01 10:03:23.23224775 7 2022-08-01 10:03:25.258672449 8 2022-08-01 10:03:25.258672451 9 2022-08-01 10:03:25.258672451 10 2022-08-01 10:03:27.3667165163 11 2022-08-01 10:03:27.366716513	Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 1 108 1 108 1 08 1 08 1 08 1 08 1 0	PD 0x42F8 (17144) 0x42F8 (17144) 0x4305 (17331) 0x4356 (17502) 0x4456 (17502) 0x4454 (17508) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4463 (17603) 0x4467 (17639)	PTR 36 64 Echo (ping) reply 64 Echo (ping) reply	id-exx0012, seq=1/256, ttl=64 id-exx0012, seq=1/256, ttl=64 id-exx0012, seq=2/512, ttl=64 id-exx0012, seq=2/512, ttl=64 id-exx0012, seq=3/768, ttl=64 id-exx0012, seq=4/1024, ttl=64 id-exx0012, seq=4/1024, ttl=64 id-exx0012, seq=5/1280, ttl=64 id-exx0012, seq=5/1280, ttl=64 id-exx0012, seq=5/1280, ttl=64
No. Time 1 2022 - 08 - 01 10:03:22.231237959 2 2022 - 08 - 01 10:03:22.231239747 3 7022 - 08 - 01 10:03:23.23224759 4 2022 - 08 - 01 10:03:23.23224759 5 7022 - 08 - 01 10:03:23.23224759 6 2022 - 08 - 01 10:03:23.23224759 7 2022 - 08 - 01 10:03:25.258672449 8 2022 - 08 - 01 10:03:25.25867249 9 2022 - 08 - 01 10:03:25.25867249 19 2022 - 08 - 01 10:03:25.25867249 10 202 - 08 - 01 10:03:27.36676618 11 2022 - 08 - 01 10:03:27.306674378	Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Protocol ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP	Length 108 108 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x4305 (17331) 0x4356 (17502) 0x4456 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17603) 0x4467 (17639) 0x4467 (17639)	PTTL Mo 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, tt1=64 id=0x0012, seq=1/256, tt1=64 id=0x0012, seq=2/512, tt1=64 id=0x0012, seq=3/768, tt1=64 id=0x0012, seq=3/768, tt1=64 id=0x0012, seq=4/1024, tt1=64 id=0x0012, seq=4/1024, tt1=64 id=0x0012, seq=5/1280, tt1=64 id=0x0012, seq=5/1280, tt1=64 id=0x0012, seq=6/1536, tt1=64 id=0x0012, seq=6/1536, tt1=64
No. Time 1 2022-08-01 10:01:22.231237959 2 3022-08-01 10:01:22.231239747 3 2022-08-01 10:01:23.232247753 5 3022-08-01 10:01:23.232247753 6 3022-08-01 10:01:23.232247753 7 3022-08-01 10:01:24.234706714 8 3022-08-01 10:01:25.258572449 8 3022-08-01 10:01:25.258572451 9 3022-08-01 10:01:26.232663169 10 2022-08-01 10:01:27.306727164 12 3022-08-01 10:01:27.30672164 12 3022-08-01 10:01:27.306747164 13 2022-08-01 10:01:28.330664677	Source 198, 51, 100, 100 198, 51, 100, 100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 108 108 108 108 108 108 108	PD 0x42F8 (17144) 0x43F8 (17144) 0x4303 (17331) 0x4350 (17331) 0x4454 (17502) 0x4454 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4467 (17639) 0x4455 (17744)	PTTL bb 64 Echo (ping) reply 64 Echo (ping	id=0x0012, seq=1/256, tt1=64 id=0x0012, seq=1/256, tt1=64 id=0x0012, seq=2/512, tt1=64 id=0x0012, seq=2/512, tt1=64 id=0x0012, seq=3/768, tt1=64 id=0x0012, seq=3/768, tt1=64 id=0x0012, seq=4/1024, tt1=64 id=0x0012, seq=4/1024, tt1=64 id=0x0012, seq=4/1026, tt1=64 id=0x0012, seq=4/1536, tt1=64 id=0x0012, seq=4/1536, tt1=64 id=0x0012, seq=4/1536, tt1=64 id=0x0012, seq=4/1536, tt1=64
No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231239747 3 7022-08-01 10:03:22.231239747 3 7022-08-01 10:03:22.23123755 5 7022-08-01 10:03:22.232247753 6 7022-08-01 10:03:23.232247751 7 7022-08-01 10:03:24.234706751 9 7022-08-01 10:03:25.258672449 9 7022-08-01 10:03:26.282666183 11 7022-08-01 10:03:27.306671644 12 7022-08-01 10:03:27.306674378 13 7022-08-01 10:03:27.30667164 12 7022-08-01 10:03:27.30667164 12 7022-08-01 10:03:27.30667164 13 7022-08-01 10:03:27.30667164 13 7022-08-01 10:03:27.30667164 13 7022-08-01 10:03:27.30667164 14 7022-08-01 10:03:27.30667153 14 7022-08-01 10:03:27.306671543 13 7022-08-01 10:03:27.306671543 14 7022-08-01 10:03:27.306671543 14 7022-08-01 10:03:27.306671543	Source 198, 51, 100, 100 198, 51, 100, 100	Destination 192. 0. 2. 100 192. 0. 2. 100	Protocol I CNP I CNP	Length 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x43f8 (17144) 0x4305 (17331) 0x4352 (17502) 0x4452 (17502) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17603) 0x4467 (17639) 0x4467 (17639) 0x4677 (17744) 0x4550 (17744)	PTH Me 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 68 Echo (ping) reply 68 Echo (ping) reply 69 Echo (ping) reply 69 Echo (ping) reply 60 Echo (ping)	id-0x0012, seq=1/256, ttl=64 id-0x0012, seq=1/256, ttl=64 id-0x0012, seq=2/512, ttl=64 id-0x0012, seq=2/512, ttl=64 id-0x0012, seq=3/766, ttl=64 id-0x0012, seq=3/1024, ttl=64 id-0x0012, seq=3/1024, ttl=64 id-0x0012, seq=3/1026, ttl=64
No. Time 1 2022 - 08 - 01 10:03:22.231237959 2 2022 - 08 - 01 10:03:22.231239747 3 7022 - 08 - 01 10:03:23.232247759 4 7022 - 08 - 01 10:03:23.232247759 5 7022 - 08 - 01 10:03:23.232247759 6 7022 - 08 - 01 10:03:23.232247759 7 7022 - 08 - 01 10:03:25.258672440 9 7022 - 08 - 01 10:03:25.258672440 9 7022 - 08 - 01 10:03:25.258672406 9 7022 - 08 - 01 10:03:25.258672406 9 7022 - 08 - 01 10:03:25.258672406 9 7022 - 08 - 01 10:03:27.306671694 12 7022 - 08 - 01 10:03:27.306671694 13 7022 - 08 - 01 10:03:27.306674571 14 7022 - 08 - 01 10:03:27.306745375 15 7022 - 08 - 01 10:03:27.30674575 14 7020 - 08 - 01 10:03:27.30674575 15 7022 - 08 - 01 10:03:27.30674575 16 7020 - 08 - 01 10:03:27.30674575 16 7020 - 08 - 01 10:03:27.30674575	Source 198, 51, 100, 100 198, 51, 100, 100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x43f8 (17144) 0x4305 (17331) 0x43b2 (17502) 0x445c (17502) 0x446c (17508) 0x4464 (17508) 0x4464 (17603) 0x4467 (17639) 0x4467 (17639) 0x4467 (17743) 0x4550 (17744) 0x4553 (17744)	PTTL 260 64 Echo (ping) reply 64 Echo (pin	id=0x0012, seq=1/256, tt1=64 id=0x0012, seq=1/256, tt1=64 id=0x0012, seq=2/512, tt1=64 id=0x0012, seq=2/512, tt1=64 id=0x0012, seq=3/766, tt1=64 id=0x0012, seq=4/1024, tt1=64 id=0x0012, seq=4/1024, tt1=64 id=0x0012, seq=4/1024, tt1=64 id=0x0012, seq=5/1280, tt1=64 id=0x0012, seq=5/1280, tt1=64 id=0x0012, seq=6/1556, tt1=64 id=0x0012, seq=7/1792, tt1=64 id=0x0012, seq=7/1792, tt1=64 id=0x0012, seq=7/164, tt1=64 id=0x0012, seq=7/164, tt1=64
 Ime 1 2022-08-01 10:01:22.231237959 2 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.231239747 5 2022-08-01 10:03:22.232247753 5 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:25.258674861 8 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 10 2022-08-01 10:03:27.366671654 11 2022-08-01 10:03:27.366671534 12 2022-08-01 10:03:27.366671534 13 2022-08-01 10:03:27.366671534 14 2022-08-01 10:03:27.366671534 15 2022-08-01 10:03:29.354795301 2022-08-01 10:03:29.35479530766 2022-08-01 10:03:29.35479530766 	Source 198, 51, 100, 100 198, 51, 100, 100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Ривнов I СИР I СИР	Length 108 1 108 1 1	PD 0x42f8 (17144) 0x43f8 (17144) 0x4305 (1731) 0x4354 (1752) 0x4454 (17502) 0x4454 (17503) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17539) 0x4467 (17639) 0x4467 (17639) 0x4550 (17744) 0x4555 (17747) 0x4553 (17747)	PTTL 26 64 Echo (ping) reply 64 Echo (ping	id-bx0012, seq=1/256, ttl=64 id-bx0012, seq=1/256, ttl=64 id-bx0012, seq=2/512, ttl=64 id-bx0012, seq=2/512, ttl=64 id-bx0012, seq=2/512, ttl=64 id-bx0012, seq=4/1024, ttl=64 id-bx0012, seq=4/1024, ttl=64 id-bx0012, seq=4/1026, ttl=64 id-bx0012, seq=4/1026, ttl=64 id-bx0012, seq=4/1266, ttl=64 id-bx0012, seq=4/1266, ttl=64 id-bx0012, seq=4/1266, ttl=64 id-bx0012, seq=2/1266, ttl=64 id-bx0012, seq=2/1266, ttl=64 id-bx0012, seq=2/1268, ttl=64 id-bx0012, seq=2/1268, ttl=64 id-bx0012, seq=2/1268, ttl=64 id-bx0012, seq=2/1268, ttl=64 id-bx0012, seq=2/1268, ttl=64 id-bx0012, seq=2/2688, ttl=64
No. Time 1 2022 - 08 - 01 10:03:22.231237959 2 2022 - 08 - 01 10:03:22.231239747 3 2022 - 08 - 01 10:03:22.231239747 3 2022 - 08 - 01 10:03:22.231239747 4 2022 - 08 - 01 10:03:22.32224775 5 2022 - 08 - 01 10:03:23.23224775 6 2022 - 08 - 01 10:03:25.258672449 8 2022 - 08 - 01 10:03:25.258672449 9 2022 - 08 - 01 10:03:25.258672449 9 2022 - 08 - 01 10:03:25.258672449 10 2022 - 08 - 01 10:03:27.306671641 10 2022 - 08 - 01 10:03:27.306671641 12 2022 - 08 - 01 10:03:27.306671641 13 2022 - 08 - 01 10:03:27.30667164738 13 2022 - 08 - 01 10:03:28.3306647573 14 2022 - 08 - 01 10:03:28.330667153 15 2022 - 08 - 01 10:03:28.330667153 16 2022 - 08 - 01 10:03:28.330667153 16 2022 - 08 - 01 10:03:28.330667153 16 2022 - 08 - 01 10:03:28.330667153 18 2022 - 08 - 01 10:03:28.330657153 18 2022 - 08 - 01 10:03:28.3305759244	Source 198, 51, 100, 100 198, 51, 100, 100	Destination 192. 0. 2. 100 192. 0. 2. 100	Риовсай ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP	Leogth 108 1 108 1 1	PD 0x42f8 (17144) 0x43f8 (17144) 0x4305 (17331) 0x4352 (17502) 0x4454 (17502) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4677 (17639) 0x4675 (17744) 0x4555 (17744) 0x4555 (17744) 0x4555 (17744) 0x4557 (17747) 0x4597 (17815)	PTTL Mo 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping	id-0x0012, seq=1/256, ttl=64 id-0x0012, seq=2/512, ttl=64 id-0x0012, seq=2/512, ttl=64 id-0x0012, seq=2/512, ttl=64 id-0x0012, seq=3/766, ttl=64 id-0x0012, seq=3/766, ttl=64 id-0x0012, seq=3/126, ttl=64 id-0x0012, seq=3/1260, ttl=64 id-0x0012, seq=3/2680, ttl=64
No. Time 1 2022-08-01 10:01:22.231237959 2 3022-08-01 10:01:22.231239747 3 2022-08-01 10:01:23.232247753 5 2022-08-01 10:01:23.232247753 5 2022-08-01 10:01:23.232247753 6 2022-08-01 10:01:24.234706714 7 2022-08-01 10:01:25.25872449 8 2022-08-01 10:01:25.258672461 9 2022-08-01 10:01:25.258672461 10 2022-08-01 10:01:27.306671564 12 2022-08-01 10:01:27.306671564 12 2022-08-01 10:01:27.30667151 13 2022-08-01 10:01:27.30667151 15 2022-08-01 10:01:27.30667151 15 2022-08-01 10:01:27.30667151 16 2022-08-01 10:01:28.330664671 14 2022-08-01 10:01:28.3306615151 15 2022-08-01 10:01:28.3306615151 16 2022-08-01 10:01:01:28.33067151 17 2022-08-01 10:01:01:03.73879520706 17 2022-08-01 10:01:01:03.73879520706 17 2022-08-01 10:01:01:03.73879520706 17 2022-08-01 10:01:01:03.73879520706	Source 198, 51, 100, 100 198, 51, 100, 100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Ривной ICMP	Length 108 108 108 108 108 108 108 108	PD 0x42F8 (17144) 0x4305 (1731) 0x43b3 (1731) 0x43b2 (17502) 0x445c (17502) 0x445c (17502) 0x4464 (17508) 0x4463 (17603) 0x4467 (1763) 0x4467 (1763) 0x4467 (1763) 0x4467 (1763) 0x44550 (17744) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4557 (17815) 0x4697 (17815)	PTTL bb 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 67 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping	id=0x0012, seq=1/256, tt1=64 id=0x0012, seq=1/256, tt1=64 id=0x0012, seq=2/512, tt1=64 id=0x0012, seq=2/512, tt1=64 id=0x0012, seq=3/768, tt1=64 id=0x0012, seq=4/1024, tt1=64 id=0x0012, seq=4/1024, tt1=64 id=0x0012, seq=4/1024, tt1=64 id=0x0012, seq=4/1026, tt1=64
No. Time 1 2022 - 08 - 01 10:03:22.23123959 2 2022 - 08 - 01 10:03:22.231239747 3 7022 - 08 - 01 10:03:22.231239747 3 7022 - 08 - 01 10:03:22.231239747 5 7022 - 08 - 01 10:03:22.23224775 5 7022 - 08 - 01 10:03:23.23224775 6 7022 - 08 - 01 10:03:23.23224775 7 7022 - 08 - 01 10:03:25.256672449 8 7022 - 08 - 01 10:03:26.282666183 11 7022 - 08 - 01 10:03:27.306671644 12 7022 - 08 - 01 10:03:27.366747378 13 7022 - 08 - 01 10:03:27.36671654 14 7022 - 08 - 01 10:03:27.354936706 17 7022 - 08 - 01 10:03:29.354935704 18 7022 - 08 - 01 10:03:29.354935704 18 7022 - 08 - 01 10:03:27.36757247 18 7022 - 08 - 01 10:03:27.354936705 18 7022 - 08 - 01 10:03:27.354936706 17 7022 - 08 - 01 10:03:27.345937241 18 7022 - 08 - 01 10:03:27.345937241 18 7022 - 08 - 01 10:03:27.34593704 18 7022 - 08 - 01 10:03:27.34593704 <t< td=""><td>Source 198, 51, 100, 100 198, 51, 100, 100</td><td>Destination 192. 0. 2. 100 192. 0. 2. 100</td><td>Ривски ТСНР</td><td>Length 108 1 108 1 1</td><td>PD 0x42f8 (17144) 0x43f8 (17144) 0x4305 (17331) 0x4352 (17502) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4677 (17639) 0x4555 (17744) 0x4555 (17744) 0x4555 (17747) 0x4557 (17815) 0x4672 (18042)</td><td>PTIL Mo 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 68 Echo (ping) reply 69 Echo (ping) reply 60 Echo (ping) repl</td><td>id-0x0012, seq=1/256, ttl=64 id-0x0012, seq=2/512, ttl=64 id-0x0012, seq=2/512, ttl=64 id-0x0012, seq=2/512, ttl=64 id-0x0012, seq=3/766, ttl=64 id-0x0012, seq=3/1024, ttl=64 id-0x0012, seq=3/1024, ttl=64 id-0x0012, seq=3/1026, ttl=64 id-0x0012, seq=3/2086, ttl=64</td></t<>	Source 198, 51, 100, 100 198, 51, 100, 100	Destination 192. 0. 2. 100 192. 0. 2. 100	Ривски ТСНР	Length 108 1 108 1 1	PD 0x42f8 (17144) 0x43f8 (17144) 0x4305 (17331) 0x4352 (17502) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4677 (17639) 0x4555 (17744) 0x4555 (17744) 0x4555 (17747) 0x4557 (17815) 0x4672 (18042)	PTIL Mo 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 68 Echo (ping) reply 69 Echo (ping) reply 60 Echo (ping) repl	id-0x0012, seq=1/256, ttl=64 id-0x0012, seq=2/512, ttl=64 id-0x0012, seq=2/512, ttl=64 id-0x0012, seq=2/512, ttl=64 id-0x0012, seq=3/766, ttl=64 id-0x0012, seq=3/1024, ttl=64 id-0x0012, seq=3/1024, ttl=64 id-0x0012, seq=3/1026, ttl=64 id-0x0012, seq=3/2086, ttl=64
No. Time 1 2022 - 08 - 01 10:03:22,231237959 2 2022 - 08 - 01 10:03:22,231239747 3 2022 - 08 - 01 10:03:22,231239747 3 2022 - 08 - 01 10:03:23,23224775 4 2022 - 08 - 01 10:03:23,23224775 5 2022 - 08 - 01 10:03:23,23224775 7 2022 - 08 - 01 10:03:25,258672440 8 2022 - 08 - 01 10:03:25,258672440 9 2022 - 08 - 01 10:03:25,258672440 9 2022 - 08 - 01 10:03:25,258672440 9 2022 - 08 - 01 10:03:25,258672440 9 2022 - 08 - 01 10:03:25,258672440 10 2022 - 08 - 01 10:03:25,258672440 10 2022 - 08 - 01 10:03:27,306671631 12 2022 - 08 - 01 10:03:27,306674571 13 202 - 08 - 01 10:03:28,330667153 14 2022 - 08 - 01 10:03:29,354397064 18 2022 - 08 - 01 10:03:29,354397064 18 2022 - 08 - 01 10:03:31,402772177 21 2022 - 08 - 01 10:03:31,402774775 21 2022 - 08 - 01 10:03:31,402774775 21 2022 - 08 - 01 10:03:31,402774775 <	Source 198, 51, 100, 100 198, 51, 100, 100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Ривной ТСМР	Length 108 1 108 1 1	PD 0x42F8 (17144) 0x43F8 (17144) 0x4305 (17331) 0x43b3 (17331) 0x43b5 (17502) 0x4454 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17603) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x4559 (17744) 0x4553 (17747) 0x4597 (17815) 0x4677 (18042) 0x4672 (18042)	PTTL M6 64 Echo (ping) reply 64 Echo (ping	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/766, ttl=64 id=0x0012, seq=3/766, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=3/1280, ttl=64 id=0x0012, seq=3/1280, ttl=64 id=0x0012, seq=3/1280, ttl=64 id=0x0012, seq=3/1280, ttl=64 id=0x0012, seq=3/2048, tttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012,
No. Time 1 2022-08-01 10:03:22.23123759 2 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.231239747 5 2022-08-01 10:03:22.231239747 6 2022-08-01 10:03:22.2324275 5 2022-08-01 10:03:23.2322475 6 2022-08-01 10:03:25.258672469 8 2022-08-01 10:03:25.258672461 9 2022-08-01 10:03:25.258674661 10 2022-08-01 10:03:27.306671694 12 2022-08-01 10:03:27.30667153 13 2022-08-01 10:03:27.30667153 14 2022-08-01 10:03:27.30667153 15 2022-08-01 10:03:27.30667153 16 2022-08-01 10:03:27.30667153 16 2022-08-01 10:03:27.3067154378 16 2022-08-01 10:03:03.787952076 17 2022-08-01 10:03:03.787952076 18 2022-08-01 10:03:31.402774771 20 202-08-01 10:03:31.402774771 20 202-08-01 10:03:31.2.42669554 20 202-08-01 10:03:31.2.426693542 20	Source 198, 51, 100, 100 198, 51, 100, 100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Ривнові ІСНР І	Length 108 108 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x43f8 (1731) 0x43s0 (1731) 0x43s1 (1731) 0x4454 (1762) 0x4454 (1763) 0x4464 (17508) 0x4464 (1763) 0x4464 (1763) 0x4464 (1763) 0x4464 (1763) 0x4467 (1763) 0x4455 (1774) 0x4553 (1774) 0x4553 (1774) 0x4554 (1774) 0x4557 (18042) 0x4677 (18042) 0x4673 (18042)	PTTL 26 64 Echo (ping) reply 64 Echo (ping	id-0x0012, seq=1/256, ttl=64 id-0x0012, seq=1/256, ttl=64 id-0x0012, seq=2/512, ttl=64 id-0x0012, seq=2/512, ttl=64 id-0x0012, seq=2/162, ttl=64 id-0x0012, seq=4/1024, ttl=64 id-0x0012, seq=4/1024, ttl=64 id-0x0012, seq=5/1280, ttl=64 id-0x0012, seq=5/1280, ttl=64 id-0x0012, seq=5/1280, ttl=64 id-0x0012, seq=3/1280, ttl=64 id-0x0012, seq=3/1281, ttl=64 id-0x0012, seq=1/12816, ttl=64
 No. Tme 1 2022 - 08 - 01 10:03:22,231239747 3 2022 - 08 - 01 10:03:22,23224753 5 2022 - 08 - 01 10:03:22,23224753 5 2022 - 08 - 01 10:03:23,23224753 6 2022 - 08 - 01 10:03:25,258672449 8 2022 - 08 - 01 10:03:26,232666183 11:022 - 08 - 01 10:03:27,36671644 12:022 - 08 - 01 10:03:27,36671644 12:022 - 08 - 01 10:03:27,36671644 12:022 - 08 - 01 10:03:27,36671645 13:022 - 08 - 01 10:03:29,354936706 17:022 - 08 - 01 10:03:29,354936706 17:022 - 08 - 01 10:03:27,354936705 14:8:022 - 08 - 01 10:03:29,354935704 18:022 - 08 - 01 10:03:12,42669354 12:022 - 08 - 01 10:03:12,42669354 22:022 - 08 - 01 10:03:12,426695691 	Source 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100	Destination 192. 0. 2. 100 192. 0. 2. 100	Ризвозі 1СНР	Longth 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x43f8 (17144) 0x43b3 (17331) 0x43b3 (17331) 0x445e (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4667 (17639) 0x467 (17639) 0x467 (17639) 0x4550 (17744) 0x4550 (17744) 0x4550 (17744) 0x4550 (17747) 0x4597 (17815) 0x4674 (18042) 0x468a (18058) 0x468a (18058)	PTIL Mo 64 Echo (ping) reply 64 Echo (ping) reply	id-ex0012, seq=1/256, ttl=64 id-ex0012, seq=2/512, ttl=64 id-ex0012, seq=2/512, ttl=64 id-ex0012, seq=2/766, ttl=64 id-ex0012, seq=3/766, ttl=64 id-ex0012, seq=3/1024, ttl=64 id-ex0012, seq=3/1024, ttl=64 id-ex0012, seq=3/1026, ttl=64 id-ex0012, seq=11/2816, ttl=64 id-ex0012, seq=11/2816, ttl=64
 Tme 1 2022-08-01 10:03:22,23123/059 2 0322-08-01 10:03:22,23123/047 3 2022-08-01 10:03:23,232247/65 4 2022-08-01 10:03:23,232247/65 5 2022-08-01 10:03:23,232247/55 5 2022-08-01 10:03:23,232247/55 5 2022-08-01 10:03:24,234706571 7 2022-08-01 10:03:25,258672449 8 2022-08-01 10:03:25,258674661 9 2022-08-01 10:03:27,306671694 12 2022-08-01 10:03:27,306671694 12 2022-08-01 10:03:28,3306647153 15 2022-08-01 10:03:28,33066467153 15 2022-08-01 10:03:28,33066467153 16 2022-08-01 10:03:28,33066467153 16 2022-08-01 10:03:28,33066467153 16 2022-08-01 10:03:28,33066467153 16 2022-08-01 10:03:28,33067154 17 2022-08-01 10:03:28,33067154 17 2022-08-01 10:03:28,33067154 12 2 2022-08-01 10:03:28,33067154 12 2 2022-08-01 10:03:28,33067154 12 2 2022-08-01 10:03:32,426695691 22 2022-08-01 10:03:32,426695691 22 2022-08-01 10:03:32,426695691 22 7022-08-01 10:03:32,426695691 20 202-08-01 10:03:32,42669	Source 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100	Destination 192.0.2.100	Protection ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	100 108 108 108 108 108 108 108 108 108 108	PD (9x4758 (17144) (9x4278 (17134) (9x4305 (17531) (9x4356 (17502) (9x4454 (17502) (9x4454 (17502) (9x4464 (17508) (9x4464 (17508) (9x4467 (1763)) (9x4467 (1763)) (9x4467 (1763)) (9x4556 (17744) (9x4555 (17744) (9x4557 (17745) (9x4557 (17815) (9x4677 (18042) (9x468a (18058) (9x468a (18058) (9x468a (18058)	PTIL M0 64 Echo (ping) reply 64 Echo (ping) reply	id-ox0012, seq=1/256, ttl=64 id-ox0012, seq=2/512, ttl=64 id-ox0012, seq=2/512, ttl=64 id-ox0012, seq=3/768, ttl=64 id-ox0012, seq=3/768, ttl=64 id-ox0012, seq=3/768, ttl=64 id-ox0012, seq=3/128, ttl=64 id-ox0012, seq=3/1286, ttl=64 id-ox0012, seq=11/2816, ttl=64
No. Time 1 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.2224750 4 2022-08-01 10:03:23.23224775 5 2022-08-01 10:03:23.23224775 6 2022-08-01 10:03:25.25867460 8 2022-08-01 10:03:25.25867461 9 2022-08-01 10:03:25.25867461 10 2022-08-01 10:03:27.30667164 11 2022-08-01 10:03:27.30667164 13 2022-08-01 10:03:28.3306667153 13 2022-08-01 10:03:28.330667153 14 2022-08-01 10:03:28.330667153 15 2022-08-01 10:03:28.33067153 16 2022-08-01 10:03:28.33067153 18 2022-08-01 10:03:28.330672153 19 2022-08-01 10:03:28.330672153 19 2022-08-01 10:03:28.330672153 10 20:28-08-01 10:03:28.330672153 10 20:29.08-01 10:03:28.3487981722 20 202-08-01 10:03:28.348798172 2	Source 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100	Destination 192.0.2.100	Protection ICMP	108 108 108 108 108 108 108 108	PD 0x4278 (17144) 0x4305 (17331) 0x4354 (177331) 0x43545 (177331) 0x44545 (17502) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x4677 (17639) 0x4555 (17747) 0x4597 (17815) 0x4573 (17047) 0x4597 (17815) 0x4674 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTIL 26 64 Echo (ping) reply 64 Echo (ping) reply	id-0x0012, seq=1/256, ttl=64 id-0x0012, seq=2/512, ttl=64 id-0x0012, seq=2/512, ttl=64 id-0x0012, seq=2/512, ttl=64 id-0x0012, seq=4/1024, ttl=64 id-0x0012, seq=4/10246, ttd
No. Time 1 2022-08-01 10:03:22.23123/059 2 3022-08-01 10:03:22.23123/4769 4 2022-08-01 10:03:23.232247753 5 3022-08-01 10:03:23.232247753 5 3022-08-01 10:03:23.232247753 6 2022-08-01 10:03:25.258672449 8 2022-08-01 10:03:25.258672449 9 2022-08-01 10:03:25.258672449 10 2022-08-01 10:03:27.306671694 12 2022-08-01 10:03:27.306671694 12 2022-08-01 10:03:27.30667153 13 2022-08-01 10:03:28.3306646775 14 2022-08-01 10:03:28.3306646715 15 2022-08-01 10:03:21.33267150 16 2022-08-01 10:03:21.42.34709512 19 2022-08-01 10:03:12.0.378759241 19 2022-08-01 10:03:11.402724775 21 2022-08-01 10:03:12.4266935691 22 2022-08-01 10:03:12.426695691 22 2022-08-01 10:03:32.426695691 22 7022-08-01 10:03:32.426695691	Source 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100	Destination 192.0.2.100	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 108 108 108 108 108 108 108	PD (9x4278 (17144) (9x4278 (17144) (9x4305 (17331) (9x4452 (17502) (9x4454 (17502) (9x4454 (17502) (9x4464 (17508) (9x4464 (17508) (9x4464 (17508) (9x4464 (17508) (9x4464 (17603) (9x4467 (1763)) (9x4675 (17742) (9x4553 (17744) (9x4553 (17747) (9x4557 (17042) (9x4573 (18042) (9x4673 (18042) (9x4688 (18058) (9x4688 (18058)) (9x4688 (18058)) (9x4688 (18058)) (9x4688 (18058	PTIL M0 64 Echo (ping) reply 64 Echo (ping) reply	id-0x0012, seq=1/256, ttl=64 id-0x0012, seq=1/256, ttl=64 id-0x0012, seq=1/512, ttl=64 id-0x0012, seq=1/512, ttl=64 id-0x0012, seq=1/66, ttl=64 id-0x0012, seq=1/66, ttl=64 id-0x0012, seq=1/66, ttl=64 id-0x0012, seq=1/66, ttl=64 id-0x0012, seq=1/166, ttl=64 id-0x0012, seq=1/166, ttl=64 id-0x0012, seq=1/128, ttl=64 id-0x0012, seq=1/12816, ttl=64 id-0x0012, seq=11/2816, ttl=64
No. Time 1 2022-08-01 10:03:22.23123959 2 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.231239747 5 2022-08-01 10:03:22.23224753 5 2022-08-01 10:03:23.23224753 6 2022-08-01 10:03:25.258672449 8 2022-08-01 10:03:25.258672449 9 2022-08-01 10:03:25.258674661 10 2022-08-01 10:03:27.30667159 13 2022-08-01 10:03:27.30667153 13 2022-08-01 10:03:27.30667153 15 2022-08-01 10:03:27.30667153 16 2022-08-01 10:03:27.30667153 16 2022-08-01 10:03:27.30667153 16 2022-08-01 10:03:27.3067154 16 2022-08-01 10:03:27.3067153 16 2022-08-01 10:03:27.3067153 17 2022-08-01 10:03:27.3067154 18 2022-08-01 10:03:27.22669324 22 2022-08-01 10:03:27.24669354 22 2022-08-01 10:03:27.2426095591 4 frame 11:0:03:32.426695591 5 frame 2: 108	Source 198.51,100,100 198.51	Destination 192.0.2.100 192.0	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	100 108 108 108 108 108 108 108	PD 0x42F8 (17144) 0x435 (1731) 0x435 (1731) 0x435 (1731) 0x435 (1752) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x467 (17744) 0x4559 (17744) 0x4559 (17744) 0x4559 (17744) 0x4559 (17745) 0x4597 (17815) 0x4677 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTIL 26 64 Echo (ping) reply 64 Echo (ping) reply	id-bx0012, seq=1/256, ttl=64 id-bx0012, seq=1/256, ttl=64 id-bx0012, seq=1/256, ttl=64 id-bx0012, seq=2/512, ttl=64 id-bx0012, seq=2/5126, ttl=64 id-bx0012, seq=2/128, ttl=64 id-bx0012, seq=11/2816, ttl=64
No. Time 1 3022-08-01 10:03:22.23123959 2 2022-08-01 10:03:22.231239747 3 7022-08-01 10:03:22.231239747 3 7022-08-01 10:03:22.231239747 5 7022-08-01 10:03:23.232247753 5 7022-08-01 10:03:23.232247753 6 7022-08-01 10:03:25.258672449 8 7022-08-01 10:03:25.258674861 9 7022-08-01 10:03:27.36667164 10 7022-08-01 10:03:27.36667164 11 7022-08-01 10:03:27.36667164 12 7022-08-01 10:03:27.36667165 13 7022-08-01 10:03:29.354936706 14 7022-08-01 10:03:29.354935704 18 7022-08-01 10:03:29.3549357241 18 7022-08-01 10:03:12.426693254 19 7022-08-01 10:03:11.402772717 20 702-08-01 10:03:12.426693254 22 2022-08-01 10:03:12.42669354 22 2022-08-01 10:03:12.426695691	Source 198.51.100.100	Destination 192.0.2.100 192.0	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 108 108 108 108 108 108 108	PD 0x4278 (17144) 0x4305 (17331) 0x4352 (17532) 0x4352 (17502) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4677 (17639) 0x4677 (17639) 0x4677 (17639) 0x4550 (17744) 0x4550 (17744) 0x4550 (17747) 0x4597 (17815) 0x4677 (18042) 0x4688 (18058) 0x4688 (18058) 0x4688 (18058) 0x4688 (18058)	PTIL Mo 64 Echo (ping) reply 64 Echo (p	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/266, ttl=64 id=0x0012, seq=1/126, ttl=64 id=0x0012, seq=1/126, ttl=64 id=0x0012, seq=1/128, ttl=64 id=0x0012, seq=1/12816, ttl=64
 Tme 1 2022-08-01 10:03:22.23123059 2 0322-08-01 10:03:22.231230747 3 022-08-01 10:03:22.231230747 3 022-08-01 10:03:22.2224750 4 022-08-01 10:03:23.2224750 5 022-08-01 10:03:23.2224751 5 022-08-01 10:03:23.2224751 7 022-08-01 10:03:25.25872449 8 022-08-01 10:03:25.258672449 8 022-08-01 10:03:25.258672461 9 022-08-01 10:03:25.258674661 9 022-08-01 10:03:27.306671694 12 022-08-01 10:03:27.306671694 12 022-08-01 10:03:27.30667153 15 022-08-01 10:03:29.354395331 16 022-08-01 10:03:29.354395331 16 022-08-01 10:03:10.3787930476 17 022-08-01 10:03:10.3787930476 18 022-08-01 10:03:11.40277217 18 022-08-01 10:03:11.402774775 21 022-08-01 10:03:22.42669354 22 022-08-01 10:03:22.426695691 Frame 2: 108 bytes on wire (864 bit (Hernet II, src: Cisco b9:77:08 (5) WH-Tag 0	Source 198.51.100.100 198.51.100.000 198.51.000 198.50 198.50 198.50 198.50 198.50 19	Destination 192.0.2.100 192.0	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	100 108 108 108	PD 0x42f8 (17144) 0x43f8 (17144) 0x4305 (17331) 0x4452 (17502) 0x4454 (17503) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17503) 0x4467 (17503) 0x4467 (17639) 0x4467 (17639) 0x4555 (17744) 0x4555 (17744) 0x4555 (17747) 0x4557 (17042) 0x4568 (18058) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTR 26 64 Echo (ping) reply 64 Echo (ping) reply	00 00 50 56 50 88 57 56 77 68 26 00 97 97 88 26 97 97 88 26 97 98 26 90 90 97 98 26 90 90 97 98 26 90 90 97 98 26 90 97 97 98 26 90 97 97 98 26 90 97 97 98 26 90 97 <td< td=""></td<>
No. Time 1 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.23224753 4 2022-08-01 10:03:23.23224753 5 2022-08-01 10:03:23.23224753 6 2022-08-01 10:03:23.23224753 7 2022-08-01 10:03:25.258674601 8 2022-08-01 10:03:25.25867461 9 2022-08-01 10:03:25.25867461 9 2022-08-01 10:03:27.30667164 10 2022-08-01 10:03:27.30667164 11 2022-08-01 10:03:27.30667164 12 2022-08-01 10:03:28.3306667153 13 2022-08-01 10:03:20.378798172 14 2022-08-01 10:03:20.378798172 19 2022-08-01 10:03:20.378798172 19 2022-08-01 10:03:20.378798172 19 2022-08-01 10:03:20.378798172 20 202-08-01 10:03:20.378798172 20 202-08-01 10:03:20.378798172 20 202-08-01 10:03:20.378798172 20 202-08-01 10:03:20.378798172 20 202	Source 198.51,100,100 198.51	Destination 192.0.2.100 192.0	Protection ICMP	108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x43f8 (17144) 0x4305 (17331) 0x4352 (17502) 0x4352 (17502) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x4677 (17639) 0x46753 (17744) 0x4555 (17744) 0x4555 (17747) 0x4597 (17815) 0x4677 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTH M6 64 Echo (ping) reply 64 Echo (ping) reply	id-0x0012, seq=1/256, ttl=64 id-0x0012, seq=2/512, seq=3/766, ttl=64 id-0x0012, seq=2/512, seq=3/766, ttl=64 id-0x0012, seq=3/102, ttl=64 id-0x0012, seq=11/2816, ttl=64 id-0x0012, seq=1
No. Time 1 2022-08-01 10:03:22.23123/059 2 3022-08-01 10:03:22.23123/4769 4 2022-08-01 10:03:23.232247753 5 3022-08-01 10:03:23.232247753 5 3022-08-01 10:03:23.232247753 6 2022-08-01 10:03:23.232247753 7 3022-08-01 10:03:25.258572449 8 2022-08-01 10:03:25.258572449 9 2022-08-01 10:03:27.305672164 12 2022-08-01 10:03:27.305672164 12 2022-08-01 10:03:27.305672164 12 2022-08-01 10:03:28.33066477 14 2022-08-01 10:03:28.33066457153 15 2022-08-01 10:03:28.33066457153 16 2022-08-01 10:03:21.30.378795244 17 2022-08-01 10:03:21.40272217 20 202-08-01 10:03:12.426693561 17 202-08-01 10:03:21.40277217 21 2022-08-01 10:03:12.426695561 22 2022-08-01 10:03:32.426695561 22 2022-08-01 10:03:32.426695561 20 0000 0000 0000 0	Source Source 198.51,100,100 198.51,	Destination 192.0.2.100 192.0	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	100 108 108 108	PD (9x42F8 (17144) (9x42F8 (17144) (9x4305 (17331) (9x4452 (17502) (9x4454 (17502) (9x4454 (17508) (9x4464 (17508) (9x4464 (17508) (9x4464 (17508) (9x4464 (17508) (9x4464 (17508) (9x4467 (1763)) (9x4675 (17742) (9x4553 (17742) (9x4553 (17742) (9x4553 (17742) (9x4553 (17742) (9x4574 (18042) (9x468a (18058) (9x468a (19x68)) (9x468a (19x68)) (9x468a (19x68)) (9x468a (19x68	PTIL M0 64 Echo (ping) reply 64 Echo (ping) reply	id-exx0012, seq=1/256, ttl=64 id-exx0012, seq=2/512, ttl=64 id-exx0012, seq=2/512, ttl=64 id-exx0012, seq=3/766, ttl=64 id-exx0012, seq=3/786, ttl=64 id-exx0012, seq=3/1286, ttl=64 id-exx0012, seq=11/2816, ttl=64 id-exx0012, se
No. Time 1 2022-08-01 10:03:22.23123959 2 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.231239747 5 2022-08-01 10:03:22.231239747 5 2022-08-01 10:03:22.23224775 5 2022-08-01 10:03:23.23224775 7 2022-08-01 10:03:25.258672449 8 2022-08-01 10:03:25.258672461 9 2022-08-01 10:03:27.306671694 12 2022-08-01 10:03:27.306671694 13 2022-08-01 10:03:27.30667153 13 2022-08-01 10:03:27.30667153 14 2022-08-01 10:03:27.30667153 15 2022-08-01 10:03:27.30671694 17 2022-08-01 10:03:27.3067153 16 2022-08-01 10:03:27.3067153 16 2022-08-01 10:03:27.3067153 16 2022-08-01 10:03:27.3067154378 17 2022-08-01 10:03:31.402774775 20 2022-08-01 10:03:31.402774775 20 2022-08-01 10:03:31.42669354 22 2022-08-01 10:03:32.426695691 9	Source 198.51.100.100 198.51	Destination 192.0.2.100 192.0	Protection ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x43f8 (17144) 0x43b3 (17331) 0x43b3 (17331) 0x4454 (17503) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x4677 (17639) 0x4559 (17744) 0x4559 (17744) 0x4559 (17744) 0x4559 (17745) 0x4597 (17815) 0x4677 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTTL 26 64 Echo (ping) reply 64 Echo (ping) reply	id-0x0012, seq-1/256, ttl-64 id-0x0012, seq-1/266, ttl-64 id-0x0012, seq-1/286, ttl-64 id-0x0012, seq-1/2816, ttl-64 <t< td=""></t<>
No. Time 1 3022-08-01 10:03:22.23123959 2 2022-08-01 10:03:22.231239747 3 X022-08-01 10:03:22.231239747 3 X022-08-01 10:03:22.231239747 5 X022-08-01 10:03:22.2224750 4 X022-08-01 10:03:23.23224775 5 X022-08-01 10:03:23.23224775 6 X022-08-01 10:03:25.25867460 8 X022-08-01 10:03:25.25867461 9 X022-08-01 10:03:25.25867461 10 X022-08-01 10:03:27.30667164 11 X022-08-01 10:03:27.30667164 12 X022-08-01 10:03:27.30667164 13 X022-08-01 10:03:28.3306467153 14 X022-08-01 10:03:29.354936706 17 X022-08-01 10:03:20.3787952241 18 X022-08-01 10:03:11.402727217 20 X022-08-01 10:03:11.402727217 20 X022-08-01 10:03:12.42669354 22 2022-08-01 10:03:32.426695691 2 10:03:32.426695691 3 10:03:32.426695691 4 10:03:32.426695691 5 5	Source 198.51.100.100 198.51	Destination 192.0.2.100 192.0	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x43f8 (17144) 0x4305 (17331) 0x4352 (17502) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4677 (17639) 0x4677 (17639) 0x4677 (17741) 0x4555 (17744) 0x4555 (17744) 0x4556 (17744) 0x4556 (17744) 0x4557 (17747) 0x4597 (17815) 0x4674 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTIL M0 64 Echo (ping) reply 64 Echo (ping) reply	id-exc0012, seq=1/256, ttl=64 id-exc0012, seq=2/512, ttl=64 id-exc0012, seq=2/1241, ttl=64 id-exc0012, seq=2/12416, ttl=64 id-exc0012, seq=2/1266, ttl=64 id-exc0012, seq=11/2816, ttl=64 id-exc0012, seq=10/566, ttl=64 id-exc00
<pre>No. Tme 1 2022-08-01 10:03:22.23123059 2 2022-08-01 10:03:22.231230747 3 2022-08-01 10:03:22.231230747 4 2022-08-01 10:03:22.2324769 4 2022-08-01 10:03:22.2324769 5 2022-08-01 10:03:22.2324769 7 2022-08-01 10:03:25.258674661 9 2022-08-01 10:03:25.258674661 12 2022-08-01 10:03:25.258674661 12 2022-08-01 10:03:25.258674661 13 2022-08-01 10:03:27.306671694 12 2022-08-01 10:03:27.306671694 12 2022-08-01 10:03:27.306671694 13 2022-08-01 10:03:27.306671594 13 2022-08-01 10:03:27.306671594 14 2022-08-01 10:03:27.306671594 15 2022-08-01 10:03:27.306671594 16 2022-08-01 10:03:27.306671594 17 2022-08-01 10:03:20.3583906715 16 2022-08-01 10:03:20.378059207 16 2022-08-01 10:03:21.420693594 22 2022-08-01 10:03:21.420693594 22 2022-08-01 10:03:21.420693594 22 2022-08-01 10:03:21.420693594 22 2022-08-01 10:03:21.420693594 22 2022-08-01 10:03:21.420693594 22 2022-08-01 10:03:21.420693594 22 2022-08-01 10:03:21.420693594 22 2022-08-01 10:03:21.420693594 22 2022-08-01 10:03:21.420693594 22 2022-08-01 10:03:21.420693594 22 2022-08-01 10:03:21.420693594 22 2022-08-01 10:03:21.420693594 22 2022-08-01 10:03:21.420693594 22 2022-08-01 10:03:21.420693594 22 2022-08-01 10:03:21.420693594 22 2022-08-01 10:03:21.420693594 22 2022-08-01 10:03:21.420693594 22 2022-08-01 10:03:21.420693594 22 2022-08-01 10:03:21.420693594 23 2022-08-01 10:03:21.420693594 24 2022-08-01 10:03:21.420693594 25 2022-09.01 10:03:21.420693594 25 2022-09.01 10:03:21.420693594 25 2022-09.01 10:03:21.420693594 25 2022-09.01 10:03:21.420693594 25 2022-09.01 10:03:21.420693594 25 2022-09.01 10:03:21.420693594 25 2022-09.01 10:03:21.420693594 25 2022-09.01 10:03:21.420693594 25 2022-09.01 10:03:21.420693594 25 2022-09.01 10:03:21.420693594 25 2022-09.01 10:03:21.420693594 25 2022-09.01 10:03:21.420693594 25 2022-09.01 10:03:21.02024 25 2022-09.01 10:03:21.420693594 25 2002400000000000000000000000000000000</pre>	Source 198.51.100.100 198.50	Destination 192.0.2.100 192.0	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	100 108 108 108	PD 0x42f8 (17144) 0x43f8 (17144) 0x4305 (17331) 0x4452 (17502) 0x4454 (17503) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x4550 (17744) 0x4555 (17744) 0x4555 (17747) 0x4557 (17815) 0x4577 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTTL 26 64 Echo (ping) reply 64 Echo (ping) reply	<pre> id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/1024, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x0012, seq=10, seq=0, seq=0, seq=0, seq=0, seq=0, seq=0, seq=0, seq=0, seq=0</pre>
No. Time 1 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.23224753 4 2022-08-01 10:03:23.23224753 5 2022-08-01 10:03:23.23224753 6 2022-08-01 10:03:25.258672449 8 2022-08-01 10:03:25.258674661 9 2022-08-01 10:03:25.25867461 9 2022-08-01 10:03:25.25867461 10 2022-08-01 10:03:25.25867461 11 2022-08-01 10:03:27.30667104 12 2022-08-01 10:03:26.282663169 13 2022-08-01 10:03:28.3306667153 13 2022-08-01 10:03:20.378798172 14 2022-08-01 10:03:20.378798172 19 2022-08-01 10:03:20.378798172 19 2022-08-01 10:03:20.378798172 19 2022-08-01 10:03:20.378798172 20 202-08-01 10:03:20.378798172 20 202-08-01 10:03:20.378798172 20 202-08-01 10:03:20.378798172 20 202-08-01 10:03:20.2466095691 20	Source 198.51,100,100 198.51	Destination 192.0.2.100 192.0	Protection ICMP	108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x4305 (17331) 0x4352 (17502) 0x4352 (17502) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x4677 (17639) 0x4677 (17749) 0x4555 (17744) 0x4555 (17747) 0x4557 (17741) 0x4557 (17745) 0x4677 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTH 26 64 Echo (ping) reply 64 Echo (ping) reply	id-excell2, seq=1/256, ttl=64 id-excell2, seq=2/512, ttl=64 id-excell2, seq=2/512, ttl=64 id-excell2, seq=2/512, ttl=64 id-excell2, seq=2/162, ttl=64 id-excell2, seq=2/164, ttl=64 id-excell2, seq=2/164, ttl=64 id-excell2, seq=2/166, ttl=64 id-excell2, seq=11/2816, ttl=64 id-excell2,
<pre>No. Tme 1 2022-08-01 10:01:22.21123/059 2 2022-08-01 10:01:22.21123/059 2 2022-08-01 10:01:22.21223/17 3 2022-08-01 10:01:23.232247/69 4 2022-08-01 10:01:23.232247/69 5 2022-08-01 10:01:23.232247/69 7 2022-08-01 10:01:25.258674861 9 2022-08-01 10:01:25.258674861 12 2022-08-01 10:01:25.258674861 12 2022-08-01 10:01:25.258674861 13 2022-08-01 10:01:25.258674861 13 2022-08-01 10:01:27.30667159 14 2022-08-01 10:01:27.30667159 15 2022-08-01 10:01:27.30667159 16 2022-08-01 10:01:28.33066467715 15 2022-08-01 10:01:28.3306646715 15 2022-08-01 10:01:28.3306646715 17 2022-08-01 10:01:28.3306646715 17 2022-08-01 10:01:28.3306646715 17 2022-08-01 10:01:28.3306646715 17 2022-08-01 10:01:28.3306646715 17 2022-08-01 10:01:28.3306646715 17 2022-08-01 10:01:28.3306646715 12 2022-08-01 10:01:28.3306646715 12 2022-08-01 10:01:28.3306646715 12 2022-08-01 10:01:28.3306646715 12 2022-08-01 10:01:28.3306646715 12 2022-08-01 10:01:28.3306646715 12 2022-08-01 10:01:28.3306646715 12 2022-08-01 10:01:28.3306646715 12 2022-08-01 10:01:28.3306646715 12 2022-08-01 10:01:28.3306646715 12 2022-08-01 10:01:28.3306646715 12 2022-08-01 10:01:28.3306646715 14 202-08-01 10:01:28.3306646715 15 202-08-01 10:01:28.3306646715 12 2022-08-01 10:01:28.3306646715 14 202-08-01 10:01:28.3306646715 12 2022-08-01 10:01:28.3306646715 14 202-08-01 10:01:28.3306646715 14 2022-08-01 10:01:28.3306646715 14 2022-08-01 10:01:28.3306646715 14 2022-08-01 10:01:28.3306646715 14 2022-08-01 10:01:28.32.4266935691 2 Frame 2: 108 bytes on wire (864 bit 5 thernet II, 5rc: Cisco b9:77:08 (5 10</pre>	Source Source 198.51.100.100 198.51.	Destination 192.0.2.100 192.0	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	100 108 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x43f8 (17144) 0x4305 (17331) 0x4452 (17502) 0x4454 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x4467 (17749) 0x4550 (17744) 0x4553 (17747) 0x4557 (17741) 0x4597 (17815) 0x4673 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTR 26 64 Echo (ping) reply 64 Echo (ping) reply	<pre>id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012,</pre>
No. Time 1 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.23224753 5 2022-08-01 10:03:22.32224753 5 2022-08-01 10:03:23.23224753 6 2022-08-01 10:03:25.258672449 8 2022-08-01 10:03:25.258672449 9 2022-08-01 10:03:25.258672449 9 2022-08-01 10:03:25.258674861 10 2022-08-01 10:03:27.306671504 12 2022-08-01 10:03:27.3066745743 13 2022-08-01 10:03:27.30667153 13 2022-08-01 10:03:27.30667153 15 2022-08-01 10:03:20.35439630706 17 2022-08-01 10:03:20.378798072 19 2022-08-01 10:03:20.378798172 19 2022-08-01 10:03:20.378798172 19 2022-08-01 10:03:21.402774775 21 2022-08-01 10:03:30.378798172 19 2022-08-01 10:03:31.402774775 21 2022-08-01 10:03:32.42669354 22 2022-08-01 10:03:32.426695591 • Frame 2: 108 bytes on wire (@64 bit • Tithermet 11, Src: Cisco b9:77:06 (Se4 bit • Thermet 11, Src: 0, 50:07:06 (Se3) • 0. 0. • 0.0 0. • 0.0 0.	Source 198.51.100.100 198.51	Destination 192.0.2.100 192.0	Protection ICMP	108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x43f8 (17144) 0x43b3 (17331) 0x4454 (17502) 0x4454 (17502) 0x4454 (17503) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x4677 (17639) 0x4556 (17744) 0x4559 (17744) 0x4557 (17747) 0x4597 (17815) 0x4678 (18042) 0x4668 (18058) 0x4668 (18058) 0x4668 (18058)	PTH 26 64 Echo (ping) reply 64 Echo (ping) reply	<pre>id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/1024, ttl=64 id=0x0012, seq=2/10246, ttl=64 id=0x0012, seq=2/</pre>
<pre>No. Time 1 2022-08-01 10:03:22.23123/059 2 2032-08-01 10:03:22.23123/059 2 2032-08-01 10:03:23.232247/69 4 2022-08-01 10:03:23.232247/69 4 2022-08-01 10:03:23.232247/59 5 2022-08-01 10:03:23.232247/59 7 2022-08-01 10:03:25.2585/2246 9 2022-08-01 10:03:25.2585/2246 12 2032-08-01 10:03:25.2585/2246 13 2022-08-01 10:03:25.2585/2461 13 2022-08-01 10:03:27.3065/2154 13 2022-08-01 10:03:27.3065/2154 13 2022-08-01 10:03:28.330664677 14 2022-08-01 10:03:28.320695691 2 2022-08-01 10:03:28.426695691 2 2022-08-01 10:03:28.426695691 2 002-000 000 000 000 000 000 000 000 000 000</pre>	Source 198.51.100.100 198.50	Destination 192.0.2.100 192.0	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	100 108 108 108	PD 0x4278 (17144) 0x4305 (17331) 0x4352 (17502) 0x4352 (17502) 0x4454 (17508) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4675 (17743) 0x4555 (17744) 0x4555 (17744) 0x4555 (17744) 0x4557 (17747) 0x4597 (17815) 0x4677 (18042) 0x4688 (18058) 0x4688 (18058) 0x4688 (18058) 0x4688 (18058)	PTIL M0 64 Echo (ping) reply 64 Echo (ping) reply	<pre>id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/766, ttl=64 id=0x0012, seq=3/786, ttl=64 id=0x0012,</pre>
<pre>No. Tme 1 2022-08-01 10:03:22.23123059 2 2022-08-01 10:03:22.231230747 3 2022-08-01 10:03:22.231230747 3 2022-08-01 10:03:22.231230747 5 2022-08-01 10:03:22.23224755 5 2022-08-01 10:03:22.23224755 7 2022-08-01 10:03:25.25672449 8 2022-08-01 10:03:25.25672449 12 2022-08-01 10:03:25.25672449 13 2022-08-01 10:03:27.306671694 12 2022-08-01 10:03:27.306671694 12 2022-08-01 10:03:27.306671694 12 2022-08-01 10:03:27.30667153 16 2022-08-01 10:03:27.30667153 16 2022-08-01 10:03:27.30667153 16 2022-08-01 10:03:27.30667153 16 2022-08-01 10:03:20.3306467153 16 2022-08-01 10:03:20.378759241 12 2022-08-01 10:03:20.378759241 12 2022-08-01 10:03:21.402772775 21 2022-08-01 10:03:21.42669354 22 2022-08-01 10:03:22.426695691</pre>	Source 198.51.100.100 198.51	Destination 192.0.2.100 192.0	Protection ICMP	100 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x43f8 (17144) 0x4305 (17331) 0x4452 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x4677 (17639) 0x4677 (17744) 0x4559 (17744) 0x4559 (17744) 0x4559 (17744) 0x4559 (17745) 0x4677 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTTL 26 G4 Echo (ping) reply G4 Echo (ping	1d-0x0012, seq-1/256, ttl-64 1d-0x0012, seq-1/234, ttl-64 1d-0x0012, seq-1/236, ttl-64 1d-0x0012, seq-1/236, ttl-64 1d-0x0012, seq-1/2816, ttl-64 1d-0x00012, seq-1/2816, ttl-64 <t< td=""></t<>
No. Time 1 3022-08-01 10:03:22.231239747 3 3022-08-01 10:03:22.231239747 3 3022-08-01 10:03:22.231239747 3 3022-08-01 10:03:22.231239747 3 3022-08-01 10:03:22.23224753 5 3022-08-01 10:03:23.23224753 5 3022-08-01 10:03:23.23224753 5 3022-08-01 10:03:23.23224753 6 3022-08-01 10:03:25.258672469 8 3022-08-01 10:03:25.258674861 9 3022-08-01 10:03:25.258674861 10 3022-08-01 10:03:25.258674861 11 3022-08-01 10:03:25.258674861 13 3022-08-01 10:03:27.306671694 13 3022-08-01 10:03:28.33066467153 13 2022-08-01 10:03:28.33066467153 16 2022-08-01 10:03:20.378798172 19 2022-08-01 10:03:20.378798172 19 2022-08-01 10:03:20.378798172 20 202-08-01 10:03:20.378798172 20 202-08-01 10:03:20.378798172 20 202-08-01 10:03:20.378798172 20 202-08-01 10:03:20.378798172 20 202-08-01 10:03:20.426695691 20 202-08-01 10:03:20.426695691 9.0	Source 198.51.100.100 101.102 101.102 101.102 101.102 101.102.100.100, D	Destination 192.0.2.100 192.0	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x43f8 (17144) 0x4305 (17331) 0x4352 (17502) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x467 (17639) 0x4677 (17639) 0x4677 (17749) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4557 (17815) 0x4674 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTH M6 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/162, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x0012, seq=1/282, seq=164

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が**Egress**に設定されている場合、イー サネットヘッダーにポートVLANタグ102が含まれるパケットは、入力方向のバックプレーンイン ターフェイスでキャプチャされます。

タスクの要約を次の表に示します。

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

タスク2

FCMとCLIを使用して、バックプレーンインターフェイスと前面インターフェイスEthernet1/2の 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場所で設定されます。

- 前面インターフェイス:インターフェイスEthernet1/2上のポートVLAN 102を持つパケット 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

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

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

Overview Interfaces Logical Devices Security Engine Platform Settings		System	Tools Help admin
		Packet Capture	Troubleshooting Logs
Capture Session Fiter List			
	C Refresh	Capture Session Delet	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。[Session Name] を入力し、 [Save and Run] をクリックしてキャプチャをアクティブにします。

Overview Interfaces Logical Devices Security Engine R	latform Settings	System Tools Help a	dmin
Select an instance: ftd1		Save and Run Save Can	cel
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	
	FTD Ethernet1/9, Ethernet1/10	Application Capture Direction All Packets Egress Packet	
		Capture Filter Apply Filter Capture All	
Ethernet1/1			

FXOS CLI

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

1. アプリケーションのタイプと識別子を特定します。

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

確認

FCM

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

Overview Interface	s Logical Devices Security Engine	Platform Settings				System Tools	Help	admin
Capture Session Fit	er List							
					c	Refresh Capt	ure Session	De
a 🗻 cap1	Drop Count: 0	Operational State: up	Buffer Size: 256 MB		Snap Length: 1518 Bytes			1
Interface Name	Filter	File Size (in bytes)	File Name	Device Name				
Ethernet1/2	None	95040	cap1-ethernet-1-2-0.pcap	ftd1	4			
Ethernet1/2 - Ethernet1	/10 None	368	cap1-vethernet-1175.pcap	ftd1	⊻			
Ethernet1/2 - Ethernet1	/9 None	13040	cap1-vethernet-1036.pcap	ftd1	1			

FXOS CLI

scope packet-captureでキャプチャの詳細を確認します。

```
firepower# scope packet-capture
firepower /packet-capture # show session cap1
Traffic Monitoring Session:
   Packet Capture Session Name: cap1
   Session: 1
   Admin State: Enabled
   Oper State: Up
   Oper State Reason: Active
   Config Success: Yes
   Config Fail Reason:
   Append Flag: Overwrite
   Session Mem Usage: 256 MB
   Session Pcap Snap Len: 1518 Bytes
   Error Code: 0
   Drop Count: 0
Physical ports involved in Packet Capture:
   Slot Id: 1
   Port Id: 2
   Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap
   Pcapsize: 410444 bytes
   Filter:
   Sub Interface: 0
   Application Instance Identifier: ftd1
   Application Name: ftd
Application ports involved in Packet Capture:
  Slot Id: 1
   Link Name: link12
   Port Name: Ethernet1/2
   App Name: ftd
   Sub Interface: 0
   Application Instance Identifier: ftd1
Application ports resolved to:
  Name: vnic1
  Eq Slot Id: 1
   Eq Port Id: 9
   Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1036.pcap
   Pcapsize: 128400 bytes
   Vlan: 102
   Filter:
   Name: vnic2
   Eq Slot Id: 1
   Eq Port Id: 10
   Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1175.pcap
   Pcapsize: 2656 bytes
```

vlan: 102 Filter: キャプチャファイルの収集

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

ファイル分析のキャプチャ

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

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

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

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	0xc009 (49161)	64 Echo (ping) reque	id=0x0013, seq=1/256, ttl=64 (no response found!)
	2 2022-08-01 11:33:19.070695347	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping) reque	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 (49161)	64 ECRO (ping) reque	id=0x0013, seq=1/256, ttl=64 (no response found!)
	4 2022-08-01 11:33:19.071218458	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping) reque	id=0x0013, seq=1/256, ttl=64 (no response found!)
	5 2022-08-01 11:33:20.072036625	192.0.2.100	198.51.100.100	ICMP	108	0xc0ae (49326)	64 Echo (ping) reque	id=0x0013, seq=2/512, ttl=64 (no response found!)
	6 2022-08-01 11:33:20.072038399	192.0.2.100	198.51.100.100	ICMP	102	0xc0ae (49326)	64 Echo (ping) reque	id=0x0013, seg=2/512, ttl=64 (no response found!)
	7 2022-08-01 11:33:21.073266030	192.0.2.100	198,51,100,100	ICMP	108	0xc167 (49511)	64 Echo (ping) reque	id=0x0013, seg=3/768, ttl=64 (no response found!)
	8 2022-08-01 11:33:21.073268327	192.0.2.100	198,51,100,100	ICMP	102	8xc167 (49511)	64 Echo (ping) reque	id=0x0013, seg=3/768, ttl=64 (no response found!)
	9 2022-08-01 11:33:22.074576640	192.0.2.100	198,51,100,100	ICMP	108	0xc175 (49525)	64 Echo (ping) reque	id=0x0013, seg=4/1024, ttl=64 (no response found))
	10 2022-08-01 11:33:22.074578010	192.0.2.100	198.51.100.100	TCMP	102	Bxc175 (49525)	64 Echo (ping) reque	id=0x0013, seq=4/1024, ttl=64 (no response found))
	11 2022-08-01 11:22:22 075770090	102 0 2 100	109 51 100 100	TCMD	102	0xc209 (40672)	64 Echo (ping) reque	id=0x0013, seq=5/1390, ttl=64 (no response found1)
	12 2022-08-01 11:33.23.075701512	102.0.2.100	100 51 100 100	TCMD	100	0xc208 (49072)	64 Echo (ping) reque	id=0x0013, seq=5/1200, tt1=64 (no response found1)
	12 2022-08-01 11.33.23.073781313	102.0.2.100	100 51 100 100	TCMD	102	0xc208 (49072)	64 Echo (ping) reque	id_0x0013, seq=5/1280, tt1=64 (no response found1)
	13 2022-08-01 11:33:24.081839490	192.0.2.100	198.51.100.100	TCMP	108	0xc211 (49681)	64 Echo (ping) reque	1d=0x0013, seq=0/1530, tt1=04 (no response found)
	14 2022-08-01 11:33:24.081841386	192.0.2.100	198.51.100.100	ICMP	102	0xc211 (49681)	64 Echo (ping) reque	1d=0x0013, seq=6/1536, ttl=64 (no response found)
	15 2022-08-01 11:33:25.105806249	192.0.2.100	198.51.100.100	ICMP	108	0xc2e2 (49890)	64 Echo (ping) reque	1d=0x0013, seq=7/1792, ttl=64 (no response found!)
	16 2022-08-01 11:33:25.105807895	192.0.2.100	198.51.100.100	ICMP	102	0xc2e2 (49890)	64 Echo (ping) reque	1d=0x0013, seq=7/1792, ttl=64 (no response found!)
	17 2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	ICMP	108	0xc3b4 (50100)	64 Echo (ping) reque	<pre>id=0x0013, seq=8/2048, ttl=64 (no response found!)</pre>
	18 2022-08-01 11:33:26.129838114	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100)	64 Echo (ping) reque	id=0x0013, seq=8/2048, ttl=64 (no response found!)
	19 2022-08-01 11:33:27.153828653	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294)	64 Echo (ping) reque	id=0x0013, seq=9/2304, ttl=64 (no response found!)
	20 2022-08-01 11:33:27.153830201	192.0.2.100	198.51.100.100	ICMP	102	0xc476 (50294)	64 Echo (ping) reque	id=0x0013, seq=9/2304, ttl=64 (no response found!)
	21 2022-08-01 11:33:28.177847175	192.0.2.100	198.51.100.100	ICMP	108	0xc516 (50454)	64 Echo (ping) reque	: id=0x0013, seq=10/2560, ttl=64 (no response found!)
	22 2022-08-01 11:33:28.177849075	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (50454)	64 Echo (ping) reque	id=0x0013, seq=10/2560, ttl=64 (no response found!)
	23 2022-08-01 11:33:29.201804760	192.0.2.100	198.51.100.100	ICMP	108	0xc578 (50552)	64 Echo (ping) reque	id=0x0013, seq=11/2816, ttl=64 (no response found!)
	24 2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	102	0xc578 (50552)	64 Echo (ping) reque	id=0x0013, seq=11/2816, ttl=64 (no response found!)
	25 2022-08-01 11:33:30.225834765	192.0.2.100	198.51.100.100	ICMP	108	0xc585 (50565)	64 Echo (ping) reque	id=0x0013, seq=12/3072, ttl=64 (no response found!)
	26 2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (50565)	64 Echo (ping) reque	id=0x0013, seg=12/3072, ttl=64 (no response found!)
	27 2022-08-01 11:33:31.249828955	192.0.2.100	198.51.100.100	ICMP	108	0xc618 (50712)	64 Echo (ping) reque	id=0x0013, seg=13/3328, ttl=64 (no response found!)
	28 2022-08-01 11:33:31.249831121	192.0.2.100	198.51.100.100	ICMP	102	0xc618 (50712)	64 Echo (ping) reque	id=0x0013, seg=13/3328, ttl=64 (no response found!)
	29 2022-08-01 11:33:32.273867960	192.0.2.100	198.51.100.100	ICMP	108	0xc64f (50767)	64 Echo (ping) reque	id=0x0013, seg=14/3584, ttl=64 (no response found1)
<.							of cone (pang) reque	an one and any start of the response realisty
	forme 1, 100 butes on vice (064 bit	c) 100 butos es	stuned (BEA bits) a	n intenfere e	ntuno un	1 14 0		000 50 07 bd b0 77 00 00 50 56 0d 00 b0 00 36 00 00 . V
11	Frame 1: 108 Dytes on wire (864 Dit	s), 108 bytes ca	ptured (864 bits) c	n interface ca	ipture_uo_	1, 10 0		000 56 97 00 09 77 00 00 50 50 50 90 08 00 89 20 80 08 A W P V W A
í,	Ethernet II, SFC: VMware 90:08:De (0015015619016810	e), DST: CISCO D9:/	7:00 (58:97:00	1:09:77:00	e)		020 40 01 84 53 c0 00 02 64 c6 33 64 64 08 00 84 7c
1	VN-Tag							010 00 13 00 01 f2 h0 o7 62 00 00 00 00 ch 7f 06 00h
	1	= Direct:	ion: From Bridge					040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b
	.0	= Pointer	r: vif_id					ese 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ···· !"# \$%&'()"+
		= Destina	ation: 10					060 2c 2d 2e 2f 30 31 32 33 34 35 36 37
	···· ··· ··· ··· ··· ··· ··· ···	= Looped:	: No 🧹	4				
	0	= Reserve	ed: 0	1 I -				
	000	= Version	n: 0					
	0000 000	00 0000 = Source:	: 0					
L	Type: 802.1Q Virtual LAN (0x8100))						
¥ 8	802.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 102						
	000 = Priority: 0	Best Effort (defa	ault) (0)					
	0 = DEI: Inelig	gible		3 1				
	0000 0110 0110 = ID: 102			·				
	Type: IPv4 (0x0800)							
> 1	Internet Protocol Version 4. Src: 1	92.0.2.100, Dst:	198.51.100.100					
	Internet Control Message Protocol			2				
Ľ								

2番目のパケットを選択し、キーポイントを確認します。

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

No. Time	Source	Destination	Protocol	Length	PD	IP TTL Info		
1 2022-08-01 11:33:19.070693081	192.0.2.100	198.51.100.100	ICMP	108 1	0xc009 (49161)	64 Echo (ping) re	equest i	d=0x0013, seq=1/256, ttl=64 (no response found!)
2 2022-08-01 11:33:19.070695347	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping) re	equest i	d=0x0013, seq=1/256, ttl=64 (no response found!)
3 2022-08-01 11:33:19.071217121	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping) re	equest i	d=0x0013, seq=1/256, ttl=64 (no response found!)
4 2022-08-01 11:33:19.071218458	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping) re	equest i	d=0x0013, seq=1/256, ttl=64 (no response found!)
5 2022-08-01 11:33:20.072036625	192.0.2.100	198.51.100.100	ICMP	108	0xc0ae (49326)	64 Echo (ping) re	equest i	d=0x0013, seq=2/512, ttl=64 (no response found!)
6 2022-08-01 11:33:20.072038399	192.0.2.100	198.51.100.100	ICMP	102	0xc0ae (49326)	64 Echo (ping) re	equest i	d=0x0013, seq=2/512, ttl=64 (no response found!)
7 2022-08-01 11:33:21.073266030	192.0.2.100	198.51.100.100	ICMP	108	0xc167 (49511)	64 Echo (ping) re	equest i	d=0x0013, seq=3/768, ttl=64 (no response found!)
8 2022-08-01 11:33:21.073268327	192.0.2.100	198.51.100.100	ICMP	102	0xc167 (49511)	64 Echo (ping) re	equest i	d=0x0013, seq=3/768, ttl=64 (no response found!)
9 2022-08-01 11:33:22.074576640	192.0.2.100	198.51.100.100	ICMP	108	0xc175 (49525)	64 Echo (ping) re	equest i	d=0x0013, seq=4/1024, ttl=64 (no response found!)
10 2022-08-01 11:33:22.074578010	192.0.2.100	198.51.100.100	ICMP	102	0xc175 (49525)	64 Echo (ping) re	equest i	d=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 (49672)	64 Echo (ping) re	equest i	d=0x0013, seq=5/1280, ttl=64 (no response found!)
12 2022-08-01 11:33:23.075781513	192.0.2.100	198.51.100.100	ICMP	102	0xc208 (49672)	64 Echo (ping) re	equest i	d=0x0013, seq=5/1280, ttl=64 (no response found!)
13 2022-08-01 11:33:24.081839490	192.0.2.100	198.51.100.100	ICMP	108	0xc211 (49681)	64 Echo (ping) re	equest i	d=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	Øxc211 (49681)	64 Echo (ping) re	equest i	d=0x0013, seq=6/1536, ttl=64 (no response found!)
15 2022-08-01 11:33:25.105806249	192.0.2.100	198.51.100.100	ICMP	108	0xc2e2 (49890)	64 Echo (ping) re	equest i	d=0x0013, seq=7/1792, ttl=64 (no response found1)
16 2022-08-01 11:33:25.105807895	192.0.2.100	198.51.100.100	ICMP	102	0xc2e2 (49890)	64 Echo (ping) re	equest i	d=0x0013, seq=7/1792, ttl=64 (no response found!)
17 2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	ICMP	108	0xc3b4 (50100)	64 Echo (ping) re	equest i	d=0x0013, seq=8/2048, ttl=64 (no response found!)
18 2022-08-01 11:33:26.129838114	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100)	64 Echo (ping) re	equest i	d=0x0013, seq=8/2048, ttl=64 (no response found!)
19 2022-08-01 11:33:27.153828653	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294)	64 Echo (ping) re	equest i	d=0x0013, seq=9/2304, ttl=64 (no response found!)
20 2022-08-01 11:33:27.153830201	192.0.2.100	198.51.100.100	ICMP	102	0xc476 (50294)	64 Echo (ping) re	equest i	d=0x0013, seq=9/2304, ttl=64 (no response found!)
21 2022-08-01 11:33:28.177847175	192.0.2.100	198.51.100.100	ICMP	108	0xc516 (50454)	64 Echo (ping) re	equest i	d=0x0013, seq=10/2560, ttl=64 (no response found!)
22 2022-08-01 11:33:28.177849075	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (50454)	64 Echo (ping) re	equest i	d=0x0013, seq=10/2560, ttl=64 (no response found!)
23 2022-08-01 11:33:29.201804760	192.0.2.100	198.51.100.100	ICMP	108	0xc578 (50552)	64 Echo (ping) re	equest i	d=0x0013, seq=11/2816, ttl=64 (no response found!)
24 2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	102	0xc578 (50552)	64 Echo (ping) re	equest i	d=0x0013, seq=11/2816, ttl=64 (no response found!)
25 2022-08-01 11:33:30.225834765	192.0.2.100	198.51.100.100	ICMP	108	0xc585 (50565)	64 Echo (ping) re	equest i	d=0x0013, seq=12/3072, ttl=64 (no response found!)
26 2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (50565)	64 Echo (ping) re	equest i	d=0x0013, seq=12/3072, ttl=64 (no response found!)
27 2022-08-01 11:33:31.249828955	192.0.2.100	198.51.100.100	ICMP	108	0xc618 (50712)	64 Echo (ping) re	equest i	d=0x0013, seq=13/3328, ttl=64 (no response found!)
28 2022-08-01 11:33:31.249831121	192.0.2.100	198.51.100.100	ICMP	102	0xc618 (50712)	64 Echo (ping) re	equest i	d=0x0013, seq=13/3328, ttl=64 (no response found!)
29 2022-08-01 11:33:32.273867960	192.0.2.100	198.51.100.100	ICMP	108	0xc64f (50767)	64 Echo (ping) re	equest i	d=0x0013, seq=14/3584, ttl=64 (no response found!)
<								
> Frame 2: 102 bytes on wire (816 bit	s), 102 bytes ca	ptured (816 bits) o	n interface ca	pture_u0	_1, id 0		0000	58 97 bd b9 77 0e 00 50 56 9d e8 be 81 00 00 66 X ··· w ·· P V ····· f
> Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:b	e), Dst: Cisco b9:7	7:0e (58:97:bd	1:b9:77:0	e)		0010	08 00 45 00 00 54 c0 09 40 00 40 01 8d a3 c0 00 ··E··T·· @·@····
802.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 102						0020	02 64 c6 33 64 64 08 00 8d 7c 00 13 00 01 f2 b9 ·d·3dd···
000 = Priority:	Best Effort (defa	ult) (0) 📕					0030	e7 62 00 00 00 00 cb 7f 06 00 00 00 00 10 11 .b
0 = DEI: Ineli	gible		5 1				0040	12 13 14 15 16 17 18 19 14 10 1c 10 1e 17 20 21
0000 0110 0110 = ID: 102							0050	22 23 24 23 20 27 28 29 28 20 20 20 20 20 21 30 31 #\$M& () "+,","01 32 33 34 35 36 37 234567
Type: IPv4 (0x0800)								234307
> Internet Protocol Version 4, Src: 1	92.0.2.100, Dst:	198.51.100.100 🔎						
> Internet Control Message Protocol		6						

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

- 1. 各ICMPエコー応答はキャプチャされ、2回表示されます。
- 2. 元のパケットヘッダーにはVLANタグが付いていません。
- 3. 内部スイッチは、出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	1P 1D	IP TTL Info		
	1 2022-08-01 11:33:19.071512698	198.51.100.100	192.0.2.100	ICMP	108 ┥	0x4f27 (20263)	64 Echo (ping) repl	y id	=0x0013, seq=1/256, ttl=64
	2 2022-08-01 11:33:19.071514882	198.51.100.100	192.0.2.100	ICMP	108	0x4f27 (20263)	64 Echo (ping) repl	y id	=0x0013, seq=1/256, ttl=64
	3 2022-08-01 11:33:20.072677302	198.51.100.100	192.0.2.100	ICMP	108	0X4110 (20475)	04 ECHO (bruß) Lebr	y id	=0x0013, seq=2/512, ttl=64
	4 2022-08-01 11:33:20.072679384	198.51.100.100	192.0.2.100	ICMP	108	0x4ffb (20475)	64 Echo (ping) repl	y id	=0x0013, seq=2/512, ttl=64
	5 2022-08-01 11:33:21.073913640	198.51.100.100	192.0.2.100	ICMP	108	0x50ac (20652)	64 Echo (ping) repl	y id	=0x0013, seq=3/768, ttl=64
	6 2022-08-01 11:33:21.073915690	198.51.100.100	192.0.2.100	ICMP	108	0x50ac (20652)	64 Echo (ping) repl	y 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) repl	y 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) repl	y 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) repl	y 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) repl	y id	=0x0013, seq=5/1280, ttl=64
1	11 2022-08-01 11:33:24.082407896	198.51.100.100	192.0.2.100	ICMP	108	0x528e (21134)	64 Echo (ping) repl	y id	=0x0013, seq=6/1536, ttl=64
1	12 2022-08-01 11:33:24.082410099	198.51.100.100	192.0.2.100	ICMP	108	0x528e (21134)	64 Echo (ping) repl	y id	=0x0013, seq=6/1536, ttl=64
1	13 2022-08-01 11:33:25.106382424	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64 Echo (ping) repl	y id	=0x0013, seq=7/1792, ttl=64
1	14 2022-08-01 11:33:25.106384549	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64 Echo (ping) repl	y id	=0x0013, seq=7/1792, ttl=64
1	15 2022-08-01 11:33:26.130437851	198.51.100.100	192.0.2.100	ICMP	108	0x53a6 (21414)	64 Echo (ping) repl	y id	=0x0013, seq=8/2048, ttl=64
1	16 2022-08-01 11:33:26.130440320	198.51.100.100	192.0.2.100	ICMP	108	0x53a6 (21414)	64 Echo (ping) repl	y id	=0x0013, seq=8/2048, ttl=64
1	17 2022-08-01 11:33:27.154398212	198.51.100.100	192.0.2.100	ICMP	108	0x5446 (21574)	64 Echo (ping) repl	y id	=0x0013, seq=9/2304, ttl=64
1	18 2022-08-01 11:33:27.154400198	198.51.100.100	192.0.2.100	ICMP	108	0x5446 (21574)	64 Echo (ping) repl	y id	=0x0013, seq=9/2304, ttl=64
1	19 2022-08-01 11:33:28.178469866	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64 Echo (ping) repl	y 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) repl	y id	=0x0013, seq=10/2560, ttl=64
	21 2022-08-01 11:33:29.202395869	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21748)	64 Echo (ping) repl	y id	=0x0013, seq=11/2816, ttl=64
	22 2022-08-01 11:33:29.202398067	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21748)	64 Echo (ping) repl	y id	=0x0013, seq=11/2816, ttl=64
	23 2022-08-01 11:33:30.226398735	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64 Echo (ping) repl	y id	=0x0013, seq=12/3072, ttl=64
	24 2022-08-01 11:33:30.226401017	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64 Echo (ping) repl	y id	=0x0013, seq=12/3072, ttl=64
1	25 2022-08-01 11:33:31.250387808	198.51.100.100	192.0.2.100	ICMP	108	0x55f2 (22002)	64 Echo (ping) repl	y id	=0x0013, seq=13/3328, ttl=64
	26 2022-08-01 11:33:31.250389971	198.51.100.100	192.0.2.100	ICMP	108	0x55f2 (22002)	64 Echo (ping) repl	y id	=0x0013, seq=13/3328, ttl=64
1	27 2022-08-01 11:33:32.274416011	198.51.100.100	192.0.2.100	ICMP	108	0x5660 (22112)	64 Echo (ping) repl	y id	=0x0013, seq=14/3584, ttl=64
	28 2022-08-01 11:33:32.274418229	198.51.100.100	192.0.2.100	ICMP	108	0x5660 (22112)	64 Echo (ping) repl	y id	=0x0013, seq=14/3584, ttl=64
	29 2022-08-01 11:33:33.298397657	198.51.100.100	192.0.2.100	ICMP	108	0x56e7 (22247)	64 Echo (ping) repl	y id	=0x0013, seq=15/3840, ttl=64
<									
> En	ame 1: 108 bytes on wire (864 bit	s), 108 bytes ca	ptured (864 bits) o	n interface ca	pture_u0_	8, id 0		0000	00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00 ·PV···X· ··w··&··
> Et	hernet II, Src: Cisco b9:77:0e (5	8:97:bd:b9:77:0e), Dst: VMware 9d:e	8:be (00:50:50	:9d:e8:be)		0010	00 0a 81 00 00 66 08 00 45 00 00 54 4f 27 00 00 ·····f·· E··TO'··
✓ VN	- Tag							0020	40 01 3e 86 c6 33 64 64 c0 00 02 64 00 00 95 7c
	θ	= Directi	ion: To Bridge					0030	00 13 00 01 f2 b9 e7 62 00 00 00 00 cb 7f 06 00bb
	.0	= Pointer	<pre>vif_id</pre>					0040	00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 15
		= Destina	tion: 0					0050	1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ····· ! # \$3& ()*+
	0	= Looped:	NO	11				0000	2C 20 20 27 50 51 52 53 54 55 56 57 ,/0125 456/
		= Reserve	d: 0	• I					
		= Version	1: 0						
	0000 0000	00 1010 = Source:	10						
	Type: 802.1Q Virtual LAN (0x8100))							
× 80	2.10 Virtual LAN, PRI: 0, DEI: 0,	ID: 102							
	000 = Priority: H	Best Effort (defa	oult) (0)						
	0 = DEI: Inelig	zible		21					
	0000 0110 0110 = ID: 102	-		·					
	Type: IPv4 (0x0800)								
> In	ternet Protocol Version 4, Src: 1	98.51.100.100, D	st: 192.0.2.100						
> In	ternet Control Message Protocol			2					

No. Time	Source	Destination	Protocol	Length	19 ID	IP TTL 11/0	_	
1 2022-08-01 11:33:19.071512698	198.51.100.100	192.0.2.100	ICMP	108 ┥	0x4f27 (20263)	64 Echo (ping) reply	y id	i=0x0013, seq=1/256, ttl=64
2 2022-08-01 11:33:19.071514882	198.51.100.100	192.0.2.100	ICMP	108	0x4f27 (20263)	64 Echo (ping) reply	y id	i=0x0013, seq=1/256, ttl=64
3 2022-08-01 11:33:20.072677302	198.51.100.100	192.0.2.100	ICMP	108	0X4TTD (20475)	ea Ecno (ping) repiy	y id	i=0x0013, seq=2/512, ttl=64
4 2022-08-01 11:33:20.072679384	198.51.100.100	192.0.2.100	ICMP	108	0x4ffb (20475)	64 Echo (ping) reply	y id	d=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	y id	i=0x0013, seq=3/768, ttl=64
6 2022-08-01 11:33:21.073915690	198.51.100.100	192.0.2.100	ICMP	108	0x50ac (20652)	64 Echo (ping) reply	y id	i=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	y id	i=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	y id	i=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	y id	i=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	y id	i=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	y id	i=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	y id	i=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	y id	i=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	y id	i=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	y id	i=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	y id	i=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	y id	i=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	y id	d=0x0013, seq=9/2304, ttl=64
19 2022-08-01 11:33:28.178469866	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64 Echo (ping) reply	y id	i=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	y id	d=0x0013, seq=10/2560, ttl=64
21 2022-08-01 11:33:29.202395869	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21748)	64 Echo (ping) reply	y id	d=0x0013, seq=11/2816, ttl=64
22 2022-08-01 11:33:29.202398067	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21748)	64 Echo (ping) reply	y id	i=0x0013, seq=11/2816, ttl=64
23 2022-08-01 11:33:30.226398735	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64 Echo (ping) reply	y id	d=0x0013, seq=12/3072, ttl=64
24 2022-08-01 11:33:30.226401017	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64 Echo (ping) reply	y id	d=0x0013, seq=12/3072, ttl=64
25 2022-08-01 11:33:31.250387808	198.51.100.100	192.0.2.100	ICMP	108	0x55f2 (22002)	64 Echo (ping) reply	y id	i=0x0013, seq=13/3328, ttl=64
26 2022-08-01 11:33:31.250389971	198.51.100.100	192.0.2.100	ICMP	108	0x55f2 (22002)	64 Echo (ping) reply	y id	d=0x0013, seq=13/3328, ttl=64
27 2022-08-01 11:33:32.274416011	198.51.100.100	192.0.2.100	ICMP	108	0x5660 (22112)	64 Echo (ping) reply	y id	d=0x0013, seq=14/3584, ttl=64
28 2022-08-01 11:33:32.274418229	198.51.100.100	192.0.2.100	ICMP	108	0x5660 (22112)	64 Echo (ping) reply	y id	d=0x0013, seq=14/3584, ttl=64
29 2022-08-01 11:33:33.298397657	198.51.100.100	192.0.2.100	ICMP	108	0x56e7 (22247)	64 Echo (ping) reply	y id	d=0x0013, seq=15/3840, ttl=64
¢								
> Frame 2: 108 bytes on wire (864 bit	s), 108 bytes ca	ptured (864 bits) o	n interface ca	pture u0	8, id 0		0000	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 (00:50:50	:9d:e8:be	2)		0010	00 0a 81 00 00 66 08 00 45 00 00 54 4f 27 00 00 ·····f·· E··TO'··
VN-Tag					·		0020	40 01 3e 86 c6 33 64 64 c0 00 02 64 00 00 95 7c @·>··3dd ···d···
0	= Directi	ion: To Bridge					0030	00 13 00 01 f2 b9 e7 62 00 00 00 00 cb 7f 06 00bb
.0	= Pointer	vif id					0040	00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b
	= Destina	tion: 0					0050	1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ···· !"# \$%&'()"+
0	= Looped:	No	• •				0060	2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,/0123 4567
	= Reserve	d: 0	•					
	= Version	: 0						
0000 000	00 1010 = Source:	10						
Type: 802.10 Virtual LAN (0x8100))							
802.10 Virtual LAN, PRI: 0, DEI: 0.	ID: 182							
000 = Priority: 1	Best Effort (defa	ult) (0)						
	rible		2					
0000 0110 0110 = ID: 102			·					
Type: IPv4 (0x0800)								
> Internet Protocol Version 4, Src: 1	98.51.100.100. D	st: 192.0.2.100						
> Internet Control Message Protocol			2					

説明

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

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

•ポートVLANタグの挿入後。

VNタグの挿入後。

操作順では、VNタグはポートVLANタグの挿入よりも後の段階で挿入されます。ただし、キャプ チャファイルでは、VNタグが付いたパケットは、ポートVLANタグが付いたパケットよりも前に 表示されます。この例では、ICMPエコー要求パケットのVLANタグ102によって、Ethernet1/2が 入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でパケットキャプチャが設定されると、スイッチは各パケット を同時に2回キャプチャします。内部スイッチは、セキュリティモジュール上のアプリケーション によってすでにタグ付けされたパケットを、ポートVLANタグとVNタグを使用して受信します。 ポートVLANタグは、内部シャーシがパケットをネットワークに転送するために使用する出力イ ンターフェイスを示します。この例では、ICMPエコー応答パケット内のVLANタグ102によって 、Ethernet1/2が出力インターフェイスとして識別されます。

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

タスクの要約を次の表に示します。

キャプチャ キャプチャされたパ

タスク キャプチャ イャプチャ たいたい 方向 キャプチャされたトラフィッ ポイント ケットの内部ポート 方向 キャプチャされたトラフィッ

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	10	02	入力のみ	ホスト198.51.100.100からホ 192.0.2.100へのICMPエコー
Ethernet1/2でのキャプチャ の設定と確認	Interface Ethernet1/2	1	02	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 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

VI ΔΝ

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

トポロジ、パケットフロー、およびキャプチャポイント



コンフィギュレーション

FCM

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

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

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	e 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、セッション名を指定して、[Save and Run] をクリックしてキャプチャをアクティブにしま

9 0				
Overview Interfaces Logical Devices Security Engine Platform Settings				System Tools Help admin
Select an instance: ftd1 v			Save and Run Save	Cancel
Subinterface selection Ethernet1/2.205 Ethernet1/2.205 Subinterfaces(2) Ethernet1/2		Session Name* Selected Interfaces Buffer Size Snap length: Store Packets	cap1 Ethernet1/2.205 256 MB 1518 Dytes Overwrite	
Ethernet1/1	FID Ethernet1/9, Ethernet1/10	Capture Filter	Apply Filter Capture All	

3.ポートチャネルサブインターフェイスの場合、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 CLI

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

1. アプリケーションのタイプと識別子を特定します。

firepower#	scope ssa					
firepower	/ssa # sho	w app-insta	nce			
App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version
Deploy Type	e Turbo Mod	e Profile Na	ame Cluster	State Cluster Ro	ole	
					-	
ftđ	ftd1	1	Enabled	Online	7.2.0.82	7.2.0.82
Container	No	RP20	Not Appl	icable None		
ftd	ftd2	1	Enabled	Online	7.2.0.82	7.2.0.82
Container	No	RP20	Not Appl	icable None		
2. ポー	トチャネル・	インターフ	ェイスの場合	合は、そのメンバ-	ーインターフェイ	イスを特定します。

firepower# connect fxos
<output skipped>
firepower(fxos)# show port-channel summary

	P - Op III porc-channer (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	e Protocol Member Ports								
Channel									
1 Pol(SU) Eth	LACP Eth1/3(P) Eth1/3(P)								
1 Po1(SU) Eth 3 キャプチャヤッジ	LACP Eth1/3(P) Eth1/3(P) ションを作成します。								
1 Pol(SU) Eth 3. キャプチャセッ:	LACP Eth1/3(P) Eth1/3(P) ションを作成します。								
1 Po1(SU) Eth 3. キャプチャセッ	LACP Eth1/3(P) Eth1/3(P) ションを作成します。								
1 Po1(SU) Eth 3. キャプチャセッ:	LACP Eth1/3(P) Eth1/3(P) ションを作成します。								
1 Pol(SU) Eth 3.キャプチャセッ: firepower# scope pack	LACP Eth1/3(P) Eth1/3(P) ションを作成します。 et-capture								
1 Pol(SU) Eth 3.キャプチャセッ: firepower# scope packet firepower /packet-capt	LACP Eth1/3(P) Eth1/3(P) ションを作成します。 et-capture cure # create session cap1								

,,, _,	
firepower /packet-capture/session/phy-pc	rt* # set app ftd
firepower /packet-capture/session/phy-pc	rt* # set app-identifier ftd1
firepower /packet-capture/session/phy-pc	rt* # set subinterface 205
firepower /packet-capture/session/phy-pc	rt* # up
<pre>firepower /packet-capture/session* # ena</pre>	ble
<pre>firepower /packet-capture/session* # com</pre>	mit
firepower /packet-capture/session #	
ポートチャネルサブインターフェイスの	場合、各ポートチャネルメンバーインターフェイスのパ
ケットキャプチャを作成します。	

```
firepower# scope packet-capture
firepower /packet-capture # create filter vlan207
firepower /packet-capture/filter* # set ovlan 207
firepower /packet-capture/filter* # up
firepower /packet-capture* # create session cap1
firepower /packet-capture/session* create phy-port Eth1/3
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # set app-identifier ftd1
firepower /packet-capture/session/phy-port* # set subinterface 207
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # create phy-port Eth1/4
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # set app-identifier ftd1
firepower /packet-capture/session/phy-port* # set subinterface 207
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # enable
firepower /packet-capture/session* # commit
firepower /packet-capture/session #
確認
```

FCM

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

Overview	Interfaces I	ogical Devices Security Engine	Platform Settings					System Tools	Help admin
Capture Ser	sion Efter List								
							G Refresh	Capture Session Delete Al Sessions	
•	cap1	Drop Count: 0	Oper	ational State: up	Bof	fer Size: 256 MB	Snap Length: 1518 Bytes		A .8.2
Interface N	ime	Filter		File Size (in bytes)	File Name	Device Na	55e		
Ethernet1/2	205	None		233992	cap1-ethernet-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キャプチャもFCMで表示されます 。ただし、次のように編集することはできません。

Overview Interfaces Li	ogical Devices Security Engine Platform Settings						System To	ols H	elp admin
Capture Session Fiter List									
					C. Refresh	Capture Session	Delete Al Ser	sions	
Cap1	Drop Count: 0	Operational State: up	Buffer Size	e: 256 MB	Snap Length: 1518 Bytes				181
Interface Name	Filter	File Size (in bytes)	File Name	Device Name					
Ethernet1/4.207	None	624160	cap1-ethernet-1-4-0.pcap	Not available	(t				
Ethernet1/3.207	None	160	cap1-ethernet-1-3-0.pcap	Not available	*				

FXOS CLI

scope packet-captureでキャプチャの詳細を確認します。

```
firepower# scope packet-capture
firepower /packet-capture # show session cap1
Traffic Monitoring Session:
   Packet Capture Session Name: cap1
  Session: 1
   Admin State: Enabled
   Oper State: Up
   Oper State Reason: Active
  Config Success: Yes
  Config Fail Reason:
  Append Flag: Overwrite
  Session Mem Usage: 256 MB
  Session Pcap Snap Len: 1518 Bytes
  Error Code: 0
  Drop Count: 0
Physical ports involved in Packet Capture:
   Slot Id: 1
   Port Id: 2
   Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap
   Pcapsize: 9324 bytes
  Filter:
   Sub Interface: 205
   Application Instance Identifier: ftd1
   Application Name: ftd
メンバーインターフェイスEthernet1/3およびEthernet1/4を持つポートチャネル1:
```

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

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

```
Physical ports involved in Packet Capture:
   Slot Id: 1
   Port Id: 3
   Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-3-0.pcap
   Pcapsize: 160 bytes
  Filter:
   Sub Interface: 207
  Application Instance Identifier: ftd1
   Application Name: ftd
  Slot Id: 1
   Port Id: 4
   Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-4-0.pcap
   Pcapsize: 624160 bytes
   Filter:
   Sub Interface: 207
   Application Instance Identifier: ftd1
   Application Name: ftd
```

キャプチャファイルの収集

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

ファイル分析のキャプチャ

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

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

No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info		
F	1 2022-08-04 07:21:56.993302102	192.0.2.100	198.51.100.100	ICMP	112	0x9574 (38260)	64 Echo (ping) reque	est i	d=0x0022, seq=1/256, ttl=64 (no response found!)
	2 2022-08-04 07:21:56.993303597	192.0.2.100	198.51.100.100	ICMP	102	0x9574 (38260)	64 Echo (ping) reque	est i	d=0x0022, seq=1/256, ttl=64 (no response found!)
	3 2022-08-04 07:22:06.214264777	192.0.2.100	198.51.100.100	ICMP	112	0x9a81 (39553)	64 Echo (ping) reque	est i	d=0x0022, seq=10/2560, ttl=64 (no response found!)
	4 2022-08-04 07:22:06.214267373	192.0.2.100	198.51.100.100	ICMP	102	0x9a81 (39553)	64 Echo (ping) reque	est i	d=0x0022, seq=10/2560, ttl=64 (no response found!)
	5 2022-08-04 07:22:07.215113393	192.0.2.100	198.51.100.100	ICMP	112	0x9ac3 (39619)	64 Echo (ping) reque	est i	d=0x0022, seq=11/2816, ttl=64 (no response found!)
	6 2022-08-04 07:22:07.215115445	192.0.2.100	198.51.100.100	ICMP	102	0x9ac3 (39619)	64 Echo (ping) reque	est i	d=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 i	d=0x0022, seq=12/3072, ttl=64 (no response found)
	8 2022-08-04 07:22:08.229940829	192.0.2.100	198.51.100.100	ICMP	102	0x9b33 (39731)	64 Echo (ping) reque	est 1	d=0x0022, seq=12/3072, tt1=64 (no response found!)
	9 2022-08-04 07:22:09.253944601	192.0.2.100	198.51.100.100	ICMP	112	0x9c0e (39950)	64 Echo (ping) reque	est 1	d=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 1	d=0x0022, seq=13/3328, tt1=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 i	d=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	0x9000 (40139)	64 Echo (ping) reque	est in	d=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	TCMP	102	0x9084 (40324)	64 Echo (ping) reque	est i	d=0x0022, seq=15/3840, ttl=64 (no response found!)
	14 2022-08-04 07:22:11.301933000	192.0.2.100	198.51.100.100	TCMP	112	0x9004 (40324)	64 Echo (ping) reque	ist i	d=0x0022, seq=15/3040, ttl=64 (no response found!)
	16 2022 00 04 07:22:12:525950521	102.0.2.100	100 51 100 100	TCMD	102	0x90a2 (40354)	64 Echo (ping) reque	ist i	d=0x0022, seq=10/4096, ttl=64 (no response found!)
	17 2022-00-04 07-22-12-525757895	192.0.2.100	198.51.100.100	ICMP	112	0x9007 (40554)	64 Echo (ping) reque	ist i	d=0x0022, seq=10/4050, ttl=64 (no response foundl)
	19 2022-08-04 07:22:13:320900040	192.0.2.100	198.51.100.100	TCMP	102	0x9007 (40455)	64 Echo (ping) reque	act in	d=0x0022, seq=17/4352, ttl=64 (no response found1)
	10 2022-00-04 07:22:15:520990250	192.0.2.100	198.51.100.100	ICMP	112	0x9007 (40455)	64 Echo (ping) reque	art in	d=0x0022, seq=17/4552, tt1=64 (no response found1)
	20 2022-00-04 07:22:14.341944775	192.0.2.100	198.51.100.100	TCMP	102	0x9063 (40554)	64 Echo (ping) reque	set in	d=0x0022, seq=18/4608, ttl=64 (no response found1)
	21 2022-08-04 07:22:15.365941588	192.0.2.100	198.51.100.100	TCMP	112	8x9efb (48699)	64 Echo (ping) reque	est in	d=0x0022, seq=19/4864, ttl=64 (no response found1)
	22 2022-08-04 07:22:15.365942566	192.0.2.100	198,51,100,100	ICMP	102	0x9efb (40699)	64 Echo (ping) reque	st i	d=0x0022, seq=19/4864, ttl=64 (no response foundl)
	23 2022-08-04 07:22:16.389973843	192.0.2.100	198,51,100,100	ICMP	112	0x9fe8 (40936)	64 Echo (ping) reque	est i	d=0x0022, sea=20/5120, ttl=64 (no response found!)
	24 2022-08-04 07:22:16.389975129	192.0.2.100	198,51,100,100	ICMP	102	0x9fe8 (40936)	64 Echo (ping) reque	est i	d=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	ost i	d=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 i	d=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	ICMP	112	0xa11e (41246)	64 Echo (ping) reque	est i	d=0x0022, seg=22/5632, ttl=64 (no response found!)
ż.						; ;			
	Correct 112 but on when (000 bit	a) 442 hotes as	stund (not black)	a laterfree er		1 11 0		0000	22 76 62 00 00 4b 00 50 56 0d c0 be 00 26 00 54
2	Frame 1: 112 bytes on wire (896 bit	(s), 112 bytes ca	ptured (896 bits) o	n interface ca	pture_ue_	1, 10 0		0000	az 76 72 88 88 10 00 50 50 90 88 08 89 26 88 54 VVVV 12 VVV 61
	Ethernet II, Src: VMware 9d:e8:be (0012012010016810	e), Dst: a2:/6:T2:0	0:00:10 (a2:76	STT2:00:00	(10)		0010	95 74 49 99 49 91 b8 38 c9 99 92 64 c6 33 64 64 t@.@8d.3dd
1	vn- rag	= Directi	ion: Econ Pridae					0030	08 00 eb 95 00 22 00 01 88 73 eb 62 00 00 00 00
	A	= Pointer	wif id					0040	d9 9d 00 00 00 00 00 00 10 11 12 13 14 15 16 17
	00 0000 0101 0100	= Destina	ation: 84					0050	18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 ······ !"#\$%&'
		= Looped:	No	4				0060	28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ()*+,/ 01234567
		= Reserve	d: 0	•					
		= Version	1: 0						
		00 0000 = Source:	. 0						
	Type: 802.10 Virtual LAN (0x8100)							
V 1	802.10 Virtual LAN, PRI: 0, DEI: 0,	ID: 102							
ĽĽ	000 = Priority:	Best Effort (defa	ault) (0)						
	0 = DEI: Ineli	gible		21					
	0000 0110 0110 = ID: 102	0		·					
П	Type: 802.1Q Virtual LAN (0x8100)							
× 1	802.10 Virtual LAN, PRI: 0, DEI: 0,	ID: 205							
П	000 = Priority:	Best Effort (defa	ault) (0)						
	0 = DEI: Ineli	gible							
	0000 1100 1101 = ID: 205								
	Type: IPv4 (0x0800)			-					
>	Internet Protocol Version 4, Src: 1	192.0.2.100, Dst:	198.51.100.100						
>	Internet Control Message Protocol								
1									
_									

2番目のパケットを選択し、キーポイントを確認します。

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

2. 元のパケットヘッダーにはVLANタグ205が付いています。

	io. Time	Source	Destination P	otocol Length	PD	IP TTL Info		
	1 2022-08-04 07:21:56.993302102	192.0.2.100	198.51.100.100 I	CMP 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 I	CMP 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 I	CMP 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 I	CMP 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 I	CMP 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 I	CMP 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 I	CMP 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 I	CMP 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 I	CMP 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 I	CMP 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 I	CMP 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 I	CMP 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 I	CMP 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 I	CMP 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 I	CMP 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 I	CMP 102	0x9da2	(40354) 64 Echo	(ping) request	id=0x0022, seq=16/4096, ttl=64 (no response found!)
	17 2022-08-04 07:22:13.326988040	192.0.2.100	198.51.100.100 I	CMP 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 I	CMP 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 I	CMP 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 I	CMP 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 I	CMP 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 I	CMP 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 I	CMP 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 I	CMP 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 I	CMP 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 I	CMP 102	0xa079	(41081) 64 Echo	(ping) request	id=0x0022, seq=21/5376, ttl=64 (no response found!)
	27 2022-08-04 07:22:18.437954335	192.0.2.100	198.51.100.100 I	CMP 112	0xa11e	(41246) 64 Echo	(ping) request	id=0x0022, seq=22/5632, ttl=64 (no response found!)
<								
5	Frame 2: 102 bytes on wire (816 bit	s), 102 bytes ca	ptured (816 bits) on	interface capture	u0 1, id 0		00	00 a2 76 f2 00 00 1b 00 50 56 9d e8 be 81 00 00 cd ·v····P V·····
	Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:b	e), Dst: a2:76:f2:00:	00:1b (a2:76:f2:00	:00:1b)		00:	10 08 00 45 00 00 54 95 74 40 00 40 01 b8 38 c0 00 ··E··T·t @·@··8··
	802.10 Virtual LAN, PRI: 0, DEI: 0,	ID: 205			,		003	20 02 64 c6 33 64 64 08 00 eb 95 00 22 00 01 88 73 ·d·3dd·· ···"···s
н	000 = Priority: B	est Effort (defa	ault) (0)				003	30 eb 62 00 00 00 00 d9 9d 00 00 00 00 00 00 10 11 ·b·····
Т	0 = DEI: Inelig	ible		1			004	40 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21!
Т	0000 1100 1101 = ID: 205		2	1			00	50 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 "#\$%%'() "+,/01
Т	Type: IPv4 (0x0800)						000	32 33 34 35 30 37 234567
	Internet Protocol Version 4, Src: 1	92.0.2.100, Dst:	198.51.100.100					
	Internet Control Message Protocol							

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

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

1001を挿入します。

4. 内部スイッチは、追加のVNタグを挿入します。

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info		
5	1 2022-08-04 08:18:24.572548869	192.168.247.100	192.168.247.102	ICMP	128	0x609e (24734)	255 Echo (ping) re	quest	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	quest	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	quest	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	quest	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	quest	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	quest	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	quest	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	quest	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	quest	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	quest	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	quest	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	quest	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	quest	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	quest	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	quest	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	quest	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	quest	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	quest	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) re	quest	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	quest	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) re	quest	1d=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) re	quest	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) re	quest	1d=0x007b, seq=11/2816, tt1=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) re	quest	1d=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) re	quest	1d=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) re	quest	1d=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) re	quest	1d=0x007b, seq=13/3328, ttl=255 (no response found!)
<									
> 1	Frame 1: 128 bytes on wire (1024 bits), 128 bytes capt	ured (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 ·······&···
> 1	Ethernet II, Src: Cisco d6:ec:00 (00:	17:df:d6:ec:00),	Dst: a2:76:f2:00:0	0:1c (a2:76:f2	:00:00:10	:)		0010	00 00 81 00 03 e9 81 00 00 cf 08 00 45 00 00 64E.d
× 1	/N-Tag							0020	60 9e 00 00 ff 01 ea dd c0 a8 f7 64 c0 a8 f7 66
	1	= Direction	: From Bridge					0030	08 00 05 C8 00 70 00 00 00 00 00 02 40 8C 4a 78 ·····{···M·JX
	.0	= Pointer:	vif_id					0040	ab cd
	00 0000 0011 1101	= Destinati	on: 61					0050	ab cd
	···· ··· ··· ··· ··· 0 ····	= Looped: N	0	4				0070	ab cd
	···· ··· ···· ··· ··· ·0·· ····	<pre> = Reserved:</pre>	0						
		<pre> = Version:</pre>	9						
	0000 0000	0000 = Source: 0							
L	Type: 802.1Q Virtual LAN (0x8100)								
1 8	802.1Q Virtual LAN, PRI: 0, DEI: 0, I	D: 1001							
	000 Be	st Effort (defaul	t) (0)	2					
	0 = DEI: Ineligi	ble		2					
	0011 1110 1001 = ID: 1001								
L	Type: 802.10 Virtual LAN (0x8100)								
Y 1	802.1Q Virtual LAN, PRI: 0, DEI: 0, 1	D: 207							
	000 Be	st Effort (defaul	t) (0)						
	0 = DEI: Ineligi	ble		_					
	0000 1100 1111 = ID: 207			21					
	Type: IPv4 (0x0800)			-					
20	Internet Protocol Version 4, Src: 192	.168.247.100, Dst	: 192.168.247.102	_					
2	Internet Control Méssage Protocol								
15									
_								-	

2番目のパケットを選択し、キーポイントを確認します。

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

1 1022-08-40 0812145.275248869 192.168.247.100 1079 128 2 1022-08-40 0812145.27528670 192.168.247.100 1079 128 2 022-08-40 0812145.27528670 192.168.247.100 1079 128 0 022-08-40 0812145.27528671 192.168.247.100 1079 128 0 022-08-40 0812145.27528671 192.168.247.100 1079 128 0x6009 (24735) 255 Echo (1010) request 14-00007b, seq-17256, tt12-35 (mo response foundl) 5 0222-08-40 0812145.2757844 192.168.247.100 1079 128 0x6009 (24735) 255 Echo (1010) request 14-00007b, seq-37168, tt12-35 (mo response foundl) 7 0222-08-40 0812145.275144514 192.168.247.100 1079 128 0x600 (2475) 255 Echo (1010) request 14-00007b, seq-37168, tt12-35 (mo response foundl) 10 0222-08-40 0812145.275145145 192.168.247.100 1079 128 0x600 (2475) 255 Echo (1010) request 14-00007b, seq-37168, tt12-35 (mo response foundl) 112 12 0222-08-40 0812145.275415459 192.168.247.100 1079 128 0	No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info		
2 2022-08-04 08:18:24.57256073 192.168.277.102 109 192.68.277.102 109 118 08:007 (2475) 255 [cho (rpin) request 14:00070, seq-1725, ttl=255 (no response found]) 4 2022-08-04 08:18:24.57286616 192.168.277.102 109 118 08:009 (2475) 255 [cho (rpin) request 14:00070, seq-1725, ttl=255 (no response found]) 6 2022-08-04 08:18:24.57298713 192.168.277.102 109 118 08:000 (2475) 255 [cho (rpin) request 14:00070, seq-1725, ttl=255 (no response found]) 7 2022-08-04 08:18:24.57298713 192.168.277.102 109 118 08:000 (2475) 255 [cho (rpin) request 14:00070, seq-1725, ttl=255 (no response found]) 8 202-08-04 08:18:24.572987248 192.168.277.102 109 118 08:000 (2475) 255 [cho (rpin) request 14:00070, seq-1726, ttl=255 (no response found]) 9 202-08-04 08:18:24.57298548 192.168.277.102 109 118 08:001 (2477) 255 [cho (rpin) request 14:00070, seq-1726, ttl=255 (no response found]) 10 202-08-04 08:18:24.574105151 193.168.277.102 109 118 08:061 (2477) 255 [cho (rpin) request 14:00070, seq-1726, ttl=255 (no response found]) 11 2022-08-04 08:18:24.57915419 193.168.277.102 109 118 08:061 (2477) 255 [cho (rpin) request 14:00070, seq-1726, ttl=255 (no response found]) 12 2022-08-04 08:18:24.57915419 193.168.277.102 109 128 08:061 (2477) 255 [cho (rpin) request 14:00070, seq-1726, ttl=255 (no response found]) 12 2022-08-04 08:18:24.57915419 193.168.277.102 109 128 08:063 (2478) 255 [cho (rpin) request 14:00070, seq-1736, ttl=255 (no response found]) 12 2022-08-04 08:18:24.57915419 193.168.277.102 109 128 08:063 (2478) 255 [cho (rpin) request 14:00070, seq-1735, ttl=255 (no response found]) 12 2022-08-04 08:18:24.57915419 193.168.277.102 109 128 08:063 (2478) 255 [cho (rpin) request 14:00070, seq-1735, ttl=255 (no response found]) 12 2022-08-04 08:18:24.57915419 192.168.277.102 109 128 08:064 (2474) 255 [cho (rpin) request 14:00070, seq-1735, ttl=255 (no response found]) 12 2022-08-04 08:18:24.57915419 192.168.277.102 109 128 08:064 (2474) 255 [cho (rpin) request 14:000070, seq-1735, ttl=255 (no response found]) 12 2022-08-04 08:18:24.57915419	Γ.	1 2022-08-04 08:18:24.572548869	192.168.247.100	192.168.247.102	ICMP	128	0x609e (24734)	255 Echo (ping) request	id=0x007b,	seq=0/0, ttl=255 (no response found!)
2 222-06-04 09:112:45:72266350 192.166.27.100 192.106.27.102 10P 128 00:6097 (2473) 255 Eth (pinc) request id=0007b, seq=1/25b, ttl=255 (no response found]) 5 2022-06-04 09:112:45:73724751 192.166.27.100 192.166.27.		2 2022-08-04 08:18:24.572550073	192.168.247.100	192.168.247.102	ICMP	118	0x609e (24734)	255 Echo (ping) request	id=0x007b,	seq=0/0, ttl=255 (no response found!)
4 2022-08-44 08:118:24.573287676 192.168.27.100 192.168.27.100 102.168.27.100 <td></td> <td>3 2022-08-04 08:18:24.573286630</td> <td>192.168.247.100</td> <td>192.168.247.102</td> <td>ICMP</td> <td>128</td> <td>0x609f (24735)</td> <td>255 Echo (ping) request</td> <td>id=0x007b,</td> <td>seq=1/256, ttl=255 (no response found!)</td>		3 2022-08-04 08:18:24.573286630	192.168.247.100	192.168.247.102	ICMP	128	0x609f (24735)	255 Echo (ping) request	id=0x007b,	seq=1/256, ttl=255 (no response found!)
5 2022-08-04 08:18:24.57379658 192.168.27.100 192.168.27.100 128 0x66400 24736) 255 tcho (ping) request 1d-0x007b, seq-2/512, ttl-255 (no response found]) 7 2022-08-04 08:18:24.573095748 192.168.27.100 112.102.168.27.100 112.102.168.27.100 192.168.27.100 112.102.168.27.100		4 2022-08-04 08:18:24.573287640	192.168.247.100	192.168.247.102	ICMP	118	0x609f (24735)	255 Echo (ping) request	id=0x007b,	seq=1/256, ttl=255 (no response found!)
6 2022-08-40 0818124.573795748 152.168.47.100 162.168.47.100 162.168.47.100 162.168.47.100 162.168.47.100 162.168.47.100 162.168.47.100 162.168.47.100 162.168.47.100 162.168.47.100 162.168.47.100 162.168.47.100 162.168.47.100 162.168.47.100		5 2022-08-04 08:18:24.573794751	192.168.247.100	192.168.247.102	ICMP	128	0x60a0 (24736)	255 Echo (ping) request	id=0x007b,	seq=2/512, ttl=255 (no response found!)
7 2022-08-40 08:18:24.57436638 192.166.247.100 1029 128 0x6041 (2477) 255 fcho (ping) request id-0x007b, seq-3/768, ttl-255 (no response found]) 9 2022-08-40 08:18:24.57401541 192.166.247.100 1029 128.647.100 1019 128.647.100 1029 128.647.100 1019		6 2022-08-04 08:18:24.573795748	192.168.247.100	192.168.247.102	ICMP	118	0x60a0 (24736)	255 Echo (ping) request	id=0x007b,	seq=2/512, ttl=255 (no response found!)
8 202-08-40 8:18:24.57646552 192.168.27.100 102 112 0xc6a1 (2477) 255 Echo (ping) request id=0x007b, seq=4/126, ttl=255 (no response found)) 10 202-08-40 08:18:24.57641551 192.168.27.100 192.168.27.102 107P 118 0xc6a2 (2478) 255 Echo (ping) request id=0x007b, seq=4/126, ttl=255 (no response found)) 11 202-08-40 08:18:24.57541561 192.168.27.100 192.168.27.102 107P 118 0xc6a3 (2479) 255 Echo (ping) request id=0x007b, seq=4/126, ttl=255 (no response found)) 12 202-08-40 08:18:24.575415611 192.168.27.100 192.168.27.102 107P 118 0xc6a3 (2479) 255 Echo (ping) request id=0x007b, seq=4/156, ttl=255 (no response found)) 13 202-08-40 08:18:24.575416671 192.168.27.100 192.168.27.102 107P 118 0xc6a4 (2474) 255 Echo (ping) request id=0x007b, seq=4/156, ttl=255 (no response found)) 105 21.08.27.102 107P 118 0xc6a4 (2472) 255 Echo (ping) request id=0x007b, seq=4/128, ttl=255 (no response found)) 16 202-08-40 08:18:24.5754456451 92.108.27.100 102.108.27.102 107P 118 0xc6a4 (2472) 255 Echo (ping) request id=0x007b, seq=4/128, ttl=255 (no response foun		7 2022-08-04 08:18:24.574368638	192.168.247.100	192.168.247.102	ICMP	128	0x60a1 (24737)	255 Echo (ping) request	id=0x007b,	seq=3/768, ttl=255 (no response found!)
9 2022-08-40 08:18:24.57543151 192.168.247.100<		8 2022-08-04 08:18:24.574369574	192.168.247.100	192.168.247.102	ICMP	118	0x60a1 (24737)	255 Echo (ping) request	id=0x007b,	seq=3/768, ttl=255 (no response found!)
10 202-08-04 08:18:24.574025415 192.168.247.100 120 120 242.738) 255 Echo (ping) request id-exx007b, seq-4/1024, ttl=255 (no response found) 11 2022-08-04 08:18:24.575443601 192.168.247.100 120.102.168.247.100 120 120 255 Echo (ping) request id-exx07b, seq-5/1208, ttl=255 (no response found) 13 2022-08-04 08:18:24.575443601 192.168.247.100 120.168.247.100 120.168.247.100 120.168.247.100 120.168.247.100 121.68.247.100 122.168.247.100 121.68.247.100 122.168.247.100 12		9 2022-08-04 08:18:24.574914512	192.168.247.100	192.168.247.102	ICMP	128	0x60a2 (24738)	255 Echo (ping) request	id=0x007b,	seq=4/1024, ttl=255 (no response found!)
11 2022-08-04 08:18:24.57544360 192.168.247.100 12/022-08-04 08:18:24.57544360 12/022-08-04 08:18:24.57543160 192.168.247.100 12/022-08-04 08:18:24.57543160 192.168.247.100 <td></td> <td>10 2022-08-04 08:18:24.574915415</td> <td>192.168.247.100</td> <td>192.168.247.102</td> <td>ICMP</td> <td>118</td> <td>0x60a2 (24738)</td> <td>255 Echo (ping) request</td> <td>id=0x007b,</td> <td>seq=4/1024, ttl=255 (no response found!)</td>		10 2022-08-04 08:18:24.574915415	192.168.247.100	192.168.247.102	ICMP	118	0x60a2 (24738)	255 Echo (ping) request	id=0x007b,	seq=4/1024, ttl=255 (no response found!)
12 2022-08-04 08:18:24.57543601 102.168.247.100		11 2022-08-04 08:18:24.575442569	192.168.247.100	192.168.247.102	ICMP	128	0x60a3 (24739)	255 Echo (ping) request	id=0x007b,	seq=5/1280, ttl=255 (no response found!)
13 2022-08-04 08:18:24.575918119 192.168.247.100 122.168.247.100 128 0x60a4 (24740) 255 Echo (ping) request id-0x007b, seq-6/1536, ttl-255 (no response found1) 15 2022-08-04 08:18:24.57640561 192.168.247.100 192.168.247.100 120.168.247.100		12 2022-08-04 08:18:24.575443601	192.168.247.100	192.168.247.102	ICMP	118	0x60a3 (24739)	255 Echo (ping) request	id=0x007b,	seq=5/1280, ttl=255 (no response found!)
14 2022-08-04 08:18:24.5790957 192.168.247.100 192.168.247.100 120.168.247.100<		13 2022-08-04 08:18:24.575918119	192.168.247.100	192.168.247.102	ICMP	128	0x60a4 (24740)	255 Echo (ping) request	id=0x007b,	seq=6/1536, ttl=255 (no response found!)
15 2022-08-04 08:18:24.57640875 192.168.247.100 192.168.247.100 128 0x60a5 (24741) 255 Echo (ping) request id-0x007b, seq-7/1792, ttl-255 (no response found1) 17 2022-08-04 08:18:24.576808561 192.168.247.100 192.168.247.100 118 0x60a5 (24741) 255 Echo (ping) request id-0x007b, seq-7/1792, ttl-255 (no response found1) 18 2022-08-04 08:18:24.576808561 192.168.247.100 192.168.247.102 1CHP 118 0x60a6 (2472) 255 Echo (ping) request id-0x007b, seq-8/2048, ttl-255 (no response found1) 19 2022-08-04 08:18:24.57789523 192.168.247.100 192.168.247.102 1CHP 118 0x60a7 (2473) 255 Echo (ping) request id-0x007b, seq-9/204b, ttl-255 (no response found1) 21 2022-08-04 08:18:24.57789523 192.168.247.102 1CHP 118 0x60a7 (2474) 255 Echo (ping) request id-0x007b, seq-9/2304, ttl-255 (no response found1) 22 2022-08-04 08:18:24.577898290 192.168.247.102 1CHP 118 0x60a8 (24744) 255 Echo (ping) request id-0x007b, seq-1/256b, ttl-255 (no response found1) 23 2022-08-04 08:18:24.57890809 192.168.247.102 1CHP 118 0x60a9 (24745) 255 Echo (ping) request id-0x007b, seq-1/256b, ttl-255 (no response found1) 24 2022-08-04 08:18:24.57890809 192.168.247.102 1CHP 118 0x60a9 (24745)<		14 2022-08-04 08:18:24.575919057	192.168.247.100	192.168.247.102	ICMP	118	0x60a4 (24740)	255 Echo (ping) request	id=0x007b,	seq=6/1536, ttl=255 (no response found!)
16 2022-08-04 08:18:24.57688651 192.168.247.100 122.168.247.100<		15 2022-08-04 08:18:24.576407671	192.168.247.100	192.168.247.102	ICMP	128	0x60a5 (24741)	255 Echo (ping) request	id=0x007b,	seq=7/1792, ttl=255 (no response found!)
17 2022-08-04 08:18:24.578865643 192.168.247.100 192.168.247.100 128 0x60a6 (24742) 255 Echo (ping) request id=0x007b, seq=6/2048, ttl=255 (no response found1) 19 2022-08-04 08:18:24.577895234 192.168.247.100 129.168.247.102 ICMP 128 0x60a6 (24742) 255 Echo (ping) request id=0x007b, seq=6/2048, ttl=255 (no response found1) 20 2022-08-04 08:18:24.577987534 192.168.247.100 192.168.247.102 ICMP 128 0x60a7 (24743) 255 Echo (ping) request id=0x007b, seq=6/2048, ttl=255 (no response found1) 21 2022-08-04 08:18:24.577987534 192.168.247.100 192.168.247.102 ICMP 128 0x60a8 (24744) 255 Echo (ping) request id=0x007b, seq=1/0256b, ttl=255 (no response found1) 22 2022-08-04 08:18:24.577987534 192.168.247.102 ICMP 128 0x60a8 (24744) 255 Echo (ping) request id=0x007b, seq=1/0256b, ttl=255 (no response found1) 24 2022-08-04 08:18:24.57890209 192.168.247.102 ICMP 128 0x60a9 (24745) 255 Echo (ping) request id=0x007b, seq=1/236b, ttl=255 (no response found1) 24 2022-08-04 08:18:24.57890409 192.168.247.102 ICMP 128 0x60a9 (24745) 255 Echo (ping) request id=0x007b, seq=1/286b, ttl=255 (no response found1) 26 2022-08-04 08:18:24.578904099 192.168.247.102 ICMP 118 <td></td> <td>16 2022-08-04 08:18:24.576408585</td> <td>192.168.247.100</td> <td>192.168.247.102</td> <td>ICMP</td> <td>118</td> <td>0x60a5 (24741)</td> <td>255 Echo (ping) request</td> <td>id=0x007b,</td> <td>seq=7/1792, ttl=255 (no response found!)</td>		16 2022-08-04 08:18:24.576408585	192.168.247.100	192.168.247.102	ICMP	118	0x60a5 (24741)	255 Echo (ping) request	id=0x007b,	seq=7/1792, ttl=255 (no response found!)
18 2022-08-04 08:18:24.5794885561 192.168.247.100 110		17 2022-08-04 08:18:24.576885643	192.168.247.100	192.168.247.102	ICMP	128	0x60a6 (24742)	255 Echo (ping) request	id=0x007b,	seq=8/2048, ttl=255 (no response found!)
19 2022-08-04 08:18:24.577939428 192.168.247.100 192.168.247.100 128 0x60a7 24743) 255 Echo (ping) request id-0x007b, seq-9/2304, ttl-255 (no response found]) 21 2022-08-04 08:18:24.577987632 192.168.247.100 192.168.24		18 2022-08-04 08:18:24.576886561	192.168.247.100	192.168.247.102	ICMP	118	0x60a6 (24742)	255 Echo (ping) request	id=0x007b,	seq=8/2048, ttl=255 (no response found!)
20 2022-08-04 08:18:24.57798523 192.168.247.100 192.168.247.101 100 192.168.247.100 120.168.247.100 192.168.247		19 2022-08-04 08:18:24.577394328	192.168.247.100	192.168.247.102	ICMP	128	0x60a7 (24743)	255 Echo (ping) request	id=0x007b,	seq=9/2304, ttl=255 (no response found!)
21 2022-08-04 08:18:24.577982632 102.168.247.100 102.168.247.100 128 0x60a8 (24744) 255 Echo (ping) request id-0x087b, seq-10/2566, ttl-255 (no response found)) 23 2022-08-04 08:18:24.5778489781 192.168.247.100 192.168.247.102 ICMP 128 0x60a8 (24744) 255 Echo (ping) request id-0x087b, seq-10/2566, ttl-255 (no response found)) 24 2022-08-04 08:18:24.5784489781 192.168.247.100 192.168.247.102 ICMP 128 0x60a9 (24745) 255 Echo (ping) request id-0x087b, seq-11/2816, ttl-255 (no response found)) 24 2022-08-04 08:18:24.5784489781 192.168.247.100 192.168.247.102 ICMP 128 0x60a9 (24745) 255 Echo (ping) request id-0x087b, seq-11/2816, ttl-255 (no response found)) 25 2022-08-04 08:18:24.578404897 192.168.247.100 192.168.247.102 ICMP 128 0x60a9 (24746) 255 Echo (ping) request id-0x087b, 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 118 0x60a9 (24746) 255 Echo (ping) request id-0x087b, seq-12/3072, ttl-255 (no response found)) 27 2022-08-04 08:18:24.579426962 192.168.247.102 ICMP 128 0x60a9 (24747) 255 Echo (ping) request id-0x087b, seq-12/3072, ttl-255 (no response found)) 27 2022-08-04 08:18:24.579426962<		20 2022-08-04 08:18:24.577395234	192.168.247.100	192.168.247.102	ICMP	118	0x60a7 (24743)	255 Echo (ping) request	id=0x007b,	seq=9/2304, ttl=255 (no response found!)
22 2022-08-04 08:18:24.57989290 192.168.247.100 192.168.247.100 126.247.100 128 0x60a8 (24745) 255 Echo (ping) request id-0x007b, seq-10/256b, ttl-255 (no response foundl) 24 2022-08-04 08:18:24.57894090 192.168.247.100 192.168.247.100 126.247.102 104P 118 0x60a9 (24745) 255 Echo (ping) request id-0x007b, seq-11/281b, ttl-255 (no response foundl) 25 2022-08-04 08:18:24.578940901 192.168.247.100		21 2022-08-04 08:18:24.577987632	192.168.247.100	192.168.247.102	ICMP	128	0x60a8 (24744)	255 Echo (ping) request	id=0x007b,	seq=10/2560, ttl=255 (no response found!)
23 2022-08-04 08:18:24.578448761 102.168.247.100 102.168.247.100 128 0x60a9 (24745) 225 Echo (ping) request id-0x087b, seq-11/2816, ttl-255 (no response found1) 24 2022-08-04 08:18:24.5784090043 192.168.247.100 12.168.247.102 1CMP 118 0x60a9 (24745) 225 Echo (ping) request id-0x087b, seq-11/2816, ttl-255 (no response found1) 25 2022-08-04 08:18:24.5784090043 192.168.247.100 192.168.247.102 1CMP 118 0x60a9 (24745) 225 Echo (ping) request id-0x087b, seq-12/3072, ttl-255 (no response found1) 26 2022-08-04 08:18:24.5784090047 192.168.247.100 192.168.247.102 ICMP 118 0x60a9 (24745) 225 Echo (ping) request id-0x087b, seq-12/3072, ttl-255 (no response found1) 27 2022-08-04 08:18:24.579420962 192.168.247.100 192.168.247.102 ICMP 128 0x60a9 (24747) 255 Echo (ping) request id-0x087b, seq-12/3072, ttl-255 (no response found1) 27 2022-08-04 08:18:24.579420962 192.168.247.102 ICMP 128 0x60a9 (24747) 255 Echo (ping) request id-0x087b, seq-12/3072, ttl-255 (no response found1) 21 2022-08-04 08:18:24.579420962 192.168.247.102 ICMP 128 0x60a9 (24747) 255 Echo (ping) request id-0x087b, seq-12/3072, ttl-255 (no response found1) 21 2022-08-04 04 06:18:24.579420962 192.168.247.10		22 2022-08-04 08:18:24.577989290	192.168.247.100	192.168.247.102	ICMP	118	0x60a8 (24744)	255 Echo (ping) request	id=0x007b,	seq=10/2560, ttl=255 (no response found!)
24 2022-08-04 08:18:24.57840499 192.168.247.100 192.168.247.100 126.247.100 128 0x60a9 (24745) 255 Echo (ping) request id-0x007b, seq-11/2816, ttl-255 (no response foundl) 26 2022-08-04 08:18:24.578900097 192.168.247.100 192.168.247.100 128.0x60a9 (24745) 255 Echo (ping) request id-0x007b, seq-11/2816, ttl-255 (no response foundl) 26 2022-08-04 08:18:24.57900097 192.168.247.100 192.168.247.100 128.0x60a9 (24745) 255 Echo (ping) request id-0x007b, seq-12/3072, ttl-255 (no response foundl) 27 2022-08-04 08:18:24.579426962 192.168.247.100 128.0x60a9 (24745) 255 Echo (ping) request id-0x007b, seq-13/3028, ttl-255 (no response foundl) 27 2022-08-04 08:18:24.579426962 192.168.247.100 128.0x60a9 (24745) 255 Echo (ping) request id-0x007b, seq-13/3028, ttl-255 (no response foundl) 26 2022-08-04 08:18:24.579426962 192.168.247.100 128.0x60a9 (24745) 255 Echo (ping) request id-0x007b, seq-13/3328, ttl-255 (no response foundl) 27 2022-08-04 08:18:24.579426962 192.168.247.100 128.0x60a9 (24745) 255 Echo (ping) request id-0x007b, seq-13/3328, ttl-255 (no response foundl) 28 2020 triater 192.168.247.100 128.0x60a9 (24745) 255 Echo (ping) request id-0x007b, seq-13/3328, ttl-255 (no response foundl) 29 10 00 00 00 0170 011207 118 0x60a9 (100 017) 128.0x607b, se		23 2022-08-04 08:18:24.578448781	192.168.247.100	192.168.247.102	ICMP	128	0x60a9 (24745)	255 Echo (ping) request	id=0x007b,	seq=11/2816, ttl=255 (no response found!)
25 2022-08-04 08:18:24.578900043 192.168.247.100 192.168.247.102 ICHP 128 0x60aa (24746) 255 Echo (ping) request id-0x007b, seq-12/3072, ttl=255 (no response foundl) 26 2022-08-04 08:18:24.578900043 192.168.247.100 192.168.247.102 ICHP 118 0x60aa (24746) 255 Echo (ping) request id-0x007b, seq-12/3072, ttl=255 (no response foundl) 27 2022-08-04 08:18:24.579426062 192.168.247.100 192.168.247.102 ICHP 128 0x60aa (24746) 255 Echo (ping) request id-0x007b, seq-12/3072, ttl=255 (no response foundl) 27 2022-08-04 08:18:24.579426062 192.168.247.100 192.168.247.102 ICHP 128 0x60ab (24747) 255 Echo (ping) request id-0x007b, seq-12/3072, ttl=255 (no response foundl) 27 2022-08-04 08:18:24.579426062 192.168.247.100 192.168.247.102 ICHP 128 0x60ab (24747) 255 Echo (ping) request id-0x007b, seq-12/3072, ttl=255 (no response foundl) 27 2022-08-04 08:18:24.579426062 192.168.247.100 192.168.247.102 ICHP 128 0x60ab (24747) 255 Echo (ping) request id-0x007b, seq-12/3072, ttl=255 (no response foundl) 27 2022-08-04 08:18:24.579426062 192.168.247.102 ICHP 128 0x60ab (24747) 255 Echo (ping) request id-0x007b, seq-12/3072, ttl=255 (no response foundl) 27 2022-08-04 08:18:24.579426062 192.168.247.102 ICHP 128 0x60ab (24747) 255 Echo (ping) request id-0x007b, seq-12/3072, ttl=255 (no response foundl) 0000 a2 76 f2 00 00 if of d6 de c 00 81 00 0cf		24 2022-08-04 08:18:24.578449909	192.168.247.100	192.168.247.102	ICMP	118	0x60a9 (24745)	255 Echo (ping) request	id=0x007b,	seq=11/2816, ttl=255 (no response found!)
26 2022-08-04 08:18:24.578908097 192.168.247.100 192.168.247.102 ICMP 118 0x60ab (24746) 255 Echo (ping) request id=0x007b, seq=12/3072, ttl=255 (no response foundl) 27 2022-08-04 08:18:24.579426962 192.168.247.100 192.168.247.100 122.168.247.100 122.168.247.100 122.168.247.100 128 0x60ab (24747) 255 Echo (ping) request id=0x007b, seq=12/3072, ttl=255 (no response foundl) 2 Frame 2: 118 bytes on wire (044 bits), 118 bytes captured (044 bits) on interface capture_u0_3, id 0 0000 a2 76 f2 00 00 1c 00 17 df d6 ec 00 81 00 00 ef v v v 2 Ethernet II, Spr: Cisco d6e:c00 (00:171df:d6:ec:00), Dst: a2:76:f2:00:00:1c (a2:76:f2:00:00:1c) v <t< td=""><td></td><td>25 2022-08-04 08:18:24.578900043</td><td>192.168.247.100</td><td>192.168.247.102</td><td>ICMP</td><td>128</td><td>0x60aa (24746)</td><td>255 Echo (ping) request</td><td>id=0x007b,</td><td>seq=12/3072, ttl=255 (no response found!)</td></t<>		25 2022-08-04 08:18:24.578900043	192.168.247.100	192.168.247.102	ICMP	128	0x60aa (24746)	255 Echo (ping) request	id=0x007b,	seq=12/3072, ttl=255 (no response found!)
27 2022-08-04 08:18:24.579426962 192.168.247.100 102.168.247.102 ICMP 128 0x60ab (24747) 255 Echo (ping) request id-0x007b, seq-13/3328, ttl=255 (no response foundl) > Frame 2: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface capture_u0_3, id 0 0000 a2 76 f2 00 00 ic 00 17 df d6 ec 00 81 00 00 cf ····································		26 2022-08-04 08:18:24.578900897	192.168.247.100	192.168.247.102	ICMP	118	0x60aa (24746)	255 Echo (ping) request	id=0x007b,	seq=12/3072, ttl=255 (no response found!)
b Frame 2: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface capture_u0_3, id 0 0000 a2 76 f2 00 00 1c 00 17 df d6 ec 00 81 00 00 cf b Ethernet III, Src: Clsco d6:ec:00 (00:17:df:d6:ec:00), Dst: a2:76:f2:00:00:1c (a2:76:f2:00:00:1c) 0000 a2 76 f2 00 00 1c 00 17 df d6 ec 00 81 00 00 cf 802.10 Virtual LAN, PRI: 0, DEI: 0, ID: 207 000 0000 111 = ID: 207 000 <		27 2022-08-04 08:18:24.579426962	192.168.247.100	192.168.247.102	ICMP	128	0x60ab (24747)	255 Echo (ping) request	id=0x007b,	seq=13/3328, ttl=255 (no response found!)
>> Frame 2: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface capture_u0_3, id 0 >> fthermet II, Src: Cisco dise::00 (00:17:df:doi:ec:00), Dst: a2:76:f2:00:00:1c (a2:76:f2:00:00:1c) >> 00:00 a2 76 f2 00 00 1c 00 17 df d6 ec 00 81 00 00 cf >> 00:00 a2 76 f2 00 00 1c 00 17 df d6 ec 00 81 00 00 cf >> 00:00 a2 76 f2 00 00 1c 00 17 df d6 ec 00 81 00 00 cf >> 00:00 a2 6 f2 00 00 1c 00 17 df d6 ec 00 81 00 00 cf >> 00:00 a2 6 f2 00 00 1c 00 17 df d6 ec 00 80 00 66 d0 00 00 00 00 ef >> 00:00 a2 6 f2 00 00 1c 00 17 df d6 ec 00 80 00 66 d0 00 00 00 00 ef >> 00:00 a2 6 f2 00 00 1c 00 17 df d6 ec 00 00 00 00 ef >> 00:00 a2 6 f2 00 00 1c 00 17 df d6 ec 00 80 00 66 d0 00 00 00 ef >> 00:00 a2 da bc da	<									
Ethernet II, Sr:: Clsco d5:ec:00 (00:17:df:d5:ec:00), Dst: a2:76:f2:00:00:1C (a2:76:f2:00:00:1C) 0010 08 00 45 00 00 64 60 9e 000 00 ff 01 ea dd c0 a8 -E-d'	> En	ame 2: 118 hytes on wire (944 hits)	118 bytes cant	uned (944 hits) on	nterface cant	une ue a	id 0		a2 76 f2 g	0 00 1c 00 17 df d6 ec 00 81 00 00 cf
802.10 Virtual LAN, PRI: 0, DEI: 0, ID: 207 0020 67 64 c0 a8 77 66 08 00 es 60 00 00 00 edf. -(> Et	hernet II. Src: Cisco d6:ec:00 (00:	17:df:d6:ec:00).	Dst: a2:76:f2:00:0	1:1c (a2:76:f2	:00:00:1	c)	0010	08 00 45 0	00 00 64 60 9e 00 00 ff 01 ea dd c0 a8 ··E··d`· ·····
000 Priority: Best Effort (default) (0)	80	2.10 Virtual LAN, PRI: 0. DEL: 0. I	D: 207				- /	0020	f7 64 c0 a	18 f7 66 08 00 e5 c8 00 7b 00 00 00 00 00 .df{
DEI: Ineligible 0000 1100 1111 = 10: 207 Turo:		000 Priority: Res	st Effort (defaul	t) (0)				0030	00 02 4d s	ic 4a 78 ab cd ab cd ab cd ab cd ab cd ··M·Jx······
0000 1100 1111 = ID: 207 1100 2		= DEI: Ineligi	le	() (0)				0040	ab cd ab c	d ab cd ab cd ab cd ab cd ab cd ab cd ······
Type: TBut (dyped)		0000 1100 1111 = ID: 207			2			0050	ab cd ab c	dabcdabcd abcdabcdabcdabcd · · · · · · · · · · · · · · · · · · ·
		Type: TPv4 (0x0800)			4			0060	ab cd ab c	d ab cd ab cd ab cd ab cd ab cd ab cd
Difference Protocol Version 4, Src: 192.168.247.100, Dst: 192.168.247.102	TO	ternet Protocol Version 4. Src: 192	.168.247.100. Dst	: 192.168.247.102				0070	ab cd ab c	d ab cd
Internet Control Message Protocol	In	ternet Control Message Protocol								
	1									

説明

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

- •ポートVLANタグの挿入後。
- VNタグの挿入後。

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

タスクの要約を次の表に示します。

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

パケット キャプチャ フィルタ

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

トポロジ、パケットフロー、およびキャプチャポイント



コンフィギュレーション

FCM

ホスト192.0.2.100からホスト198.51.100.100へのICMPエコー要求パケットのキャプチャフィル タを設定し、インターフェイスEthernet1/2のパケットキャプチャに適用するには、FCMで次の手 順を実行します。
- 1. [Tools] > [Packet Capture] > [Filter List] > [Add Filter] を使用して、キャプチャフィルタを作成します。
- 2. [Filter Name]、[Protocol]、[Source IPv4]、[Destination IPv4] を指定し、[Save] をクリックします。

Capture Session	niter List	scunty Engine Mat	orm Settings	_	_	_	_		_	_	_	System Tools	Help admin
Filter List													idd Filter
Filter Name		From	10-6			То	The f	Prot	Protocol	Inner vlan	Outer vian	EtherType	
filter_icmp	00:00:00:00:00:00	192.0.2.100	11	0	00:00:00:00:00:00	192.0.2.100		0	1	0	0	0	/8
				Edit Packet Filter Name* Protocol EtherType Inner vlan Source IPr4 IPr6 Port NAC	Filer	Outer vian Destnation IPv4 IPv6 Port MAC	0 196.51.100.100 11 0 00:00:00:00:00:00:00 Save	© 8					

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

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

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

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 Ethernet1/2 Buffer Size 256 MB Snap length: 1518 Store Packets OvernumRe
Ethernet1/3 FTD Ethernet1/10	Capture Filter Apply Filter Capture All Adoly. Another. Filter Create Filter Apply Filter_kmp Y To Ethernet1/2 Y
Ethemet1/1	

FXOS CLI

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

実行します。

1. アプリケーションのタイプと識別子を特定します。

firepower# scope ssa firepower /ssa# show app-instance App Name Identifier Slot ID Admin State Oper State Running Version Startup Version Deploy Type Turbo Mode Profile Name Cluster State Cluster Role _____ ____ _____ ____ ftd1 ftd 1 Enabled Online 7.2.0.82 7.2.0.82 Native No Not Applicable None 2. https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtmlでIPプロトコル番 号を特定します。この場合、ICMPプロトコル番号は1です。

3.キャプチャセッションを作成します。

2. firepower# scope packet-capture firepower /packet-capture # create filter filter_icmp firepower /packet-capture/filter* # set destip 198.51.100.100 firepower /packet-capture/filter* # set protocol 1 firepower /packet-capture/filter* # set srcip 192.0.2.100 firepower /packet-capture/filter* # exit firepower /packet-capture* # create session cap1 firepower /packet-capture/session* # create phy-port Ethernet1/2 firepower /packet-capture/session/phy-port* # set app ftd firepower /packet-capture/session/phy-port* # set app-identifier ftd1 firepower /packet-capture/session/phy-port* # set filter filter_icmp firepower /packet-capture/session/phy-port* # exit firepower /packet-capture/session* # enable firepower /packet-capture/session* # commit firepower /packet-capture/session # 確認

FCM

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

Overview Inter	faces Logical Devices S	ecurity Engine Plat	form Settings									System Tools	Help admin
Canture Session	Filter List												
Filter List												A	dd Filter
		From				То							_
Filter Name	мас	IPv4	IPv6	Port	MAC	IPv4	IPv6	Port	Protocol	Inner vlan	Outer vlan	EtherType	
filter_icmp	00:00:00:00:00:00	192.0.2.100		0	00:00:00:00:00:00	198.51.100.100		0	1	0	0	0	/ 5

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

Overview	Interfaces	Logical Devices Se	ecurity Engine	Platform Settings					System Tools He	lp admin
Capture S	ession Filter L	ist								
								C Refresh Capture Session	Delete All Sessions	
•	cap1	Dro	p Count: 0		Operational State: up	1	Buffer Size: 256 MB	Snap Length: 1518 Bytes		8 2
Interface	Name	Filter		File Size (in bytes)	File Name	Device Name				
Ethernet1/	2	filter_icmp		84340	cap1-ethernet-1-2-0.pcap	fid1	¥			

scope packet-captureでキャプチャの詳細を確認します。

firepower# scope packet-capture firepower /packet-capture # show filter detail Configure a filter for packet capture: Name: filter_icmp Protocol: 1 Ivlan: 0 Ovlan: 0 Src Ip: 192.0.2.100 Dest Ip: 198.51.100.100 Src MAC: 00:00:00:00:00:00 Dest MAC: 00:00:00:00:00:00 Src Port: 0 Dest Port: 0 Ethertype: 0 Src Ipv6: :: Dest Ipv6: :: firepower /packet-capture # show session cap1 Traffic Monitoring Session: Packet Capture Session Name: cap1 Session: 1 Admin State: Enabled Oper State: Up Oper State Reason: Active Config Success: Yes Config Fail Reason: Append Flag: Overwrite Session Mem Usage: 256 MB Session Pcap Snap Len: 1518 Bytes Error Code: 0 Drop Count: 0 Physical ports involved in Packet Capture: Slot Id: 1 Port Id: 2 Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap Pcapsize: 213784 bytes Filter: filter_icmp Sub Interface: 0 Application Instance Identifier: ftd1 Application Name: ftd キャプチャファイルの収集

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

ファイル分析のキャプチャ

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

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

4. 内部スイッチは、追加のVNタグを挿入します。

No	o. Time	Source	Destination	Protocol	Length	IP ID	19 T	TL Info					^
Г	1 2022-08-02 15:46:55.603277760	192.0.2.100	198.51.100.100	ICMP	108 -	0x0012 (:	18) (64 Echo (ping) request	id=0x0018,	seq=349/23809,	ttl=64 (n	or
	2 2022-08-02 15:46:55.603279688	192.0.2.100	198.51.100.100	ICMP	102	0x0012 (:	18)	64 Echo (ping) request	id=0x0018,	seq=349/23809,	ttl=64 (n	or
	3 2022-08-02 15:46:56.627139252	192.0.2.100	198.51.100.100	ICMP	108	0x00db (219)	64 Echo (ping) request	id=0x0018,	seq=350/24065,	ttl=64 (n	or
	4 2022-08-02 15:46:56.627140919	192.0.2.100	198.51.100.100	ICMP	102	0x00db ()	219)	64 Echo (ping) request	id=0x0018,	seq=350/24065,	ttl=64 (n	or
	5 2022-08-02 15:46:57.651185193	192.0.2.100	198.51.100.100	ICMP	108	0x01cb (4	459)	64 Echo (ping) request	id=0x0018,	seq=351/24321,	ttl=64 (n	or
	6 2022-08-02 15:46:57.651186787	192.0.2.100	198.51.100.100	ICMP	102	0x01cb (4	459)	64 Echo (ping) request	id=0x0018,	seq=351/24321,	ttl=64 (n	or
	7 2022-08-02 15:46:58.675153317	192.0.2.100	198.51.100.100	ICMP	108	0x01d6 (4	470)	64 Echo (ping) request	id=0x0018,	seq=352/24577,	ttl=64 (n	or
	8 2022-08-02 15:46:58.675154503	192.0.2.100	198.51.100.100	ICMP	102	0x01d6 (4	470)	64 Echo (ping) request	id=0x0018,	seg=352/24577,	ttl=64 (n	or
	9 2022-08-02 15:46:59.699152639	192.0.2.100	198.51.100.100	ICMP	108	0x01f4 (500)	64 Echo (ping) request	id=0x0018,	seg=353/24833,	ttl=64 (n	or
	10 2022-08-02 15:46:59.699153835	192.0.2.100	198.51.100.100	ICMP	102	0x01f4 (500)	64 Echo (ping) request	id=0x0018,	seg=353/24833,	ttl=64 (n	or
	11 2022-08-02 15:47:00.723142641	192.0.2.100	198.51.100.100	ICMP	108	0x01f9 (505)	64 Echo (ping) request	id=0x0018,	seg=354/25089,	ttl=64 (n	or
	12 2022-08-02 15:47:00.723144643	192.0.2.100	198.51.100.100	ICMP	102	0x01f9 (505)	64 Echo (ping) request	id=0x0018,	seg=354/25089,	ttl=64 (n	or
	13 2022-08-02 15:47:01.747162204	192.0.2.100	198,51,100,100	ICMP	108	0x026e (622)	64 Echo (pine) request	id=0x0018.	seg=355/25345.	ttl=64 (n	or
	14 2022-08-02 15:47:01.747163783	192.0.2.100	198,51,100,100	ICMP	102	0x026e (622)	64 Echo (pine) request	id=0x0018.	seg=355/25345.	ttl=64 (n	or
	15 2022-08-02 15:47:02.771209952	192.0.2.100	198,51,100,100	TCMP	108	0x02bc (700)	64 Echo (pine) request	id=0x0018.	seg=356/25601.	ttl=64 (n	or
	16 2022-08-02 15:47:02.771211062	192.0.2.100	198,51,100,100	TCMP	102	0x02bc (700)	64 Echo (pine) request	id=0x0018.	seg=356/25601.	ttl=64 (n	or
	17 2022-08-02 15:47:03.772258550	192.0.2.100	198,51,100,100	ICMP	108	0x032f (815)	54 Echo (pine) request	id=0x0018.	seq=357/25857.	ttl=64 (n	or
	18 2022-08-02 15:47:03.772259724	192.0.2.100	198,51,100,100	ICMP	102	0x032f (815)	54 Echo (pine) request	id=0x0018.	seq=357/25857.	ttl=64 (n	or
	19 2022-08-02 15:47:04 791118519	192.0.2.100	198.51.100.100	TCMP	102	exeasef (1039)	64 Echo (ping) request	id=0x0018,	seq=358/26113	ttl=64 (n	
	20 2022-08-02 15:47:04 791110515	192.0.2.100	198.51.100.100	TCMP	102	exerter (1039)	64 Echo (ping) request	id=0x0018,	seq=358/26113	ttl=64 (n	
1	20 2022-00-02 1514/1041/51115/21	152.0.2.100	190.91.100.100	10.4	102	0,0401 (.	10337	of Leno (prife	/ request	10-040010,	364-330/20113,	(in	, <u> </u>
È													-
>	Frame 1: 108 bytes on wire (864 bi	ts), 108 bytes ca	ptured (864 bits) c	n interface	capture_u0_	1, 1 0000	58 97 bd I	09 77 0e 00 9	0 56 9d 0	28 be 89 26	80 0a X…w…	P V &	
>	Ethernet II, Src: VMware 9d:e8:be	(00:50:56:9d:e8:t	e), Dst: Cisco b9:7	7:0e (58:97:	bd:b9:77:0e) 0010	00 00 81 0	00 00 66 08 0	45 00 0	0 54 00 12	40 00 ·····	d Jdd Jd	.
Ň	VN-Tag					0020	0 00 18 01	5d e2 46 e9 6	2 66 66 6	00 00 01 06	96 07 grint	h	
	1	= Direct	ion: From Bridge			0040	00 00 00 00	0 10 11 12 1	3 14 15 1	6 17 18 19	1a 1b		
	.0	= Pointe	r: v1t_1d			0050	1c 1d 1e :	If 20 21 22 3	3 24 25 2	26 27 28 29	2a 2b ···· !"	# \$%&'()"+	
		= Destin	ation: 10			0060	2c 2d 2e 3	2f 30 31 32 3	3 34 35 3	36 37	,/012	3 4567	
	0 0	= Looped	: No 4										
		= Reserv	ed: Ø										
		= Versio	n: 0										
	0000 00	300 0000 = Source	: 0										
	Type: 802.1Q Virtual LAN (0x810	3)		_									
~	802.1Q Virtual LAN, PRI: 0, DEI: 0	, ID: 102											
	000 = Priority:	Best Effort (def	ault) (0) 🗧										
	0 = DEI: Inel:	igible	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		2										
L													
1													
<						>							

2番目のパケットを選択し、キーポイントを確認します。

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

N	o. Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info						^
ſ	- 1 2022-08-02 15:46:55.603277760	192.0.2.100	198.51.100.100	ICMP	108 1	0x0012 (18)	64 Echo (p:	ing) request	id=0x0018,	seq=349/23809,	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 (p)	ing) request	id=0x0018,	seq=349/23809,	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 (p:	ing) request	id=0x0018,	seq=350/24065,	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 (p:	ing) request	id=0x0018,	seq=350/24065,	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 (p:	ing) request	id=0x0018,	seq=351/24321,	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 (p:	ing) request	id=0x0018,	seq=351/24321,	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 (p:	ing) request	id=0x0018,	seq=352/24577,	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 (p:	ing) request	id=0x0018,	seq=352/24577,	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 (p:	ing) request	id=0x0018,	seq=353/24833,	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 (p:	ing) request	id=0x0018,	seq=353/24833,	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 (p:	ing) request	id=0x0018,	seq=354/25089,	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 (p	ing) request	id=0x0018,	seq=354/25089,	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 (p	ing) request	id=0x0018,	seq=355/25345,	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 (p:	ing) request	id=0x0018,	seq=355/25345,	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 (p:	ing) request	id=0x0018,	seq=356/25601,	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 (p:	ing) request	id=0x0018,	seq=356/25601,	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 (p:	ing) request	id=0x0018,	seq=357/25857,	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 (p:	ing) request	id=0x0018,	seq=357/25857,	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 (p:	ing) request	id=0x0018,	seq=358/26113,	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 (p:	ing) request	id=0x0018,	seq=358/26113,	ttl=64 (no r	~
<												>	
5	Frame 2: 102 bytes on wire (816 bi	ts), 102 bytes ca	optured (816 bits) o	n interface ca	pture u0 1	, it 0000 58	97 bd b9 77 Øe Ø	050569de	8 be 81 00 0	0 66 X···w··	P V · · · · ·	٠f	_
5	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	0010 08	00 45 00 00 54 0	0 12 40 00 4	10 01 4d 9b c	0 00 ··E··T·	· @.@.M.		
~	802.10 Virtual LAN, PRI: 0, DEI: 0	, ID: 102				0020 02	64 c6 33 64 64 0	800 9e670	90 18 01 5d e	2 46 ·d·3dd·	· .g]	- F	
	000 = Priority:	Best Effort (def	ault) (0)			0030 e9	62 00 00 00 00 c	1 a6 0c 00 0	00 00 00 00 1	0 11 ·b·····			
L	0 = DEI: Ineli	gible	3			0040 12	13 14 15 16 17 1	8 19 1a 1b 1	lc 1d 1e 1f 2	0 21		1	
	0000 0110 0110 = ID: 102					0050 22	23 24 25 26 27 2	8292a2b2	2c 2d 2e 2f 3	0 31 "#\$%&'() *+,/(91	
	Type: IPv4 (0x0800)					0060 32	55 54 55 36 37			234567			
>	Internet Protocol Version 4, Src:	192.0.2.100, Dst:	198.51.100.100										
>	Internet Control Message Protocol		2										

説明

前面インターフェイスでパケットキャプチャが設定されると、スイッチは各パケットを同時に2回 キャプチャします。 •ポートVLANタグの挿入後。

• VNタグの挿入後。

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

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

タスクの要約を次の表に示します。

タスク	キャプ チャポ イント	キャプチャされたパ ケットの内部ポート VLAN	方向	ユーザフィル タ	キャプチャされたトラフィ
前面インターフェイ スEthernet1/2のフ ィルタを使用してパ ケットキャプチャを 設定および確認しま す	Etherne t1/2	102	入力の み	プロトコル :ICMP Source:192.0.2 .100 送信先 :198.51.100.10 0	ホスト192.0.2.100からホス 198.51.100.100へのICMPエ 要求

Firepower 4100/9300内部スイッチキャプチャファイルの収集

FCM

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

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

Overview Interfaces Logi	cal Devices Security Engine	Platform Settings			System To	ols Help admin
Capture Session Filter List						
					Capture Session Delete Al Ses	sions
ap1	Drop Count: 0	Operational State: up	Buffer Size: 256 MB		Snap Length: 1518 Bytes	9.8.2
Interface Name	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 T	ools Help admin
Capture Session Fiter Lis	t					
					C Refresh Capture Session Delete Al Se	ssions
			-			
Cap1	Drop Count: 0	Operational State: DOWN - Session_Admin_Shut	Buffer Size: 256 MB		Snap Length: 1518 Bytes	201
Interface Name	Filter	File Size (in bytes)	File Name	Device Name		
Ethernet1/2	None	218828	cap1-ethemet-1-2-0.pcap	ftd1	上	

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 Plat	form Settings			System Tools Help admin
Capture Session Fiter List					
				C Refresh Capture :	Session Delete Al Sessions
a D cap1	Drop Count: 0 Op	erational State: DOWN - Session_Admin_Shut	Buffer Size: 256 MB	Snap Length: 1518 E	Bytes 🥒 🗉 🔯
Interface Name	Filter	File Size (in bytes)	File Name	Device Name	
Ethernet1/2	None	218828	cap1-ethemet-1-2-0.pcap	ftd1	Ł
Commetayz	Hone	210020	caha-ameniar-a-s-oiheab		2

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

FXOS CLI

キャプチャファイルを収集するには、FXOS CLIで次の手順を実行します。

1. アクティブなキャプチャを停止します。

```
firepower# scope packet-capture
firepower /packet-capture # scope session cap1
firepower /packet-capture/session # disable
firepower /packet-capture/session* # commit
firepower /packet-capture/session # up
firepower /packet-capture # show session cap1 detail
Traffic Monitoring Session:
  Packet Capture Session Name: cap1
  Session: 1
   Admin State: Disabled
   Oper State: Down
   Oper State Reason: Admin Disable
  Config Success: Yes
  Config Fail Reason:
  Append Flag: Overwrite
  Session Mem Usage: 256 MB
  Session Pcap Snap Len: 1518 Bytes
  Error Code: 0
  Drop Count: 0
Physical ports involved in Packet Capture:
  Slot Id: 1
  Port Id: 2
  Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap
  Pcapsize: 115744 bytes
  Filter:
  Sub Interface: 0
  Application Instance Identifier: ftd1
  Application Name: ftd
  2. local-mgmtコマンドスコープからキャプチャファイルをアップロードします。
```

firepower# connect local-mgmt

firepower(local-mgmt)# copy /packet-capture/session-1/cap1-ethernet-1-2-0.pcap ? ftp: Dest File URI Dest File URI http: Dest File URI https: Dest File URI scp: sftp: Dest File URI Dest File URI tftp: usbdrive: Dest File URI volatile: Dest File URI workspace: Dest File URI

firepower(local-mgmt)# copy /packet-capture/session-1/cap1-ethernet-1-2-0.pcap ftp://ftpuser@10.10.10.1/cap1-ethernet-1-2-0.pcap Password: ポートチャネルインターフェイスの場合は、各メンバーインターフェイスのキャプチャファイル

ホートナャネルインダーノェイスの場合は、各メンハーインダーノェイスのキャノナャノアイル をコピーします。

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

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

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

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

の設定と検証 Secure Firewall 3100

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

次に、switchオプションを指定したcaptureコマンドを示します。

> capture cap_sw switch ?

buffer	Configure size of capture buffer, default is 256MB
ethernet-type	Capture Ethernet packets of a particular type, default is IF
interface	Capture packets on a specific interface
ivlan	Inner Vlan
match	Capture packets based on match criteria

ovlan	Outer Vlan
packet-length	Configure maximum length to save from each packet, default is
	64 bytes
real-time	Display captured packets in real-time. Warning: using this
	option with a slow console connection may result in an
	excessive amount of non-displayed packets due to performance
	limitations.
stop	Stop packet capture
trace	Trace the captured packets
type	Capture packets based on a particular type
<cr></cr>	

パケットキャプチャ設定の一般的な手順は次のとおりです。

1. 入力インターフェイスを指定します。

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

> capture capsw switch interface ?

Available interfaces to listen: in_data_uplink1 Capture packets on internal data uplink1 interface

in_mgmt_uplink1 Capture packets on internal mgmt uplink1 interface

inside Name of interface Ethernet1/1.205

management Name of interface Management1/1

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

```
> capture capsw switch interface inside ethernet-type ?
802.1Q
<0-65535> Ethernet type
arp
ip
ip6
pppoed
pppoes
rarp
sgt
vlan
3. 一致条件を指定します。capture matchオプションは、一致基準を指定します。
```

> capture capsw switch interface inside match ?

<0-255> Enter protocol number (0 - 255) ah eigrp esp gre icmp icmp6 igmp igrp ip ipinip ipsec Mac-address filter mac nos ospf рср

pim pptp sctp snp spi SPI value tcp udp <cr>

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

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

6. キャプチャの詳細を確認します。

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

> show capture capsw
27 packet captured on disk using switch capture
Reading of capture file from disk is not supported

>show capture capsw	detail
Packet Capture info	
Name:	capsw
Session:	1
Admin State:	enabled
Oper State:	up
Oper State Reason:	Active
Config Success:	yes
Config Fail Reason:	
Append Flag:	overwrite
Session Mem Usage:	256
Session Pcap Snap I	Jen: 1518
Error Code:	0
Drop Count:	0
Total Physical ports	involved in Packet Capture: 1
Physical port:	
Slot Id:	1
Port Id:	1
Pcapfile:	/mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize:	18838
Filter:	capsw-1-1
Packet Capture Filte	er Info
Name:	capsw-1-1
Protocol:	0
T1	

Protocol:	0
Ivlan:	0
Ovlan:	205
Src Ip:	0.0.0.0

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

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

7. 必要に応じてキャプチャを停止します。

```
> capture capsw switch stop
>show capture capsw detail
Packet Capture info
 Name:
                    capsw
                   1
Session:
 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
                   capsw-1-1
Name:
Protocol:
                   0
                  0
Tvlan:
Ovlan:
                  205
                   0.0.0.0
Src Ip:
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
                   0
Src Port:
Dest Port:
                   0
Ethertype:
                   0
Total Physical breakout ports involved in Packet Capture: 0
0 packet captured on disk using switch capture
Reading of capture file from disk is not supported
```

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

バージョン7.2では、内部スイッチのキャプチャ設定はFMCまたはFDMではサポートされていま せん。ASAソフトウェアバージョン9.18(1)以降の場合、内部スイッチキャプチャはASDMバージ ョン7.18.1.x以降で設定できます。

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

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

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



トポロジ、パケットフロー、およびキャプチャポイント

コンフィギュレーション

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

1. nameifを確認します。

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

> show nameif		
Interface	Name	Security
Port-channel1	inside	0
Ethernet1/2	outside	0
Management1/1	diagnostic	0
· · · ·		

2. キャプチャセッションを作成します。

> capture capsw switch interface inside
 3. キャプチャセッションを有効にします。

> no capture capsw switch stop 確認

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

> show capture capsw detail Packet Capture info Name: capsw 1 Session: enabled Admin State: 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 0 Error Code: Drop Count: 0

Total Physical ports involved in Packet Capture: 1

Physical port:	
Slot Id:	1
Port Id:	1
Pcapfile:	/mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize:	12653
Filter:	capsw-1-1

Packet Capture Filter Info Name: capsw-1-1 Protocol: 0 0 Ivlan: Ovlan: 0 0.0.0.0 Src Ip: Dest Ip: 0.0.0.0 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: Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

79 packets captured on disk using switch capture

Reading of capture file from disk is not supported ポートチャネル1の場合、キャプチャはすべてのメンバーインターフェイスで設定されます。

> show capture cap	sw detail
Packet Capture inf	0
Name:	capsw
Session:	1
Admin State:	enabled
Oper State:	up
Oper State Reaso	n: Active
Config Success:	yes
Config Fail Reaso	n:
Append Flag:	overwrite
Session Mem Usage	: 256
Session Pcap Snap	Len: 1518
Error Code:	0
Drop Count:	0
Total Physical por	ts 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 Fil	ter Info
Name:	capsw-1-4
Protocol:	0
Ivlan:	0
Ovlan:	0
Src Ip:	0.0.0
Dest Ip:	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
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 Fil	ter Info
Name:	capsw-1-3
Protocol:	0
Ivlan:	0
Ovlan:	0
Src Ip:	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

56 packet captured on disk using switch capture

Reading of capture file from disk is not supported ポートチャネルメンバーインターフェイスは、FXOSのlocal-mgmtコマンドシェルでshow portchannel summary コマンドを使用して確認できます。

> connect fxos KSEC-FPR3100-1 connect local-mgmt KSEC-FPR3100-1(local-mgmt) show portchannel summary Flags: D - Down P - Up in port-channel (members) I - Individual H - Hot-standby (LACP only) s - Suspended r - Module-removed S - Switched R - Routed U - Up (port-channel) M - Not in use. Min-links not met _____ Protocol Member Ports Group Port-Type Channel _____ Pol(U) Eth LACP Eth1/3(P) Eth1/4(P) 1 LACP KeepAlive Timer: _____ Channel PeerKeepAliveTimerFast _____ Po1(U) False 1 Cluster LACP Status: _____ Channel ClusterSpanned ClusterDetach ClusterUnitID ClusterSysID _____ Po1(U) False False 0 1 clust ASAのFXOSにアクセスするには、connect fxos adminコマンドを実行します。マルチコンテキス トの場合は、管理コンテキストでコマンドを実行します。

キャプチャファイルの収集

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

ファイル分析のキャプチャ

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

1. ICMPエコー要求パケットだけがキャプチャされます。

2. 元のパケットヘッダーにはVLANタグが付いていません。

No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info	^
F	1 2022-08-07 19:50:06.925768	192.0.2.100	198.51.100.100	ICMP	102	0x9a10 (39440)	64 Echo (ping) request	id=0x0034, seq=1/256, ttl=64 (no res
	2 2022-08-07 19:50:07.921684	192.0.2.100	198.51.100.100	ICMP	102	0x9a3a (39482)	64 Echo (ping) request	id=0x0034, seq=2/512, ttl=64 (no res
	3 2022-08-07 19:50:08.924468	192.0.2.100	198.51.100.100	ICMP	102	0x9aa6 (39590)	64 Echo (ping) request	id=0x0034, seq=3/768, ttl=64 (no res
	4 2022-08-07 19:50:09.928484	192.0.2.100	198.51.100.100	ICMP	102	0x9afe (39678)	64 Echo (ping) request	id=0x0034, seq=4/1024, ttl=64 (no r€
	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 r€
	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 r€
	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 r€
	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 r€
	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 r€
	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 🗸
<								>
> En	ame 1: 102 bytes on wire (816 bits)	, 102 bytes capt	ured (816 bits)			0000 bc e7 12	34 9a 14 00 50 56 9d e8	be 08 00 45 00 ···4···P V····E·
> Et!	nernet II, Src: VMware 9d:e8:be (00	:50:56:9d:e8:be)	, Dst: Cisco 34:9a:	14 (bc:e7:12:3	84:9a:14)	0010 00 54 9a	10 40 00 40 01 b3 9c c0	00 02 64 c6 33 ·T··@·@· ·····d·3
> Int	ternet Protocol Version 4, Src: 192	.0.2.100, Dst: 1	98.51.100.100		2	0020 64 64 08	00 c6 91 00 34 00 01 61	17 f0 62 00 00 dd4ab
> Int	ternet Control Message Protocol				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 2t 30	31 32 33 34 35 & ()*+,/012345
						0000 36 37 55	22 22 22	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VI ANタグが付いていません。

					2.2	12 4 4	0.01		,							
No	Time		Source	Destination	Protocol	Length	IP ID		IP TTL Info							^
ſ	1 2022-08-07 2	0:40:58.657533	192.0.2.100	198.51.100.100	ICMP	102	0x9296	(37526)	64 Echo	(ping)	request	id=0x0035,	seq=1/256,	ttl=64 (nd	o nes	
	2 2022-08-07 2	0:40:59.658611	192.0.2.100	198.51.100.100	ICMP	102	0x9370	(37744)	64 Echo	(ping)	request	id=0x0035,	seq=2/512,	ttl=64 (nd	o res	
	3 2022-08-07 2	0:41:00.655662	192.0.2.100	198.51.100.100	ICMP	102	0x93f0	(37872)	64 Echo	(ping)	request	id=0x0035,	seq=3/768,	ttl=64 (nd	o res	
	4 2022-08-07 2	0:41:01.659749	192.0.2.100	198.51.100.100	ICMP	102	0x946f	(37999)	64 Echo	(ping)	request	id=0x0035,	seq=4/1024,	ttl=64 (r	no re	
	5 2022-08-07 2	0:41:02.660624	192.0.2.100	198.51.100.100	ICMP	102	0x94a4	(38052)	64 Echo	(ping)	request	id=0x0035,	seq=5/1280,	ttl=64 (r	no re	
	6 2022-08-07 2	0:41:03.663226	192.0.2.100	198.51.100.100	ICMP	102	0x952d	(38189)	64 Echo	(ping)	request	id=0x0035,	seq=6/1536,	ttl=64 (r	no re	
	7 2022-08-07 2	0:41:04.661262	192.0.2.100	198.51.100.100	ICMP	102	0x958d	(38285)	64 Echo	(ping)	request	id=0x0035,	seq=7/1792,	ttl=64 (r	no re	
	8 2022-08-07 2	0:41:05.665955	192.0.2.100	198.51.100.100	ICMP	102	0x95d8	(38360)	64 Echo	(ping)	request	id=0x0035,	seq=8/2048,	ttl=64 (r	no re	
	9 2022-08-07 2	0:41:06.666538	192.0.2.100	198.51.100.100	ICMP	102	0x964b	(38475)	64 Echo	(ping)	request	id=0x0035,	seq=9/2304,	ttl=64 (r	no re	
	10 2022-08-07 2	0:41:07.667298	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 2	0:41:08.670540	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 2	0:41:09.668278	192.0.2.100	198.51.100.100	ICMP	102	Øx9831	(38961)	64 Echo	(ping)	request	id=0x0035,	seq=12/3072	, ttl=64 ((no r	
	13 2022-08-07 2	0:41:10.672417	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 2	0:41:11.671369	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 2	0:41:12.675462	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 2	0:41:13.674903	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 2	0:41:14.674093	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 2	0:41:15.676904	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	~
<															>	
>	Frame 1: 102 bytes	on wire (816 bit	ts), 102 bytes cap	tured (816 bits)			0000	bc e7 1	2 34 9a 2c (0 50 5	6 9d e8	be 08 00 45	004.,	·P V·····	E٠	
>	Ethernet II, Src: \	VMware 9d:e8:be ((00:50:56:9d:e8:be), Dst: Cisco 34:9a:	2c (bc:e	7:12:34:9a:2c)	0010	00 54 9	2 96 40 00	10 01 b	b 16 c0	00 02 64 c6	33 ·T··@·	@· ····d	- 3	
>	Internet Protocol V	Version 4, Src: 1	192.0.2.100, Dst:	198.51.100.100		-	0020	64 64 0	8 00 58 a8 0	30 35 6	0 01 4d	23 f0 62 00	00 dd · · X	·5 · · M# · b		
>	Internet Control Me	essage Protocol				2	0030	00 00 9	e c8 04 00 0	00 00	0 00 10	11 12 13 14	15			
		0					0040	16 17 1	8 19 1a 1b	lc 1d 1	e 1f 20	21 22 23 24	25		\$%	
							0050	26 27 2	8 29 2a 2b 3	2c 2d 2	e 2f 30	31 32 33 34	35 & ()*4	,/0123	45	
							0060	36 37 5	5 55 55 55				670000	1		
-																

説明

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

タスクの要約を次の表に示します。

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

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



トポロジ、パケットフロー、およびキャプチャポイント

コンフィギュレーション

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

1. nameifを確認します。

<pre>> show nameif</pre>					
Interface	Name	Security			
Ethernet1/1.205	inside	0			
Ethernet1/2	outside	0			
Management1/1	diagnostic	0			
> show nameif					
Interface	Name	Security			
Port-channel1.205	inside	0			
Ethernet1/2	outside	0			
Management1/1	diagnostic	0			
2. キャプチャセッションを作成します。					

> capture capsw switch interface inside
 3. キャプチャセッションを有効にします。

> no capture capsw switch stop 確認

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

> show capture capsw detail Packet Capture info Name: capsw 1 Session: enabled Admin State: Oper State: up Oper State Reason: Active Config Success: yes Config Fail Reason: Append Flag: overwrite Session Mem Usage: 256 Session Pcap Snap Len: 1518 Error Code: 0 Drop Count: 0

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id:	1
Port Id:	1
Pcapfile:	/mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize:	6360
Filter:	capsw-1-1

Packet Capture Filter Info

Name:	capsw-1-1
Protocol:	0
Ivlan:	0
Ovlan:	205
Src Ip:	0.0.0.0
Dest Ip:	0.0.0.0
Src Ipv6:	::
Dest Ipv6:	::
Src MAC:	00:00:00:00:00:00
Dest MAC:	00:00:00:00:00:00
Src Port:	0
Dest Port:	0
Ethertype:	0

Total Physical breakout ports involved in Packet Capture: 0

46 packets captured on disk using switch capture

Reading of capture file from disk is not supported この場合、外部VLAN Ovlan=205のフィルタが作成され、インターフェイスに適用されます。

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

> show capture capsw	/ detail
Packet Capture info	
Name:	capsw
Session:	1
Admin State:	enabled
Oper State:	up
Oper State Reason:	Active
Config Success:	yes
Config Fail Reason:	
Append Flag:	overwrite
Session Mem Usage:	256
Session Pcap Snap I	en: 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 Filte	er Info
Name:	capsw-1-4
Protocol:	0
Ivlan:	0
Ovlan:	205
Src Ip:	0.0.0.0
Dest Ip:	0.0.0.0
Src Ipv6:	::
Dest Ipv6:	::
Src MAC:	00:00:00:00:00
Dest MAC:	00:00:00:00:00:00
Src Port:	0
Dest Port:	0
Ethertype:	0
Physical port:	
Slot Id:	1
Port Id:	3
Pcapfile:	/mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-3-0.pcap
Pcapsize:	5600
Filter:	capsw-1-3
Packet Capture Filte	er Info
Name:	capsw-1-3
Protocol:	0
Ivlan:	0
Ovlan:	205
Src Ip:	0.0.0.0
Dest Ip:	0.0.0.0
Src Ipv6:	::
Dest Ipv6:	::
Src MAC:	00:00:00:00:00
Dest MAC:	00:00:00:00:00
Src Port:	0
Dest Port:	0
Ethertype:	0

Total Physical breakout ports involved in Packet Capture: $\boldsymbol{0}$

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。

> cor	nnect fxo	S						
KSEC-	-FPR3100-	1 connect local	-mgmt					
KSEC-	-FPR3100-	1(local-mgmt) s	now port	channel	summa	ry		
Flags	s: D - D	own P - U	Jp in pc	ort-chann	el (m	embers)		
I - 1	Individua	l H - Hot-stand	dby (LAC	P only)				
s - \$	Suspended	r - Module-re	emoved					
s - s	Switched	R - Routed						
U - U	Jp (port-	channel)						
M - 1	Not in us	e. Min-links not	t met					
Grou <u>r</u>	Port-	Туре Ра	rotocol	Member	Ports			
	Channel							
1	Pol(U)	Eth Li	ACP	Eth1/3(P)	Eth1/4(P)		
LACP	KeepAliv	e Timer:						
	Channel	PeerKeepAliveT:	imerFast					
1	Po1(U)	False						
Clust	er LACP	Status:						
	Channel	ClusterSpanned	Cluste	rDetach	Clus	terUnitID	ClusterSysID	
1	Po1(U)	False	Fal	se	0		clust	 + → → □

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

キャプチャファイルの収集

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

ファイル分析のキャプチャ

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

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

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 r€	
	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	~
<								>	
>	Frame 1: 106 bytes on wire (848 bits	;), 106 bytes car	otured (848 bits)			0000 bc e7	12 34 9a 14 00 50 56 9d e8	be 81 00 00 cd ···4···P V·····	_
>	Ethernet II, Src: VMware_9d:e8:be (0	00:50:56:9d:e8:be	e), Dst: Cisco_34:9a	:14 (bc:e7:	12:34:9a:14)	0010 08 00	45 00 00 54 41 1f 40 00 40	01 0c 8e c0 00 ··E··TA·@·@·····	
\sim	802.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 205				0020 02 64	c6 33 64 64 08 00 06 67 00	37 00 01 b0 2c ·d·3dd·· ·g·7···,	
	000 Beriority: Be	est Effort (defa	ult) (0)			0030 f0 62	00 00 00 00 8e fe 03 00 00	00 00 00 10 11 ·b·····	
	0 = DEI: Inelig	ible				0040 12 13	14 15 16 17 18 19 1a 1b 1c	1d 1e 1f 20 21	
	0000 1100 1101 = ID: 205				2	0050 22 23	24 25 26 27 28 29 28 20 20	20 20 27 30 31 #\$4& () -+,/01	
	Type: IPv4 (0x0800)				2	0000 32 33	34 33 30 37 33 33 33 33	25456700 00	
	Trailer: 55555555								
>	Internet Protocol Version 4, Src: 19	2.0.2.100, Dst:	198.51.100.100						
>	Internet Control Message Protocol								
1.7									

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	こはVLANタグ 20 5	5が付いていま	ミす。
-----------	-------	----------------------	---------	-----

No.	Time	Source	Destination	Protocol	Length	IP ID		IP TTL Info							^
Г	1 2022-08-07 21:21:01.607187	192.0.2.100	198.51.100.100	ICMP	106	0x411f	(16671)	64 Ech	o (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 Ech	o (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 Ech	o (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 Ech	o (ping)	request	id=0x0037,	seq=4/1024,	ttl=64	(no re	
	5 2022-08-07 21:21:05.609409	192.0.2.100	198.51.100.100	ICMP	106	0x4310	(17168)	64 Ech	o (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 Ech	o (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 Ech	o (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 Ech	o (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 Ech	o (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 Ech	o (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 Ech	o (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 Ech	o (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 Ech	o (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 Ech	o (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 Ech	o (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 Ech	o (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 Ech	o (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 Ech	o (ping)	request	id=0x0037,	seq=18/4608	, ttl=64	(no r	~
<														>	
>	Frame 1: 106 bytes on wire (848 bits)	, 106 bytes capt	ured (848 bits)			0000	bc e7	12 34 9a 14	00 50	56 9d e8	be 81 00 00	cd4.	·P V····		
>	Ethernet II, Src: VMware 9d:e8:be (00):50:56:9d:e8:be)	, Dst: Cisco 34:9a:	14 (bc:e7:12:3	4:9a:14)	0010	08 00	45 00 00 54	41 1f	40 00 40	01 0c 8e c0	00 ··E··T	A. 0.0.		
\sim	802.10 Virtual LAN, PRI: 0, DEI: 0, 1	ID: 205	-			0020	02 64	c6 33 64 64	08 00	06 67 00	37 00 01 b0	2c · d · 3dc	1 ·g·7·	···,	
LĽ	000 = Priority: Be	st Effort (defau)	lt) (0)			0030	f0 62 (00 00 00 00	8e fe	03 00 00	00 00 00 10	11 ·b····	•• ••••		
	0 = DEI: Ineligible					0040	12 13	14 15 16 17	18 19	1a 1b 1c	1d 1e 1f 20	21			
	0000 1100 1101 = ID: 205					0050	22 23	24 25 26 27	28 29	2a 2b 2c	2d 2e 2f 30	31 "#\$%&	() *+,	/01	
	Type: IPv4 (0x0800) 2					0000	32 33	34 35 36 37	55 55	55 55		234567	00 00		
	Trailer: 55555555														
>	Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100														
>	Internet Control Message Protocol														
1 4															

説明

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

タスクの要約を次の表に示します。

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

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

内部インターフェイスでのパケットキャプチャ

セキュアファイアウォールには、2つの内部インターフェイスがあります。

• in_data_uplink1:アプリケーションを内部スイッチに接続します。

in_mgmt_uplink1:管理インターフェイスへのSSHなど、管理接続用の専用パケットパス、またはFMCとFTD間の管理接続(sftunnelとも呼ばれる)を提供します。

タスク1

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

トポロジ、パケットフロー、およびキャプチャポイント



コンフィギュレーション

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

1. キャプチャセッションを作成します。

capture capsw switch interface in_data_uplink1
 2. キャプチャセッションを有効にします。

> no capture capsw switch stop 確認

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

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 L	en: 1518
Error Code:	0
Drop Count:	0
Total Physical ports	involved in Packet Capture: 1
Physical port:	
Slot Id:	1
Port Id:	18
Pcapfile:	/mnt/disk0/packet-capture/sess-1-capsw-data-uplink1.pcap
Pcapsize:	7704
Filter:	capsw-1-18
Packet Capture Filte	r 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
Dest MAC:	00:00:00:00:00:00
Src Port:	0
Dest Port:	0
Ethertype:	0

Total Physical breakout ports involved in Packet Capture: 0

66 packets captured on disk using switch capture

Reading of capture file from disk is not supported

この場合、キャプチャは内部ID 18(セキュアファイアウォール3130のin_data_uplink1インターフ ェイス)を持つインターフェイスで作成されます。FXOS local-mgmtコマンドシェルのshow portmanager switch statusコマンドは、インターフェイスIDを示します。

> connect fxos

•••			
KSEC-FPR3100-1	connect	local-mgmt	

KSEC-FPR3100-1(local-mgmt) show portmanager switch status

Dev/Port	Mode	Link	Speed	Duplex	Loopback Mode	Port Manager
0/1	SGMII	Up	1G	Full	None	Link-Up
0/2	SGMII	Up	1G	Full	None	Link-Up
0/3	SGMII	Up	1G	Full	None	Link-Up
0/4	SGMII	Up	1G	Full	None	Link-Up
0/5	SGMII	Down	1G	Half	None	Mac-Link-Down
0/6	SGMII	Down	1G	Half	None	Mac-Link-Down
0/7	SGMII	Down	1G	Half	None	Mac-Link-Down
0/8	SGMII	Down	1G	Half	None	Mac-Link-Down
0/9	1000_BaseX	Down	1G	Full	None	Link-Down
0/10	1000_BaseX	Down	1G	Full	None	Link-Down

0/11	1000_BaseX	Down	1G	Full	None	Link-Down
0/12	1000_BaseX	Down	1G	Full	None	Link-Down
0/13	1000_BaseX	Down	1G	Full	None	Link-Down
0/14	1000_BaseX	Down	1G	Full	None	Link-Down
0/15	1000_BaseX	Down	1G	Full	None	Link-Down
0/16	1000_BaseX	Down	1G	Full	None	Link-Down
0/17	1000_BaseX	Up	1G	Full	None	Link-Up
0/18	KR2	Up	50G	Full	None	Link-Up
0/19	KR	Up	25G	Full	None	Link-Up
0/20	KR	Up	25G	Full	None	Link-Up
0/21	KR4	Down	40G	Full	None	Link-Down
0/22	n/a	Down	n/a	Full	N/A	Reset
0/23	n/a	Down	n/a	Full	N/A	Reset
0/24	n/a	Down	n/a	Full	N/A	Reset
0/25	1000_BaseX	Down	1G	Full	None	Link-Down
0/26	n/a	Down	n/a	Full	N/A	Reset
0/27	n/a	Down	n/a	Full	N/A	Reset
0/28	n/a	Down	n/a	Full	N/A	Reset
0/29	1000_BaseX	Down	1G	Full	None	Link-Down
0/30	n/a	Down	n/a	Full	N/A	Reset
0/31	n/a	Down	n/a	Full	N/A	Reset
0/32	n/a	Down	n/a	Full	N/A	Reset
0/33	1000_BaseX	Down	1G	Full	None	Link-Down
0/34	n/a	Down	n/a	Full	N/A	Reset
0/35	n/a	Down	n/a	Full	N/A	Reset
0/36	n/a	Down	n/a	Full	N/A	Reset

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

キャプチャファイルの収集

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

ファイル分析のキャプチャ

パケットキャプチャファイルリーダーアプリケーションを使用して、インターフェイス in_data_uplink1のキャプチャファイルを開きます。キーポイントを確認します。この場合、 ICMPエコー要求パケットとエコー応答パケットがキャプチャされます。これらは、アプリケーションから内部スイッチに送信されるパケットです。

No.	Time	4	Source	Destination	Protocol	Length	IP ID		IP T	TL Info							^
	1 2022-08-07 22:40:06.685606	4	192.0.2.100	198.51.100.100	ICMP	102	0x4d93	(19859)		64 Echo	(ping)	request	id=0x003a,	seq=33/8448,	ttl=64	(repl	
4-	2 2022-08-07 22:40:06.685615		198.51.100.100	192.0.2.100	ICMP	102	0x6cdc	(27868)		64 Echo	(ping)	reply	id=0x003a,	seq=33/8448,	ttl=64	(requ	
	3 2022-08-07 22:40:07.684219		192.0.2.100	198.51.100.100	ICMP	102	Øx4de8	(19944)		64 EChO	(ping)	request	id=0x003a,	seq=34/8704,	ttl=64	(repl	
	4 2022-08-07 22:40:07.689300		198.51.100.100	192.0.2.100	ICMP	102	Øx6db2	(28082)		64 Echo	(ping)	reply	id=0x003a,	seq=34/8704,	ttl=64	(requ	
	5 2022-08-07 22:40:08.685736		192.0.2.100	198.51.100.100	ICMP	102	Øx4edc	(20188)		64 Echo	(ping)	request	id=0x003a,	seq=35/8960,	ttl=64	(repl	
	6 2022-08-07 22:40:08.690806		198.51.100.100	192.0.2.100	ICMP	102	Øx6dbf	(28095)		64 Echo	(ping)	reply	id=0x003a,	seq=35/8960,	ttl=64	(requ	
	7 2022-08-07 22:40:09.690737		192.0.2.100	198.51.100.100	ICMP	102	0x4f2d	(20269)		64 Echo	(ping)	request	id=0x003a,	seq=36/9216,	ttl=64	(repl	
	8 2022-08-07 22:40:09.690744		198.51.100.100	192.0.2.100	ICMP	102	0x6e80	(28288)		64 Echo	(ping)	reply	id=0x003a,	seq=36/9216,	ttl=64	(requ	
	9 2022-08-07 22:40:10.692266		192.0.2.100	198.51.100.100	ICMP	102	0x4fb1	(20401)		64 Echo	(ping)	request	id=0x003a,	seq=37/9472,	ttl=64	(repl	
	10 2022-08-07 22:40:10.692272		198.51.100.100	192.0.2.100	ICMP	102	Øx6ed5	(28373)		64 Echo	(ping)	reply	id=0x003a,	seq=37/9472,	ttl=64	(requ	
	11 2022-08-07 22:40:11.691159		192.0.2.100	198.51.100.100	ICMP	102	0x5008	(20488)		64 Echo	(ping)	request	id=0x003a,	seq=38/9728,	ttl=64	(repl	
	12 2022-08-07 22:40:11.691166		198.51.100.100	192.0.2.100	ICMP	102	0x6f3b	(28475)		64 Echo	(ping)	reply	id=0x003a,	seq=38/9728,	ttl=64	(requ	
	13 2022-08-07 22:40:12.692135		192.0.2.100	198.51.100.100	ICMP	102	0x50b8	(20664)		64 Echo	(ping)	request	id=0x003a,	seq=39/9984,	ttl=64	(repl	
	14 2022-08-07 22:40:12.697209		198.51.100.100	192.0.2.100	ICMP	102	0x6fd7	(28631)		64 Echo	(ping)	reply	id=0x003a,	seq=39/9984,	ttl=64	(requ	
	15 2022-08-07 22:40:13.697320		192.0.2.100	198.51.100.100	ICMP	102	0x5184	(20868)		64 Echo	(ping)	request	id=0x003a,	seq=40/10240	, ttl=64	(rep	
	16 2022-08-07 22:40:13.697327		198.51.100.100	192.0.2.100	ICMP	102	0x703e	(28734)		64 Echo	(ping)	reply	id=0x003a,	seq=40/10240	, ttl=64	(rec	
	17 2022-08-07 22:40:14.698512		192.0.2.100	198.51.100.100	ICMP	102	0x51d8	(20952)		64 Echo	(ping)	request	id=0x003a,	seq=41/10496	, ttl=64	(rep	
	18 2022-08-07 22:40:14.698518		198.51.100.100	192.0.2.100	ICMP	102	0x70dd	(28893)		64 Echo	(ping)	reply	id=0x003a,	seq=41/10496	, ttl=64	(rec	~
<																>	
> Fr	ame 1: 102 bytes on wire (816 bit	s)	, 102 bytes captu	ured (816 bits)			0000	00 50 5	6 9d	e7 50 b	oc e7	12 34 9a	15 08 00 45	00 - PV - P	4	E ·	
> Et	hernet II, Src: Cisco 34:9a:15 (b	oc : (e7:12:34:9a:15),	Dst: VMware 9d:e7:	50 (00:50:56:9	d:e7:50)	0010	00 54 4	d 93	40 00 4	10 01	00 1a c0	00 02 64 c6	33 ·TM·@·(3	1-3	
> In	ternet Protocol Version 4, Src: 1	192	.0.2.100, Dst: 19	98.51.100.100			0020	64 64 0	8 00	7f 15	30 3a	00 21 39	3f f0 62 00	00 dd	- 197-b)	
> In	ternet Control Message Protocol						0030	00 00 8	b 1a	05 00 0	99 99	00 00 10	11 12 13 14	15			
	0						0040	16 17 1	8 19	1a 1b 1	lc 1d	1e 1f 20	21 22 23 24	25	·· ·· 174	#\$%	
							0050	26 27 2	8 29	2a 2b 2	2c 2d	2e 2f 30	31 32 33 34	35 &'()*+,	/0123	45	
							0060	36 37 5	5 55	55 55				670000			

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

タスクの要約を次の表に示します。

キャプチ 内部フィ タスク 方向 キャプチャされたトラフィック ャポイン ルタ ホスト192.0.2.100からホスト アップリンクインターフェイス in_data_uplink1でパケットキャプチャを in_data_u なし 198.51.100.100へのICMPエコー 入力のみ ホスト198.51.100.100からホスト plink1 設定および確認する 192.0.2.100へのICMPエコー応答

タスク 2

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

トポロジ、パケットフロー、およびキャプチャポイント



コンフィギュレーション

インターフェイスin_mgmt_uplink1でパケットキャプチャを設定するには、ASAまたはFTD CLIで 次の手順を実行します。

1. キャプチャセッションを作成します。

capture capsw switch interface in_mgmt_uplink1
 2. キャプチャセッションを有効にします。

> no capture capsw switch stop

確認

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

> show capture cap	osw detail
Packet Capture inf	lo
Name:	capsw
Session:	1
Admin State:	enabled
Oper State:	up
Oper State Reaso	on: Active
Config Success:	yes
Config Fail Reaso	on:
Append Flag:	overwrite
Session Mem Usage	256
Session Pcap Snap) Len: 1518
Error Code:	0
Drop Count:	0
Total Physical por Physical port:	ts involved in Packet Capture: 1
Slot Id:	1
Port Id:	19
Pcapfile:	/mnt/disk0/packet-capture/sess-1-capsw-mgmt-uplink1.pcap
Pcapsize:	137248
Filter:	capsw-1-19
Packet Capture Fil	ter Info
Name:	capsw-1-19
Protocol:	0
Ivlan:	0
Ovlan:	0
Src Ip:	0.0.0.0
Dest Ip:	0.0.0.0
Src Ipv6:	::
Dest Ipv6:	::
Src MAC:	00:00:00:00:00
Dest MAC:	00:00:00:00:00
Src Port:	0

Total Physical breakout ports involved in Packet Capture: 0

281 packets captured on disk using switch capture

0 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上で作成されます。この内部ID 19は 、セキュアファイアウォール3130上のin_mgmt_uplink1インターフェイスです。FXOS localmgmt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。

> connect fxos

Dest Port:

Ethertype:

KSEC-FPR3100-1 connect local-mgmt

KSEC-FPR3100-1(local-mgmt) show portmanager switch status

Dev/Port	Mode	Link	Speed	Duplex	Loopback Mode	Port Manager
0/1	SGMII	Up	1G	Full	None	Link-Up
0/2	SGMII	Up	1G	Full	None	Link-Up
0/3	SGMII	Up	1G	Full	None	Link-Up
0/4	SGMII	Up	1G	Full	None	Link-Up
0/5	SGMII	Down	1G	Half	None	Mac-Link-Down

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

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

キャプチャファイルの収集

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

ファイル分析のキャプチャ

パケットキャプチャファイルリーダーアプリケーションを使用して、インターフェイス in_mgmt_uplink1のキャプチャファイルを開きます。キーポイントを確認します。この場合、管理 IPアドレス192.0.2.200からのパケットのみが表示されます。例としては、SSH、Sftunnel、 ICMPエコー応答パケットなどがあります。これらは、アプリケーション管理インターフェイスか ら内部スイッチ経由でネットワークに送信されるパケットです。

No.	Time	Source	Destination	Protocol	Length	IP ID		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	0xb7d2	(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	0xb7d6	(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	0xb7d7	(47063)	64 39181 → 8305 [ACK] Seq=69004 Ack=967 Win=1384 Len=0 TSval
	218 2022-08-07 23:21:52.030118	192.0.2.200	192.0.2.100	ICMP	78	0xbf02	(48898)	64 Echo (ping) reply id=0x0001, seq=4545/49425, ttl=64
	219 2022-08-07 23:21:53.042744	192.0.2.200	192.0.2.100	ICMP	78	0xbf59	(48985)	64 Echo (ping) reply id=0x0001, seq=4546/49681, ttl=64
	220 2022-08-07 23:21:53.073144	192.0.2.200	192.0.2.100	SSH	170	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
	225 2022 00 07 22.21.55 126700	102 0 2 200	102 0 2 100	TCMD	70	Avhfc1	(10000)	Aa-1++ CO102/0626-000 100000-bi vinon (min) oda 14
<								,
>	Frame 1: 747 bytes on wire (5976 bits	s), 747 bytes cap	tured (5976 bi	ts)		0000	a4 53 0e	11 38 2a bc e7 12 34 9a 00 08 00 45 00 ·S··8*·· ·4····E·
>	Ethernet II, Src: Cisco_34:9a:00 (bc:	e7:12:34:9a:00),	Dst: Cisco_11	:38:2a (a4:53:0e:11:	:38:2a)	0010	02 d9 4a	3d 40 00 40 06 68 b4 c0 00 02 c8 c0 00 ···J=@·@·h·····
>	Internet Protocol Version 4, Src: 192	2.0.2.200, Dst: 1	92.0.2.101			0020	02 65 20	71 e6 05 67 10 2a c5 d0 e3 60 d4 80 18 ·e q··g· ····K···
>	Transmission Control Protocol, Src Po	ort: 8305, Dst Po	rt: 58885, Seq	: 1, Ack: 1, Len: 67	77	0030	10 14 27 3d 41 17	02 03 02 20 22 62 01 00 06 70 95 7T 91 02
>	Transport Layer Security					0050	07 40 75	19 a4 d5 df 64 d8 fe 66 8e 9b cc 8d 2f $\cdot \theta u \cdot \cdot \cdot d \cdot f \cdot \cdot \cdot /$
						0060	92 b2 1a	64 e7 20 36 03 8e 48 02 5a 7c 85 30 d4 ···d· 6· ·H·Z ·0·
						0070	fa c0 a8	56 b8 ad a7 7e 19 3a c1 9c 4b 57 0e e0 ···V···~ ·:··KW··
						0080	be ef 95	22 84 c1 c1 9d 9f 24 78 b4 15 1c 44 0e ···"···· ·\$x···D·
						0090	ea cb 43	9e 1f fd a7 70 75 e5 6b a4 f8 2b ee 47 ···C····p u·k··+·G
						00a0	2f 86 73	8f b1 e1 b5 c6 57 e3 a8 46 0e cb 26 b7 /·s···· W··F··&·
						00b0	5b c7 e3	09 54 f3 c1 ff 26 d9 87 ea 51 3d 20 08 [···T··· &···Q= ·
						0000	16 †đ cb	T5 4T 91 98 5e 86 15 17 55 68 6t 5d 04 ····O··^ ···Uho]·

説明

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

タスクの要約を次の表に示します。

タスク	キャプチ ャポイン ト	内部フ ィルタ	方向	キャプチャされたトラフィック
管理アップリンク インターフェイス でのパケットキャ プチャの設定と確 認	in_mgmt_ uplink1	なし	入力のみ (管理インターフェイ スから内部スイッチを 介してネットワークへ)	FTD管理IPアドレス192.0.2.200からホス 192.0.2.100へのICMPエコー応答 Ftd管理IPアドレス192.0.2.200からFMC ドレス192.0.2.101へのSFTUNNEL FTD管理IPアドレス192.0.2.200からホス 192.0.2.100へのSSH

パケット キャプチャ フィルタ

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

コンフィギュレーション

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

1. nameifを確認します。

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

2. ARPまたはICMPのキャプチャセッションを作成します。

> capture capsw switch interface inside ethernet-type arp

> capture capsw switch interface inside match icmp 198.51.100.100 確認

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

> show capture capsw detail Packet Capture info Name: capsw Session: 1 Admin State: disabled down Oper State: 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 /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap Pcapfile: Pcapsize: 0 Filter: capsw-1-1 Packet Capture Filter Info Name: capsw-1-1 Protocol: 0 0 Ivlan: Ovlan: 0 0.0.0.0 Src Ip: 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 Dest Port: 0 2054 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 これは、ICMPのフィルタの検証です。IPプロトコル1はICMPです。

> show capture capsw detail

Packet Capture info	
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 I	Len: 1518
Error Code:	0
Drop Count:	0

Total Physical ports involved in Packet Capture: 1

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

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

0 packets captured on disk using switch capture

Reading of capture file from disk is not supported

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

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

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

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

平均応答時間

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

1. キャプチャを停止します。

asa# capture capsw switch stop

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

```
asa# show capture capsw detail
Packet Capture info
Name:
                  capsw
Session:
                  1
                 disabled
Admin State:
 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
                 0
Ovlan:
                 0.0.0.0
Src Ip:
                 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
Dest Port:
                  0
Ethertype:
                  0
Total Physical breakout ports involved in Packet Capture: 0
886 packets captured on disk using switch capture
Reading of capture file from disk is not supported

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

asa# copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap ?
cluster: Copy to cluster: file system
disk0: Copy to disk0: file system

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

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

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

1. 診断CLIに移動します。

> system support diagnostic-cli
Attaching to Diagnostic CLI ... Click 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower> enable Password: <-- Enter firepower# 2. キャプチャを停止します。

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

firepower# show capture capsw detail Packet Capture info Name: capsw Session: 1 Admin State: disabled Oper State: down Oper State Reason: Session_Admin_Shut Config Success: yes Config Fail Reason: Append Flag: overwrite Session Mem Usage: 256 Session Pcap Snap Len: 1518 Error Code: 0 Drop Count: 0 Total Physical ports involved in Packet Capture: 1 Physical port: Slot Id: 1 Port Id: 1 Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap 139826 Pcapsize: Filter: capsw-1-1

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

Total Physical breakout ports involved in Packet Capture: 0

886 packets captured on disk using switch capture

Reading of capture file from disk is not supported

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

```
firepower# copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap ?
cluster:
                Copy to cluster: file system
disk0:
                Copy to disk0: file system
disk1:
                Copy to disk1: file system
flash:
                Copy to flash: file system
                Copy to ftp: file system
ftp:
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
                Copy to system: file system
system:
tftp:
                Copy to tftp: file system
```

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

139826 bytes copied in 0.532 secs

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

1. キャプチャを停止します。

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

> show capture capsw detail Packet Capture info Name: capsw Session: 1 Admin State: disabled Oper State: down Oper State Reason: Session_Admin_Shut Config Success: yes Config Fail Reason: Append Flag: overwrite

Session Mem Usage: 256 Session Pcap Snap Len: 1518 Error Code: 0 Drop Count: 0 Total Physical ports involved in Packet Capture: 1 Physical port: Slot Id: 1 Port Id: 1 Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap Pcapsize: 139826 Filter: capsw-1-1 Packet Capture Filter Info capsw-1-1 Name: 0 Protocol: Ivlan: 0 Ovlan: 0 Src Ip: 0.0.0.0 0.0.0.0 Dest Ip: Src Ipv6: :: Dest Ipv6: :: 00:00:00:00:00:00 Src MAC: Dest MAC: 00:00:00:00:00:00 0 Src Port: Dest Port: 0 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

3. エキスパートモードに移行し、ルートモードに切り替えます。

> expert
admin@firepower:~\$ sudo su
root@firepower:/home/admin

4. キャプチャファイルを/ngfw/var/common/:

root@KSEC-FPR3100-1:/home/admin cp /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
/ngfw/var/common/
root@KSEC-FPR3100-1:/home/admin 1s -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] を選択します。



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

Firewall Management Center Devices / Troubleshoot / File Download	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy Q 🤣 🌣 🙆 lab_domain \ admin 🔻 🔤
		Device FPR3100- File sess-1-ca	l psw-ethernet	v -1-1-0.pcap			Threat Defense CLI Packet Capture Packet Tracer
				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」が表示されます。
- アクティブなスイッチキャプチャは削除できません。
- アプリケーションでスイッチキャプチャを読み取ることができません。ユーザはファイルを エクスポートする必要があります。
- dump、decode、packet-number、traceなどの特定のデータプレーンキャプチャオプションは、スイッチキャプチャではサポートされていません。
- マルチコンテキストASAの場合、データインターフェイスのスイッチキャプチャはユーザコンテキストで設定されます。in_data_uplink1およびin_mgmt_uplink1インターフェイスでのスイッチキャプチャは、管理コンテキストでのみサポートされます。

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

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

関連情報

- Firepower 4100/9300シャーシマネージャおよびFXOS CLIコンフィギュレーションガイド
- <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。