Sichere Firewall- und FirePOWER-interne Switch-Erfassung konfigurieren und überprüfen

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Allgemeiner Überblick über die Systemarchitektur Allgemeiner Überblick über den internen Switch-Betrieb Paketfluss und Erfassungspunkte Konfiguration und Verifizierung für Firepower 4100/9300 Paketerfassung an einer physischen oder Port-Channel-Schnittstelle Paketerfassung an Backplane-Schnittstellen Paketerfassung auf Anwendungs- und Anwendungs-Ports Paketerfassung auf einer Subschnittstelle einer physischen oder Port-Channel-Schnittstelle Paketerfassungsfilter Sammeln von FirePOWER 4100/9300-internen Switch-Erfassungsdateien Richtlinien, Einschränkungen und Best Practices für die interne Switch-Paketerfassung Konfiguration und Verifizierung auf einer sicheren Firewall 3100 Paketerfassung an einer physischen oder Port-Channel-Schnittstelle Paketerfassung auf einer Subschnittstelle einer physischen oder Port-Channel-Schnittstelle Paketerfassung an internen Schnittstellen Paketerfassungsfilter Erfassen von Dateien für den internen Secure Firewall 3100-Switch Richtlinien, Einschränkungen und Best Practices für die interne Switch-Paketerfassung Zugehörige Informationen

Einleitung

In diesem Dokument werden die Konfiguration und Verifizierung der FirePOWER und der interne Switch für die sichere Firewall beschrieben.

Voraussetzungen

Anforderungen

Grundlegendes Produktwissen, Erfassungsanalyse

Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Sichere 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
- Adaptive Security Appliance (ASA) 9.18(1)x
- Adaptive Security Appliance Device Manager (ASDM) 7.18.1.x
- Wireshark 3.6.7 (https://www.wireshark.org/download.html)

Hintergrundinformationen

Allgemeiner Überblick über die Systemarchitektur

Aus Sicht des Paketflusses kann die Architektur der Firepower 4100/9300 und der Secure Firewall 3100 wie in der folgenden Abbildung dargestellt dargestellt werden:



Das Gehäuse umfasst folgende Komponenten:

 Interner Switch - Leitet Pakete vom Netzwerk an die Anwendung weiter und umgekehrt. Der interne Switch wird mit den Frontschnittstellen verbunden, die sich auf dem integrierten Schnittstellenmodul oder externen Netzwerkmodulen befinden und mit externen Geräten, z. B. Switches, verbunden werden. Beispiele für Schnittstellen an der Vorderseite sind Ethernet 1/1, Ethernet 2/4 usw. "Front" ist keine starke technische Definition. In diesem Dokument werden Schnittstellen, die mit externen Geräten verbunden sind, von den Backplane- oder Uplink-Schnittstellen unterschieden.

 Backplane oder Uplink - eine interne Schnittstelle, die das Sicherheitsmodul (SM) mit dem internen Switch verbindet. Diese Tabelle zeigt die Backplane-Schnittstellen f
ür Firepower 4100/9300 und die Uplink-Schnittstelle f
ür Secure Firewall 3100:

Plattform	Anzahl unterstützter Sicherheitsmodule	Backplane/Uplink- Schnittstellen	Anwendungsschn en
Firepower 4100 (außer Firepower 4110/4112)	1	SM1: Ethernet1/9 Ethernet 1/10	Interne Daten0/0 Interne Daten0/1
FirePOWER 4110/4112	1	Ethernet1/9	Interne Daten0/0
FirePOWER 9300	3	SM1: Ethernet1/9 Ethernet 1/10 SM2: Ethernet 1/11 Ethernet 1/12 SM3: Ethernet 1/13 Ethernet 1/14	Interne Daten0/0 Interne Daten0/1 Interne Daten0/0 Interne Daten0/1 Interne Daten0/0 Interne Daten0/1
Sichere Firewall 3100	1	SM1: in_data_uplink1	Interne Daten0/1

Bei zwei Backplane-Schnittstellen pro Modul führen der interne Switch und die Anwendungen auf den Modulen Datenverkehr-Load-Balancing über die beiden Schnittstellen durch.

- Sicherheitsmodul, Security Engine oder Blade das Modul, in dem Anwendungen wie FTD oder ASA installiert sind. Firepower 9300 unterstützt bis zu drei Sicherheitsmodule.
- Zugeordnete Anwendungsschnittstelle Anwendungen wie FTD oder ASA ordnen die Backplane- oder Uplink-Schnittstellen internen Schnittstellen zu. Mit anderen Worten: Die Backplane- oder Uplink-Schnittstellen sind in Anwendungen als interne Schnittstellen sichtbar.

Verwenden Sie den Befehl show interface detail, um interne Schnittstellen zu überprüfen:

```
> 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

Allgemeiner Überblick über den internen Switch-Betrieb

FirePOWER 4100/9300

Zur Weiterleitungsentscheidung verwendet der interne Switch einen Schnittstellen-VLAN-Tag oder Port-VLAN-Tag und einen virtuellen Netzwerk-Tag (VN-Tag).

Das Port-VLAN-Tag wird vom internen Switch verwendet, um eine Schnittstelle zu identifizieren. Der Switch fügt den Port-VLAN-Tag in jedes Eingangspaket ein, das an den Frontschnittstellen empfangen wurde. Der VLAN-Tag wird automatisch vom System konfiguriert und kann nicht manuell geändert werden. Der Tag-Wert kann in der **fxos-**Befehlsshell überprüft werden:

```
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
```

Der VN-Tag wird ebenfalls vom internen Switch eingefügt und für die Weiterleitung der Pakete an die Anwendung verwendet. Es wird automatisch vom System konfiguriert und kann nicht manuell geändert werden.

Das Port-VLAN-Tag und das VN-Tag werden gemeinsam mit der Anwendung genutzt. Die Anwendung fügt die jeweiligen VLAN-Tags für die Ausgangsschnittstelle und die VN-Tags in jedes Paket ein. Wenn ein Paket von der Anwendung vom internen Switch an den Backplane-Schnittstellen empfangen wird, liest der Switch den VLAN-Tag der Ausgangsschnittstelle und den VN-Tag, identifiziert die Anwendung und die Ausgangsschnittstelle, entfernt den VLAN-Tag des Ports und den VN-Tag und leitet das Paket an das Netzwerk weiter.

Sichere Firewall 3100

Wie bei Firepower 4100/9300 wird das Port-VLAN-Tag vom internen Switch verwendet, um eine Schnittstelle zu identifizieren.

Das Port-VLAN-Tag wird mit der Anwendung gemeinsam genutzt. Die Anwendung fügt die entsprechenden VLAN-Tags für die Ausgangsschnittstelle in jedes Paket ein. Wenn ein Paket von der Anwendung vom internen Switch der Uplink-Schnittstelle empfangen wird, liest der Switch den VLAN-Tag der Ausgangsschnittstelle, identifiziert die Ausgangsschnittstelle, entfernt den VLAN-Tag des Ports und leitet das Paket an das Netzwerk weiter.

Paketfluss und Erfassungspunkte

Die Firepower 4100/9300 und die Secure Firewall 3100 unterstützen die Paketerfassung an den Schnittstellen des internen Switches.

Diese Abbildung zeigt die Paketerfassungspunkte entlang des Paketpfads innerhalb des Chassis und der Anwendung:



Die wichtigsten Punkte sind:

- 1. Eingangs-Erfassungspunkt an der Vorderseite des internen Switches. Eine Front-Schnittstelle ist jede Schnittstelle, die mit den Peer-Geräten wie Switches verbunden ist.
- 2. Eingangs-Erfassungspunkt der Datenebenenschnittstelle
- 3. Snort Capture Point
- 4. Ausgangspunkt der Datenebenenschnittstelle
- 5. Interner Eingangs-Erfassungspunkt an der Backplane oder dem Uplink des Switches Eine Backplane- oder Uplink-Schnittstelle verbindet den internen Switch mit der Anwendung.

Der interne Switch unterstützt nur Eingangs-Schnittstellenerfassungen. Das heißt, dass nur die

Pakete erfasst werden können, die vom Netzwerk oder von der ASA-/FTD-Anwendung empfangen wurden. Egress-Paketerfassungen werden nicht unterstützt.

Konfiguration und Verifizierung auf FirePOWER 4100/9300

Die FirePOWER 4100/9300-internen Switch-Erfassungen können unter **Tools > Packet Capture** auf FCM oder im **Bereich Packet-Capture** in FXOS CLI konfiguriert werden. Eine Beschreibung der Optionen zur Paketerfassung finden Sie im *Konfigurationsleitfaden für Cisco Firepower 4100/9300 FXOS Chassis Manager* oder im *Konfigurationsleitfaden für Cisco Firepower 4100/9300 FXOS CLI*, Kapitel **Fehlerbehebung**, Abschnitt **Paketerfassung**.

Diese Szenarien beziehen sich auf häufige Anwendungsfälle von FirePOWER 4100/9300-internen Switch-Erfassungen.

Paketerfassung an einer physischen oder Port-Channel-Schnittstelle

Verwenden Sie den FCM und die CLI, um eine Paketerfassung an der Schnittstelle Ethernet1/2 oder Port-Channel1 zu konfigurieren und zu überprüfen. Bei einer Port-Channel-Schnittstelle müssen Sie alle physischen Mitglieds-Schnittstellen auswählen.



Topologie, Paketfluss und Erfassungspunkte

Konfiguration

Befolgen Sie die folgenden Schritte auf FCM, um eine Paketerfassung an den Schnittstellen Ethernet1/2 oder Port-Channel1 zu konfigurieren:

1. Verwenden Sie **Tools > Packet Capture > Capture Session**, um eine neue Erfassungssitzung zu erstellen:

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

2. Wählen Sie die Schnittstelle **Ethernet1/2 aus**, geben Sie den Sitzungsnamen an, und klicken Sie auf **Save and Run**, um die Erfassung zu aktivieren:

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	
Etherneti/2	Buffer Size 256 MB	
Ethernet1/3	Store Packets Overwrite Append	
Ethernet1/1 FTD Ethernet1/10	Capture Filter Apply Filter Capture All	
Ethernet1/5 (Portchannel1)		
Ethernet1/4 (Portchannel1)		

3. Wählen Sie bei einer Port-Channel-Schnittstelle alle physischen Member-Schnittstellen aus, geben Sie den Sitzungsnamen an, und klicken Sie auf **Save and Run**, um die Erfassung zu aktivieren:

Overview Interfaces Logical Devices Security Engine Platform Settings				f	System Tools Help admin
Select an instance: ftd1 v			Save and Run	Save Cano	d
ftd1	Session Name* Selected Interfaces	cap1 Ethernet1/S, Ethernet1/4			
Ehernet/2	Buffer Size	256 MB			
Ethernet1/3	Store Packets	Overwrite Append			
Ethernet1/1 Ethernet1/10	Capture Filter	Apply Filter Capture All			
Etherset//5 Cortchannels					
Ethernet1/4 (Portchannel1)					

FXOS-CLI

Führen Sie die folgenden Schritte auf der FXOS-CLI aus, um eine Paketerfassung an den Schnittstellen Ethernet1/2 oder Port-Channel1 zu konfigurieren:

1. Identifizieren Sie den Anwendungstyp und die Kennung:

firepower#	scope ssa					
firepower /	ssa # show	app-instanc	e			
App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version
Deploy Type	e Turbo Mode	e Profile Na	me Cluster S	State Cluster Ro	ole	
ftd	ftd1	1	Enabled	Online	7.2.0.82	7.2.0.82
Native	No		Not Appli	icable None		

2. Geben Sie bei einer Port-Channel-Schnittstelle deren Mitgliedsschnittstellen an:

firepower# connect fxos <output skipped=""></output>									
<pre>firepower(fxos)# show port-channel summary</pre>									
Flags: D - Down P - Up in port-channel (members)									
I - Individual H - Hot-standby (LACP only)									
s - Suspended r - Module-removed									
S - Switched R - Routed									
U - Up (port-channel)									
M - Not in use. Min-links not met									
Group Port- Type Protocol Member Ports Channel									
1 Pol(SU) Eth LACP Eth1/4(P) Eth1/5(P) 3. Eine Aufzeichnungssitzung erstellen:									

firepower# scope packet-capture
firepower /packet-capture # create session cap1
<pre>firepower /packet-capture/session* # create phy-port Eth1/2</pre>
firepower /packet-capture/session/phy-port* # set app ftd
<pre>firepower /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 #
Für Port-Channel-Schnittstellen wird eine separate Erfassung für jede M

Fur Port-Channel-Schnittstellen wird eine separate Erfassung für jede Member-Schnittstelle konfiguriert:

```
firepower# scope packet-capture
firepower /packet-capture # create session cap1
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # set app-identifier ftd1
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # enable
firepower /packet-capture/session* # commit
firepower /packet-capture/session # Commit
firepower /p
```

FCM

Überprüfen Sie den Schnittstellennamen, stellen Sie sicher, dass der Betriebsstatus aktiv ist und

dass die Dateigröße (in Byte) ansteigt:

	Overview	Interfaces	Logical Devices	Security Engine	Platform	Settings					System	Tools	Help	admin
Γ														
ſ	Capture Session Filer List													
C Refresh Capture Session Delete Al Sessions														
ľ	•	cap1	Drop Coun	t: 0	Operation	nal State: up		Buffer Size: 256 MB Snap Length: 1518			Bytes			
	Interface Na	ime	Filter			File Size (in bytes)		File Name	Device Name					
	Ethernet1/2		None		-	28632		cap1-ethernet-1-2-0.pcap	ftd1		*			

Port-Channel1 mit Mitgliedsschnittstellen Ethernet1/4 und Ethernet1/5:

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
🔺 🔳 cap1	Drop Count: 0	Operational State: up	Buffer Size: 256	мв	Snap Length: 1518 Bytes	
Interface Name	Filter	File Size (in bytes	i) File Name	Device Name		
Ethernet1/S	None	160	cap1-ethernet-1-5-0.pcap	ftd1	2	
Ethernet1/4	None	85000	cap1-ethernet-1-4-0.pcap	ftd1	≚	

FXOS-CLI

Überprüfen Sie die Erfassungsdetails in der Paketerfassung:

```
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
Port-Channel 1 mit den Mitgliedsschnittstellen Ethernet1/4 und Ethernet1/5:
```

```
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
Erfassungsdateien erfassen
```

Befolgen Sie die Schritte im Abschnitt Sammeln von FirePOWER 4100/9300-internen Switch-

Erfassungsdateien.

Analyse der Erfassungsdatei

Öffnen Sie die Erfassungsdatei für Ethernet1/2 mit einer Anwendung zum Lesen der Paketerfassungsdatei. Wählen Sie das erste Paket aus, und überprüfen Sie die Schlüsselpunkte:

- 1. Es werden nur ICMP-Echoanforderungspakete erfasst. Jedes Paket wird erfasst und zweimal angezeigt.
- 2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.
- 3. Der interne Switch fügt den zusätzlichen Port-VLAN-Tag **102 ein**, der die Eingangsschnittstelle Ethernet1/2 identifiziert.
- 4. Der interne Switch fügt einen zusätzlichen VN-Tag ein.

No. Time	Source	Destination	Protocol	Length	19 ID	IP TTL Info	
1 2022-07-13 06:23:58.285080930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (40428)	64 Echo (ping) reque	t id=0x001a, seq=7/1792, ttl=64 (no response found!)
2 2022-07-13 06:23:58.285082858	192.0.2.100	198.51.100.100	ICMP	102	0x9dec (40428)	64 Echo (ping) reque	t id=0x001a, seq=7/1792, ttl=64 (no response found!)
3 2022-07-13 06:23:59.309048886	192.0.2.100	198.51.100.100	ICMP	108	0x9ed0 (40656)	64 Echo (ping) reque	t id=0x001a, seq=8/2048, ttl=64 (no response found!)
4 2022-07-13 06:23:59.309193731	192.0.2.100	198.51.100.100	ICMP	102	0x9ed0 (40656)	64 Echo (ping) reque	t id=0x001a, seq=8/2048, ttl=64 (no response found!)
5 2022-07-13 06:24:00.333054190	192.0.2.100	198.51.100.100	ICMP	108	0x9f20 (40736)	64 Echo (ping) reque	t id=0x001a, seq=9/2304, ttl=64 (no response found!)
6 2022-07-13 06:24:00.333056014	192.0.2.100	198.51.100.100	ICMP	102	0x9f20 (40736)	64 Echo (ping) reque	t id=0x001a, seg=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	t id=0x001a, seg=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	t id=0x001a, seg=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	t id=0x001a, seg=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	t id=0x001a, seg=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	t id=0x001a, seg=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	t id=0x001a, seg=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	t id=0x001a, seg=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	t id=0x001a, seg=13/3328, ttl=64 (no response found!)
15 2022-07-13 06:24:05 453156612	192.0.2.100	198.51.100.100	TCMP	108	0xa16a (41322)	64 Echo (ning) reque	t id=0x001a, seg=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	t id=0x001a, seg=14/3584, ttl=64 (no response foundl)
17 2022-07-13 06:24:05.477127687	192.0.2.100	198.51.100.100	ICMP	108	0xa1e9 (41449)	64 Echo (ping) reque	t = (d=0x001a, seq=15/3840, tt]=64 (no response found1)
19 2022-07-13 06-24-06 477120990	192 0 2 100	109 51 100 100	TCMP	102	0xa1e9 (41449)	64 Echo (ping) reque	t = (d=0x001a) seq=15/3040, $t=t=64$ (no response found1)
10 2022-07-13 06-24-07 501201314	102 0 2 100	100 51 100 100	TCMP	102	0x0165 (41445)	64 Echo (ping) reque	t id=0x001a, seq=16/4006, ttl=64 (no response found1)
20 2022-07-13 06:24:07.501291314	102.0.2.100	100 51 100 100	TCMP	103	0x01f6 (41462)	64 Echo (ping) reque	t id=0x001a, seq=16/4096, ttl=64 (no response found1)
20 2022-07-13 00:24:07.301293041	192.0.2.100	100 51 100 100	ICNP	102	0x3110 (41402)	64 Echo (ping) reque	t id=0x0010, seq=10/4050, tt1=64 (no response found!)
22 2022-07-13 00.24.00.525003950	102.0.2.100	100 51 100 100	TCMD	103	0x0257 (41550)	64 Echo (ping) reque	t id=0x0010, seq=17/4352, tt1=64 (no response found1)
22 2022-07-13 00:24:00.525092000	192.0.2.100	198.51.100.100	TCHP	102	0x8237 (41559)	64 Echo (ping) reque	t id-0x001a, seq=17/4352, tt1=64 (no response found1)
23 2022-07-13 00:24:09.549230500	192.0.2.100	198.51.100.100	TCHP	108	0x8289 (41041)	64 Echo (ping) reque	t id 0x001a, seq=10/4000, ttl=04 (no response found1)
24 2022-07-13 00:24:09.549238504	192.0.2.100	198.51.100.100	TCHP	102	0xa2a9 (41041)	64 Echo (ping) reque	t id=0x001a, seq=18/4008, ttl=04 (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	t 1d=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 (41/97)	64 Echo (ping) reque	t 1d=0x001a, seq=19/4864, tt1=64 (no response found!)
27 2022-07-13 06:24:11.597086027	192.0.2.100	198.51.100.100	ICMP	108	0xa349 (41801)	64 Echo (ping) reque	t 1d=0x001a, seq=20/5120, tt1=64 (no response found!)
28 2022-07-13 06:24:11.597088170	192.0.2.100	198.51.100.100	ICMP	102	0xa349 (41801)	64 Echo (ping) reque	t 1d=0x001a, seq=20/5120, tt1=64 (no response found!)
29 2022-07-13 06:24:12.621061022	192.0.2.100	198.51.100.100	ICMP	108	0xa30c (41948)	64 Echo (ping) reque	t 1d=0x001a, seq=21/53/6, tt1=64 (no response round!)
<							
> Frame 1: 108 bytes on wire (864 bit	(s), 108 bytes (captured (864 bits)	on interface	capture_u	u0_1, id 0		0000 58 97 bd b9 77 0e 00 50 56 9d e8 be 89 26 80 0a X…w…P V&…
> Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8	:be), Dst: Cisco b9	:77:0e (58:97:	bd:b9:77:	:0e)		0010 00 00 81 00 00 66 08 00 45 00 00 54 9d ec 40 00 ·····f··E··T··@·
✓ VN-Tag							0020 40 01 af c0 c0 00 02 64 c6 33 64 64 08 00 4e a2 @·····d ·3dd··N·
1	= Direc	tion: From Bridge					0030 00 1a 00 07 f4 64 ce 62 00 00 00 00 20 a2 07 00 ·····d·b ····
.0	= Point	er: vif_id					0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b
	= Desti	nation: 10					0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 20 ····· !"# \$7&`()"+
···· ··· ··· ··· ··· · ··· · 0. · · · ·	= Loope	d: No	A				0000 2C 20 2e 2t 30 31 32 33 34 35 30 3/ ,*./0123 450/
0	= Reser	ved: 0	-				
	= Versi	on: 0					
0000 000	00 0000 = Sourc	e: 0					
Type: 802.10 Virtual LAN (0x8100))						
802.10 Virtual LAN, PRI: 0, DEI: 0.	ID: 102						
000 = Priority:	Best Effort (de	fault) (0)					
0 = DEI: Inelia	gible	, , , ,	2				
0000 0110 0110 = ID: 102			-				
Type: IPv4 (0x0800)							
> Internet Protocol Version 4, Src: 1	92.0.2.100, Dst	t: 198.51.100.100					
> Internet Control Message Protocol			2				
in the sought in			-				

Wählen Sie das zweite Paket aus, und überprüfen Sie die wichtigsten Punkte:

- 1. Es werden nur ICMP-Echoanforderungspakete erfasst. Jedes Paket wird erfasst und zweimal angezeigt.
- 2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.
- 3. Der interne Switch fügt den zusätzlichen Port-VLAN-Tag **102 ein**, der die Eingangsschnittstelle Ethernet1/2 identifiziert.

No.	Time	Source	Destination	Protocol	Length	1P 1D	IP TTL Info			
Г	1 2022-07-13 06:23:58.285080930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (48	28) 64 Ech	o (ping)	request	id=0x001a, seq=7/1792, ttl=64 (no response found!)
	2 2022-07-13 06:23:58.285082858	192.0.2.100	198.51.100.100	ICMP	102	0x9dec (40	28) 64 Ech	o (ping)	request	id=0x001a, seq=7/1792, ttl=64 (no response found!)
	3 2022-07-13 06:23:59.309048886	192.0.2.100	198.51.100.100	ICMP	108	0x9ed0 (40	56) 64 Ech	o (ping)	request	id=0x001a, seq=8/2048, ttl=64 (no response found!)
	4 2022-07-13 06:23:59.309193731	192.0.2.100	198.51.100.100	ICMP	102	0x9ed0 (40	56) 64 Ech	o (ping)	request	id=0x001a, seq=8/2048, ttl=64 (no response found!)
	5 2022-07-13 06:24:00.333054190	192.0.2.100	198.51.100.100	ICMP	108	0x9f20 (40	36) 64 Ech	o (ping)	request	id=0x001a, seq=9/2304, ttl=64 (no response found!)
	6 2022-07-13 06:24:00.333056014	192.0.2.100	198.51.100.100	ICMP	102	0x9f20 (40	36) 64 Ech	o (ping)	request	id=0x001a, seq=9/2304, ttl=64 (no response found!)
	7 2022-07-13 06:24:01.357173530	192.0.2.100	198.51.100.100	ICMP	108	0x9f2d (40	49) 64 Ech	o (ping)	request	id=0x001a, seq=10/2560, ttl=64 (no response found!)
	8 2022-07-13 06:24:01.357174708	192.0.2.100	198.51.100.100	ICMP	102	0x9f2d (40	49) 64 Ech	o (ping)	request	id=0x001a, seq=10/2560, ttl=64 (no response found!)
	9 2022-07-13 06:24:02.381073741	192.0.2.100	198.51.100.100	ICMP	108	0x9f88 (40	40) 64 Ech	o (ping)	request	id=0x001a, seq=11/2816, ttl=64 (no response found!)
	10 2022-07-13 06:24:02.381074999	192.0.2.100	198.51.100.100	ICMP	102	0x9f88 (40	40) 64 Ech	o (ping)	request	id=0x001a, seq=11/2816, ttl=64 (no response found!)
	11 2022-07-13 06:24:03.405199041	192.0.2.100	198.51.100.100	ICMP	108	0xa077 (41	(79) 64 Ech	o (ping)	request	id=0x001a, seq=12/3072, ttl=64 (no response found!)
	12 2022-07-13 06:24:03.405200261	192.0.2.100	198.51.100.100	ICMP	102	0xa077 (41	(79) 64 Ech	o (ping)	request	id=0x001a, seq=12/3072, ttl=64 (no response found!)
	13 2022-07-13 06:24:04.429155683	192.0.2.100	198.51.100.100	ICMP	108	0xa10f (41	31) 64 Ech	o (ping)	request	id=0x001a, seq=13/3328, ttl=64 (no response found!)
	14 2022-07-13 06:24:04.429156831	192.0.2.100	198.51.100.100	ICMP	102	0xa10f (41	31) 64 Ech	o (ping)	request	id=0x001a, seq=13/3328, ttl=64 (no response found!)
	15 2022-07-13 06:24:05.453156612	192.0.2.100	198.51.100.100	ICMP	108	0xa16a (41	22) 64 Ech	o (ping)	request	id=0x001a, seq=14/3584, ttl=64 (no response found!)
	16 2022-07-13 06:24:05.453158052	192.0.2.100	198.51.100.100	ICMP	102	0xa16a (41	22) 64 Ech	o (ping)	request	id=0x001a, seq=14/3584, ttl=64 (no response found!)
	17 2022-07-13 06:24:06.477127687	192.0.2.100	198.51.100.100	ICMP	108	0xa1e9 (41	49) 64 Ech	o (ping)	request	id=0x001a, seq=15/3840, ttl=64 (no response found!)
	18 2022-07-13 06:24:06.477129899	192.0.2.100	198.51.100.100	ICMP	102	0xa1e9 (41	49) 64 Ech	o (ping)	request	id=0x001a, seq=15/3840, ttl=64 (no response found!)
	19 2022-07-13 06:24:07.501291314	192.0.2.100	198.51.100.100	ICMP	108	0xa1f6 (41	62) 64 Ech	o (ping)	request	id=0x001a, seq=16/4096, ttl=64 (no response found!)
	20 2022-07-13 06:24:07.501293041	192.0.2.100	198.51.100.100	ICMP	102	0xa1f6 (41	62) 64 Ech	o (ping)	request	id=0x001a, seq=16/4096, ttl=64 (no response found!)
	21 2022-07-13 06:24:08.525089956	192.0.2.100	198.51.100.100	ICMP	108	0xa257 (41	59) 64 Ech	o (ping)	request	id=0x001a, seq=17/4352, ttl=64 (no response found!)
	22 2022-07-13 06:24:08.525092088	192.0.2.100	198.51.100.100	ICMP	102	0xa257 (41	59) 64 Ech	o (ping)	request	id=0x001a, seq=17/4352, ttl=64 (no response found!)
	23 2022-07-13 06:24:09.549236500	192.0.2.100	198.51.100.100	ICMP	108	0xa2a9 (41	41) 64 Ech	o (ping)	request	id=0x001a, seq=18/4608, ttl=64 (no response found!)
	24 2022-07-13 06:24:09.549238564	192.0.2.100	198.51.100.100	ICMP	102	0xa2a9 (41	41) 64 Ech	o (ping)	request	id=0x001a, seq=18/4608, ttl=64 (no response found!)
	25 2022-07-13 06:24:10.573110146	192.0.2.100	198.51.100.100	ICMP	108	0xa345 (41	97) 64 Ech	o (ping)	request	id=0x001a, seq=19/4864, ttl=64 (no response found!)
	26 2022-07-13 06:24:10.573112504	192.0.2.100	198.51.100.100	ICMP	102	0xa345 (41	97) 64 Ech	o (ping)	request	id=0x001a, seq=19/4864, ttl=64 (no response found!)
	27 2022-07-13 06:24:11.597086027	192.0.2.100	198.51.100.100	ICMP	108	0xa349 (41	01) 64 Ech	o (ping)	request	id=0x001a, seq=20/5120, ttl=64 (no response found!)
	28 2022-07-13 06:24:11.597088170	192.0.2.100	198.51.100.100	ICMP	102	0xa349 (41	01) 64 Ech	o (ping)	request	id=0x001a, seq=20/5120, ttl=64 (no response found!)
	29 2022-07-13 06:24:12.621061022	192.0.2.100	198.51.100.100	ICMP	108	0xa3dc (41	48) 64 Ech	o (ping)	request	id=0x001a, seq=21/5376, ttl=64 (no response found!)
<										
5	Frame 2: 102 bytes on wire (816 bi	ts), 102 bytes	captured (816 bits)	on interface	capture u	01. id 0			0	58 97 bd b9 77 0e 00 50 56 9d e8 be 81 00 00 66 X···w··P V·····f
5	Ethernet II. Src: VMware 9d:e8:be	(00:50:56:9d:e8	:be), Dst: Cisco b9:	77:00 (58:97:	bd:b9:77:	80)			0	010 08 00 45 00 00 54 9d ec 40 00 40 01 af c0 c0 00 ··E··T·· @·@·····
4	802.10 Virtual LAN, PRI: 0, DEI: 0	, ID: 102				/			0	020 02 64 c6 33 64 64 08 00 4e a2 00 1a 00 07 f4 64 ··d·3dd·· N·····d
	000 = Priority:	Best Effort (de	fault) (0)	-					0	030 ce 62 00 00 00 00 20 a2 07 00 00 00 00 00 10 11 ·b·····
	0 = DEI: Ineli	gible		2					0	840 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 I
	0000 0110 0110 = ID: 102			-					0	050 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 "#\$%&"() "+,/01
	Type: IPv4 (0x0800)									32 33 34 35 36 37 234567
>	Internet Protocol Version 4, Src: :	192.0.2.100, Ds	t: 198.51.100.100	2						
>	Internet Control Message Protocol			2						
•										

Öffnen Sie die Erfassungsdateien für Portchannel1-Mitgliedsschnittstellen. Wählen Sie das erste Paket aus, und überprüfen Sie die wichtigsten Punkte:

1. Es werden nur ICMP-Echoanforderungspakete erfasst. Jedes Paket wird erfasst und zweimal angezeigt.

- 2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.
- 3. Der interne Switch fügt ein zusätzliches Port-VLAN-Tag **1001 ein**, das die Eingangsschnittstelle Port-Channel1 identifiziert.
- 4. Der interne Switch fügt einen zusätzlichen VN-Tag ein.

					-	- 0	-				
No.	Time	Source	Destination	Protocol	Length	IP ID		IP TTL Info			^
-	1 2022-08-05 23:07:31.865872877	192.0.2.100	198.51.100.100	ICMP	108	0x322e	(12846)	64 Echo (ping) requ	st id=0x002d, s	eq=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)	64 Echo (ping) requ	st id=0x002d, s	eq=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)	64 Echo (ping) requ	st id=0x002d, s	eq=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)	64 Echo (ping) requ	st id=0x002d, s	eq=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)	64 Echo (ping) requ	st id=0x002d, s	eq=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)	64 Echo (ping) requ	st id=0x002d, s	eq=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)	64 Echo (ping) requ	st id=0x002d, s	eq=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)	64 Echo (ping) requ	st id=0x002d, s	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)	64 Echo (ping) requ	st id=0x002d, s	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)	64 Echo (ping) requ	st id=0x002d, s	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)	64 Echo (ping) requ	st id=0x002d, s	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)	64 Echo (ping) requ	st id=0x002d, s	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)	64 Echo (ping) requ	st id=0x002d, s	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)	64 Echo (ping) requ	st id=0x002d, s	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)	64 Echo (ping) requ	st id=0x002d, s	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)	64 Echo (ping) requ	st id=0x002d, s	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)	64 Echo (ping) requ	st id=0x002d, s	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)	64 Echo (ping) requ	st id=0x002d, s	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)	64 Echo (ping) requ	st id=0x002d, s	seq=254/65024, ttl=64	(nc ~
<											>
>	Frame 1: 108 bytes on wire (864 bits)), 108 bytes cap	tured (864 bits) on	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	1
>	Ethernet II, Src: VMware_9d:e8:be (00	0:50:56:9d:e8:be), Dst: a2:76:f2:00	:00:25 (a	2:76:f2:00:00:25	5) 0010	00 00	81 00 03 e9 08 00 45 00	00 54 32 2e 40	00 ···· E··T2.@·	
	VN-Tag					0020	40 01	1b 7f c0 00 02 64 c6 33	64 64 08 00 1e	d6 @d .3dd	
111	1	= Directio	on: From Bridge			0030	00 2d	00 f5 a6 a2 ed 62 00 00	00 00 7a 2f 0b	00 ·-···b ····z/··	
н	.0	= Pointer:	: vif_id			0040	00 00	00 00 10 11 12 13 14 15	16 17 18 19 1a		
н	00 0000 0101 0100	= Destinat	tion: 84			0050	10 10	10 17 20 21 22 23 24 25	26 27 28 29 2a	20 1 # \$58 ()*+	ť
н	0	= Looped:	No 4			0000	20 20	2e 2f 30 31 32 33 34 33	30 37	,/0123 430/	
н	0	= Reserved	d: 0								
н		= Version	: 0								
н	0000 0000	0000 = Source:	0								
IL	Type: 802.10 Virtual LAN (0x8100)										
	802.1Q Virtual LAN, PRI: 0, DEI: 0, I	ID: 1001									
	000 Be Priority: Be	st Effort (defau	ult) (0)								
н	0 = DEI: Ineligi	ble	2								
н	0011 1110 1001 = ID: 1001		5								
	Type: IPv4 (0x0800)										
IП	Internet Protocol Version 4, Src: 192	2.0.2.100, Dst:	198.51.100.100 🚬								
	Internet Control Message Protocol		2								
-											

Wählen Sie das zweite Paket aus, und überprüfen Sie die wichtigsten Punkte:

- 1. Es werden nur ICMP-Echoanforderungspakete erfasst. Jedes Paket wird erfasst und zweimal angezeigt.
- 2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.
- 3. Der interne Switch fügt ein zusätzliches Port-VLAN-Tag **1001 ein**, das die Eingangsschnittstelle Port-Channel1 identifiziert.

No	p. Time	Source	Destination	Protocol	Length	IP ID		IP T	TL Info			1				^
r.	1 2022-08-05 23:07:31.865872877	192.0.2.100	198.51.100.100	ICMP	108	Øx322e	(12846)		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	0x322e	(12846)		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)		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)		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)		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)		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)		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	(13171)		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)		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	(13351)		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	(13534)		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)		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)		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)		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)		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)		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)		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)		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)		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	ture u0 3,	i 0000	a2 76	f2 00	00 25 (90 50	56 9d e8	be 81 00 03	e9 ·v···%·P	v		_
>	Ethernet II, Src: VMware 9d:e8:be (00	0:50:56:9d:e8:be)	, Dst: a2:76:f2:00	:00:25 (a2:76:	f2:00:00:2	25) 0010	08 00	45 00	00 54 3	32 2e	40 00 40	01 1b 7f c0	00 ··E··T2.	0.0		
	802.10 Virtual LAN, PRI: 0, DEI: 0, 1	ID: 1001				0020	02 64	c6 33	64 64 (98 00	1e d6 00	2d 00 f5 a6	a2 ·d·3dd··			
ш	000 Be	st Effort (defau	lt) (0)			0030	ed 62	00 00	00 00 7	7a 2f	0b 00 00	00 00 00 10	11 ·b····z/			
ш	0 = DEI: Ineligi	ble	3			0040	12 13	14 15	16 17 1	18 19	1a 1b 1c	1d 1e 1f 20	21		1	
ш	0011 1110 1001 = ID: 1001					0050	22 23	24 25	26 27 2	28 29	2a 2b 2c	2d 2e 2f 30	31 "#\$%&'()	*+,/01	1	
ш	Type: IPv4 (0x0800)					0060	32 33	34 35	36 37				234567			
н	Internet Protocol Version 4, Src: 192	2.0.2.100, Dst: 1	98.51.100.100													
н	Internet Control Message Protocol		2													
	· · · · ·															

Erklärung

Wenn eine Paketerfassung an einer vorderen Schnittstelle konfiguriert ist, erfasst der Switch gleichzeitig jedes Paket zweimal:

- Nach dem Einfügen des Port-VLAN-Tags.
- Nach dem Einfügen des VN-Tags.

In der Reihenfolge der Vorgänge wird das VN-Tag zu einem späteren Zeitpunkt eingefügt als das Port-VLAN-Tag. In der Erfassungsdatei wird das Paket mit dem VN-Tag jedoch vor dem Paket mit dem Port-VLAN-Tag angezeigt.

In dieser Tabelle ist die Aufgabe zusammengefasst:

Aufgabe	Erfassung spunkt	Internes Port-VLAN in erfassten Paketen	Richtung	Erfasster Datenverkehr
Konfigurieren und Überprüfen der Paketerfassung an der Schnittstelle	Ethernet1/ 2	102	Nur Eingang	ICMP-Echo-Anfragen von Host 192.0.2.100 an Host 198.51.100.
Ethernet1/2 Konfiguration und Verifizierung der Paketerfassung an der Schnittstelle Port- Channel1 mit den Mitgliedsschnittstellen Ethernet1/4 und Ethernet1/5	Ethernet1/ 4 Ethernet1/ 5	1001	Nur Eingang	ICMP-Echo-Anfragen von Host 192.0.2.100 an Host 198.51.100.

Paketerfassung an Backplane-Schnittstellen

Verwenden Sie den FCM und die CLI, um eine Paketerfassung an Backplane-Schnittstellen zu konfigurieren und zu überprüfen.

Topologie, Paketfluss und Erfassungspunkte



Konfiguration

FCM

Führen Sie die folgenden Schritte auf FCM aus, um die Paketerfassung an Backplane-Schnittstellen zu konfigurieren: 1. Verwenden Sie **Tools > Packet Capture > Capture Session**, um eine neue Erfassungssitzung zu erstellen:

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

2. Um Pakete auf allen Backplane-Schnittstellen zu erfassen, wählen Sie die Anwendung und anschließend Alle Backplane-Ports aus der Dropdown-Liste Capture On (Erfassung auf) aus. Sie können auch die spezifische Backplane-Schnittstelle auswählen. In diesem Fall sind die Backplane-Schnittstellen Ethernet1/9 und Ethernet1/10 verfügbar. Geben Sie den Sitzungsnamen an, und klicken Sie auf Save and Run, um die Aufzeichnung zu aktivieren:

Select an instance: ftd1 Save and Run Save Cancel ftd1 ftd1 Selected Interfaces None Buffer Size 256 MB V	overview interfaces cogical bevices security crigine Platform settings	System ioois neip aunin									
ftd1 Session Name* cap1 Selected Interfaces None Buffer Size 256 MB	Select an instance: ftd1 Save and Run Save Cancel										
Selected Interfaces None Buffer Size Z56 MB	ftd1	Session Name* cap1									
Ethemetl/2 Ethemetl/1	Ethernet1/2	Selected Interfaces None Buffer Size 256 MB Snap length: 1518 Store Packets Overwrite Capture On Al Backplane Ports Itd Ethernet1/9 Ethernet1/10 Al Backplane Ports									

FXOS-CLI

Führen Sie die folgenden Schritte auf der FXOS-CLI aus, um die Paketerfassung an Backplane-Schnittstellen zu konfigurieren:

1. Identifizieren Sie den Anwendungstyp und die Kennung:

firepower	# scope s	sa					
firepower	/ssa# sh	ow app-insta	nce				
App Name	Identif	ier Slot ID	Admin Stat	e Oper State	Running Vers	ion Startup Version	
Deploy Ty	pe Turbo I	Mode Profile	Name Cluster	State Cluste	r Role		
ftd	ftd1	1	Enabled	Online	7.2.0.82	7.2.0.82	
Native	No		Not App	olicable None			
2. Ein	e Aufzeich	nungssitzur	ng erstellen:				

firepower# scope packet-capture
firepower /packet-capture # create session cap1
firepower /packet-capture/session* # create phy-port Eth1/9
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # set app-identifier ftd1

```
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # create phy-port Eth1/10
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # enable
firepower /packet-capture/session* # commit
firepower /packet-capture/session #
Verifizierung
```

FCM

Überprüfen Sie den **Schnittstellennamen**, stellen Sie sicher, dass der **Betriebsstatus** aktiv ist und dass die **Dateigröße (in Byte)** ansteigt:

Overview	Interfaces	Logical Devices Security Er	gine Platform	Settings				System	Tools	Help	admin
Capture Ses	sion Fiter L	ist									
							Capture Session	Delete Al	Sessions		
•	cap1	Drop Count: 0	Operation	mal State: up	Buffer Size: 256 MB	3	Snap Length: 1518 Bytes		(٩. [
Interface N	ame	Filter		File Size (in bytes)	File Name	Device Name					
Ethernet1/10		None	1	194352	cap1-ethernet-1-10-0.pcap	ftd1	*				
Ethernet1/9		None		286368	cap1-ethernet-1-9-0.pcap	ftd1	<u>+</u>				

FXOS-CLI

Überprüfen Sie die Erfassungsdetails in der Paketerfassung:

```
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

Erfassungsdateien erfassen
```

Befolgen Sie die Schritte im Abschnitt Sammeln von FirePOWER 4100/9300-internen Switch-Erfassungsdateien.

Analyse der Erfassungsdatei

Öffnen Sie die Erfassungsdateien mit einer Anwendung zum Lesen von Paketerfassungsdateien. Bei mehr als einer Backplane-Schnittstelle müssen alle Erfassungsdateien für jede Backplane-Schnittstelle geöffnet werden. In diesem Fall werden die Pakete an der Backplane-Schnittstelle Ethernet1/9 erfasst.

Wählen Sie das erste und das zweite Paket aus, und überprüfen Sie die Schlüsselpunkte:

- 1. Jedes ICMP-Echo-Anforderungspaket wird erfasst und zweimal angezeigt.
- 2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.
- 3. Der interne Switch fügt den zusätzlichen Port-VLAN-Tag **103 ein**, der die Ausgangsschnittstelle Ethernet1/3 identifiziert.
- 4. Der interne Switch fügt einen zusätzlichen VN-Tag ein.

No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info		
	1 2022-07-14 20:20:36.513854256	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64 Echo (ping) requ	uest	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) requ	uest	id=0x0001, seq=15/3840, ttl=64 (reply in 3)
	3 2022-07-14 20:20:36.514117394	198.51.100.100	9 192.0.2.100	ICMP	108	0xcc2c (52268)	64 Echo (ping) repl	ly	id=0x0001, seq=15/3840, ttl=64 (request in 2)
	4 2022-07-14 20:20:36.514119312	198.51.100.100	9 192.0.2.100	ICMP	108	Øxcc2c (52268)	64 Echo (ping) repl	ly :	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) requ	uest	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) requ	uest	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) repl	ly :	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) repl	ly :	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) requ	uest	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) requ	uest	id=0x0001, seq=17/4352, ttl=64 (reply in 11)
	11 2022-07-14 20:20:38.562048288	198.51.100.100	9 192.0.2.100	ICMP	108	0xccc4 (52420)	64 Echo (ping) repl	ly :	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]	ly :	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) requ	uest	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) requ	uest	id=0x0001, seq=18/4608, ttl=64 (reply in 15)
	15 2022-07-14 20:20:39.585936554	198.51.100.100	9 192.0.2.100	ICMP	108	0xcd8d (52621)	64 Echo (ping) repl	ly :	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) repl	ly :	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) requ	uest	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) requ	uest	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 (52623)	64 Echo (ping) repl	ly :	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 (52623)	64 Echo (ping) repl	ly :	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) requ	uest	id=0x0001, seq=20/5120, ttl=64 (no response found!)
	22 2022-07-14 20:20:41.633806997	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64 Echo (ping) requ	uest	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 (52790)	64 Echo (ping) repl	ly :	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 (52790)	64 Echo (ping) repl	ly :	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 (23536)	64 Echo (ping) requ	uest	id=0x0001, seq=21/5376, ttl=64 (no response found!)
	26 2022-07-14 20:20:42.657711660	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64 Echo (ping) requ	uest	id=0x0001, seq=21/5376, ttl=64 (reply in 27)
	27 2022-07-14 20:20:42.657980675	198.51.100.100	9 192.0.2.100	ICMP	108	0xce49 (52809)	64 Echo (ping) repl	ly :	id=0x0001, seq=21/5376, ttl=64 (request in 26)
	28 2022-07-14 20:20:42.657981971	198.51.100.100	9 192.0.2.100	ICMP	108	0xce49 (52809)	64 Echo (ping) repl	ly	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) requ	uest	id=0x0001, seq=22/5632, ttl=64 (no response found!)
<									
~	Frame 1: 100 butes on wine (064 bi	te) 100 beter	anturned (REA hitc)	on interface (antuna u	0.0 14.0			an sa sa sa od az sa sa az bid ba zz zid an za an an
1	Ethannat II Spc: Cisco b0:77:2d (59, 100 Dytes (d) Det: Whate of	107-50 (00-50-1	terodroze	50)		00	10 00 00 10 00 00 67 08 00 45 00 00 54 59 90 40 00
ú	Ethernet II, Srt: CISCO_09:77:20 (58:97:00:09:77:2	(d), DSC: VMware_90	107130 (001301	sorantes.	50)		00	20 40 01 f4 1c c0 00 02 64 c6 33 64 64 08 00 22 68 @d .3dd"h
1	vn- tag	= Dinor	tion: To Bridge					00	30 00 01 00 0f 89 7a d0 62 00 00 00 00 b3 d7 09 00z.b
	A	- Doint	on wif id					00	40 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b
	00 0000 0000 0000	= Dorti	nation: A					00	50 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ···· !"# \$%&'()*+
		= 10000	d: No					00	60 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,/0123 4567
		- Roson	u. no	4					
		- Monei	veu. o						
		100 1010 - Counc	01. 10						
	Turney 002 10 Wintural LAN (0000 0	00 1010 = Sourc	e; 10						
J	Type: 802.10 VIPtual LAN (0x810	70, 103		_					
٦	and virtual LAN, PRI: 0, DEI: 0	, 10: 105	fault) (a)						
	000 = Priority:	Best Effort (de	rault) (0)	2					
		igible		5					
	0000 0110 0111 = 1D: 103								
	Type: 19V4 (0x0800)	102 0 2 100 0-1	. 100 51 100 500	_					
2	Internet Protocol Version 4, Src:	192.0.2.100, Dst	: 198.51.100.100	2					
1	internet control Message Protocol			4					

No. Time	Source	Destination	Protocol	Length	IP ID		IP TTL Info							
- 1 2022-07-14 20:20:36.513854256	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (3	22928)	64 Echo	(ping)	request	id=0x0001	, seg=15/3846	, ttl=64	(no response found!)	
2 2022-07-14 20:20:36.513857289	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (3	22928)	64 Echo	(ping)	request	id=0x0001	, seg=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	198.51.100.100	9 192.0.2.100	ICMP	108	Øxcc2c (52268)	64 Echo	(ping)	reply	id=0x0001	, seg=15/3840	, ttl=64		
5 2022-07-14 20:20:37.537723822	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (3	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 (;	23848)	64 Echo	(ping)	request	id=0x0001	, seg=16/4096	, ttl=64	(reply in 7)	
7 2022-07-14 20:20:37,538046165	198,51,100,100	9 192.0.2.100	ICMP	108	Oxccob (52379)	64 Echo	(ping)	reply	id=0x0001	, seg=16/4096	, ttl=64	(request in 6)	
8 2022-07-14 20:20:37.538048311	198.51.100.100	9 192.0.2.100	ICMP	108	Oxcc9b (52379)	64 Echo	(ping)	reply	id=0x0001	, seg=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	, seg=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	seg=17/4352	. ttl=64	(reply in 11)	
11 2022-07-14 20:20:38,562048288	198,51,100,10	3 192.0.2.100	ICMP	108	Oxccc4 (52428)	64 Echo	(ping)	reply	id=0x0001	seg=17/4352	. ttl=64	(request in 10)	
12 2022-07-14 20:20:38,562050333	198.51.100.10	3 192.0.2.100	ICMP	108	Oxccc4 (52420)	64 Echo	(ping)	reply	id=0x0001	seg=17/4352	, ttl=64	(
13 2022-07-14 20:20:39,585677043	192.0.2.100	198,51,100,100	TCMP	108	0x5h46 (3	23366)	64 Echo	(ning)	request	id=0x0001	seg=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	seg=18/4608	. ttl=64	(reply in 15)	
15 2022-07-14 20:20:39.585936554	198,51,100,10	192.0.2.100	TCMP	108	excd8d (52621)	64 Echo	(ning)	renly	id=0x0001	seg=18/4608	ttl=64	(request in 14)	
16 2022-07-14 20:20:39,585937900	198.51.100.100	192.0.2.100	ICMP	108	Øxcd8d (52621)	64 Echo	(ping)	reply	id=0x0001	seg=18/4688	. ttl=64	(request in it)	
17 2022-07-14 20:20:40.609804804	192.0.2.100	198.51.100.100	TCMP	108	exsb7b (23419)	64 Echo	(ping)	request	id=0x0001	seg=19/4864	, ttl=64	(no response found!)	
18 2022-07-14 20:20:40 609807618	192.0.2.100	198.51.100.100	TCMP	108	exsh7h (23419)	64 Echo	(ning)	request	id=0x0001	seq=19/4864	tt1=64	(renly in 19)	
19 2022-07-14 20:20:40.610179685	198.51.100.10	3 192.0.2.100	ICMP	108	excdaf (52623)	64 Echo	(ping)	renly	id=0x0001	seg=19/4864	, ttl=64	(request in 18)	
20 2022-07-14 20:20:40 610181044	198.51.100.10	3 192.0.2.100	TCMP	108	avedaf (52623)	64 Echo	(ning)	renly	id-exeent	sen=19/4864	ttl=64	(request in is)	
21 2022-07-14 20:20:41.633805153	192.0.2.100	198.51.100.100	TCMP	108	Øx5b7e (23422)	64 Echo	(ping)	request	id=0x0001	seq=20/5120	ttl=64	(no response found!)	
22 2022-07-14 20:20:41 633806007	192.0.2.100	198.51.100.100	TCMP	108	avsh7e (23422)	64 Echo	(ning)	request	id-avaga1	seq=20/5120	ttl=64	(renly in 23)	
23 2022-07-14 20:20:41.634084102	198.51.100.10	192.0.2.100	TCMP	108	Bxce36 (52798)	64 Echo	(ping)	renly	id=0x0001	seq=20/5120	ttl=64	(request in 22)	
24 2022-07-14 20:20:41 634085368	198.51.100.10	192.0.2.100	TCMP	108	0xce36 (52798)	64 Echo	(ping)	renly	id=exeee1	seq=20/5120	ttl=64	(request in it)	
25 2022-07-14 20:20:42 657700909	102 0 2 100	109 51 100 100	TCMD	100	avshfa (22526)	64 Echo	(ping)	request	id=0x0001	seq=21/5276	++1=64	(no response found))	
26 2022-07-14 20:20:42.057705050	192.0.2.100	198.51.100.100	TCMP	108	exshfe (23536)	64 Echo	(ping)	request	id=exeee1	seq=21/5376	ttl=64	(reply in 27)	
27 2022-07-14 20:20:42.657090675	109 51 100 100	192 8 2 188	TCMD	109	Bycod9 (1	52899)	64 Echo	(ping)	request	id-exeee1	sog=21/5376	++1=64	(request in 26)	
28 2022-07-14 20:20:42.057980075	108 51 100 100	3 102 0 2 100	TCMP	108	Byce49 (52800)	64 Echo	(ping)	centy	id-exeee1	seq=21/5376	ttl=64	(request in 20)	
20 2022-07-14 20:20:42:057501571	102 0 2 100	109 51 100 100	TCMD	100	0x5c53 (22634)	64 Echo	(ping)	request	id-avagan	seq=22/5633	++1-64	(no response found))	
	15110111100	15015111001100	1018	100	ousest (23034)	04 2010	(Pring)	request		, seq-22, 5051	,	(no response roundry	
<														
> Frame 2: 108 bytes on wire (864 bit	s), 108 bytes	captured (864 bits)) on inte	rface capture_u	0_8, id 0					000 00 50	56 9d e7 50	58 97 b	d b9 77 2d 89 26 00 00	-PVPX
Ethernet II, Src: Cisco b9:77:2d (5)	8:97:bd:b9:77:	2d), Dst: VMware_9	d:e7:50 (00:50:56:9d:e7:	:50)					9919 09 0 4	81 00 00 67	08 00 4	5 00 00 54 59 90 40 00	g. E. TY-@-
✓ VN-Tag										0020 40 01	14 1c c0 00	02 64 C	6 33 64 64 08 00 22 68	@d .3ddh
0	= Direc	tion: To Bridge								0000 0000	00 01 89 78	10 62 0	0 00 00 00 03 07 09 00	·····z·b
.0	= Point	er: vif_id								3050 1c 1d	10 1f 20 21	22 23 2	4 15 16 17 18 19 18 10 A 25 26 27 28 20 2a 2h	1"# \$78'()*+
	= Desti	nation: 0								3868 2C 2d	2e 2f 30 31	32 33 3	4 35 36 37	
···· ··· ··· ··· ··· 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))													
✓ 802.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 103													
000 = Priority: E	Best Effort (de	fault) (0)												
0 = DEI: Inelig	gible		31											
0000 0110 0111 = ID: 103			- 1											
Type: IPv4 (0x0800)														
> Internet Protocol Version 4, Src: 1	92.0.2.100, Ds	t: 198.51.100.100	2											
> Internet Control Message Protocol			21											

Wählen Sie das dritte und das vierte Paket aus, und überprüfen Sie die Hauptpunkte:

- 1. Jede ICMP-Echoantwort wird erfasst und zweimal angezeigt.
- 2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.
- 3. Der interne Switch fügt den zusätzlichen Port-VLAN-Tag **102 ein**, der die Ausgangsschnittstelle Ethernet1/2 identifiziert.
- 4. Der interne Switch fügt einen zusätzlichen VN-Tag ein.

			<u> </u>				<u> </u>							
No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info							
-	1 2022-07-14 20:20:36.513854256	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (229	28) 64 Echo	(ping)	request	id=0x0001	seg=15/3840.	ttl=64	(no response found)	0
	2 2022-07-14 20:20:36.513857289	192.0.2.100	198, 51, 100, 100	TCMP	108	av5998 (229	28) 64 Echo	(ning)	request	id=exeen1	seg=15/3840.	tt1=64	(reply in 3)	·
1	2 2022-07-14 20:20:26 514117204	109 51 100 100	102 0 2 100	TCMD	109 4	BXCC2C (522	69) 64 Echo	(ning)	caply	id=0x0001	100=15/2040	++1-64	(request in 2)	
	4 2022 07 14 20:20:30:514117394	100 51 100 100	102.0.2.100	TCHO	100	040020 (522	(0) (4 Teho	(ping)	reply	id-0x0001	seq-15/3040,	++1-64	(request in it)	
	4 2022-07-14 20:20:30.314119312	198.51.100.100	192.0.2.100	TCHP	100	0x0020 (322	00) 04 ECHO	(prug)	repry	10-0x0001	, seq=15/3040,	++1-64	(an annance found)	
	5 2022-07-14 20:20:37.537723822	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (230	40) 64 ECNO	(ping)	request	10=0x0001	, seq=16/4096,	111-04	(no response tound)	.)
	6 2022-07-14 20:20:37.537726588	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (230	40) 64 Echo	(ping)	request	1d=0x0001	, 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 (523	79) 64 Echo	(ping)	reply	id=0x0001	, 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 (523	79) 64 Echo	(ping)	reply	id=0x0001	, seq=16/4096,	tt1=64		
	9 2022-07-14 20:20:38.561776064	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (232	23) 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 (232	23) 64 Echo	(ping)	request	id=0x0001	, seq=17/4352,	ttl=64	(reply in 11)	
	11 2022-07-14 20:20:38.562048288	198.51.100.100	192.0.2.100	ICMP	108	0xccc4 (524	20) 64 Echo	(ping)	reply	id=0x0001	, seq=17/4352,	ttl=64	(request in 10)	
	12 2022-07-14 20:20:38.562050333	198.51.100.100	192.0.2.100	ICMP	108	Øxccc4 (524	20) 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 (233	66) 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 (233	66) 64 Echo	(ping)	request	id=0x0001	, seq=18/4608,	ttl=64	(reply in 15)	
	15 2022-07-14 20:20:39.585936554	198.51.100.100	192.0.2.100	ICMP	108	0xcd8d (526	21) 64 Echo	(ping)	reply	id=0x0001	, seq=18/4608,	ttl=64	(request in 14)	
	16 2022-07-14 20:20:39.585937900	198.51.100.100	192.0.2.100	ICMP	108	0xcd8d (526	21) 64 Echo	(ping)	reply	id=0x0001	seg=18/4608.	ttl=64		
	17 2022-07-14 20:20:40.609804804	192.0.2.100	198,51,100,100	ICMP	108	0x5b7b (234	19) 64 Echo	(ping)	request	id=0x0001	seg=19/4864.	tt1=64	(no response found)	0
	18 2022-07-14 20:20:40.609807618	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (234	19) 64 Echo	(ping)	request	id=0x0001	seg=19/4864.	tt1=64	(reply in 19)	·
	19 2022-07-14 20:20:40.610179685	198, 51, 100, 100	192.0.2.100	TCMP	108	Øxcd8f (526	23) 64 Echo	(ping)	reply	id=0x0001	seg=19/4864.	tt1=64	(request in 18)	
	20 2022-07-14 20:20:40 610181944	198.51.100.100	192.0.2.100	TCMP	108	excdaf (526	23) 64 Echo	(ning)	renly	id=0x0001	seg=19/4864	tt1=64	(requese in is)	
	21 2022-07-14 20-20-41 622905152	102 0 2 100	100 51 100 100	TCMP	109	0x5h7a (224	22) 64 Echo	(ping)	request	id=0x0001	seq=20/5120	++1-64	(no response found)	0
	22 2022-07-14 20:20:41:033003133	102 0 2 100	100 51 100 100	TCMD	100	0x5b7c (234	22) 64 Echo	(ping)	request	id=0x0001	seq=20/5120,	++1-64	(renly in 22)	'
	22 2022-07-14 20:20:41.033000997	100 51 100 100	103 0 3 100	TCMD	100	000076 (234	22) 04 ECHO	(ping)	request	id-0x0001	seq-20/5120,	++1-64	(reply in 25)	
	23 2022-07-14 20:20:41.634084102	198.51.100.100	192.0.2.100	ICHP	108	0xce36 (527	90) 64 ECNO	(ping)	repty	10=0x0001	, seq=20/5120,	111=04	(request in 22)	
	24 2022-07-14 20:20:41.634085368	198.51.100.100	192.0.2.100	ICMP	108	0xce36 (52/	90) 64 Echo	(ping)	repty	10=0x0001	, seq=20/5120,	tt1=64	· · · · · · · · · · · · · · · · · · ·	
	25 2022-07-14 20:20:42.657709898	192.0.2.100	198.51.100.100	ICMP	108	0X5DT0 (235	36) 64 Echo	(ping)	request	1d=0x0001	, seq=21/53/6,	tt1=64	(no response tound))
	26 2022-07-14 20:20:42.657711660	192.0.2.100	198.51.100.100	ICMP	108	0x5bt0 (235	36) 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	192.0.2.100	ICMP	108	0xce49 (528	89) 64 Echo	(ping)	reply	id=0x0001	, seq=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 (528	09) 64 Echo	(ping)	reply	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 (236	34) 64 Echo	(ping)	request	id=0x0001	, seq=22/5632,	ttl=64	(no response found)
ć 💷														
× E	name 3: 100 butes on wine (064 bit	e) 100 butos c	anturned (OEA hits)	on interface	canture ut	o id o				000 00 50	56 0d e8 he 5	9 07 h/	1 h0 77 00 90 26 00	00 . DV
1	themest II. Sect Cisco b0:77:00 (5	9,07,bd,b0,77,0	a) Det: Where od:	on Incertace	capcure_uc	(a) 10 0				010 00 00	81 00 00 66 0	8 00 45	00 00 54 cc 2c 00	00f. ET
1	thernet II, Src: Cisco D9:77:0e (S	8:97:00:09:77:00	e), Dst: vMware_9d:	68:06 (00:20	:50:90:68:0	e)				010 00 00	c1 89 c6 33 6	4 64 66	00 00 54 00 00 23	68 @3ddd.*b
Y	N-Tag		lass and the							030 00 01	00 0f 89 7a d	8 62 88	00 02 00 00 00 20	00 g
	0	= Direct	ion: To Bridge							040 00 00	00 00 10 11 1	2 13 14	15 16 17 18 19 1a	1b
	.0	= Pointe	er: vif_id							050 1c 1d	1e 1f 20 21 2	2 23 24	25 26 27 28 29 2a	2b ···· !"# \$%8'()*+
		= Destin	nation: 0						e	060 2c 2d	2e 2f 30 31 3	2 33 34	35 36 37	/0123 4567
	···· ··· ··· ··· ··· ··· ··· ···	= Looped	1: No	41										,
	0	· ···· = Reserv	ved: 0											
		· · ··· = Versio	on: 0											
	0000 000	00 1010 = Source	2: 10											
ь	Type: 802.1Q Virtual LAN (0x8100))												
× 8	02.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 102												
	000 = Priority: E	Best Effort (def	ault) (0)	-										
Т	0 = DEI: Inelig	ible		21										
1	0000 0110 0110 = ID: 102	-		- I										
	Type: IPv4 (0x0800)													
> 1	nternet Protocol Version 4. Src: 1	98.51.100.100.1	Dst: 192.0.2.100											
> 1	nternet Control Message Protocol			21										
1				-										
-														

Erklärung

Wenn eine Paketerfassung auf einer Backplane-Schnittstelle konfiguriert ist, erfasst der Switch gleichzeitig jedes Paket zweimal. In diesem Fall empfängt der interne Switch Pakete, die bereits von der Anwendung auf dem Sicherheitsmodul mit dem Port-VLAN-Tag und dem VN-Tag markiert wurden. Der VLAN-Tag identifiziert die Ausgangsschnittstelle, über die das interne Chassis die Pakete an das Netzwerk weiterleitet. Der VLAN-Tag 103 in den ICMP-Echoanforderungspaketen identifiziert Ethernet1/3 als Ausgangsschnittstelle, während der VLAN-Tag 102 in den ICMP-Echoantwortpaketen Ethernet1/2 als Ausgangsschnittstelle identifiziert. Der interne Switch entfernt den VN-Tag und den VLAN-Tag der internen Schnittstelle, bevor die Pakete an das Netzwerk weitergeleitet werden.

In dieser Tabelle ist die Aufgabe zusammengefasst:

Aufgabe	Erfassu ngspunk t	Internes Port-VLAN in erfassten Paketen	Richtu ng	Erfasster Datenverkehr
Konfiguration und Überprüfung der Paketerfassung an Backplane-Schnittstellen	Backpla ne- Schnittst ellen	102 103	Nur Eingan g	ICMP-Echo-Anfragen von Host 192.0.2.100 an Host 198.51.10 ICMP-Echo-Antworten von Hos 198.51.100.100 zu Host 192.0.2

Paketerfassung auf Anwendungs- und Anwendungs-Ports

Die Paketerfassung für Anwendungs- oder Anwendungsports wird immer an Backplane-Schnittstellen und zusätzlich an den vorderen Schnittstellen konfiguriert, wenn der Benutzer die Richtung der Anwendungserfassung angibt.

Es gibt hauptsächlich zwei Anwendungsfälle:

- Konfigurieren Sie die Paketerfassung an Backplane-Schnittstellen f
 ür Pakete, die eine bestimmte Front-Schnittstelle verlassen. Konfigurieren Sie beispielsweise die Paketerfassung auf der Backplane-Schnittstelle Ethernet1/9 f
 ür Pakete, die die Schnittstelle Ethernet1/2 verlassen.
- Konfigurieren Sie die gleichzeitige Paketerfassung an einer bestimmten Front- und Backplane-Schnittstelle. Konfigurieren Sie z. B. die gleichzeitige Paketerfassung an Schnittstelle Ethernet1/2 und an Rückwandschnittstelle Ethernet1/9 für Pakete, die Schnittstelle Ethernet1/2 verlassen.

Dieser Abschnitt behandelt beide Anwendungsfälle.

Aufgabe 1

Verwenden Sie den FCM und die CLI, um eine Paketerfassung auf der Backplane-Schnittstelle zu konfigurieren und zu überprüfen. Es werden Pakete erfasst, für die der Anwendungsport Ethernet1/2 als Ausgangsschnittstelle identifiziert wird. In diesem Fall werden ICMP-Antworten erfasst.

Topologie, Paketfluss und Erfassungspunkte



Konfiguration

FCM

Führen Sie die folgenden Schritte auf FCM aus, um eine Paketerfassung auf der FTD-Anwendung und dem Anwendungsport Ethernet1/2 zu konfigurieren:

1. Verwenden Sie **Tools > Packet Capture > Capture Session**, um eine neue Erfassungssitzung zu erstellen:

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

2. Wählen Sie die Anwendung Ethernet1/2 in der Anwendungsport-Dropdown-Liste aus, und wählen Sie Egress Packet in Application Capture Direction (Anwendungserfassungsrichtung) aus. Geben Sie den Sitzungsnamen an, und klicken Sie auf Save and Run, um die Aufzeichnung zu aktivieren:

Overview Interfaces Logical Devices Security Engine	Platform Settings			System Tools H	ielp admin
Select an instance: ftd1 v			Save and Run	Save Cancel	
ftd1		Session Name*	cap1		
		Selected Interfaces	None		
Ethamat1/2		Buffer Size	256 MB 👻		
Euremetz/2		Snap length:	1518 Bytes		
		Store Packets	Overwrite Append		
		Capture On	ftd 👻		
Ethernet1/3		Application Port	Ethernet1/2		
	FID Ethernet1/9, Ethernet1/10	Application Capture Direction	All Packets Egress Packet		
		Capture Filter	Apply Filter Capture All		
Ethernet1/1					
1					

Führen Sie die folgenden Schritte auf der FXOS-CLI aus, um die Paketerfassung an Backplane-Schnittstellen zu konfigurieren:

1. Identifizieren Sie den Anwendungstyp und die Kennung:

```
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
_____ ____
ftdftd11NativeNo
                         Enabled Online
                                                 7.2.0.82 7.2.0.82
                          Not Applicable None
  2. Eine Aufzeichnungssitzung erstellen:
firepower# scope packet-capture
firepower /packet-capture # create session cap1
firepower /packet-capture/session* # create app-port 1 112 Ethernet1/2 ftd
firepower /packet-capture/session/app-port* # set app-identifier ftd1
firepower /packet-capture/session/app-port* # set filter ""
firepower /packet-capture/session/app-port* # set subinterface 0
firepower /packet-capture/session/app-port* # up
firepower /packet-capture/session* # commit
firepower /packet-capture/session #
Verifizierung
```

FCM

Überprüfen Sie den **Schnittstellennamen**, stellen Sie sicher, dass der **Betriebsstatus** aktiv ist und dass die **Dateigröße (in Byte)** ansteigt:

ſ	Overview	Interfaces	Logical Devices	Security Engine	Platform Settings				System Tools	Help	admin	
1	Capture Session Fiter List											
								Capture Session	Delete All Sessions	6		
ſ	•	cap1	Drop Count	t: 0	Operational State: up	Buffer Size: 256	мв	Snap Length: 1518 Bytes			8	
I	Interface Na	ime	Filter		File Size (in bytes)	File Name	Device Name					
	Ethernet1/2	Ethernet1/10	None		576	cap1-vethernet-1175.pcap	ftd1	少				
	Ethernet1/2	Ethernet1/9	None		4360	cap1-vethemet-1036.pcap	ftd1	4				

FXOS-CLI

Überprüfen Sie die Erfassungsdetails in der Paketerfassung:

```
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:
```

Erfassungsdateien erfassen

Befolgen Sie die Schritte im Abschnitt **Sammeln von FirePOWER 4100/9300-internen Switch-**Erfassungsdateien.

Analyse der Erfassungsdatei

Öffnen Sie die Erfassungsdateien mit einer Anwendung zum Lesen von Paketerfassungsdateien. Bei mehreren Backplane-Schnittstellen müssen alle Erfassungsdateien für jede Backplane-Schnittstelle geöffnet werden. In diesem Fall werden die Pakete an der Backplane-Schnittstelle Ethernet1/9 erfasst.

Wählen Sie das erste und das zweite Paket aus, und überprüfen Sie die Schlüsselpunkte:

- 1. Jede ICMP-Echoantwort wird erfasst und zweimal angezeigt.
- 2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.
- 3. Der interne Switch fügt den zusätzlichen Port-VLAN-Tag **102 ein**, der die Ausgangsschnittstelle Ethernet1/2 identifiziert.
- 4. Der interne Switch fügt einen zusätzlichen VN-Tag ein.

No. Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info	
1 2022-08-01 10:03:22.231237959	198.51.100.100	192.0.2.100	ICMP	108 ┥	0x42f8 (17144)	64 Echo (ping) reply	/ id=0x0012, seq=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) reply	id=0x0012, seg=1/256, ttl=64
3 2022-08-01 10:03:23.232244769	198.51.100.100	192.0.2.100	ICMP	108	0X4303 (17331)	64 ECHO (ping) repi	id=0x0012, seq=2/512, ttl=64
4 2022-08-01 10:03:23.232247753	198.51.100.100	192.0.2.100	ICMP	108	0x43b3 (17331)	64 Echo (ping) reply	id=0x0012, seq=2/512, ttl=64
5 2022-08-01 10:03:24.234703981	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64 Echo (ping) reply	/ id=0x0012, seq=3/768, ttl=64
6 2022-08-01 10:03:24.234706751	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64 Echo (ping) reply	/ id=0x0012, seq=3/768, ttl=64
7 2022-08-01 10:03:25.258672449	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64 Echo (ping) reply	/ id=0x0012, seq=4/1024, ttl=64
8 2022-08-01 10:03:25.258674861	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64 Echo (ping) reply	/ id=0x0012, seq=4/1024, ttl=64
9 2022-08-01 10:03:26.282663169	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64 Echo (ping) reply	/ id=0x0012, seq=5/1280, ttl=64
10 2022-08-01 10:03:26.282666183	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64 Echo (ping) reply	/ id=0x0012, seq=5/1280, ttl=64
11 2022-08-01 10:03:27.306671694	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64 Echo (ping) reply	/ id=0x0012, seq=6/1536, ttl=64
12 2022-08-01 10:03:27.306674378	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64 Echo (ping) reply	/ id=0x0012, seq=6/1536, ttl=64
13 2022-08-01 10:03:28.330664677	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64 Echo (ping) reply	/ id=0x0012, seq=7/1792, ttl=64
14 2022-08-01 10:03:28.330667153	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64 Echo (ping) reply	/ id=0x0012, seq=7/1792, ttl=64
15 2022-08-01 10:03:29.354795931	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64 Echo (ping) reply	/ id=0x0012, seq=8/2048, ttl=64
16 2022-08-01 10:03:29.354936706	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64 Echo (ping) reply	/ 1d=0x0012, seq=8/2048, tt1=64
17 2022-08-01 10:03:30.378795204	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64 Echo (ping) reply	/ 1d=0x0012, seq=9/2304, tt1=64
18 2022-08-01 10:03:30.378798172	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64 Echo (ping) reply	/ 1d=0x0012, seq=9/2304, tt1=64
19 2022-08-01 10:03:31.402772217	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64 Echo (ping) reply	/ 1d=0x0012, seq=10/2560, tt1=64
20 2022-08-01 10:03:31.402774775	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64 Echo (ping) reply	/ 1d=0x0012, seq=10/2560, tt1=64
21 2022-08-01 10:03:32.426693254	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64 Echo (ping) reply	/ 1d=0x0012, seq=11/2816, tt1=64
LE 2022-00-01 10:03:32:420033031	150.51.100.100	17210121100	1010	100	0,4000 (10050)	ou cono (pring) i oprij	TA-AVAATE' 204-TYLEATA' CCT-A4
c Frame 1: 108 bytes on wire (864 bi orthowness force buttles)	ts), 108 bytes ca	ptured (864 bits)	on interface	capture_u	0_8, id 0		0000 00 50 56 5d e8 be 58 97 bd b9 77 0e 80 26 00 00 - PVXW&
> Etherhet II, Src: Cisco D9:77:00 (58:97:00:09:77:0e), DSt: VMWare_90	1:68:06 (00:50:	2019016810	be)		0020 40 01 4a b5 c6 33 64 64 c0 00 02 64 00 00 90 04 @-J3ddd
0		ion: To Bridge					0030 00 12 00 01 dd a4 e7 62 00 00 00 00 e3 0d 09 00b
.0	= Pointe	r: vif id					0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b
	= Destin	ation: 0					0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ···· !"# \$%&"()"+
···· ··· ··· ··· ··· · ··· · ··· · · ··· ·	= Looped	: No	A				0000 2c 2d 2e 2t 30 31 32 33 34 35 36 37 ,/0123 4567
0	= Reserve	ed: 0	7 I				
	= Version	n: 0					
0000 00	00 1010 = Source	: 10					
Type: 802.1Q Virtual LAN (0x8100)						
802.1Q Virtual LAN, PRI: 0, DEI: 0	, ID: 102						
000 = Priority:	Best Effort (defa	ault) (0)	-				
0 = DEI: Ineli	gible		3				
0000 0110 0110 = ID: 102			2				
Type: IPv4 (0x0800)							
Internet Protocol Version 4, Src:	198.51.100.100, D	st: 192.0.2.100	-				
Internet Control Message Protocol			Z				
Internet Control Message Protocol			2				
Internet Control Message Protocol			2				
Internet Control Message Protocol	Source	Destination	Protocol	Length	PD	PTTL Mo	
Internet Control Message Protocol No. Time 1 2022-08-01 10:03:22.231237959	Source 198.51.100.100	Destination 192.0.2.100	Protocol	Length 108 -	PD 0x42f8 (17144)	₽TTL №0 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64
Internet Control Message Protocol 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	₽D 0x42f8 (17144) 0x42f8 (17144)	PTTL 140 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64
Internet Control Message Protocol No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:23.232244769	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 (17331)	PTTL 260 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
Internet Control Message Protocol Internet Control Message Protocol Internet 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:23.232247759 4 2022-08-01 10:03:23.232247759	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 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x4303 (17331) 0x43b3 (17331)	PTTL Ho 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
Internet Control Message Protocol No. Tme 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:23.23224769 4 2022-08-01 10:03:23.23224769 5 2022-08-01 10:03:24.234703981	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	Length 108 1 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x4303 (17331) 0x4303 (17331) 0x445e (17502)	PTTL Me 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=3/768, ttl=64
Internet Control Message Protocol No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231230747 3 2022-08-01 10:03:23.23224769 4 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:24.23470391 6 2022-08-01 10:03:24.234706751	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 08 108 108 108 108 108 108 108 108 108 1	PD 0x42f8 (17144) 0x42f8 (17144) 0x4303 (17331) 0x43b3 (17502) 0x445e (17502)	PTL We 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
Internet Control Message Protocol Internet Control Message Protocol Internet Control Message Protocol 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:23.23224753 5 2022-08-01 10:03:23.23224753 5 2022-08-01 10:03:23.23224753 5 2022-08-01 10:03:23.23224753 5 2022-08-01 10:03:23.23224753 5 2022-08-01 10:03:23.2324753 5 2022-08-01 10:03:23.2324753 5 2022-08-01 10:03:23.232475 5 2022-08-01 10:03:23.232475 5 2022-08-01 10:03:23.232475 5 2022-08-01 10:03:23.232475 5 2022-08-01 10:03:23.232475 5 2022-08-01 10:03:23.232475 5 2022-08-01 10:03:23.232475 5 2022-08-01 10:03:23.232475 5 2022-08-01 10:03:23.232475 5 2022-08-01 10:03:23.232475 5 2022-08-01 10:03:23.232475 5 2022-08-01 10:03:23.232475 5 2022-08-01 10:03:23.232475 5 2022-08-01 5 202	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 ICMP ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 1 108 1 108 1 08 108 1 08 108 1 08 108 108 108 108 108 108 108 108 108 1	PD 0x42f8 (17144) 0x42f8 (17144) 0x4303 (17331) 0x445c (17502) 0x445c (17502) 0x445c (17502) 0x445c (17502)	PTTL He 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=3/768, ttl=64
Internet Control Message Protocol No. Time 1 2022-08-01 10:03:22.231237959 2 2002-08-01 10:03:22.231237959 2 0022-08-01 10:03:23.23224709 3 0022-08-01 10:03:23.23224779 5 0022-08-01 10:03:23.232247753 5 0022-08-01 10:03:24.234709816 6 0022-08-01 10:03:25.258674061 8 0022-08-01 10:03:25.258674061 0 0024-08-01 10:03:25.258674061 0 0024-024706716	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 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	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 (1731) 0x4354 (17502) 0x4456 (17502) 0x4456 (17502) 0x4464 (17508) 0x4464 (17508)	PTIL M6 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 id=0x0012, seq=4/1024, ttl=64
Internet Control Message Protocol No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237479 3 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.2312347753 5 2022-08-01 10:03:22.232247753 5 2022-08-01 10:03:22.232247753 6 2022-08-01 10:03:22.232247753 5 2022-08-01 10:03:22.232247753 7 2022-08-01 10:03:25.258672449 8 2022-08-01 10:03:25.258672449 8 2022-08-01 10:03:25.258672451 9 2022-08-01 10:03:26.232663169 9 2022-08-08 -01 10:03:26.232663169 9 2022-08-01 10:03:26.232663169	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 ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 1 108 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x4303 (17341) 0x4303 (17331) 0x4352 (17321) 0x4452 (17502) 0x4464 (17508) 0x4464 (17508) 0x4664 (17508) 0x4664 (17603)	PTL 146 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=3/1024, ttl=64 id=0x0012, seq=3/1024, ttl=64 id=0x0012, seq=3/1024, ttl=64
Internet Control Message Protocol Internet Control Message Protocol Internet Control Nessage Protocol Intern	Source 198.51.100.100 198.51.00.100 198.51.00.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100	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	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 1 108 108 108 108 108 108 108 108 108 108	₽ D 0x42f8 (17144) 0x42f8 (17144) 0x43b3 (17331) 0x43b3 (17331) 0x445e (17502) 0x445e (17508) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508)	PTL Me 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 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64
Internet Control Message Protocol No. Tmme 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231230747 3 2022-08-01 10:03:22.321224769 4 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:24.2347086751 7 2022-08-01 10:03:24.2347086751 7 2022-08-01 10:03:25.258672449 8 2022-08-01 10:03:25.258672451 9 2022-08-01 10:03:26.232663169 10 2022-08-01 10:03:27.3066751634 11 2022-08-01 10:03:27.306671694	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 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Protocol ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP	Length 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x4305 (17341) 0x4305 (17331) 0x4456 (17502) 0x4456 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17603) 0x4467 (17633) 0x4467 (17633)	PTL 140 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=3/1024, ttl=64 id=0x0012, seq=3/1024, ttl=64 id=0x0012, seq=3/1024, 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=3/1586, ttl=64
Internet Control Message Protocol Internet Control Message Protocol 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 3 2022-08-01 10:03:22.231237479 4 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:25.258749 8 2022-08-01 10:03:25.25874861 9 2022-08-01 10:03:25.258749 10 2022-08-01 10:03:25.258674601 10 2022-08-01 10:03:27.366751604 11 2022-08-01 10:03:27.366751604 12 2022-08-01 10:03:27.366751634 13 2022-08-01 10:03:27.366751634 13 2022-08-01 10:03:27.366751634	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	Destrution 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 ICMP	Length 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x4258 (17331) 0x4352 (17502) 0x4454 (17502) 0x4464 (17508) 0x4463 (17603) 0x4463 (17603) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639)	PTL Me 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=3/1024, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=6/5136, ttl=64 id=0x0012, seq=6/5136, ttl=64 id=0x0012, seq=6/5136, ttl=64
Internet Control Message Protocol No. Tme 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 2 0022-08-01 10:03:22.231230747 3 2022-08-01 10:03:23.232247793 5 2022-08-01 10:03:23.232247793 5 2022-08-01 10:03:23.232247793 7 0022-08-01 10:03:25.2586774061 9 2022-08-01 10:03:25.2586774061 9 2022-08-01 10:03:25.2586774061 10 10:03:25.2586774061 10 2022-08-01 10:03:25.236676704 12 2022-08-01 10:03:27.3066767194 12 2022-08-01 10:03:27.3066767184 13 2022-08-01 10:03:28.338066457 14 2022-08-01 10:03:28.338066457 14 2022-08-01 10:03:28.33806457	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	Destruction 192, 0, 2, 100 192, 0, 100 192, 0, 100 192, 0, 100 192, 0, 100 192, 0, 100	Protocol ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP	Length 108 1 108 1 1	PD 0x42f8 (17144) 10x42f8 (17144) 10x42f8 (17144) 10x4350 (1731) 0x4454 (17502) 0x4454 (17502) 0x4464 (17508) 0x4464 (17508) 0x4462 (17639) 0x4462 (17639) 0x4467 (17639) 0x467 (17639) 0x4550 (17744)	▶ TTL № 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 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1356, ttl=64 id=0x0012, seq=5/1356, ttl=64 id=0x0012, seq=5/1356, ttl=64 id=0x0012, seq=5/1356, ttl=64 id=0x0012, seq=5/1376, ttl=64 id=0x0012, seq=5/1376, ttl=64 id=0x0012, seq=5/1376, ttl=64 id=0x0012, seq=5/1780, ttl=64 id=0x0012, seq=5/1792, ttl=64 id=0x
Internet Control Message Protocol No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231230747 3 2022-08-01 10:03:22.321244706 5 2022-08-01 10:03:23.232244705 5 2022-08-01 10:03:24.234703981 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 10:03:26.28266136 10 2022-08-01 10:03:27.306674513 11 2022-08-01 10:03:27.3066745378 13 2022-08-01 10:03:28.3306646771 14 2022-08-01 10:03:28.3306646771 15 2022-08-01 10:03:28.33066467153 15 2022-08-01 10:03:28.33066467153 15 2022-08-01 10:03:28.3306647153 15 2022-08-01 10:03:28.3306647153 15 2022-08-01 10:03:28.3306647153 15 2022-08-01 10:03:28.3306647153 15 2022-08-01 10:03:28.3306647153	Source 198, 51, 100, 100 198, 51, 100, 100	Destrution 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 I CMP I CMP	Longth 108 108 108 108 108 108 108 108	P D 0x4276 (17144) 0x4276 (17144) 0x4303 (17331) 0x4353 (17331) 0x4455 (17502) 0x4456 (17502) 0x4464 (17508) 0x4455 (17633) 0x4464 (17683) 0x4467 (17639) 0x4467 (17639) 0x4452 (17744) 0x4550 (17747)	PTL 146 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=3/108, 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=5/1536, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=7/1792, ttl=64
Internet Control Message Protocol Internet Control Message Protocol 1 2022-08-01 10:03:22.211237959 2 2022-08-01 10:03:23.21224705 3 2022-08-01 10:03:23.212247753 5 2022-08-01 10:03:23.212247753 5 2022-08-01 10:03:24.24707511 7 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 1 2022-08-01 10:03:27.306676194 12 2022-08-01 10:03:27.306676194 13 2022-08-01 10:03:27.306676194 13 2022-08-01 10:03:27.306676194 13 2022-08-01 10:03:27.306676194 13 2022-08-01 10:03:27.30677137 13 2022-08-01 10:03:27.30677137 14 2022-08-01 10:03:27.30677137 15 2022-08-01 10:03:27.30677137 15 2022-08-01 10:03:27.30677137 16 2022-08-01 10:03:27.35430700	Source 198, 51, 100, 100 198, 51, 100, 100	Destination 192, 0, 2, 100 192, 0, 100 192, 0, 100 192, 0, 100 192, 0, 100 192, 0, 100	Protocol ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP	Length 108 1 108 1 1	P.D 0x42f8 (17144) 0x42f8 (17141) 0x4305 (17331) 0x4352 (17331) 0x4455 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17633) 0x4464 (1763) 0x4467 (1763) 0x4467 (1763) 0x4467 (1763) 0x4455 (17744) 0x4553 (17747)	PTT, 146 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=3/1024, 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=7/1792, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=7/1792, ttl=64
Internet Control Message Protocol In. Tme 1 2022-08-01 10:03;22,23123759 2 2022-08-01 10:03;22,23123747 3 2022-08-01 10:03;23,232247763 5 2022-08-01 10:03;23,232247763 5 2022-08-01 10:03;24,242470391 6 2022-08-01 10:03;24,242470391 7 2022-08-01 10:03;25,2586724801 9 2022-08-01 10:03;25,2586724801 10 2022-08-01 10:03;25,2586724801 10 2022-08-01 10:03;25,2586724801 10 2022-08-01 10:03;27,36667478 13 2022-08-01 10:03;27,36667478 13 2022-08-01 10:03;28,330666775 14 2022-08-01 10:03;29,354975931 15 2022-08-01 10:03;29,354975931 16 2022-08-01 10:03;29,354975931 16 2022-08-01 10:03;29,354975937 17 2022-08-01 10:03;29,354975937 17 2022-08-01 10:03;29,354975937	Source 198.51, 100.100 198.51, 100.100	Destruction 192, 0, 2, 100 192, 0, 100 192,	Protocol I CHP I CHP	Longth 108 108 108 108 108 108 108 108	PD (9x42f8 (17144) (9x42f8 (17144) (9x43b3 (17341) 9x43b3 (17341) 9x445e (17502) 9x445e (17502) 9x4464 (17508) 9x4462 (17603) 9x4462 (17603) 9x4462 (17639) 9x4462 (17639) 9x4467 (17639) 9x4556 (17744) 9x4553 (17747) 9x4553 (17747)	PTL 140 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=7/256, ttl=64 id=0x0012, seq=7/512, 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=4/1024, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=8/2048, ttl=64 id=0x0012, seq=8/2048, ttl=64 id=0x0012, seq=8/2048, ttl=64 id=0x0012, seq=8/2048, ttl=64
Internet Control Message Protocol No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237479 3 2022-08-01 10:03:22.231237479 3 2022-08-01 10:03:22.231237479 5 2022-08-01 10:03:22.232247953 5 2022-08-01 10:03:22.232247953 6 2022-08-01 10:03:22.23470753 7 2022-08-01 10:03:22.2528670861 9 2022-08-01 10:03:25.258670861 9 2022-08-01 10:03:25.258670861 10 2022-08-01 10:03:27.306671694 12 2022-08-01 10:03:27.306671694 13 2022-08-01 10:03:27.30667153 15 2022-08-01 10:03:29.354959311 16 2022-08-01 10:03:29.354959311 16 2022-08-01 10:03:29.354959314 18 2022-08-01 10:03:30.3787951204 18 2022-08-01 10:03:30.3787951204	Source 138.51,100.100 138.51,100.100 138.51,100.100 138.51,100.100 138.51,100.100 138.51,100.100 138.51,100.100 138.51,100.100 138.51,100.100 138.51,100.100 138.51,100.100 138.51,100.100	Destination 192, 0, 2, 100 192, 0, 2, 100	Protocol ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP	Longth 108 108 108 108 108 108 108 108	P.D 0x42f8 (17144) 0x42f8 (17144) 0x42f8 (17331) 0x43b3 (17331) 0x4455 (17502) 0x4464 (17508) 0x4462 (1763) 0x4455 (17741) 0x4556 (17741) 0x4553 (17747) 0x4553 (17747) 0x4559 (17741)	PTL 146 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=3/1024, 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=5/1356, ttl=64 id=0x0012, seq=5/1356, ttl=64 id=0x0012, seq=5/1356, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=8/2048, ttl=64 id=0x0012, seq=8/2048, ttl=64 id=0x0012, seq=8/2048, ttl=64
Internet Control Message Protocol In. Tme 1 2022-08-01 10:03:22,231237959 2 2022-08-01 10:03:22,231237959 3 2022-08-01 10:03:22,231237959 4 2022-08-01 10:03:23,23224779 5 2022-08-01 10:03:23,23224779 5 2022-08-01 10:03:24,23470981 6 2022-08-01 10:03:25,258674861 9 2022-08-01 10:03:25,258674861 9 2022-08-01 10:03:27,306674781 1 2022-08-01 10:03:27,306674781 1 2022-08-01 10:03:27,306674781 1 2022-08-01 10:03:27,306674781 1 2022-08-01 10:03:28,330661657 1 2022-08-01 10:03:29,343970513 1 6 2022-08-01 10:03:29,343970513 1 6 2022-08-01 10:03:29,343970751 1 6 2022-08-01 10:03:20,3136,378795204 1 8 2022-08-01 10:03:21,316,378795204 1 8 2022-08-01 10:03:21,316,378795204 1 8 2022-08-01 10:03:21,314,2072217 1 9 202-08-01 10:03:21,314,2072217 1 9 202-08-01 10:03:21,314,2072217 1 9 202-08-01 10:03:21,314,2072217 1 9 202-08-01 10:03:21,314,2072217 1 9 202-08-01 10:03:21,314,2072217 1 9 202-08-01 10:03:21,314,2072217 1 9 202-08-01 10:03:21,314,2072217 1 9 202-08-	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	Destination 192.0.2.100	Protocol ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP	Length 108 108 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17144) 0x43f8 (17141) 0x43b3 (1731) 0x445e (17502) 0x445e (17502) 0x445e (17502) 0x445e (17502) 0x445e (17502) 0x4452 (17633) 0x4452 (17633) 0x4455 (17744) 0x4553 (17747) 0x4553 (17747) 0x4557 (17815) 0x4597 (17815) 0x4597 (18162)	▶ TT, № 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=5/1280, ttl=64 id=0x0012, seq=5/2304, ttl=64 id=0x0012, seq=9/2304, ttl=64 id=0x0012, seq=9/2304, ttl=64 id=0x0012, seq=9/2304, ttl=64 id=0x0012, seq=9/2304, ttl=64 id=0x0012, seq=9/2306, ttl=64 id=0x
Internet Control Message Protocol In. Tme 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231230747 3 2022-08-01 10:03:22.231230747 3 2022-08-01 10:03:23.232247763 5 2022-08-01 10:03:23.232247763 5 2022-08-01 10:03:24.2347086751 7 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:27.306674538 11 2022-08-01 10:03:27.306674637 12 2022-08-01 10:03:27.306674537 13 2022-08-01 10:03:28.3306646775 14 2022-08-01 10:03:28.3306646775 15 2022-08-01 10:03:29.354959311 16 2022-08-01 10:03:20.337875244 18 2022-08-01 10:03:20.330796704 18 2022-08-01 10:03:30.378795244 18 2022-08-01 10:03:30.378795247 2 2022-08-01 10:03:30.378795244 17 2022-08-01 10:03:31.402772177 20 2022-08-01 10:03:31.40277217 20 2022-08-01 10:03:31.40277217 20 2022-08-01 10:03:31.40277217 20 2022-08-01 10:03:31.40277217	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	Destruction 192, 0, 2, 100 192, 0, 100 192, 0, 2, 100 192, 0, 2, 100 192, 0, 2, 100 192,	Protocol I CHVP I CH	Length 108 108 108 108 108 108 108 108	P.D 0x4276 (17144) 0x4276 (17144) 0x4303 (17331) 0x4350 (17331) 0x4456 (17502) 0x4456 (17502) 0x4456 (17502) 0x4456 (17502) 0x4464 (17508) 0x4464 (1763) 0x4467 (1763) 0x4467 (1763) 0x4550 (17744) 0x4553 (17747) 0x4553 (17747) 0x4559 (17747) 0x4559 (17747) 0x4559 (17747) 0x4557 (17845) 0x4597 (1815) 0x4597 (18162)	PTL 146 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=4/1024, ttl=64 id=0x0012, seq=6/1536, ttl=64 id=0x0012, seq=6/1536, ttl=64 id=0x0012, seq=6/1536, ttl=64 id=0x0012, seq=6/1536, ttl=64 id=0x0012, seq=8/2048, ttl=64 id=0x0012, seq=8/2048, ttl=64 id=0x0012, seq=8/2048, ttl=64 id=0x0012, seq=9/2304, ttl=64
Internet Control Message Protocol In. Time 1 2022-08-01 10:03:22,231237959 2 8022-08-01 10:03:22,231237959 3 8022-08-01 10:03:22,23123747 3 8022-08-01 10:03:23,232247763 5 7022-08-01 10:03:23,232247763 5 8022-08-01 10:03:24,2470751 7 9022-08-01 10:03:25,258674861 9 9022-08-01 10:03:25,258674861 9 0022-08-01 10:03:27,36674781 1 8022-08-01 10:03:27,36674781 1 8022-08-01 10:03:28,33066457 14 8022-08-01 10:03:29,343795931 16 2022-08-01 10:03:29,34397664 17 8022-08-01 10:03:29,34397694 18 2022-08-01 10:03:29,34397694 18 2022-08-01 10:03:21,402772217 19 2022-08-01 10:03:21,40277727777 21 2022-08-01 10:03:21,40277727775 21 2022-08-01 10:03:21,402777217 21 2022-08-01 10:03:21,4027777775 21 2022-08-01 10:03:21,402777775 21 2022-08-01 10:03:21,402774775	Source 198, 51, 100, 100 198, 51, 100, 100	Destination 192, 0, 2, 100 192, 0, 2, 100	Protocol ICHP	Length 108 108 108 108 108 108 108 108 108 108	P.D 0x42f8 (17144) 0x42f8 (17144) 0x42f8 (17131) 0x43b3 (17331) 0x4456 (17502) 0x4464 (17508) 0x4455 (17633) 0x4454 (17508) 0x4454 (17633) 0x4454 (17633) 0x4454 (17633) 0x4455 (1763) 0x4457 (17639) 0x4550 (17744) 0x4559 (17747) 0x4597 (17815) 0x467a (18042) 0x467a (18042)	PTT, 146 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 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x012, seq=7/1792, ttl=64 id=0x012, seq=7/1792, ttl=64 id=0x0
Internet Control Message Protocol In. Tme 1 2022-08-01 10:03:22,23123759 2 2022-08-01 10:03:22,23123747 3 2022-08-01 10:03:22,23123747 5 2022-08-01 10:03:23,232247763 5 2022-08-01 10:03:23,232247763 5 2022-08-01 10:03:24,234709751 7 2022-08-01 10:03:25,258674861 9 2022-08-01 10:03:25,258674861 9 2022-08-01 10:03:25,258674861 1 2022-08-01 10:03:27,306674738 13 2022-08-01 10:03:27,30667478 13 2022-08-01 10:03:29,354795931 16 2022-08-01 10:03:29,354795931 16 2022-08-01 10:03:29,354795931 17 2022-08-01 10:03:29,354795931 18 2022-08-01 10:03:29,354795931 18 2022-08-01 10:03:29,34797931 18 2022-08-01 10:03:24,3140277217 2 2022-08-01 10:03:14,02772777 2 2022-08-01 10:03:14,02772777 2 2022-08-01 10:03:12,426693054 2 2022-08-01 10:03:21,426693054 2 2022-08-01 10:03:21,426693054 2 2022-08-01 10:03:21,426693054 2 2022-08-01 10:03:21,426693054 2 2022-08-01 10:03:21,426693054 2 2022-08-01 10:03:21,426693054 2 2022-08-01 10:03:21,426693054 <tr< td=""><td>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</td><td>Destruction 192, 0, 2, 100 192, 0, 2, 100</td><td>Protocol I CHPP I CH</td><td>Length 108 108 108 108 108 108 108 108</td><td>P.D 0x4276 (17144) 0x4276 (17144) 0x4276 (17341) 0x43276 (17341) 0x4326 (17531) 0x4456 (17502) 0x4456 (17502) 0x4456 (17502) 0x4464 (17508) 0x4467 (1763) 0x4467 (1763) 0x4550 (17744) 0x4550 (17747) 0x4553 (17747) 0x4559 (17815) 0x4597 (18162) 0x4667 (18042) 0x4668 (18042) 0x4668 (18042)</td><td>PTL 146 64 Echo (ping) reply 64 Echo (ping) reply<td>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=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=7/1792, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=10/2560, ttl=64 id=0x0012, seq=10/2560,</td></td></tr<>	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	Destruction 192, 0, 2, 100 192, 0, 2, 100	Protocol I CHPP I CH	Length 108 108 108 108 108 108 108 108	P.D 0x4276 (17144) 0x4276 (17144) 0x4276 (17341) 0x43276 (17341) 0x4326 (17531) 0x4456 (17502) 0x4456 (17502) 0x4456 (17502) 0x4464 (17508) 0x4467 (1763) 0x4467 (1763) 0x4550 (17744) 0x4550 (17747) 0x4553 (17747) 0x4559 (17815) 0x4597 (18162) 0x4667 (18042) 0x4668 (18042) 0x4668 (18042)	PTL 146 64 Echo (ping) reply 64 Echo (ping) reply <td>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=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=7/1792, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=10/2560, ttl=64 id=0x0012, seq=10/2560,</td>	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=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=7/1792, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=10/2560,
Internet Control Message Protocol In. Time 1 2022-08-01 10:03:22,231237959 2 2002-08-01 10:03:22,231237959 2 2002-08-01 10:03:22,21237947 3 2022-08-01 10:03:23,232247705 5 2022-08-01 10:03:23,222247709 4 2022-08-01 10:03:24,24707051 7 2022-08-01 10:03:25,2586774061 9 2022-08-01 10:03:25,2586774061 9 2022-08-01 10:03:25,2586774061 9 2022-08-01 10:03:27,306671504 12 2022-08-01 10:03:27,306671504 12 2022-08-01 10:03:27,306671504 12 2022-08-01 10:03:28,330664575 14 2022-08-01 10:03:29,35493706 16 2022-08-01 10:03:29,35493706 16 2032-08-01 10:03:29,35493706 16 2022-08-01 10:03:21,30,37879317 16 2022-08-01 10:03:21,30,37879317 16 2022-08-01 10:03:21,4266935244 18 2022-08-01 10:03:31,402774775 21 2022-08-01 10:03:31,402774775 21 2022-08-01 10:03:31,402774775 21 2022-08-01 10:03:31,402774775 21 2022-08-01 10:03:32,426695501	Source 198, 51, 100, 100 198, 51, 100, 100	Destination 192, 0, 2, 100 192, 0, 2, 100	Protocol ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP	Longth 108 1 108 1 1	PD 0x42f8 (17144) 0x42f8 (17144) 0x42f8 (17131) 0x43b3 (17331) 0x4455 (17502) 0x4464 (17508) 0x4462 (1763) 0x4462 (1763) 0x4462 (1763) 0x4462 (1763) 0x4467 (1763) 0x4467 (1763) 0x4550 (17744) 0x4553 (17747) 0x4597 (17815) 0x4672 (18042) 0x468a (18058) 0x468a (18058)	▶ TT, b0 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=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 id=0x0012, seq=6/1536, ttl=64 id=0x0012, seq=6/1536, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=9/2048, ttl=64 id=0x0012, seq=9/2048, ttl=64 id=0x0012, seq=9/2048, ttl=64 id=0x0012, seq=9/2064, ttl=64 id=0x0012, seq=10/2560, ttl=64 id=0x0012, seq=10/2560, ttl=64 id=0x0012, seq=11/2816, ttl=64
Internet Control Message Protocol Internet Control Message Protocol 1002-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 4 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:24.234709751 7 2022-08-01 10:03:25.2586724601 9 2022-08-01 10:03:25.2586724601 9 2022-08-01 10:03:25.2586724601 1 2022-08-01 10:03:27.366747378 1 2022-08-01 10:03:27.366747378 1 2022-08-01 10:03:29.354795931 1 6 2022-08-01 10:03:29.354795931 1 7 2022-08-01 10:03:29.354795931 2 2 2022-08-01 10:03:23.426695691 2 Frame 2: 108 bytes on wire (864 bit	Source 198.51,100.100 198.51,100.100 198.51,100.100 198.51,100.100 198.51,100.100 198.51,100.100 198.51,100.100 198.51,100.100 198.51,100.100 198.51,100.100 198.51,100.100 198.51,100.100 198.51,100.100 198.51,100.100 198.51,100.100 198.51,100.100	Destruction 192.0.2.100 192.0	Protocol ICHP ICH	108 108 108 108 108 108 108 108	PD (9x42f8 (17144) (9x42f8 (17144) (9x42f8 (17144) (9x43b3 (17331) (9x445e (17502) (9x445e (17502) (9x4464 (17508) (9x4462 (17508) (9x4462 (17603) (9x4462 (17603) (9x4462 (17639) (9x4467 (17639) (9x4553 (17744) (9x4553 (17744) (9x4553 (17744) (9x4553 (17747) (9x4553 (17747) (9x4553 (17747) (9x4553 (17747) (9x4553 (18042) (9x467a (18042) (9x468a (18058) (9x468a (18058)	PTL 140 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 id=0x0012, seq=3/708, ttl=64 id=0x0012, seq=3/128, ttl=64 id=0x0012, seq=3/248, ttl=64 id=0x0012, seq=3/248, ttl=64 id=0x0012, seq=3/248, ttl=64 id=0x0012, seq=3/248, ttl=64 id=0x0012, seq=3/248, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x0
Internet Control Message Protocol Internet Control Message Protocol 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 3 2022-08-01 10:03:23.232247763 5 2022-08-01 10:03:23.222247763 5 2022-08-01 10:03:23.22247763 7 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 9 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 10:03:27.306671694 12 2022-08-01 10:03:27.30677137 14 2022-08-01 10:03:27.30677137 15 2022-08-01 10:03:27.3067719217 12 2022-08-01 10:03:27.30677195911 16 2022-08-01 10:03:27.30677195911 17 2022-08-01 10:03:27.35493706 18 2022-08-01 10:03:21.40277777217 2 2022-08-01 10:03:22.426695591 2 2022-08-01 10:03:22.426695591 2 2022-08-01 10:03:22.426695591 2 7522 108 bytes on wire (864 bit 3 (Thermet II, src: Cisco by:72:6c	Source 198.51,100.100 198.51	Destination 192, 0, 2, 100 192, 0, 100 192,	Protocol ICHP ICH	Longth 108	P D 0x4276 (17144) 0x4376 (17144) 0x4303 (17331) 0x4303 (17331) 0x4455 (17502) 0x4456 (17502) 0x4456 (17502) 0x4452 (17502) 0x4464 (17603) 0x4462 (1763) 0x4462 (1763) 0x4462 (1763) 0x44550 (17744) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTL 146 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=3/1024, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1356, ttl=64 id=0x0012, seq=5/1356, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=3/1024, ttl=64 id=0x0012, seq=3/2046, ttl=64 id=0x0012, seq=11/2816, ttl=64
Internet Control Message Protocol In. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 3 2022-08-01 10:03:22.231237959 4 2022-08-01 10:03:23.23224779 5 2022-08-01 10:03:23.23224779 5 2022-08-01 10:03:24.24707931 7 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 1 2022-08-01 10:03:27.306674737 13 2022-08-01 10:03:27.306674578 12 2022-08-01 10:03:27.306674578 13 2022-08-01 10:03:20.354936706 17 2022-08-01 10:03:30.3787959211 12 2022-08-01 10:03:31.402772177 21 2022-08-01 10:03:31.4027724777 21 2022-08-01 10:03:31.4027724777 22 2022-08-01 10:03:32.426695691 2 22 2022-08-01 10:03:32.426695691 2 22 2022-08-01 10:03:32.426695691	Source 198.51,100.100	Destination 192.0.2.100 192.0	Protocol ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP	108 108 108 108 108 108 108 108	PD (0x42f8 (17144) (0x42f8 (17144) (0x4305 (17144) (0x4305 (17144) (0x4305 (17502) (0x445e (17502) (0x445e (17502) (0x445e (17508) (0x4462 (17603) (0x4462 (17603) (0x4462 (17603) (0x4467 (17639) (0x4553 (17747) (0x4553 (17747) (0x4553 (17747) (0x4553 (17747) (0x4553 (17747) (0x4553 (17747) (0x4553 (17747) (0x4553 (17747) (0x4553 (18042) (0x468a (18058) (0x468a (18058)	PTL 140 64 Echo (ping) reply 64 Echo (ping) reply	1d=0x0012, seq=1/256, ttl=64 1d=0x0012, seq=1/256, ttl=64 1d=0x0012, seq=2/512, ttl=64 1d=0x0012, seq=2/512, ttl=64 1d=0x0012, seq=3/768, ttl=64 1d=0x0012, seq=3/768, ttl=64 1d=0x0012, seq=4/1024, ttl=64 1d=0x0012, seq=4/2048, ttl=64 1d=0x0012, seq=1/2560, ttl=64 1d=0x0012, seq=1/2566, ttl=64 1d=0x0012, seq=1/2616, ttl=64 1d=0x0012, seq=1/2616, ttl=64 1d=0x0012, seq=1/2616, ttl=64 1d=0x0012, seq=1/2616, ttl=64
Internet Control Message Protocol In. Tme 1 2022-08-01 10:03:22.23123759 2 2022-08-01 10:03:22.231237479 3 2022-08-01 10:03:22.231230747 3 2022-08-01 10:03:23.232247793 5 2022-08-01 10:03:23.23224779 5 2022-08-01 10:03:24.23470951 7 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 1 2022-08-01 10:03:27.306674738 13 2022-08-01 10:03:27.30667153 13 2022-08-01 10:03:28.330664677 14 2022-08-01 10:03:28.330664677 14 2022-08-01 10:03:29.3454939317 16 2022-08-01 10:03:21.30.37875244 18 2022-08-01 10:03:20.37875244 18 2022-08-01 10:03:21.30.37875244 12 2022-08-01 10:03:21.40277217 12 2022-08-01 10:03:21.40277217 20 2022-08-01 10:03:21.402724775 21 2022-08-01 10:03:22.42669501 20 702-08-01 10:03:22.42669501 20 702-08-01 10:03:22.42669501 20 702-08-01 10:03:22.42669501 20 702-08-01 10:03:22.42669501 20 702-08-01 10:03:22.42669501 20 702-08-01 10:03:22.42669501	Source 198.51,100.100 198.51	Destination 192.0.2.100 192.0	Protocol ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP	Longth 108 108 108 108 108 108 108 108	<pre></pre>	PTL 146 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=3/1024, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=5/1286, ttl=64 id=0x0012, seq=5/1356, ttl=64 id=0x0012, seq=5/1356, ttl=64 id=0x0012, seq=5/1356, ttl=64 id=0x0012, seq=3/1792, ttl=64 id=0x0012, seq=3/1792, ttl=64 id=0x0012, seq=3/1926, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=10/2566, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x0012, seq=0x02, seq=11/2816, ttl=64 id=0x0012, seq=0x02, seq=0
c c 2 Frame 2: 108 bytes on wire (864 bit) 6 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 3 2022-08-01 10:03:22.231237959 4 2022-08-01 10:03:23.23224705 5 2022-08-01 10:03:23.23224779 6 2022-08-01 10:03:24.244709751 7 2022-08-01 10:03:25.258672404 9 022-08-01 10:03:27.306674781 9 022-08-01 10:03:27.306674781 1 2022-08-01 10:03:27.306674781 1 2022-08-01 10:03:27.306674781 1 2022-08-01 10:03:27.306674784 1 2022-08-01 10:03:27.306574861 1 2022-08-01 10:03:27.306574789 1 2022-08-01 10:03:27.3065747861 1 2022-08-01 10:03:27.30657478 1 2022-08-01 10:03:27.30657478 1 2022-08-01 10:03:27.30657478 1 2022-08-01 10:03:31.40277217 2 2022-08-01 10:03:31.4027724775 2 2022-08-01 10:03:31.402772177 2 2022-08-01 10:03:31.4027721775 2 2	Source 198.51,100.100 198.51	Destination 192.0.2.100 192.0	Protocol ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP	108 108 108 108 108 108 108 108	PD (0x42f8 (17144) (0x42f8 (17144) (0x42f8 (17144) (0x4305 (17141) (0x4305 (171502) (0x445e (17502) (0x445e (17502) (0x4452 (17502) (0x4452 (17502) (0x4452 (17633) (0x4452 (17633) (0x4457 (17633) (0x4556 (17744) (0x4553 (17747) (0x4553 (17747) (0x4553 (17747) (0x4553 (17747) (0x4557 (18042) (0x468a (18058) (0x468a (18058)) (0x468a (18058) (0x468a (18058)	▶TT, b0 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=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=3/2018, ttl=64 id=0x0012, seq=1/2816, ttl=64 id=0x0012, seq=1/2816, ttl=64 id=0x0012, seq=11/2816, ttl=64
Internet Control Message Protocol Internet Control Message Protocol 10022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 4 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:24.24470981 7 2022-08-01 10:03:25.2586724601 9 2022-08-01 10:03:25.2586724601 9 2022-08-01 10:03:25.2586724601 1 2022-08-01 10:03:25.2586724601 1 2022-08-01 10:03:27.36674737 1 2022-08-01 10:03:27.36674737 1 2022-08-01 10:03:29.354795931 1 6 2022-08-01 10:03:29.354795931 1 7 2022-08-01 10:03:29.354795931 2 2 2022-08-01 10:03:23.426695691 2 Frame 2: 108 bytes on wire (864 bit 9 Thernet II, src: Cisco b9:77:0e (3 VH-Tag 0	Source 198.51.100.100 198.50.000 198.50.000 198.50.000 198.50.000 198.50	Destruction 192.0.2.100 192.0	Protocol ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP	108 108 108 108 108 108 108 108	PD (9x42f8 (17144) (9x42f8 (17144) (9x42f8 (17144) (9x43b0 (17331) (9x43b0 (17331) (9x43b0 (17502) (9x4464 (17502) (9x4464 (17508) (9x4464 (17508) (9x4464 (17639) (9x4467 (17639) (9x4467 (17639) (9x4553 (17744) (9x4553 (17744) (9x4553 (17744) (9x4553 (17747) (9x4553 (17747) (9x4553 (17747) (9x4553 (17747) (9x4553 (17747) (9x4574 (18042) (9x4674 (18042) (9x4674 (18042) (9x4684 (18058) (9x4684 (18058) (9x4684 (18058)) (9x4684 (18058) (9x4684 (18058)) (9x4684 (18058) (9x4684 (18058)) (9x4684 (18058) (9x4684 (18058)) (9x4684 (18058))	PTL 340 64 Echo (ping) reply 64 Echo (ping) reply	1d=0x0012, seq=1/256, ttl=64 1d=0x0012, seq=1/256, ttl=64 1d=0x0012, seq=2/512, ttl=64 1d=0x0012, seq=2/512, ttl=64 1d=0x0012, seq=3/768, ttl=64 1d=0x0012, seq=3/768, ttl=64 1d=0x0012, seq=3/768, ttl=64 1d=0x0012, seq=3/768, ttl=64 1d=0x0012, seq=4/1024, ttl=64 1d=0x0012, seq=7/1792, ttl=64 1d=0x0012, seq=7/1792, ttl=64 1d=0x0012, seq=3/2048, ttl=64 1d=0x0012, seq=10/2560, ttl=64 1d=0x0012, seq=10/2560, ttl=64 1d=0x0012, seq=11/2816, t
Internet Control Message Protocol Internet Control Message Protocol 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 3 2022-08-01 10:03:22.231237959 4 2022-08-01 10:03:23.232247053 5 2022-08-01 10:03:23.22247053 7 2022-08-01 10:03:24.2470751 7 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 1 2022-08-01 10:03:25.258674861 1 2022-08-01 10:03:25.258674861 1 2022-08-01 10:03:25.258674861 1 2022-08-01 10:03:25.258674861 1 2022-08-01 10:03:25.258674861 1 2022-08-01 10:03:25.258674861 1 2022-08-01 10:03:25.258674861 1 2022-08-01 10:03:25.258674861 1 2022-08-01 10:03:25.340567153 1 2022-08-01 10:03:25.34595706 1 2022-08-01 10:03:27.366747375 1 2022-08-01 10:03:20.37879817 1 2022-08-01 10:03:20.37879817 1 2022-08-01 10:03:21.426695591 2 2022-08-01 10:03:22.426695691 2 2022-08-01 10:03:22.426695691 2 7022-08-01 10:03:22.426695691 2 7022-08-01 10:03:22.426695691 2 7022-08-01 10:03:22.426695691 <t< td=""><td>Source 198.51,100.100 198.51</td><td>Destination 192.0.2.100 192.0</td><td>Protocol ICHP IC</td><td>Longth 108 1 108 1 1</td><td>P.D 0x4276 (17144) 0x4276 (17144) 0x4303 (17331) 0x4353 (17331) 0x4456 (17502) 0x4456 (17502) 0x4456 (17502) 0x4456 (17502) 0x4464 (17508) 0x4462 (1763) 0x4462 (1763) 0x4462 (1763) 0x4467 (1763) 0x4559 (17744) 0x4559 (17741) 0x4559 (17741) 0x4557 (1815) 0x4673 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058)</td><td>PTL 146 64 Echo (ping) reply 64 Echo (ping) reply</td><td>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=10/2560, ttl=64 id=0x0012, seq=10/2560, ttl=64 id=0x0012, seq=11/2816, ttl=64</td></t<>	Source 198.51,100.100 198.51	Destination 192.0.2.100 192.0	Protocol ICHP IC	Longth 108 1 108 1 1	P.D 0x4276 (17144) 0x4276 (17144) 0x4303 (17331) 0x4353 (17331) 0x4456 (17502) 0x4456 (17502) 0x4456 (17502) 0x4456 (17502) 0x4464 (17508) 0x4462 (1763) 0x4462 (1763) 0x4462 (1763) 0x4467 (1763) 0x4559 (17744) 0x4559 (17741) 0x4559 (17741) 0x4557 (1815) 0x4673 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTL 146 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=10/2560, ttl=64 id=0x0012, seq=10/2560, ttl=64 id=0x0012, seq=11/2816, ttl=64
Internet Control Message Protocol In. Tme 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 3 2022-08-01 10:03:22.231237959 4 2022-08-01 10:03:23.23224779 5 2022-08-01 10:03:23.23224779 5 2022-08-01 10:03:24.24779751 7 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 10 2022-08-01 10:03:27.306671594 12 2022-08-01 10:03:27.306671594 12 2022-08-01 10:03:27.306671594 12 2022-08-01 10:03:27.306671594 13 2022-08-01 10:03:27.306571594 16 2022-08-01 10:03:20.378795911 16 2022-08-01 10:03:31.40277217 20 202-08-01 10:03:31.402772177 21 2022-08-01 10:03:31.402772177 21 2022-08-01 10:03:31.402772177 22 2022-08-01 10:03:32.426695691 C Frame 2: 108 bytes on wire (864 bit Thermet 11, Src; Cisco b9:77:06 (54 MH-Tag 0 0.0000 00000 0000 0.0000 00000 0000 0 0 0.	Source 198.51,100.100 198.51	Destination 192.0.2.100 192.0	Protocol ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP	108 108 108 108 108 108 108 108	PD 0x4276 (17144) 0x4276 (17144) 0x4276 (17144) 0x4376 (17144) 0x4376 (17143) 0x4456 (17502) 0x4456 (17502) 0x4456 (17502) 0x4456 (17503) 0x4442 (1763) 0x44550 (17744) 0x4550 (17744) 0x4553 (17747) 0x4553 (17747) 0x4559 (18042) 0x4672 (18042) 0x468a (18058) 0x468a (18058)	PTL 140 64 Echo (ping) reply 64 Echo (ping) reply	1d=0x0012, seq=1/256, ttl=64 1d=0x0012, seq=1/256, ttl=64 1d=0x0012, seq=2/512, ttl=64 1d=0x0012, seq=3/768, ttl=64 1d=0x0012, seq=3/768, ttl=64 1d=0x0012, seq=3/768, ttl=64 1d=0x0012, seq=3/768, ttl=64 1d=0x0012, seq=4/1024, ttl=64 1d=0x0012, seq=4/1024, ttl=64 1d=0x0012, seq=4/1024, ttl=64 1d=0x0012, seq=5/1280, ttl=64 1d=0x0012, seq=5/1280, ttl=64 1d=0x0012, seq=5/1280, ttl=64 1d=0x0012, seq=4/1024, ttl=64 1d=0x0012, seq=4/2048, ttl=64 1d=0x0012, seq=3/2048, ttl=64 1d=0x0012, seq=1/2616, ttl=64 1d=0x0012, seq=1/2616, ttl=64 1d=0x0012, seq=11/2616, ttl=64 1d=0x0012, seq=11/2816, ttl=64
Internet Control Message Protocol In. Time 1 2022-08-01 10:03:22,231237959 2 2022-08-01 10:03:22,231237959 3 2022-08-01 10:03:23,232247753 5 2022-08-01 10:03:23,232247753 5 2022-08-01 10:03:24,242470981 6 2022-08-01 10:03:25,258674861 9 2022-08-01 10:03:25,258674861 9 2022-08-01 10:03:25,258674861 1 2022-08-01 10:03:27,306671641 1 2022-08-01 10:03:27,306671641 1 2022-08-01 10:03:27,306671641 1 2022-08-01 10:03:27,306671641 1 2022-08-01 10:03:27,306671641 1 2022-08-01 10:03:27,306671641 1 2022-08-01 10:03:27,306671641 1 2022-08-01 10:03:27,306671641 1 2022-08-01 10:03:27,30671641 1 2022-08-01 10:03:27,30671641 1 2022-08-01 10:03:31,402727217 2 0022-08-01 10:03:31,40274772217 2 0022-08-01 10:03:32,426695691 2 7022-08-01 10:03:32,426695691 2 7022-08-01 10:03:32,426695691 9 74-74 9 74-74 9 74-74 9 74-74 9 74-74 9 74-74 9 74-74 9 74-74 </td <td>Source 198.51,100.100 198.51</td> <td>Destination 192.0.2.100 192.0</td> <td>Protocol ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP</td> <td>Longth 108 108 108 108 108 108 108 108</td> <td>P.D 0x4276 (17144) 0x4276 (17144) 0x4276 (17144) 0x4276 (17144) 0x4276 (1731) 0x44256 (17502) 0x44256 (17502) 0x44264 (17508) 0x44264 (17633) 0x44267 (17639) 0x44267 (17639) 0x44267 (17639) 0x4457 (17743) 0x45590 (17744) 0x45597 (17815) 0x46747 (18842) 0x46747 (18842) 0x4674 (18058) 0x468a (18058)</td> <td>PTL 146 64 Echo (ping) reply 64 Echo (ping) reply</td> <td><pre>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=4/1024, ttl=64 id=0x0012, seq=5/1366, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=10/2566, ttl=64 id=0x0012, seq=10/2566, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x0012, seq=11,</pre></td>	Source 198.51,100.100 198.51	Destination 192.0.2.100 192.0	Protocol ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP	Longth 108 108 108 108 108 108 108 108	P.D 0x4276 (17144) 0x4276 (17144) 0x4276 (17144) 0x4276 (17144) 0x4276 (1731) 0x44256 (17502) 0x44256 (17502) 0x44264 (17508) 0x44264 (17633) 0x44267 (17639) 0x44267 (17639) 0x44267 (17639) 0x4457 (17743) 0x45590 (17744) 0x45597 (17815) 0x46747 (18842) 0x46747 (18842) 0x4674 (18058) 0x468a (18058)	PTL 146 64 Echo (ping) reply 64 Echo (ping) reply	<pre>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=4/1024, ttl=64 id=0x0012, seq=5/1366, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=10/2566, ttl=64 id=0x0012, seq=10/2566, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x0012, seq=11,</pre>
c Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 3 2022-08-01 10:03:22.231237959 4 2022-08-01 10:03:23.232247053 5 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:24.24707951 7 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:27.306674781 1 2022-08-01 10:03:27.306674781 1 2022-08-01 10:03:27.306674781 1 2022-08-01 10:03:27.306674781 1 2022-08-01 10:03:27.306674781 1 2022-08-01 10:03:27.306674781 1 2022-08-01 10:03:27.30667478941 16 2022-08-01 10:03:31.4027729172 17 2022-08-01 10:03:31.4027724775 21 2022-08-01 10:03:31.4027724775 21 2022-08-01 10:03:31.4027724775 21 2022-08-01 10:03:32.426695691 * Frame	Source 198.51.100.100 198.51	Destination 192.0.2.100 192.0	Protocol ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP	108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17144) 0x43f8 (17144) 0x43f8 (17144) 0x43f8 (17144) 0x43f8 (17144) 0x4456 (17502) 0x4456 (17502) 0x4464 (17508) 0x4462 (1763) 0x4462 (1763) 0x4455 (17744) 0x4555 (17744) 0x4555 (17747) 0x4557 (17815) 0x4677 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTL b0 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=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 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=3/2180, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=13/2816, ttl=64 id=0x0012, seq=13/281
Internet Control Message Protocol In. Tme 1 2022-08-01 10:03:22.21123759 2 2022-08-01 10:03:22.2123759 3 2022-08-01 10:03:22.2123759 4 2022-08-01 10:03:23.2224779 5 2022-08-01 10:03:23.2224779 5 2022-08-01 10:03:23.2224779 6 2022-08-01 10:03:24.2470791 7 2022-08-01 10:03:25.258672407 9 2022-08-01 10:03:25.258672407 9 2022-08-01 10:03:25.258672407 1 2022-08-01 10:03:25.258672407 1 2022-08-01 10:03:25.258672407 1 2022-08-01 10:03:27.306671594 1 2022-08-01 10:03:27.306671594 1 2022-08-01 10:03:29.354795931 1 6 2022-08-01 10:03:29.354795931 1 7 202-08-01 10:03:29.354795931 1 7 202-08-01 10:03:1.40277217 2 2022-08-01 10:03:1.40277217 2 2022-08-01 10:03:1.40277217 2 2022-08-01 10:03:23.426695691 2 Frame 2: 108 bytes on wire (864 bit) 9 0	Source 198.51,100.100 198.51	Destination 192.0.2.100 192.0	Protocol ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP	108 108 108 108 108 108 108 108	P.D 0x4276 (17144) 0x4276 (17341) 0x43276 (17341) 0x43276 (17341) 0x43256 (17531) 0x4456 (17502) 0x4456 (17502) 0x4464 (17508) 0x4465 (1763) 0x4467 (1763) 0x4467 (1763) 0x4550 (17744) 0x4550 (17744) 0x4550 (17747) 0x4553 (17747) 0x4559 (17815) 0x467a (18042) 0x467a (18042) 0x468a (18058) 0x468a (18058)	PTL 140 64 Echo (ping) reply 64 Echo (ping) reply	<pre>id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=7/1256, ttl=64 id=0x0012, seq=7/1526, ttl=64 id=0x0012, seq=7/168, ttl=64 id=0x0012, seq=7/1024, ttl=64 id=0x0012, seq=7/1024, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=10/2566, ttl=64 id=0x0012, seq=10/2566, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x0012, seq=112, seq=112, seq=12, seq</pre>
c c 2 Frame 2: 108 bytes on wire (864 bit) 1 2022-08-01 10:03:22,231237959 2 2022-08-01 10:03:22,21237947 3 2022-08-01 10:03:23,232247763 5 2022-08-01 10:03:23,232247763 5 2022-08-01 10:03:24,2470751 7 2022-08-01 10:03:25,258672404 9 2022-08-01 10:03:25,258672405 9 2022-08-01 10:03:27,3066737861 9 2022-08-01 10:03:27,30667378 1 2022-08-01 10:03:27,30667378 1 2022-08-01 10:03:27,30667378 1 2022-08-01 10:03:27,30667378 1 2022-08-01 10:03:27,30657378 16 2022-08-01 10:03:27,30657378 17 2022-08-01 10:03:31,40277217 2 2022-08-01 10:03:31,402774775 21 2022-08-01 10:03:31,40277217 21 2022-08-01 10:03:31,40277217 21 2022-08-01 10:03:31,40277217 21 2022-08-01 10:03:31,40277217 21 2022-08-01 10:03:31,40277217 21 2022-08-01 10:03:31,40277217 21	Source 138.51.100.100	Destination 192.0.2.100 192.0	Protocol ICHP IC	108 108 108 108 108 108 108 108	PD 0x4276 (17144) 0x4276 (17144) 0x4276 (17144) 0x4276 (17144) 0x4276 (17144) 0x4305 (1731) 0x445e (17502) 0x445e (17502) 0x445e (17502) 0x4454 (17508) 0x4454 (17630) 0x4455 (17743) 0x4555 (17744) 0x4553 (17747) 0x4557 (18042) 0x4676 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTL b0 64 Echo (ping) reply 64 Echo (p	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=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=7/1792, ttl=64 id=0x0012, seq=7/2018, ttl=64 id=0x0012, seq=7/2018, ttl=64 id=0x0012, seq=7/2018, ttl=64 id=0x0012, seq=1/2816, ttl=64
C C 2 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 3 022-08-01 10:03:22.231237959 4 2022-08-01 10:03:22.231237959 4 2022-08-01 10:03:23.232247753 5 022-08-01 10:03:23.232247753 5 022-08-01 10:03:25.2586774861 9 2022-08-01 10:03:25.2586774861 9 022-08-01 10:03:25.2586774861 9 022-08-01 10:03:25.2586774861 9 022-08-01 10:03:25.2586774861 10 022-08-01 10:03:25.2586774861 10 022-08-01 10:03:27.366674737 12 022-08-01 10:03:32.330607153 13 022-08-01 10:03:31.40277217 16 022-08-01 10:03:31.402772177 17 20:20-08-01 10:03:31.4027721777 21 022-08-01 10:03:31.402772177725 21 020:00-08-01 10:03:32.4266095691	Source 198.51.100.100 198.51	Destruction 192.0.2.100 192.0	Protocol ICHP ICH	108 108 108 108 108 108 108 108	PD 0x4276 (17144) 0x4276 (17144) 0x4276 (17144) 0x4276 (17144) 0x4276 (17541) 0x43256 (17522) 0x4456 (17502) 0x4456 (17502) 0x4464 (17508) 0x4464 (17638) 0x4467 (17639) 0x4467 (17639) 0x4559 (17744) 0x4559 (17747) 0x4559 (17741) 0x4559 (17741) 0x4559 (17741) 0x4559 (17741) 0x4564 (18042) 0x4674 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTL 340 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 Id=0x0012, seq=3/708, ttl=64 Id=0x0012, seq=3/708, ttl=64 Id=0x0012, seq=3/7128, ttl=64 Id=0x0012, seq=10/2566, ttl=64 Id=0x0012, seq=10/2566, ttl=64 Id=0x0012, seq=11/2816, ttl=64 Id=0x00012, seq=11/2816, ttl=64 Id=0x00012, seq=11/2816, ttl=64 Id=0x0012, seq=11/2816, ttl=64 Id=0x00012, seq=11/2816, ttl=64 Id=0x00012, seq=11/2816, ttl=64 Id=0x00012, seq=11/2816, ttl=64 Id=0x00012, seq=11/2
<pre> Internet Control Message Protocol Internet Control Message Internet Internet Control Message Internet Internet Internet Control Message Internet Internet</pre>	Source 138.51.108.100 138.51.55 155.102 1	Destination 192.0.2.100 192.0	Protocol ICHP	Longth 108 1 108 1 1	PD 0x42f8 (17144) 0x42f8 (17144) 0x42f8 (17144) 0x42f8 (17144) 0x42f8 (17144) 0x42f8 (17144) 0x42f8 (17141) 0x445e (17502) 0x4464 (17508) 0x4465 (17508) 0x4464 (17508) 0x4464 (17639) 0x4467 (17639) 0x4459 (17744) 0x4559 (17744) 0x4559 (17744) 0x4557 (17815) 0x4677 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058) 0x468a (18058)	▶TT, b0 64 Echo (ping) reply 64 Echo (ping) reply	1d=0x0012, seq=1/256, ttl=64 1d=0x0012, seq=1/256, ttl=64 1d=0x0012, seq=2/512, ttl=64 1d=0x0012, seq=3/766, ttl=64 1d=0x0012, seq=5/1280, ttl=64 1d=0x0012, seq=3/2040, ttl=64 1d=0x0012, seq=3/2040, ttl=64 1d=0x0012, seq=10/2560, ttl=64 1d=0x0012, seq=11/2816, ttl=64
Internet Control Message Protocol In. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 3 2022-08-01 10:03:22.21237959 4 2022-08-01 10:03:22.21237959 4 2022-08-01 10:03:22.22247953 5 2022-08-01 10:03:23.232247763 7 2022-08-01 10:03:24.234709511 7 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 1 2022-08-01 10:03:25.258674861 1 2022-08-01 10:03:25.238674861 1 2022-08-01 10:03:27.306674794 1 2022-08-01 10:03:27.306674594 1 2022-08-01 10:03:27.306674594 1 2022-08-01 10:03:20.354936706 1 7 2022-08-01 10:03:13.04277277 2 2022-08-01 10:03:13.042772777 2 2022-08-01 10:03:13.042772777 2 2022-08-01 10:03:13.042772777 2 2022-08-01 10:03:13.042772777 2 2022-08-01 10:03:13.0427727777 2 0022-08-01 10:03:13.0427727777 2 0022-08-01 10:03:13.0427227777 2 0022-08-01 10:03:13.042724775 2 0022-08-01 10:03:13.042724775 2 0022-08-01 10:03:13.042724775 <tr< td=""><td>Source 198.51.100.100 198.50.100 198.50.100 198.50.100 198.50.100 198.50</td><td>Destination 192.0.2.100 192.0</td><td>Protocol ICHP ICHP</td><td>108 108 108 108 108 108 108 108</td><td>PD 0x4276 (17144) 0x4276 (17144) 0x4276 (17144) 0x4276 (17341) 0x44256 (17502) 0x4456 (17502) 0x4456 (17502) 0x4456 (17503) 0x4452 (1763) 0x44556 (17744) 0x4556 (17744) 0x4557 (17747) 0x4558 (17747) 0x4559 (17743) 0x4672 (18042) 0x468a (18058) 0x468a (18058)</td><td>PTL 140 64 Echo (ping) reply 64 Echo (ping) reply</td><td>1d=0x0012, seq=1/256, ttl=64 1d=0x0012, seq=2/512, ttl=64 1d=0x0012, seq=2/512, ttl=64 1d=0x0012, seq=3/768, ttl=64 1d=0x0012, seq=3/128, ttl=64 1d=0x0012, seq=3/284, ttl=64 1d=0x0012, seq=11/2816, ttl=64 1d=0x0012, seq=11/2816, ttl=64 1d=0x0012, seq=3/1282, stg=3/282, ttl=64 1d=0x0012, seq=3/1283, stg=3/84, stg=3/84 1d=0x0012, seq=3/1284, stg=3/84<!--</td--></td></tr<>	Source 198.51.100.100 198.50.100 198.50.100 198.50.100 198.50.100 198.50	Destination 192.0.2.100 192.0	Protocol ICHP	108 108 108 108 108 108 108 108	PD 0x4276 (17144) 0x4276 (17144) 0x4276 (17144) 0x4276 (17341) 0x44256 (17502) 0x4456 (17502) 0x4456 (17502) 0x4456 (17503) 0x4452 (1763) 0x44556 (17744) 0x4556 (17744) 0x4557 (17747) 0x4558 (17747) 0x4559 (17743) 0x4672 (18042) 0x468a (18058) 0x468a (18058)	PTL 140 64 Echo (ping) reply 64 Echo (ping) reply	1d=0x0012, seq=1/256, ttl=64 1d=0x0012, seq=2/512, ttl=64 1d=0x0012, seq=2/512, ttl=64 1d=0x0012, seq=3/768, ttl=64 1d=0x0012, seq=3/128, ttl=64 1d=0x0012, seq=3/284, ttl=64 1d=0x0012, seq=11/2816, ttl=64 1d=0x0012, seq=11/2816, ttl=64 1d=0x0012, seq=3/1282, stg=3/282, ttl=64 1d=0x0012, seq=3/1283, stg=3/84, stg=3/84 1d=0x0012, seq=3/1284, stg=3/84 </td
Internet Control Message Protocol Internet Control Message Protocol 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 3 2022-08-01 10:03:22.231237959 4 2022-08-01 10:03:23.232247053 5 2022-08-01 10:03:23.22247053 7 2022-08-01 10:03:24.24707051 7 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.238674861 1 2 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 10:03:27.306771371 16 2022-08-01 10:03:27.306771371 17 2022-08-01 10:03:27.306771371 17 2022-08-01 10:03:27.306771372 19 2022-08-01 10:03:13.402777217 2 2022-08-01 10:03:13.402772172 2 2022-08-01 10:03:13.402772172 2 0022-08-01 10:03:22.426695591 2 Thermet II, src: Cisco b9:77:08 (5) 9 -0	Source 198.51,100.100 198.51	Destination 192.0.2.100 192.0	Protocol ICHP	Longth 108	P.D 0x4276 (17144) 0x4276 (17144) 0x4276 (17144) 0x4276 (17144) 0x4276 (1731) 0x44256 (17502) 0x4456 (17502) 0x4456 (17502) 0x4464 (17508) 0x4467 (1763) 0x4467 (1763) 0x4467 (1763) 0x4450 (17741) 0x4550 (17747) 0x4557 (1862) 0x4673 (18642) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTL 146 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=3/768, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=4/1024, 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=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=10/2560, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x0012, seq=</pre>
c c c c	Source 198.51.100.100 199.51.100.100 101.51.00.100 101.51.00 101.5	Destination 192.0.2.100 192.0	Protocol ICHP	108 108 108 108 108 108 108 108	PD 0x4276 (17144) 0x4276 (17144) 0x4276 (17144) 0x4276 (17144) 0x43105 (1731) 0x4350 (1731) 0x4456 (17502) 0x4456 (17502) 0x4464 (17503) 0x4462 (1763) 0x4462 (1763) 0x4462 (1763) 0x4455 (17741) 0x4550 (17741) 0x4557 (17815) 0x4597 (17815) 0x4673 (18042) 0x468a (18058) 0x468a (18058)	PTL b6 64 Echo (ping) reply 64 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=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 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=1/2816, ttl=64 id=

Erklärung

In diesem Fall ist Ethernet1/2 mit dem Port-VLAN-Tag 102 die Ausgangsschnittstelle für die ICMP-Echoantwortpakete.

Wenn die Erfassungsrichtung der Anwendung in den Erfassungsoptionen auf "**Egress**" (Ausgang) festgelegt ist, werden Pakete mit dem Port-VLAN-Tag 102 im Ethernet-Header an den Backplane-Schnittstellen in der Eingangsrichtung erfasst.

In dieser Tabelle ist die Aufgabe zusammengefasst:

Aufgabe	Erfassungsp Inter unkt erfas	rnes Port-VLAN in ssten Paketen	Richtun a	Erfasster Datenverkehr
Konfiguration und Verifizierung von Erfassungen auf Anwendungs- und Anwendungsport Ethernet1/2	Backplane- Schnittstelle n	102	Nur Eingan g	ICMP-Echo-Antworten von Ho 198.51.100.100 zu Host 192.0.2.100

Aufgabe 2

Verwenden Sie den FCM und die CLI, um eine Paketerfassung auf der Backplane-Schnittstelle und der Front-Schnittstelle Ethernet1/2 zu konfigurieren und zu überprüfen.

Die gleichzeitige Paketerfassung wird konfiguriert auf:

- Front-Schnittstelle Die Pakete mit dem Port VLAN 102 an der Schnittstelle Ethernet1/2 werden erfasst. Die erfassten Pakete sind ICMP-Echo-Anfragen.
- Backplane-Schnittstellen Pakete, bei denen Ethernet1/2 als Ausgangsschnittstelle identifiziert wird, oder Pakete mit dem Port-VLAN 102 werden erfasst. Die erfassten Pakete sind ICMP-Echoantworten.

Topologie, Paketfluss und Erfassungspunkte



Konfiguration

FCM

Führen Sie die folgenden Schritte auf FCM aus, um eine Paketerfassung auf der FTD-Anwendung und dem Anwendungsport Ethernet1/2 zu konfigurieren:

1. Verwenden Sie **Tools > Packet Capture > Capture Session**, um eine neue Erfassungssitzung zu erstellen:

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		

2. Wählen Sie die FTD-Anwendung Ethernet1/2 in der Dropdown-Liste Application Port (Anwendungsport) aus, und wählen Sie All Packets (Alle Pakete) in Application Capture Direction (Anwendungserfassungsrichtung). Geben Sie den Sitzungsnamen an, und klicken Sie auf Save and Run, um die Aufzeichnung zu aktivieren:

Overview Interfaces Logical Devices Security Engine Platform Settings Systems	tem Tools Help admin
Select an instance: ftd1	Save Cancel
ftd1 Session Name" Cap1	
Selected Interfaces None	
Ebernal 1/2 Buffer Size 256 MB V	
Snap length: 1518 Bytes	
Store Packets Overwrite Append	
Capture On ftd 🔍	
Ethernet1/3 Application Port Ethemet1/2	
Ethernet1/10 Application Capture Direction All Packets Egress Packet	
Capture Filter Apply Filter Capture All	
Ethernet1/1	

FXOS-CLI

Führen Sie die folgenden Schritte auf der FXOS-CLI aus, um die Paketerfassung an Backplane-Schnittstellen zu konfigurieren:

1. Identifizieren Sie den Anwendungstyp und die Kennung:

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 _____ ____ 1 Enabled Online 7.2.0.82 7.2.0.82 ftd ftd1 Not Applicable None Native No 2. Eine Aufzeichnungssitzung erstellen: firepower# scope packet-capture firepower /packet-capture # create session cap1 firepower /packet-capture/session* # create phy-port eth1/2 firepower /packet-capture/session/phy-port* # set app-identifier ftd1 firepower /packet-capture/session/phy-port* # exit firepower /packet-capture/session* # create app-port 1 link12 Ethernet1/2 ftd firepower /packet-capture/session/app-port* # set app-identifier ftd1 firepower /packet-capture/session* # enable firepower /packet-capture/session* # commit

firepower /packet-capture/session # commit

Verifizierung

FCM

Überprüfen Sie den **Schnittstellennamen**, stellen Sie sicher, dass der **Betriebsstatus** aktiv ist und dass die **Dateigröße (in Byte)** ansteigt:

Overview Interfaces Logical Devices Security Engine Platform Settings System Tools Help admin											
Capture Session Filter List								_			
	C Refeet										
🔺 🔳 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	2						
Ethernet1/2 - Ethernet1/10	None	368	cap1-vethernet-1175.pcap	ftd1	*						
Ethernet1/2 - Ethernet1/9	None	13040	cap1-vethernet-1036.pcap	ftd1	4						

FXOS-CLI

Überprüfen Sie die Erfassungsdetails in der Paketerfassung:

```
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:
```

Erfassungsdateien erfassen

Befolgen Sie die Schritte im Abschnitt Sammeln von FirePOWER 4100/9300-internen Switch-Erfassungsdateien.

Analyse der Erfassungsdatei

Öffnen Sie die Erfassungsdateien mit einer Anwendung zum Lesen von Paketerfassungsdateien. Bei mehreren Backplane-Schnittstellen müssen alle Erfassungsdateien für jede Backplane-Schnittstelle geöffnet werden. In diesem Fall werden die Pakete an der Backplane-Schnittstelle Ethernet1/9 erfasst.

Öffnen Sie die Erfassungsdatei für die Schnittstelle Ethernet1/2, wählen Sie das erste Paket aus, und überprüfen Sie die Schlüsselpunkte:

- 1. Nur ICMP-Echoanforderungspakete werden erfasst. Jedes Paket wird erfasst und zweimal angezeigt.
- 2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.
- 3. Der interne Switch fügt den zusätzlichen Port-VLAN-Tag **102 ein**, der die Eingangsschnittstelle Ethernet1/2 identifiziert.
- 4. Der interne Switch fügt einen zusätzlichen VN-Tag ein.

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) requ	est 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) requ	est 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) requ	est id=0x0013, seg=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) requ	est id=0x0013, seg=1/256, ttl=64 (no response found!)
	5 2022-08-01 11:33:20.072036625	192.0.2.100	198,51,100,100	TCMP	108	8xc8ae (49326)	64 Echo (ping) requ	est id=0x0013, sed=2/512, ttl=64 (no response found))
	6 2022-09-01 11-22-20 072029200	192 8 2 188	109 51 100 100	TCMP	102	0xc0ae (49326)	64 Echo (ping) requ	et id-9x9913 con-2/512 ttl-64 (no response found))
	0 2022-00-01 11:33:20.072030399	192.0.2.100	198.51.100.100	TCHP	102	0xc0ae (49520)	ou echo (ping) requ	est 10-0x0015, seq=2/512, ct1=04 (no response found))
	7 2022-08-01 11:33:21.073266030	192.0.2.100	198.51.100.100	ICMP	108	0xc167 (49511)	64 Ecno (ping) requ	est 1d=0x0013, seq=3/768, tt1=64 (no response round)
	8 2022-08-01 11:33:21.073268327	192.0.2.100	198.51.100.100	ICMP	102	0xc167 (49511)	64 Echo (ping) requ	est 1d=0x0013, seq=3/768, tt1=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) requ	est 1d=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) requ	est id=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) requ	est id=0x0013, seq=5/1280, ttl=64 (no response found!)
	12 2022-08-01 11:33:23.075781513	192.0.2.100	198.51.100.100	ICMP	102	0xc208 (49672)	64 Echo (ping) requ	est id=0x0013, seg=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	Øxc211 (49681)	64 Echo (ping) requ	est id=0x0013, seg=6/1536, ttl=64 (no response found!)
	14 2022-08-01 11:33:24.081841386	192.0.2.100	198,51,100,100	ICMP	102	0xc211 (49681)	64 Echo (ping) requ	est id=0x0013, sed=6/1536, ttl=64 (no response found!)
	15 2022-08-01 11:33:25 105806249	192.0.2.100	198,51,100,100	TCMP	108	0xc2e2 (49898)	64 Echo (ning) requ	est id=0x0013, sen=7/1792, ttl=64 (no response found))
	16 2022 08 01 11:33:25 105007005	102 0 2 100	109 51 100 100	TCMD	100	0xc2o2 (40000)	64 Echo (ping) requ	st (d-0x001) co-7/1702 ttl-64 (no resonance found)
	10 2022-08-01 11.33.23.10380/893	192.0.2.100	198.51.100.100	TCHP	102	0xc2ez (49890)	ou Echo (ping) requ	est id orobits, seq=//1/22, tileo4 (no response found)
	1/ 2022-08-01 11:33:26.1298362/8	192.0.2.100	198.51.100.100	ICMP	108	0XC304 (50100)	64 Echo (ping) requ	1d=0x0013, Seq=8/2048, ttl=64 (no response round)
	18 2022-08-01 11:33:26.129838114	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100)	64 Echo (ping) requ	est 1d=0x0013, seq=8/2048, ttl=64 (no response tound!)
	19 2022-08-01 11:33:27.153828653	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294)	64 Echo (ping) requ	est 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) requ	est 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) requ	est 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) requ	est 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) requ	est 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) requ	est id=0x0013, seg=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) requ	est id=0x0013, seg=12/3072, ttl=64 (no response found!)
	26 2022-08-01 11:33:30 225836835	192.0.2.100	198.51.100.100	TCMP	102	Bxc585 (58565)	64 Echo (ping) requ	est id=0x0013, seg=12/3072, ttl=64 (no response found))
	27 2022 00 01 11:22:21 240920055	102 0 2 100	109 51 100 100	TCMD	102	0xc610 (50713)	64 Echo (ping) room	st id-avaals sequel/332 +ti-64 (no regranme found)
	27 2022-08-01 11.33.31.249626933	192.0.2.100	198.51.100.100	TCHP	100	0x0018 (50712)	ou celo (ping) requ	est id-ocous, seq-15/5528, til-oq (ib response found)
	28 2022-08-01 11:33:31.249831121	192.0.2.100	198.51.100.100	TCMP	102	0xc618 (50/12)	64 Ecno (ping) requ	est 1d=0x0013, seq=13/3328, tt1=64 (no response round)
	29 2022-08-01 11:33:32.273867960	192.0.2.100	198.51.100.100	ICMP	108	0xc64f (50767)	64 Echo (ping) requ	est 1d=0x0013, seq=14/3584, ttl=64 (no response found!)
<								
>	Frame 1: 108 bytes on wire (864 bi	ts), 108 bytes ca	ptured (864 bits) o	n interface ca	pture_u0_	1, id 0		0000 58 97 bd b9 77 0e 00 50 56 9d e8 be 89 26 80 0a X···₩··P V····&··
>	Ethernet II, Src: VMware 9d:e8:be	(00:50:56:9d:e8:b	e), Dst: Cisco b9:7	7:0e (58:97:bd	:b9:77:0e)		0010 00 00 81 00 00 66 08 00 45 00 00 54 c0 09 40 00 ·····f·· E··T··@·
4	VN-Tag							0020 40 01 8d a3 c0 00 02 64 c6 33 64 64 08 00 8d 7c @·····d ·3dd···
	1	= Directi	ion: From Bridge					0030 00 13 00 01 f2 b9 e7 62 00 00 00 cb 7f 06 00b
	.0	= Pointer	vif id					0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b
		= Destina	tion: 10					0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ···· !"# \$%&"()"+
		= Looped:	No	• •				0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,/0123 4567
			4.0	+ 1				
		= Reserve	rd: 0					
		= Version	1: 0					
	0000 00	00 0000 = Source:	. 0					
L	Type: 802.1Q Virtual LAN (0x8100)						
4	802.1Q Virtual LAN, PRI: 0, DEI: 0	, ID: 102						
	000 = Priority:	Best Effort (defa	ault) (0)					
	0 = DEI: Ineli	gible		21				
	0000 0110 0110 = ID: 102			1				
	Type: IPv4 (8x8888)							
	Internet Protocol Version 4 Sect	192.0.2.100. Det+	198.51.100.100					
1	Internet Control Message Protocol		10010111001100					
1	incense control nessage Protocol			-				

Wählen Sie das zweite Paket aus, und überprüfen Sie die wichtigsten Punkte:

- 1. Nur ICMP-Echoanforderungspakete werden erfasst. Jedes Paket wird erfasst und zweimal angezeigt.
- 2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.
- 3. Der interne Switch fügt den zusätzlichen Port-VLAN-Tag **102 ein**, der die Eingangsschnittstelle Ethernet1/2 identifiziert.

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	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) re	equest	id=0x0013, seq=1/256, ttl=64 (no response found!)
	3 2022-08-01 11:33:19.071217121	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping) re	equest	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) re	equest	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) re	equest	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) re	equest	id=0x0013, seq=2/512, ttl=64 (no response found!)
	7 2022-08-01 11:33:21.073266030	192.0.2.100	198.51.100.100	ICMP	108	0xc167 (49511)	64 Echo (ping) re	equest	id=0x0013, seq=3/768, ttl=64 (no response found!)
	8 2022-08-01 11:33:21.073268327	192.0.2.100	198.51.100.100	ICMP	102	0xc167 (49511)	64 Echo (ping) re	equest	id=0x0013, seq=3/768, ttl=64 (no response found!)
	9 2022-08-01 11:33:22.074576640	192.0.2.100	198.51.100.100	ICMP	108	0xc175 (49525)	64 Echo (ping) re	equest	id=0x0013, seq=4/1024, ttl=64 (no response found!)
	10 2022-08-01 11:33:22.074578010	192.0.2.100	198.51.100.100	ICMP	102	0xc175 (49525)	64 Echo (ping) re	equest	id=0x0013, seg=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	id=0x0013, seg=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	id=0x0013, seg=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	id=0x0013, seg=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	id=0x0013, seg=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	id=0x0013, seg=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) re	equest	id=0x0013, seg=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	id=0x0013, seg=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	id=0x0013, seg=8/2048, ttl=64 (no response found!)
	19 2022-08-01 11:33:27,153828653	192.0.2.100	198,51,100,100	ICMP	108	0xc476 (50294)	64 Echo (ping) re	equest	id=0x0013, seg=9/2304, ttl=64 (no response found!)
H	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	id=0x0013, seg=9/2304, ttl=64 (no response found!)
	21 2022-08-01 11:33:28.177847175	192.0.2.100	198,51,100,100	ICMP	108	0xc516 (50454)	64 Echo (ping) re	equest	id=0x0013, seg=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	id=0x0013, seg=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	id=0x0013, seg=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	id=0x0013, seg=11/2816, ttl=64 (no response found))
	25 2022-08-01 11:33:30.225834765	192.0.2.100	198, 51, 100, 100	TCMP	188	8xc585 (58565)	64 Echo (ping) r	equest	id=0x0013, seg=12/3072, ttl=64 (no response foundl)
	26 2022-08-01 11:33:30.225836835	192.0.2.100	198, 51, 100, 100	TCMP	102	8xc585 (58565)	64 Echo (ping) r	equest	id=0x0013, seg=12/3072, ttl=64 (no response foundl)
	27 2022-08-01 11:33:31 249828955	192.0.2.100	198.51.100.100	TCMP	108	8xc618 (50712)	64 Echo (ping) r	equest	id=0x0013, seq=13/3328, ttl=64 (no response foundl)
	28 2022-08-01 11:33:31 249831121	192.0.2.100	198.51.100.100	TCMP	102	8xc618 (50712)	64 Echo (ping) r	equest	id=0x0013, seq=13/3328, ttl=64 (no response found1)
	20 2022-00-01 11:33:32 273967060	192 0 2 100	109 51 100 100	TCMP	109	0xc64f (50767)	64 Echo (ping) r	aquest	(d-0x0013, seq=14/3504, ttl=64 (no response found1)
÷.	29 2022-00-01 111551521275007500	19210121100	19019111001100	1CHP	100	0,0041 (30707)	ow cento (pring) in	equese	re-oxoors, seq-rayssay, cer-oa (no response roanor)
÷.	From A. ARD but a color from his		should fold hits a						
2	Frame 2: 102 bytes on wire (816 bit	(s), 102 Dytes ca	ptured (816 bits) o	n interface ca	ipture_ue_	1, 10 0		0000	3 58 97 D0 09 77 00 00 50 50 90 08 00 81 00 00 00 X W P V T
	Ethernet II, Src: VMware 90:08:De (00:50:56:90:08:0	e), DSC: C1SCO D9:7	1:06 (28:31:00	1:09:77:00	:)		0020	0 02 64 66 33 64 64 08 00 8d 7c 00 13 00 01 f2 b0 dd 3dd dd dd
Ϋ́	802.10 VIPTUAL LAN, PRI: 0, DEI: 0,	, 10: 102						0030	e7 62 00 00 00 00 cb 7f 06 00 00 00 00 00 10 11
	000 = Priority:	Best Effort (deta	suit) (0)					0046	0 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21
	0 = DEI: Ineli	gible						0056	0 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 "#\$%&'() *+,/01
	0000 0110 0110 = ID: 102							0066	0 32 33 34 35 36 37 234567
L	Type: 1PV4 (0x0800)		100 51 100 100	_					
12	Internet Protocol Version 4, Src: 1	192.0.2.100, Dst:	198.51.100.100						
12	Internet Control Message Protocol								
1									

Öffnen Sie die Erfassungsdatei für die Schnittstelle Ethernet1/9, wählen Sie das erste und das zweite Paket aus, und überprüfen Sie die Schlüsselpunkte:

- 1. Jede ICMP-Echoantwort wird erfasst und zweimal angezeigt.
- 2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.
- 3. Der interne Switch fügt den zusätzlichen Port-VLAN-Tag **102 ein**, der die Ausgangsschnittstelle Ethernet1/2 identifiziert.
- 4. Der interne Switch fügt einen zusätzlichen VN-Tag ein.

1 2022-08-01 11:33:19.071512698 198.51.100.100 192.0.2.100 ICMP 108 0x4f27 (20263) 64 Echo (ping) reply id=0x0013, seq=1/256, ttl=64	
2 2022-08-01 11:33:19.071514882 198.51.100.100 192.0.2.100 ICMP 108 00477 (20263) 64 Echo (ping) reply id=0x0013, seq=1/256, tfl=64	
3 2022-08-01 11:33:20.072677302 108-51 100-100-102-0-2-100 ICMP 108 MIDLU (20072) 88 (10) 10001 10002 (00) 3 (00-2)(513-00)	
5 AVAL 00 04 ARTSTANTOTOR ASSISTANTION ASSISTANTION AND AND AND AND AND AND AND AND AND AN	
4 2022-08-01 11:33:20,072679384 198,51,100,100 192,0,2,100 ICMP 108 0x4ffb (20475) 64 Echo (ping) reply id=0x0013, seg=2/512, ttl=64	
5 2022-08-01 11:33:21.073913640 198.51.100.100 192.0.2.100 ICMP 108 0x50ac (20052) 64 Echo (ping) reply id=0x0013, seg=3/768, ttl=64	
6 2022-08-01 11:33:21.073015690 198.51.100.100 192.0.2.100 ICMP 108 0x50ac (20652) 64 Echo (ning) renty id=0x0013. Sec=3/768. tt]=64	
7 2012 00 01 11-32-32 075220201 100 51 100 102 0 2 100 1700 100 05120 (2027) 04 5100 (2027) 10 04 510 (2027) 10 04 510 (2027)	
r_{2022} - r_{200} - r_{2012} - r_{2	
9 2022-08-01 11:35:23.076447152 198:51.108.100 192.07.100 100 100 100 000 000 000 000 000 000 000 000 000 000 000 0000	
10 2022-08-01 11:33:25.0/6440903 198.51.100.100 192.0.2.100 ICMP 108 0X51C9 (20957) 64 ECho (ping) Peply 10-0X0013, Seq=5/1280, TC1=64	
11 2022-08-01 11:33:24.082407896 198.51.100.100 192.0.2.100 ICMP 108 0x528e (21134) 64 Echo (ping) reply id=0x0013, seq=6/1536, ttl=64	
12 2022-08-01 11:33:24.082410099 198.51.100.100 192.0.2.100 ICMP 108 0x528e (21134) 64 Echo (ping) reply id=0x0013, seq=6/1536, ttl=64	
13 2022-08-01 11:33:25.106382424 198.51.100.100 192.0.2.100 ICMP 108 0x52af (21167) 64 Echo (ping) reply id=0x0013, seq=7/1792, ttl=64	
14 2022-08-01 11:33:25.106384549 198.51.100.100 192.0.2.100 ICMP 108 0x52af (21167) 64 Echo (ping) reply id=0x0013, seq=7/1792, ttl=64	
15 2022-08-01 11:33:26.130437851 198.51.100.100 192.0.2.100 ICMP 108 0x53a6 (21414) 64 Echo (ping) reply id=0x0013, seq=8/2048, ttl=64	
16 2022-08-01 11:33:26.130440320 198.51.100.100 192.0.2.100 ICMP 108 0x53a6 (21414) 64 Echo (ping) reply id=0x0013, seq=8/2048, ttl=64	
17 2022-08-01 11:33:27.154398212 198.51.100.100 192.0.2.100 ICMP 108 0x5446 (21574) 64 Echo (ping) reply id=0x0013, seq=9/2304, ttl=64	
18 2022-08-01 11:33:27.154400198 198.51.100.100 192.0.2.100 ICMP 108 0x5446 (21574) 64 Echo (ping) reply id=0x0013, seq=9/2304, ttl=64	
19 2022-08-01 11:33:28.178469866 198.51.100.100 192.0.2.100 ICMP 108 0x5493 (21651) 64 Echo (ping) reply id=0x0013, seq=10/2560, ttl=64	
20 2022-08-01 11:33:28.178471810 198.51.100.100 192.0.2.100 ICMP 108 0x5493 (21651) 64 Echo (ping) reply id=0x0013, seg=10/2560, ttl=64	
21 2022-08-01 11:33:29,202395869 198,51,100,100 192,0,2,100 ICMP 108 0x54f4 (21748) 64 Echo (ping) reply id=0x0013, seg=11/2816, ttl=64	
22 2022-08-01 11:33:29.202398067 198.51.100.100 192.0.2.100 ICMP 108 0x54f4 (21748) 64 Echo (ping) reply id=0x0013, seg=11/2816, ttl=64	
23 202-08-01 11:33:30.220(308735 198.51.100.100 102.0.2.100 TCMP 108 0x5526 (21708) 64 Frido (rind) rendy id=0x0013, securit/3072, thi=44	
$24202.08.0111+32-30.226401017$ 198 \$1.100.100 102.0.2.100 T(MP 108 00556 (21700) 64 Etho (nine) rendu (46000013. com12/3072. ± 1 = 4	
100 100	
252022 00 11153531220507000 190.531400.100 192.021400 100 192.021400 100 005312 (22002) 04 CUO (ping) reply 10-0000135, $50q^{-1}373230$, $11-04$	
26 2022-08-01 11:35:51.2505899/1 198.51.100.100 192.0.2.100 ICMP 108 0X5572 (22002) 64 ECRO (ping) Fepiy 10-0500013, 50q-13/33/8, TT1=64	
2/2022-08-01 11:33:32.2/4416011 198.51.100.100 192.0.2.100 ICMP 108 0X5660 (22112) 64 ECNO (ping) Fepiy 10-000013, 5eq=14/5584, TT1=64	
28 2022-08-01 11:33:32.274418229 198.51.100.100 192.0.2.100 ICMP 108 0x5660 (22112) 64 Echo (ping) reply id=0x0013, seq=14/3584, ttl=64	
29 2022-08-01 11:33:33.298397657 198.51.100.100 192.0.2.100 ICMP 108 0x5667 (22247) 64 Echo (ping) reply id=0x0013, seq=15/3840, ttl=64	
> Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0 000 00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00 • PV · · ·	w&
Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VMware 9d:e8:be (00:50:56:9d:e8:be) 0010 00 0a 81 00 00 66 08 00 45 00 00 54 4f 27 00 00f	E TO'
VN-Tag 0020 40 01 3e 86 c6 33 64 64 c0 00 02 64 00 00 95 7c (e)->-3	dd]
0 = Direction: To Bridge	b
.0 = Pointer: vif id	
00 0000 0000 = Destination: 0	# \$58 ()"+
0000 2c 2a 2e 2T 30 31 32 33 54 35 36 37 ,=./01	3 4567
Type: 802.10 Virtual LAN (0x8100)	
(a) an up and a contraction (waxaw)	
and a prior the second se	
Internet Protocol Version 4, Src: 198.51.100.100, DST: 192.0.2.100	
Internet control Message Protocol	

No. Time	Source	Destination	Protocol	Length	PD	IP TTL Wo	_	
1 2022-08-01 11:33:19.071512698	198.51.100.100	192.0.2.100	ICMP	108 -	0x4f27 (20263)	64 Echo (ping) repl	ly :	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	ly :	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	0X4TTD (28475)	64 ECHO (ping) repi	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	ly i	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	ly i	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	Ly :	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	ly i	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	ly i	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	Ly i	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	ly i	id=0x0013, seq=5/1280, ttl=64
11 2022-08-01 11:33:24.082407896	198.51.100.100	192.0.2.100	ICMP	108	0x528e (21134)	64 Echo (ping) repl	ly i	id=0x0013, seq=6/1536, ttl=64
12 2022-08-01 11:33:24.082410099	198.51.100.100	192.0.2.100	ICMP	108	0x528e (21134)	64 Echo (ping) repl	Ly i	id=0x0013, seq=6/1536, ttl=64
13 2022-08-01 11:33:25.106382424	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64 Echo (ping) repl	ly i	id=0x0013, seq=7/1792, ttl=64
14 2022-08-01 11:33:25.106384549	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64 Echo (ping) repl	ly i	id=0x0013, seq=7/1792, ttl=64
15 2022-08-01 11:33:26.130437851	198.51.100.100	192.0.2.100	ICMP	108	0x53a6 (21414)	64 Echo (ping) repl	ly i	id=0x0013, seq=8/2048, ttl=64
16 2022-08-01 11:33:26.130440320	198.51.100.100	192.0.2.100	ICMP	108	0x53a6 (21414)	64 Echo (ping) repl	Ly i	id=0x0013, seq=8/2048, ttl=64
17 2022-08-01 11:33:27.154398212	198.51.100.100	192.0.2.100	ICMP	108	0x5446 (21574)	64 Echo (ping) repl	ly i	id=0x0013, seq=9/2304, ttl=64
18 2022-08-01 11:33:27.154400198	198.51.100.100	192.0.2.100	ICMP	108	0x5446 (21574)	64 Echo (ping) repl	Ly i	id=0x0013, seq=9/2304, ttl=64
19 2022-08-01 11:33:28.178469866	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64 Echo (ping) repl	ly i	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	Ly i	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	Ly i	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	ly i	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	ly i	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	Ly :	id=0x0013, seq=12/3072, ttl=64
25 2022-08-01 11:33:31.250387808	198.51.100.100	192.0.2.100	ICMP	108	0x55f2 (22002)	64 Echo (ping) repl	ly i	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	Ly i	id=0x0013, seq=13/3328, ttl=64
27 2022-08-01 11:33:32.274416011	198.51.100.100	192.0.2.100	ICMP	108	0x5660 (22112)	64 Echo (ping) repl	ly i	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	ly i	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	Ly i	id=0x0013, seq=15/3840, ttl=64
<								
> Frame 2: 108 bytes on wire (864 bit	ts), 108 bytes ca	ptured (864 bits) o	n interface ca	pture_u0	_8, id 0		0000	0 00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00 ·PV···X· ··₩··&··
> Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VMware 9d:e	8:be (00:50:50	:9d:e8:b	e)		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	= Direct:	ion: To Bridge					0030	00 13 00 01 f2 b9 e7 62 00 00 00 00 cb 7f 06 00b
.0	= Pointer	<pre>r: vif_id</pre>						00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 15
0000 0000 0000	= Destina	ation: 0					0050	1 10 10 10 17 20 21 22 23 24 25 20 27 28 29 28 20 ····· ! # \$48 () **
···· ··· ··· ··· ··· ··· 0 ···· ··	= Looped:	: No 🧹	11					20 20 20 20 21 30 31 52 55 54 55 50 57
0	= Reserve	ed: 0	* I					
	= Version	n: 0						
0000 00	00 1010 = Source:	: 10						
Type: 802.1Q Virtual LAN (0x8100)							
✓ 802.1Q Virtual LAN, PRI: 0, DEI: 0	ID: 102							
000 = Priority:	Best Effort (defa	ult) (0)						
0 = DEI: Ineli	gible		31					
0000 0110 0110 = ID: 102			-					
Type: IPv4 (0x0800)								
> Internet Protocol Version 4, Src: 1	198.51.100.100, D	st: 192.0.2.100 🖌						
> Internet Control Message Protocol			2					

Erklärung

Wenn die Option All Packets in the Application Capture Direction (Alle Pakete in Anwendungserfassungsrichtung) ausgewählt ist, werden zwei gleichzeitige Paketerfassungen für den ausgewählten Anwendungsport Ethernet1/2 konfiguriert: eine Erfassung an der vorderen Schnittstelle Ethernet1/2 und eine Erfassung an ausgewählten Backplane-Schnittstellen.

Wenn eine Paketerfassung an einer vorderen Schnittstelle konfiguriert ist, erfasst der Switch gleichzeitig jedes Paket zweimal:

- Nach dem Einfügen des Port-VLAN-Tags.
- Nach dem Einfügen des VN-Tags.

In der Reihenfolge der Vorgänge wird das VN-Tag zu einem späteren Zeitpunkt eingefügt als das Port-VLAN-Tag. In der Erfassungsdatei wird das Paket mit dem VN-Tag jedoch früher angezeigt als das Paket mit dem Port-VLAN-Tag. In diesem Beispiel identifiziert der VLAN-Tag 102 in den ICMP-Echoanforderungspaketen Ethernet1/2 als Eingangsschnittstelle.

Wenn eine Paketerfassung auf einer Backplane-Schnittstelle konfiguriert ist, erfasst der Switch gleichzeitig jedes Paket zweimal. Der interne Switch empfängt Pakete, die bereits von der Anwendung auf dem Sicherheitsmodul mit dem Port-VLAN-Tag und dem VN-Tag markiert wurden. Der Port-VLAN-Tag identifiziert die Ausgangsschnittstelle, über die das interne Chassis die Pakete an das Netzwerk weiterleitet. In diesem Beispiel identifiziert der VLAN-Tag 102 in ICMP-Echo-Antwort-Paketen Ethernet1/2 als Ausgangsschnittstelle.

Der interne Switch entfernt den VN-Tag und den VLAN-Tag der internen Schnittstelle, bevor die Pakete an das Netzwerk weitergeleitet werden.

In dieser Tabelle ist die Aufgabe zusammengefasst:

Aufacho	Erfassungs	Internes Port-VLAN	Dichtung	Erfacetor Datapyorkah
Augabe	punkt	in erfassten Paketen	Richlung	Chassler Dalenverken

Konfiguration und Verifizierung von	Backplane- Schnittstelle n	102	Nur Eingang	ICMP-Echo-Antworten von He 198.51.100.100 zu Host 192.0.2.100
Anwendungs- und Anwendungsport Ethernet1/2	Schnittstelle Ethernet1/2	102	Nur Eingang	ICMP-Echo-Anfragen von Ho 192.0.2.100 an Host 198.51.100.100

Paketerfassung auf einer Subschnittstelle einer physischen oder Port-Channel-Schnittstelle

Verwenden Sie FCM und CLI, um eine Paketerfassung an der Subschnittstelle Ethernet1/2.205 oder der Port-Channel-Subschnittstelle Port-Channel1.207 zu konfigurieren und zu überprüfen. Subschnittstellen und Erfassungen an Subschnittstellen werden nur für die FTD-Anwendung im Containermodus unterstützt. In diesem Fall wird eine Paketerfassung auf Ethernet1/2.205 und Port-Channel1.207 konfiguriert.

Topologie, Paketfluss und Erfassungspunkte



Konfiguration

FCM

Führen Sie die folgenden Schritte auf FCM aus, um eine Paketerfassung auf der FTD-Anwendung und dem Anwendungsport Ethernet1/2 zu konfigurieren:

1. Verwenden Sie Tools > Packet Capture > Capture Session, um eine neue Erfassungssitzung

zu erstellen:

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

2. Wählen Sie die spezifische Anwendungsinstanz ftd1, die Subschnittstelle Ethernet1/2.205, geben Sie den Sitzungsnamen an, und klicken Sie auf Speichern und Ausführen, um die Erfassung zu aktivieren:

Overview Interfaces Logical Devices Security Engine Platform Settings	System Tools Help admin
Select an instance: ftd1	Save and Run Save Cancel
Subinterface selection Tetal Tehemet1/2.203 Tehemet1/2.203 Tehemet1/2.203 Tehemet1/2.203 Tehemet1/2 Tehemet1/2 Tehemet1/3 Tehemet1/3 Tehemet1/3 Tehemet1/1 Tehemet1/3 Tehemet1/1 Tehemet1/2	Interfaces Ethernet1/2.205 256 MB V h: 1518 Bytes ets Overwrite Append ter Apply Filter Capture All

3. Im Fall einer Port-Channel-Subschnittstelle sind aufgrund der Cisco Bug-ID <u>CSCvq3119</u>-Subschnittstellen im FCM nicht sichtbar. Verwenden Sie die FXOS-CLI, um Erfassungen auf Port-Channel-Subschnittstellen zu konfigurieren.

FXOS-CLI

Befolgen Sie diese Schritte auf der FXOS-CLI, um eine Paketerfassung an den Subschnittstellen Ethernet1/2.205 und Port-Channel1.207 zu konfigurieren:

1. Identifizieren Sie den Anwendungstyp und die Kennung:

firepower#	scope ssa									
firepower /ssa # show app-instance										
App Name	Identifie	r Slot ID	Admin State	e Oper St	tate	Running Version	Startup Version			
Deploy Typ	e Turbo Moo	de Profile M	Name 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. Geben Sie bei einer Port-Channel-Schnittstelle deren Mitgliedsschnittstellen an:										

1	Pol(SU)	Eth	LACP	Eth1/3(P)	Eth1/3(P)	
(Channel					
Group	Port-	Туре	Protocol	Member Ports		
	M - Not in	use. Min	-links not	met		
	U - Up (por	rt-channe	1)			
	S - Switche	ed R-	Routed			
	s - Suspend	ded r-	Module-re	moved		

3. Eine Aufzeichnungssitzung erstellen:

firepower# scope packet-capture
firepower /packet-capture # create session cap1
firepower /packet-capture/session* # create phy-port Eth1/2
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # set subinterface 205
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # enable
firepower /packet-capture/session* # commit
firepower /packet-capture/session # commit

Erstellen Sie für Port-Channel-Subschnittstellen eine Paketerfassung für jede Port-Channel-Member-Schnittstelle:

```
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 #
Verifizieruna
```

FCM

Überprüfen Sie den **Schnittstellennamen**, stellen Sie sicher, dass der **Betriebsstatus** aktiv ist und dass die **Dateigröße (in Byte)** ansteigt:

Overview	Interfaces	Logical Devices Security Engli	e Platform Settings								System Tools	Help admin
Capture Ses	sion Filter List											
									C Refresh	Capture Session	Delete Al Sessions)
•	cap1	Drop Count: 0		Operational	l State: up	Buffer Size: 25	6 MB		Snap Length: 1518 Bytes			
Interface No	ime	Filter			File Size (in bytes)	File Name		Device Name				
Ethernet1/2.	205	None			233992	cap1-ethemet-1-2-0.pcap		ftd1	2			
	_			_								

Port-Channel-Subschnittstellenerfassungen, die auf FXOS CLI konfiguriert wurden, sind auch auf FCM sichtbar. Sie können jedoch nicht bearbeitet werden:

Overview Interfe	aces Logical Devices Security Eng	ine Platform Settings						System Too	is Help admin
Capture Session	Fiter List								
						C Refresh	Capture Session	Delete Al Sessi	pns
in 🔳 capt	1 Drop Count: 0	Operation	nal State: up	Buffe	Size: 256 MB	Snap Length: 1518 Bytes			4.8.2
Interface Name	Filter		File Size (in bytes)	File Name	Device Name				
Ethernet1/4.207	None		624160	cap1-ethernet-1-4-0.p	cap Not available	2			
Ethernet1/3.207	None		160	cap1-ethemet-1-3-0.p	cap Not available	*			
		•							

FXOS-CLI

Überprüfen Sie die Erfassungsdetails in der Paketerfassung:

```
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
```

Port-Channel 1 mit den Mitgliedsschnittstellen Ethernet1/3 und Ethernet1/4:

```
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
```

Erfassungsdateien erfassen

Befolgen Sie die Schritte im Abschnitt **Sammeln von FirePOWER 4100/9300-internen Switch-**Erfassungsdateien.

Analyse der Erfassungsdatei

Öffnen Sie die Erfassungsdatei mit einer Anwendung zum Lesen von Paketerfassungsdateien. Wählen Sie das erste Paket aus, und überprüfen Sie die wichtigsten Punkte:

- 1. Nur ICMP-Echoanforderungspakete werden erfasst. Jedes Paket wird erfasst und zweimal angezeigt.
- 2. Der ursprüngliche Paket-Header hat den VLAN-Tag 205.
- 3. Der interne Switch fügt den zusätzlichen Port-VLAN-Tag **102 ein**, der die Eingangsschnittstelle Ethernet1/2 identifiziert.
- 4. Der interne Switch fügt einen zusätzlichen VN-Tag ein.

No.	Time Sou	urce	Destination	Protocol	Length	PD	IP TTL Info	_	
F	1 2022-08-04 07:21:56.993302102 192	2.0.2.100	198.51.100.100	ICMP	112	0x9574 (38260)	64 Echo (ping) reque	est id	d=0x0022, seq=1/256, ttl=64 (no response found!)
	2 2022-08-04 07:21:56.993303597 192	2.0.2.100	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	2.0.2.100	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	2.0.2.100	198.51.100.100	ICMP	102	0x9a81 (39553)	64 Echo (ping) reque	est id	d=0x0022, seq=10/2560, ttl=64 (no response found!)
	5 2022-08-04 07:22:07.215113393 192	2.0.2.100	198.51.100.100	ICMP	112	0x9ac3 (39619)	64 Echo (ping) reque	est id	d=0x0022, seq=11/2816, ttl=64 (no response found!)
	6 2022-08-04 07:22:07.215115445 192	2.0.2.100	198.51.100.100	ICMP	102	0x9ac3 (39619)	64 Echo (ping) reque	est id	d=0x0022, seq=11/2816, ttl=64 (no response found!)
	7 2022-08-04 07:22:08.229938577 192	2.0.2.100	198.51.100.100	ICMP	112	0x9b33 (39731)	64 Echo (ping) reque	est id	d=0x0022, seq=12/3072, ttl=64 (no response found!)
	8 2022-08-04 07:22:08.229940829 192	2.0.2.100	198.51.100.100	ICMP	102	0x9b33 (39731)	64 Echo (ping) reque	est id	d=0x0022, seg=12/3072, ttl=64 (no response found!)
	9 2022-08-04 07:22:09.253944601 192	2.0.2.100	198.51.100.100	ICMP	112	0x9c0e (39950)	64 Echo (ping) reque	est id	d=0x0022, seg=13/3328, ttl=64 (no response found!)
	10 2022-08-04 07:22:09.253946899 192	2.0.2.100	198.51.100.100	ICMP	102	0x9c0e (39950)	64 Echo (ping) reque	est in	d=0x0022, seg=13/3328, ttl=64 (no response found!)
	11 2022-08-04 07:22:10.277953070 192	2.0.2.100	198.51.100.100	ICMP	112	0x9ccb (40139)	64 Echo (ping) reque	est in	d=0x0022, seg=14/3584, ttl=64 (no response found!)
	12 2022-08-04 07:22:10.277954736 192	2.0.2.100	198.51.100.100	TCMP	102	0x9ccb (40139)	64 Echo (ning) reque	est in	d=0x0022, seg=14/3584, ttl=64 (no response found))
	13 2022-08-04 07:22:11.301931282 193	2.0.2.100	198.51.100.100	TCMP	112	0x9d84 (40324)	64 Echo (ning) reque	est in	d=0x0022, seg=15/3840, ttl=64 (no response found1)
	14 2022-08-04 07:22:11 301933600 193	2.0.2.100	198.51.100.100	TCMP	102	0x9d84 (40324)	64 Echo (ping) reque	ast in	d=0x0022, seq=15/3840, ttl=64 (no response found1)
	15 2022-08-04 07:22:12.325936521 193	2.0.2.100	198.51.100.100	TCMP	112	0x9da2 (40354)	64 Echo (ning) reque	est in	d=0x0022, seg=16/4096, ttl=64 (no response found))
	16 2022-00-04 07:22:12:325930321 19	2.0.2.100	100 51 100 100	TCMP	102	0x0da2 (40354)	64 Echo (ping) reque	act in	d=0x0022, seq=16/4006, ttl=64 (no response found1)
	17 2022-00-04 07:22:12:323537655 157	2.0.2.100	100 51 100 100	TCMP	112	0x9007 (40455)	64 Echo (ping) reque	oct in	d=0x0022, seq=17/4050, tt1=04 (no response found1)
	10 2022-00-04 07:22:13:320988040 192	2.0.2.100	198.51.100.100	TCMD	102	0x9e07 (40455)	64 Echo (ping) reque	est it	d=0x0022, seq=17/4352, ttl=64 (no response found!)
	10 2022-08-04 07.22.15.520990256 192	2.0.2.100	198.51.100.100	TCHP	102	0x9007 (40433)	64 Echo (ping) reque	est it	d-0x0022, seq=17/4532, ttl=04 (no response found:)
	19 2022-08-04 07:22:14.341944773 192	2.0.2.100	198.51.100.100	TCHP	112	0x900a (40554)	64 Echo (ping) reque	est it	d=0x0022, seq=10/4600, ttl=64 (no response found:)
	20 2022-08-04 07:22:14.341946249 192	2.0.2.100	198.51.100.100	ICMP	102	0x906a (40554)	64 Echo (ping) reque	est 10	d=0x0022, seq=18/4608, tt1=64 (no response found!)
	21 2022-08-04 07:22:15.365941588 192	2.0.2.100	198.51.100.100	ICMP	112	0X90TD (40699)	64 Echo (ping) reque	est 10	d=0x0022, seq=19/4864, ttl=64 (no response found)
	22 2022-08-04 07:22:15.365942566 192	2.0.2.100	198.51.100.100	ICMP	102	0X90TD (40699)	64 Echo (ping) reque	est 10	d=0x0022, seq=19/4864, tt1=64 (no response round!)
	23 2022-08-04 07:22:16.389973843 192	2.0.2.100	198.51.100.100	ICMP	112	0x91e8 (40936)	64 Echo (ping) reque	est 10	d=0x0022, seq=20/5120, tt1=64 (no response found!)
	24 2022-08-04 07:22:16.389975129 192	2.0.2.100	198.51.100.100	ICMP	102	0x9te8 (40936)	64 Echo (ping) reque	est 10	d=0x0022, seq=20/5120, tt1=64 (no response found!)
	25 2022-08-04 07:22:17.413936452 192	2.0.2.100	198.51.100.100	ICMP	112	0xa079 (41081)	64 Echo (ping) reque	est i	d=0x0022, seq=21/5376, ttl=64 (no response found!)
	26 2022-08-04 07:22:17.413938090 192	2.0.2.100	198.51.100.100	ICMP	102	0xa079 (41081)	64 Echo (ping) reque	est i	d=0x0022, seq=21/5376, ttl=64 (no response found!)
	27 2022-08-04 07:22:18.437954335 192	2.0.2.100	198.51.100.100	ICMP	112	0xa11e (41246)	64 Echo (ping) reque	est i	d=0x0022, seq=22/5632, ttl=64 (no response found!)
é II									
>	Frame 1: 112 bytes on wire (896 bits).	112 hytes can	tured (896 hits) or	interface car	nture ue :	1. id 0		0000	a2 76 f2 00 00 1b 00 50 56 9d e8 be 89 26 80 54
>	Frame 1: 112 bytes on wire (896 bits), Ethernet II. Src: Whware 9d:e8:be (00:	112 bytes cap 58:56:9d:e8:be	tured (896 bits) or	interface cap	pture_u0_	1, id 0		0000 0010	a2 76 f2 00 00 1b 00 50 56 9d e8 be 89 26 80 54 ···································
>	Frame 1: 112 bytes on wire (896 bits), Ethernet II, Src: WMware 9d:e8:be (00: WN-Tag	112 bytes cap 50:56:9d:e8:be	tured (896 bits) or), Dst: a2:76:f2:00	interface cap :00:1b (a2:76	pture_u0_ :f2:00:00	1, id 0 :1b)		0000 0010 0020	a2 76 f2 00 00 1b 00 50 50 9d e8 be 89 26 80 54 · · · · · · · P V · · · & · T 00 00 81 00 00 66 81 00 00 cd 08 00 45 00 00 54 · · · · · f · · · · E · T 95 74 40 00 40 01 b8 8 c 00 00 264 c6 33 64 · · tûệ e8 · · · d-3dd
>	Frame 1: 112 bytes on wire (896 bits), Ethernet II, Src: VMware 9d:e8:be (00: VN-Tag	112 bytes cap 50:56:9d:e8:be	tured (896 bits) or), Dst: a2:76:f2:00	interface ca :00:1b (a2:76	pture_u0_ :f2:00:00	1, id 0 :1b)		0000 0010 0020 0030	a2 76 f2 00 00 10 30 56 9d e8 b8 26 80 54 -v +P v *P v *P *P * & * & * & * & & & * * * * & * * & * * *
>	Frame 1: 112 bytes on wire (896 bits), Ethernet II, Src: VMware 9d:e8:be (00: VN-Tag 1	112 bytes cap 50:56:9d:e8:be = Directio	tured (896 bits) or), Dst: a2:76:f2:00 n: From Bridge vif id	interface ca 1:00:1b (a2:76	pture_u0_ :f2:00:00	1, id 0 :1b)		0000 0010 0020 0030 0040	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
>	Frame 1: 112 bytes on wire (896 bits), Ethernet II, Src: VMware 9d:e8:be (00: VN-Tag 1	112 bytes cap 50:56:9d:e8:be = Directio = Pointer:	tured (896 bits) or), Dst: a2:76:f2:00 n: From Bridge vif_id ion: 84	interface ca 1:00:1b (a2:76	pture_u0_ :f2:00:00	1, id 0 :1b)		0000 0010 0020 0030 0040 0050	a2 76 f2 00 00 1b $\frac{50}{50}$ $\frac{56}{50}$ $\frac{9d}{50}$ 88 b8 89 26 80 54 $\frac{1}{50}$
>	Frame 1: 112 bytes on wire (896 bits), Ethernet II, src: VMware 9d:e8:be (60: VM-Tag 1	112 bytes cap 50:56:9d:e8:be = Directio = Pointer: = Destinat	tured (896 bits) or), Dst: a2:76:f2:00 n: From Bridge vif_id ion: 84 No	interface cap :00:1b (a2:76	pture_u0_ :f2:00:00	1, id 0 :1b)		0000 0010 0020 0030 0040 0050 0050	a2 76 f2 00 00 10 00 56 9d e8 b8 92 f8 54 $\cdot \vee \cdot \cdot \cdot \cdot$ $\cdot \vee \cdot \cdot \cdot \cdot$ $\cdot \vee \cdot \cdot \cdot \cdot \cdot$ $\cdot \cdot \cdot$ $\cdot \vee \cdot \cdot$
>	Frame 1: 112 bytes on wire (896 bits), Ethernet II, Src: Whware 9d:e8:be (00: VN-Tag 1	112 bytes cap 50:56:9d:e8:be = Directio = Pointer: = Destinat = Looped:	tured (896 bits) or), Dst: a2:76:f2:00 n: From Bridge vif_id ion: 84 No 4	interface cap :00:1b (a2:76	pture_u0_: :f2:00:00	1, id 0 :1b)		0000 0010 0020 0030 0040 0050 0050	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
> >	Frame 1: 112 bytes on wire (896 bits), Ethernet II, Src: Wware 9d:e8:be (80: VM-Tag 1	112 bytes cap 50:56:9d:e8:be = Directio = Pointer: = Destinat = Reserved - Verrigon	tured (896 bits) or), Dst: a2:76:f2:00 n: From Bridge vif_id ion: 84 No 2	interface cap :00:1b (a2:76	pture_u0_ :f2:00:00	1, id 0 :1b)		0000 0010 0020 0030 0040 0050 0050	a2 76 f2 00 00 1b $\frac{50}{50}$ $\frac{56}{50}$ 9d e8 be 89 26 80 54 $\frac{12}{50}$
> >	Frame 1: 112 bytes on wire (896 bits), Ethernet II, Src: Whware 9d:e8:be (00: VN-Tag 1. .00 0000 0101 0100 	112 bytes cap S0:56:9d:e8:be Pointer: Destinat Cooped: Reserved Version: Version:	tured (896 bits) or), Dst: a2:76:f2:00 n: From Bridge vif_id ion: 84 No 2 0 0	interface cap :00:1b (a2:76	pture_u0_ :f2:00:00	1, id 0 :1b)		0000 0010 0020 0030 0040 0050 0050	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$
>	Frame 1: 112 bytes on wire (896 bits), Ethernet II, Src: Wware 9d:e8:be (80: WH-Tag 1	112 bytes cap 50:56:9d:e8:be = Directio = Pointer: = Dospinational = Looped: = Reserved = Version: 8000 = Source:	tured (896 bits) or), Dst: a2:76:f2:06 vif_id ion: 84 No 6 0	interface caj :00:1b (a2:76:	pture_u0_ :f2:00:00	1, id 0 :1b)		0000 0010 0020 0030 0040 0050 0060	a2 76 f2 00 00 1b $\frac{10}{50}$ $\frac{56}{50}$ 9d e8 be 89 26 80 54 $\frac{1}{50}$ $\frac{1}{5$
>	Frame 1: 112 bytes on wire (896 bits), Ethernet II, Src: Wwware 9d:e8:be (00: VNF-Tag 1. .00 0000 0101 0100 .00 .00 .00 .00 .00 0000 0101 0100 .00 .00 0000 00	112 bytes cap 50:56:9d:e8:be 	tured (896 bits) or), Dst: a2:76:f2:00 n: From Bridge vif_id ion: 84 No 0 0 0	interface ca 1989:1b (a2:76	pture_u0_ :f2:00:00	1, id 0 :1b)		0000 0010 0020 0030 0040 0050 0060	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$
> > >	Frame 1: 112 bytes on wire (896 bits), Ethernet II, Src: Whware 9d:e8:be (00: VN-Tag 1	112 bytes cap 50:56:9d:e8:be = Directio = Pointer: = Looped: = Reserved = Version: 0000 = Source: b: 102	tured (896 bits) or), Dst: a2:76:f2:00 n: From Bridge vif_id ion: 84 No 0 0 0	interface ca :00:1b (a2:76	pture_u0_ :f2:00:00	1, id 0 :1b)		0000 0010 0020 0030 0040 0050 0060	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$
> > >	Frame 1: 112 bytes on wire (896 bits), Ethernet 11, Src: Wware 9d:e8:be (00: Wir-Tag 1	112 bytes cap 50:56:9d:e8:be Pointer: Destinat Looped: Reserved: Version: 00000 = Source: 102 t Effort (defau	tured (896 bits) or), Dst: a2:76:f2:00 n: From Bridge vif_id ion: 84 No 0 0 0	interface cap :00:1b (a2:76)	pture_u0_ :f2:00:00	1, id 0 :1b)		0000 0010 0020 0030 0040 0050 0060	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$
> > >	Frame 1: 112 bytes on wire (896 bits), Ethernet II, Src: Wware 9d:e8:be (00: VN-Tag 1. .0. .00 0000 010 0100 	112 bytes cap 50:56:9d:e8:be = Directio = Pointer: = Destinat = Looped: = Reserved = Version: 0000 = Source: b: 102 t Effort (defau le	tured (896 bits) or), Dst: a2:76:f2:00 n: From Bridge vif_id ion: 84 No 0 0 0 11) (0) 3	interface ca :00:1b (a2:76	pture_u0_ :f2:00:00	1, id 0 :1b)		0000 0010 0020 0030 0040 0050 0060	a2 76 f2 00 00 1b $\frac{50}{50}$ $\frac{56}{50}$ 9d e8 be 89 26 80 54 00 00 81 00 00 66 81 00 00 00 64 00 00 54 95 74 40 00 40 1b 83 00 00 00 40 00 00 54 08 00 eb 95 00 22 00 01 88 73 eb 62 00 00 00 00 95 9d 00 00 00 00 00 00 10 11 21 21 41 51 61 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ()**,/ 01234567
> > > >	Frame 1: 112 bytes on wire (896 bits), Ethernet 11, Src: Wware 9d:e8:be (00: Wir-Tag 1	<pre>112 bytes cap 50:56:9d:e8:be = Directio = Pointer: = Destinat = Looped: = Reserved = Version 0000 = Source: D: 102 t Effort (defau le</pre>	tured (896 bits) or), Dit: a2:76:172:00 n: From Bridge vif_id ion: 84 NO 0 0 11) (0) 3	interface ca :00:1b (a2:76	pture_u0_ :f2:00:00	1, id 0 :1b)		0000 0010 0020 0030 0040 0050 0050	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$
> > >	Frame 1: 112 bytes on wire (896 bits), Ethernet II, Src: Wwware 9d:e8:be (00: Wi-Tag 1. .00 0000 0101 0100 .00 0000 0101 0100 .00 0000 000 000 .00 .0000 0000 00	<pre>112 bytes cap 50:56:9d:e8:be = Directio = Pointer: = Destinat = Looped: = Reserved = Version: 0000 = Source: b: 102 t Effort (defau le</pre>	tured (896 bits) or), Dst: a2:76:f2:00 n: From Bridge vif_id ion: 84 No 0 0 11) (0) 3	interface ca :00:1b (a2:76	pture_u0_ :f2:00:00	1, id 0 :1b)		0000 0010 0020 0030 0040 0050 0060	a2 76 f2 00 00 1b $\frac{50}{50}$ 56 9d e8 be 89 26 80 54 00 00 81 00 00 66 81 00 00 00 48 00 45 00 00 54 95 74 40 00 40 1b 83 00 00 c6 40 32 64 66 33 64 64 08 00 eb 95 00 22 00 01 88 73 eb 62 00 00 00 00 99 50 00 00 00 00 00 10 11 21 31 41 51 61 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ()*+,-/ 01234567
> > >	Frame 1: 112 bytes on wire (896 bits), Ethernet II, Src: Wware 9d:e8:be (00: Wir-Tag 1	<pre>112 bytes cap 50:56:9d:e8:be = Directio Pointer: = Destint Looped: = Reserved = Reser</pre>	tured (896 bits) or), Dit: a2:76:172:00 n: From Bridge vif_id ion: 84 No 0 0 111 (0) 3	interface ca :00:1b (a2:76	pture_u0_ :f2:00:00	1, id 0 :1b)		0000 0010 0020 0030 0040 0050 0050	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$
> > > > > > >	Frame 1: 112 bytes on wire (896 bits), Ethernet II, Src: Wware 9d:e8:be (00: Wir-Tag 1. .00 0000 0101 0100 .00 .00 .00 0000 0101 0100 .00 0000 000 0 Type: 802.10 Virtual LAN (0x8100) 802.10 Virtual LAN, PRI: 0, DE1: 0, DI 0000 DE1: Ineligibl 000 DE1: Ineligibl 000 Priority: Best 000 DE1: Ineligibl 000 Priority: Best 000 Priority: Best 000 Priority: Best 000 Priority: Best 000 000 000 	112 bytes cap 50:56:9d:e8:be = Directio = Pointer: = Destinat = Looped: = Reserved = Version: 0000 = Source: b: 102 t Effort (defau t Effort (defau	tured (896 bits) or), Dst: a2:76:f2:00 wif_id ion: 84 No 0 0 1t) (0) 3	interface ca :00:1b (a2:76	pture_u0_ :f2:00:00	1, id 0 :1b)		00000 0010 0020 0030 0040 0050 0050	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
> > > > >	Frame 1: 112 bytes on wire (896 bits), Ethernet II, Src: Wware 9d:e8:be (00: WH-Tag 1	112 bytes cap 50:56:9d:e8:be pointer: postinat copet: Reserved version: 0000 5ource: 102 t Effort (defaule 2: 205 t Effort (defaule	tured (896 bits) or), Dit: a2:76:f2:00 n: From Bridge vif_id ion: 84 No 0 0 11) (0) 3	interface ca :00:1b (a2:76	pture_u0_ :f2:00:00	1, id 0 :1b)		0000 0010 0020 0030 0040 0050 0050	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
> > >	Frame 1: 112 bytes on wire (896 bits), Ethernet II, Src: Wware 9d:e8:be (00: Wir-Tag 1	112 bytes cap 50:56:9d:e8:be = Directio = Pointer: = Destinat = Looped: = Reserved = Version: 0000 = Source: b: 102 t Effort (defau le : 205 t Effort (defau le	tured (896 bits) or), Dst: a2:76:f2:00 n: From Bridge vif_id ion: 84 No : 0 0 0 1t) (0) 3	interface cap :00:1b (a2:76	pture_u0_ :f2:00:00	1, id 0 :1b)		0000 0010 0020 0030 0040 0050 0050	a2 76 f2 00 00 1b $\frac{50}{50}$ 56 9d e8 be 89 26 80 54 00 00 81 00 00 66 81 00 00 00 48 00 45 00 00 54 95 74 40 00 40 10 b8 30 c^{-0} 00 00 26 46 33 64 64 08 00 eb 95 00 22 00 01 88 73 eb 62 00 00 00 00 99 60 00 00 00 00 00 10 11 21 31 41 51 61 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ()*+,-/ 01234567
> > >	Frame 1: 112 bytes on wire (896 bits), Ethernet II, Src: Wware 9d:e8:be (80: Wh-Tag 1	112 bytes cap 50:56:9d:e8:be = Pointer: = Pointer: = Looped: = Reserved Wersion: 0000 = Source: 102 t Effort (defaule : 205 t Effort (defaule	tured (896 bits) or), Dst: a2:76:17:00 n: From Bridge vif_id ion: 84 No 0 0 1t) (0) 2	interface cap :00:1b (a2:76	pture_u0_ :f2:00:00	1, id 0 :1b)		0000 0010 0020 0030 0050 0050	a2 76 f2 00 00 1b $\frac{50}{50}$ 56 9d e8 be 89 26 80 54 00 00 81 00 00 66 81 00 00 00 64 00 00 54 95 74 40 00 40 1b 83 00 00 c4 00 00 54 08 00 eb 95 00 22 00 01 88 73 eb 62 00 00 00 00 95 9d 00 00 00 00 00 00 10 11 21 31 41 51 61 18 19 1a 1b 1c 1d 1e 1f 20 21 22 32 42 52 62 77 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ()**,/ 01234567
>	Frame 1: 112 bytes on wire (896 bits), Ethernet 11, Src: Wware 9d:e8:be (00: Wik-Tag 1. .0 .0 .00 0000 0101 0100 .00 .00 .00 .00 .00 .00 .00 .00 .01 .02 .03 .04 .05 .00 .00 .00 .01 .02 .03 .04 .05 .06 .07 .08 .09 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000	<pre>112 bytes cap 50:56:9d:e8:be</pre>	tured (896 bits) or), Dst: a2:76:f2:00 n: From Bridge vif_id ion: 84 No 0 0 1t) (0) 1t) (0) 2 198.51.100.100	interface cap :00:1b (a2:76	pture_u0_;	1, id 0 :1b)		0000 0010 0020 0040 0050 0050 0050	a2 76 f2 00 00 1b $\frac{50}{50}$ 56 9d e8 be 89 26 80 54 00 00 81 00 00 66 81 00 00 00 48 00 45 00 00 54 95 74 40 00 40 1b 83 60 00 00 46 66 33 64 64 67 80 9d 00 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ()*+,-/ 01234567
· · · · · · · · · · · · · · · · · · ·	Frame 1: 112 bytes on wire (896 bits), Ethernet II, Src: Wware 9d:e8:be (88: Wh-Tag 1	<pre>112 bytes cap 50:56:9d:e8:be = Directio = Pointer: = Destinat = Looped: = Reserved = Version: 0000 = Source: D: 102 t Effort (defau le 0: 205 t Effort (defau le 0.2.100, Dst: :</pre>	tured (896 bits) or), Dst: a2:76:f2:00 n: From Bridge vif_id ion: 84 No 0 0 1t) (0) 1t) (0) 2 198.51.100.100	interface ca :00:1b (a2:76	pture_u0_ :f2:00:00	1, id 0 :1b)		0000 0010 0020 0040 0050 0050 0050	a2 76 f2 00 00 1b $\frac{50}{50}$ 56 9d e8 be 89 26 80 54 00 00 81 00 00 66 81 00 00 00 64 00 00 54 95 74 40 00 40 1b 83 00 00 c4 00 00 54 66 33 64 64 08 00 eb 95 00 22 00 01 88 73 eb 62 00 00 00 00 99 60 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ()*+,-/ 01234567
· · · · · · · · · · · · · · · · · · ·	Frame 1: 112 bytes on wire (896 bits), Ethernet 11, Src: Wware 9d:e8:be (00: Wik-Tag 1. .0 .0 .00 0000 0101 0100 .00 .00 .00 .01 .02 .03 .04 .05 .06 .07 .08 .09 .00 .00 .00 .00 .00 .00 .00 .01 .02 .02 .03 .04 .05 .06 .07 .08 .082.10 .00 .000 .0000 .0000 .0000 .0000 .0000 .0000 .0000 .0000 .0000 .0000 .0000 .0000 .	112 bytes cap 50:56:9d:e8:be = Pointer: = Pointer: = Reserved = Version: 0000 = Source: 0: 102 t Effort (defau le : 205 t Effort (defau le 0.2.100, Dst: :	tured (896 bits) or), DSt: a2:76:172:00 m: From Bridge vif_id ion: 84 NO 0 0 0 1 1 0 0 1 1 0 2 1 1 0 2 1 1 0 2 1 1 1 0 2 1 1 1 0 2 1 1 1 1 1 1 1 1 1 1 1 1 1	interface cap :00:1b (a2:76	pture_u0_j	1, id 0 :1b)		0000 0010 0030 0040 0040 0050 0060	a2 76 f2 00 00 1b $\frac{50}{50}$ 56 9d e8 be 89 26 80 54 00 00 81 00 00 66 81 00 00 00 48 00 45 00 00 54 95 74 40 00 40 1b b8 30 c^{-0} 00 00 26 46 33 64 64 08 00 eb 95 00 22 00 01 88 73 eb 62 00 00 00 00 99 40 00 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ()*+,-/ 01234567

Wählen Sie das zweite Paket aus, und überprüfen Sie die wichtigsten Punkte:

- 1. Nur ICMP-Echoanforderungspakete werden erfasst. Jedes Paket wird erfasst und zweimal angezeigt.
- 2. Der ursprüngliche Paket-Header hat den VLAN-Tag 205.

N	o. Time	Source	Destination	Protocol	Length	3P 3D		IP TTL Info			
1	- 1 2022-08-04 07:21:56.993302102	192.0.2.100	198.51.100.100	ICMP	112	0x9574 ((38260)	64 Echo	(ping) re	equest	id=0x0022, seq=1/256, ttl=64 (no response found!)
	2 2022-08-04 07:21:56.993303597	192.0.2.100	198.51.100.100	ICMP	102	0x9574 ((38260)	64 Echo	(ping) re	request	id=0x0022, seq=1/256, ttl=64 (no response found!)
	3 2022-08-04 07:22:06.214264777	192.0.2.100	198.51.100.100	ICMP	112	0x9a81 ((39553)	64 Echo	(ping) re	equest	id=0x0022, seq=10/2560, ttl=64 (no response found!)
	4 2022-08-04 07:22:06.214267373	192.0.2.100	198.51.100.100	ICMP	102	0x9a81 ((39553)	64 Echo	(ping) re	equest	id=0x0022, seq=10/2560, ttl=64 (no response found!)
	5 2022-08-04 07:22:07.215113393	192.0.2.100	198.51.100.100	ICMP	112	0x9ac3	(39619)	64 Echo	(ping) re	equest	id=0x0022, seq=11/2816, ttl=64 (no response found!)
	6 2022-08-04 07:22:07.215115445	192.0.2.100	198.51.100.100	ICMP	102	0x9ac3	(39619)	64 Echo	(ping) re	equest	id=0x0022, seq=11/2816, ttl=64 (no response found!)
	7 2022-08-04 07:22:08.229938577	192.0.2.100	198.51.100.100	ICMP	112	0x9b33 ((39731)	64 Echo	(ping) re	equest	id=0x0022, seq=12/3072, ttl=64 (no response found!)
	8 2022-08-04 07:22:08.229940829	192.0.2.100	198.51.100.100	ICMP	102	0x9b33 ((39731)	64 Echo	(ping) re	equest	id=0x0022, seq=12/3072, ttl=64 (no response found!)
	9 2022-08-04 07:22:09.253944601	192.0.2.100	198.51.100.100	ICMP	112	0x9c0e	(39950)	64 Echo	(ping) re	equest	id=0x0022, seq=13/3328, ttl=64 (no response found!)
	10 2022-08-04 07:22:09.253946899	192.0.2.100	198.51.100.100	ICMP	102	0x9c0e	(39950)	64 Echo	(ping) re	equest	id=0x0022, seq=13/3328, ttl=64 (no response found!)
	11 2022-08-04 07:22:10.277953070	192.0.2.100	198.51.100.100	ICMP	112	0x9ccb ((40139)	64 Echo	(ping) re	equest	id=0x0022, seq=14/3584, ttl=64 (no response found!)
	12 2022-08-04 07:22:10.277954736	192.0.2.100	198.51.100.100	ICMP	102	0x9ccb ((40139)	64 Echo	(ping) re	equest	id=0x0022, seq=14/3584, ttl=64 (no response found!)
	13 2022-08-04 07:22:11.301931282	192.0.2.100	198.51.100.100	ICMP	112	0x9d84 ((40324)	64 Echo	(ping) re	equest	id=0x0022, seq=15/3840, ttl=64 (no response found!)
	14 2022-08-04 07:22:11.301933600	192.0.2.100	198.51.100.100	ICMP	102	0x9d84 ((40324)	64 Echo	(ping) re	equest	id=0x0022, seq=15/3840, ttl=64 (no response found!)
	15 2022-08-04 07:22:12.325936521	192.0.2.100	198.51.100.100	ICMP	112	0x9da2 ((40354)	64 Echo	(ping) re	equest	id=0x0022, seq=16/4096, ttl=64 (no response found!)
	16 2022-08-04 07:22:12.325937895	192.0.2.100	198.51.100.100	ICMP	102	0x9da2 ((40354)	64 Echo	(ping) re	equest	id=0x0022, seq=16/4096, ttl=64 (no response found!)
	17 2022-08-04 07:22:13.326988040	192.0.2.100	198.51.100.100	ICMP	112	0x9e07 ((40455)	64 Echo	(ping) re	equest	id=0x0022, seq=17/4352, ttl=64 (no response found!)
	18 2022-08-04 07:22:13.326990258	192.0.2.100	198.51.100.100	ICMP	102	0x9e07 ((40455)	64 Echo	(ping) re	request	id=0x0022, seq=17/4352, ttl=64 (no response found!)
	19 2022-08-04 07:22:14.341944773	192.0.2.100	198.51.100.100	ICMP	112	0x9e6a	(40554)	64 Echo	(ping) re	request	id=0x0022, seq=18/4608, ttl=64 (no response found!)
	20 2022-08-04 07:22:14.341946249	192.0.2.100	198.51.100.100	ICMP	102	0x9e6a	(40554)	64 Echo	(ping) re	request	id=0x0022, seq=18/4608, ttl=64 (no response found!)
	21 2022-08-04 07:22:15.365941588	192.0.2.100	198.51.100.100	ICMP	112	0x9efb ((40699)	64 Echo	(ping) re	request	id=0x0022, seq=19/4864, ttl=64 (no response found!)
	22 2022-08-04 07:22:15.365942566	192.0.2.100	198.51.100.100	ICMP	102	0x9efb ((40699)	64 Echo	(ping) re	request	id=0x0022, seq=19/4864, ttl=64 (no response found!)
	23 2022-08-04 07:22:16.389973843	192.0.2.100	198.51.100.100	ICMP	112	0x9fe8	(40936)	64 Echo	(ping) re	equest	id=0x0022, seq=20/5120, ttl=64 (no response found!)
	24 2022-08-04 07:22:16.389975129	192.0.2.100	198.51.100.100	ICMP	102	0x9fe8	(40936)	64 Echo	(ping) re	equest	id=0x0022, seq=20/5120, ttl=64 (no response found!)
	25 2022-08-04 07:22:17.413936452	192.0.2.100	198.51.100.100	ICMP	112	0xa079	(41081)	64 Echo	(ping) re	equest	id=0x0022, seq=21/5376, ttl=64 (no response found!)
	26 2022-08-04 07:22:17.413938090	192.0.2.100	198.51.100.100	ICMP	102	0xa079 ((41081)	64 Echo	(ping) re	equest	id=0x0022, seq=21/5376, ttl=64 (no response found!)
	27 2022-08-04 07:22:18.437954335	192.0.2.100	198.51.100.100	ICMP	112	0xa11e ((41246)	64 Echo	(ping) re	equest	id=0x0022, seq=22/5632, ttl=64 (no response found!)
<											
5	Frame 2: 102 butes on wire (816 bi	ts) 102 bytes ca	ntured (816 hits) o	n interface c	anture ue	1. id 0					a2 76 f2 00 00 th 00 50 56 9d 08 he 81 00 00 cd
5	Ethernet II. Src: Wheare 9d:e8:be	(00:50:56:9d:e8:h	(a). Dst: a2:76:f2:0	a:00:1b (a2:7	5:f2:00:00	1; 10 0				0010	08 00 45 00 00 54 95 74 40 00 40 01 b8 38 c0 00 ··E··T·t @·@··8··
L.	882 10 Virtual LAN, PRI: 0, DET: 0	ID: 205	c/, osci azironizio							0026	0 02 64 c6 33 64 64 08 00 eb 95 00 22 00 01 88 73 ·d·3dd·····"···s
	and = Priority	Rest Effort (def	ault) (0)	_						0036	eb 62 00 00 00 00 d9 9d 00 00 00 00 00 00 10 11 .b
L	DET: Inel	gible	uure) (0)							0046	12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 !
н		Panar								0056	22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 "#\$%&'() *+,/01
н	Type: IDv4 (0v0000)			21						0066	32 33 34 35 36 37 234567
5	Internet Protocol Version 4. Src:	192.0.2.100. Dst:	198.51.100.100								
5	Internet Control Message Protocol		10010111001100								
Ľ	and control nessage Protocol										

Öffnen Sie nun die Capture-Dateien für Portchannel1.207. Wählen Sie das erste Paket und überprüfen Sie die Schlüsselpunkte

- 1. Nur ICMP-Echoanforderungspakete werden erfasst. Jedes Paket wird erfasst und zweimal angezeigt.
- 2. Der ursprüngliche Paket-Header hat den VLAN-Tag 207.
- 3. Der interne Switch fügt ein zusätzliches Port-VLAN-Tag **1001 ein**, das die Eingangsschnittstelle Port-Channel1 identifiziert.
- 4. Der interne Switch fügt einen zusätzlichen VN-Tag ein.

No. Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info		
1 2022-08-04 08:18:24.572548869	192.168.247.100	192.168.247.102	ICMP	128	0x609e (24734)	255 Echo (ping) 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, seg=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, seg=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, seg=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, seg=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	8x68a8 (24744)	255 Echo (ping) re	quest	id=0x007b, seg=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, seg=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	8x68a9 (24745)	255 Echo (ping) re	quest	id=0x007b, seg=11/2816, ttl=255 (no response found!)
24 2022-08-04 08:18:24.578449909	192.168.247.100	192.168.247.102	ICMP	118	8x68a9 (24745)	255 Echo (ping) re	quest	id=0x007b, seg=11/2816, ttl=255 (no response found!)
25 2022-08-04 08:18:24.578900043	192.168.247.100	192.168.247.102	TCMP	128	8x68aa (24746)	255 Echo (ping) re	quest	id=0x007b, seq=12/3072, ttl=255 (no response foundl)
26 2022-08-04 08:18:24 578900897	192.168.247.100	192.168.247.102	TCMP	118	8x68aa (24746)	255 Echo (ning) re	quest	id=8y887h, seg=12/3872, ttl=255 (no response foundl)
27 2022-08-04 08:18:24 570426962	192.168.247.100	192.168.247.102	TCMP	128	8x68ab (24747)	255 Echo (ping) re	quest	id=0x007b, seq=13/3328, ttl=255 (no response foundl)
							daras	······································
N								
> Frame 1: 128 bytes on wire (1024 bits), 128 bytes cap	tured (1024 bits) o	n interface ca	pture_u0_	3, id 0		0000	a2 76 t2 00 00 1c 00 17 dt d6 ec 00 89 26 80 3d · v·····&·=
> Ethernet II, Src: Cisco d6:ec:00 (00:	17:df:d6:ec:00),	Dst: a2:76:f2:00:0	9:1c (a2:76:f2	:00:00:10	:)		0010	00 00 81 00 03 e9 81 00 00 cf 08 00 45 00 00 64E.d
VN-Tag							0020	00 90 00 00 TT 01 00 00 00 00 00 00 00 00 17 00 00 00 00 TT 01 00 00 00 00 00 00 00 00 00 00 00 00
1	= Direction	: From Bridge					0030	ah cd
.0	= Pointer:	vif_id					0050	ab cd
00 0000 0011 1101	<pre> = Destinati</pre>	on: 61	A				0060	ab cd
···· ···· ···· ···· ···· 0 ····	= Looped: N	0	4				0070	ab cd
0	<pre> = Reserved:</pre>	0						
	<pre> = Version:</pre>	0						
0000 0000	0000 = Source: 0							
Type: 802.1Q Virtual LAN (0x8100)								
✓ 802.1Q Virtual LAN, PRI: 0, DEI: 0, I	D: 1001							
000 Beriority: Ber	st Effort (defaul	t) (0)	2					
0 = DEI: Ineligit	ble		3					
0011 1110 1001 = ID: 1001			-					
Type: 802.1Q Virtual LAN (0x8100)								
✓ 802.1Q Virtual LAN, PRI: 0, DEI: 0, I	D: 207							
000 Beriority: Be	st Effort (defaul	t) (0)						
0 = DEI: Ineligit	ble							
0000 1100 1111 = ID: 207			2					
Type: IPv4 (0x0800)			4					
Internet Protocol Version 4, Src: 192	.168.247.100, Ds	t: 192.168.247.102						
> Internet Control Message Protocol								

Wählen Sie das zweite Paket aus, und überprüfen Sie die wichtigsten Punkte:

- 1. Nur ICMP-Echoanforderungspakete werden erfasst. Jedes Paket wird erfasst und zweimal angezeigt.
- 2. Der ursprüngliche Paket-Header hat den VLAN-Tag 207.

N	p. Time	Source	Destination	Protocol	Length	19 ID	JP TTL Info		
1	1 2022-08-04 08:18:24.572548869	192.168.247.100	192.168.247.102	ICMP	128	0x609e (24734)	255 Echo (ping) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	st id=0x007b	, seq=10/2560, ttl=255 (no response found!)
	22 2022-08-04 08:18:24.577989290	192.168.247.100	192.168.247.102	ICMP	118	0x60a8 (24744)	255 Echo (ping) reque	st 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) reque	st id=0x007b	, seq=11/2816, ttl=255 (no response found!)
	24 2022-08-04 08:18:24.578449909	192.168.247.100	192.168.247.102	ICMP	118	0x60a9 (24745)	255 Echo (ping) reque	st id=0x007b	, seq=11/2816, ttl=255 (no response found!)
	25 2022-08-04 08:18:24.578900843	192.168.247.100	192.168.247.102	ICMP	128	0x60aa (24746)	255 Echo (ping) reque	st id=0x007b	, seq=12/3072, ttl=255 (no response found!)
	26 2022-08-04 08:18:24.578900897	192.168.247.100	192.168.247.102	ICMP	118	0x60aa (24746)	255 Echo (ping) reque	st id=0x007b	, seq=12/3072, ttl=255 (no response found!)
	27 2022-08-04 08:18:24.579426962	192.168.247.100	192.168.247.102	ICMP	128	0x60ab (24747)	255 Echo (ping) reque	st id=0x007b	, seq=13/3328, ttl=255 (no response found!)
<									
E	Ename 2: 118 butes on wine (044 bits)	118 bytes cant	uned (044 hits) on	interface car	turo uB 3	ida		00 a2 76 f2	00 00 1c 00 17 df d6 ec 00 81 00 00 cf
	Ethoppet II. Spci Cisco delocido (00)	17:df:df:oc:00)	Det: 3317616310010	anterrace cap	2:00:00:1/	10.0	00	10 08 00 45	00 00 10 00 17 01 00 00 00 01 00 00 01 00 00 01 00 00
1	RO2 10 Victual LAN DRI: 0 DEL: 0 1	D: 207	031. 82.70.12.00.0		2.00.00.10	.)	00	20 f7 64 c0	a8 f7 66 08 00 e5 c8 00 7b 00 00 00 00 .df
1	and a priority Pa	o: 207 ct Effort (dofau)	+) (0)				00	30 00 02 4d	8c 4a 78 ab cd ab cd ab cd ab cd ab cd ··M·Jx·· ·····
н	- OFIL Inclini	st Errort (verau	() (0)				06	40 ab cd ab	cd ab cd ab cd ab cd ab cd ab cd ab cd
н	0000 1100 1111 - TD: 207	ATC.		21			06	50 ab cd ab	cd ab cd ab cd ab cd ab cd ab cd ab cd
н	Type: TDyA (0y0000)			4			06	60 ab cd ab	cd ab cd ab cd ab cd ab cd ab cd ab cd
	Internet Protocol Version A Sect 103	168 247 100 De	102 168 247 102				00	70 ab cd ab	cd ab cd
Ľ	Internet Control Massage Protocol	120012471100, 05							
Ľ	Internet control nessage Protocol								
н									

Erklärung

Wenn eine Paketerfassung an einer vorderen Schnittstelle konfiguriert ist, erfasst der Switch gleichzeitig jedes Paket zweimal:

- Nach dem Einfügen des Port-VLAN-Tags.
- Nach dem Einfügen des VN-Tags.

In der Reihenfolge der Vorgänge wird das VN-Tag zu einem späteren Zeitpunkt eingefügt als das Port-VLAN-Tag. In der Erfassungsdatei wird das Paket mit dem VN-Tag jedoch früher angezeigt als das Paket mit dem Port-VLAN-Tag. Außerdem enthält bei Subschnittstellen in den Erfassungsdateien jedes zweite Paket nicht den Port-VLAN-Tag.

In dieser Tabelle ist die Aufgabe zusammengefasst:

Aufgabe	Erfassung Internes spunkt erfasster	Port-VLAN in Paketen	Richtun g	Erfasster Datenverkehr
Konfiguration und Verifizierung einer Paketerfassung an der Subschnittstelle Ethernet1/2.205	Ethernet1/ 2.205	102	Nur Eingan g	ICMP-Echo-Anfragen von Host 192.0.2.100 an Host 198.51.100
Konfiguration und Verifizierung der Paketerfassung an der Port-Channel1- Subschnittstelle mit den Mitgliedsschnittstellen Ethernet1/3 und Ethernet1/4	Ethernet1/ 3 Ethernet1/ 4	1001	Nur Eingan g	ICMP-Echo-Anfragen von 192.168.207.100 an Host 192.168.207.102

Paketerfassungsfilter

Verwenden Sie den FCM und die CLI, um eine Paketerfassung an der Schnittstelle Ethernet1/2 mit einem Filter zu konfigurieren und zu überprüfen.

Topologie, Paketfluss und Erfassungspunkte



Konfiguration

FCM

Führen Sie die folgenden Schritte auf FCM aus, um einen Erfassungsfilter für ICMP-Echo-Anforderungspakete vom Host 192.0.2.100 zum Host 198.51.100.100 zu konfigurieren und ihn auf die Paketerfassung an der Schnittstelle Ethernet1/2 anzuwenden:

1. Verwenden Sie Extras > Paketerfassung > Filterliste > Filter hinzufügen, um einen
Erfassungsfilter zu erstellen.

2. Geben Sie den Filternamen, das Protokoll, die Quell-IPv4 und die Ziel-IPv4 an, und klicken Sie auf Speichern:

Overview Inter	faces Logical Devices Se	curity Engine Plat	orm Settings									System Tools	Help admin
Cashara Cassina	COMPLEX .												
Ciltor List													
Filter List													od Filter
Filter Name	MAC	From	TRue	Port	MAC	To	TDue	Bost	Protocol	Inner vlan	Outer vlan	EtherType	
filter_icmp	00:00:00:00:00	192.0.2.100		0	00:00:00:00:00	192.0.2.100		0	1	0	0	0	/8
				Edit Packe	t Filter			(* ×					
				Filter Name*	filter_icmp								
				Protocol	ICMP_IPv4 ¥								
				EtherType	Any 👻								
				Inner vlan	0	Outer vlan	0						
				Source		Destination							
				IPv4	192.0.2.100	IPv4	198.51.100.100						
				IPv6		IPv6							
				Port	0	Port	0	_					
				MAC	00:00:00:00:00:00	MAC	00:00:00:00:00:00	•					
							Save	Cancel					

3. Verwenden Sie **Tools > Packet Capture > Capture Session**, um eine neue Erfassungssitzung zu erstellen:

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		

4. Wählen Sie Ethernet1/2 aus, geben Sie den Sitzungsnamen an, wenden Sie den Erfassungsfilter an, und klicken Sie auf Speichern und ausführen, um die Erfassung zu aktivieren:

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 Overwrite
Ethernet1/3 FTD Ethernet1/10	Capture Filter Apply Filter Copture All Apply Apply Capture All Apply Filter_Create Filter Apply To Ethemet1/2 To Ethemet1/2
Ethernet1/1	

FXOS-CLI

Führen Sie die folgenden Schritte auf der FXOS-CLI aus, um die Paketerfassung an Backplane-

Schnittstellen zu konfigurieren:

1. Identifizieren Sie den Anwendungstyp und die Kennung:

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 _____ ftđ ftd1 1 Enabled Online 7.2.0.82 7.2.0.82 Native No Not Applicable None 2. Geben Sie die IP-Protokollnummer in https://www.iana.org/assignments/protocolnumbers/protocol-numbers.xhtml an. In diesem Fall ist die ICMP-Protokollnummer 1.

3. Erstellen Sie eine Erfassungssitzung:

```
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 #
```

Verifizierung

FCM

Überprüfen Sie den **Schnittstellennamen**, stellen Sie sicher, dass der **Betriebsstatus** aktiv ist und dass die **Dateigröße (in Byte)** ansteigt:

Overview Ir	terfaces Logical Devices	Security Engine Pla	tform Settings									System Tools	Help admin
Contras Carring	Citra Liet												
Filter list									dd Filter				
					-								
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	/ 8

Überprüfen Sie den Schnittstellennamen, den Filter, stellen Sie sicher, dass der Betriebsstatus aktiv ist, und erhöhen Sie die Dateigröße (in Byte) unter Tools > Packet Capture > Capture Session:

Overview Interfaces Logical Devices Security Engine Platform Settings System To	ols Help admin
Capture Session Fitter List	
C Refresh Capture Session Delete Al S	tistions
E ap1 Drop Count: 0 Operational State: up Buffer Size: 256 MB Snap Length: 1518 Bytes	
Interface Name Filter File Size (in bytes) File Name Device Name	
Ethernet1/2 fiber_jomp 84340 cap1-ethernet-1-2-0-pcap fid1 ±	

FXOS-CLI

Überprüfen Sie die Erfassungsdetails in der Paketerfassung:

```
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
Erfassungsdateien erfassen
```

Befolgen Sie die Schritte im Abschnitt Sammeln von FirePOWER 4100/9300-internen Switch-Erfassungsdateien.

Analyse der Erfassungsdatei

Öffnen Sie die Erfassungsdatei mit einer Anwendung zum Lesen von Paketerfassungsdateien. Erstes Paket auswählen und Schlüsselpunkte prüfen

- 1. Nur ICMP-Echoanforderungspakete werden erfasst. Jedes Paket wird erfasst und zweimal angezeigt.
- 2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.

- 3. Der interne Switch fügt den zusätzlichen Port-VLAN-Tag **102 ein**, der die Eingangsschnittstelle Ethernet1/2 identifiziert.
- 4. Der interne Switch fügt einen zusätzlichen VN-Tag ein.

Ν	lo. Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info	_	^
	1 2022-08-02 15:46:55.603277	760 192.0.2.100	198.51.100.100	ICMP	108	0x0012 (18) 64 Echo (ping) request	id=0x0018, seq=349/23809, ttl=64	(no r
	2 2022-08-02 15:46:55.603279	588 192.0.2.100	198.51.100.100	ICMP	102	0x0012 (18) 64 Echo (ping) request	id=0x0018, seq=349/23809, ttl=64	(no r
	3 2022-08-02 15:46:56.627139	252 192.0.2.100	198.51.100.100	ICMP	108	0x00db (21	 64 Echo (ping) request 	id=0x0018, seq=350/24065, ttl=64	(no r
	4 2022-08-02 15:46:56.627140	919 192.0.2.100	198.51.100.100	ICMP	102	0x00db (21	 64 Echo (ping) request 	id=0x0018, seq=350/24065, ttl=64	(no r
	5 2022-08-02 15:46:57.651185	193 192.0.2.100	198.51.100.100	ICMP	108	0x01cb (45	 64 Echo (ping) request 	id=0x0018, seq=351/24321, ttl=64	(no r
	6 2022-08-02 15:46:57.651186	787 192.0.2.100	198.51.100.100	ICMP	102	0x01cb (45	 64 Echo (ping) request 	id=0x0018, seq=351/24321, ttl=64	(no r
	7 2022-08-02 15:46:58.675153	317 192.0.2.100	198.51.100.100	ICMP	108	0x01d6 (47	64 Echo (ping) request	id=0x0018, seq=352/24577, ttl=64	(no r
	8 2022-08-02 15:46:58.675154	503 192.0.2.100	198.51.100.100	ICMP	102	0x01d6 (47	64 Echo (ping) request	id=0x0018, seq=352/24577, ttl=64	(no r
	9 2022-08-02 15:46:59.699152	539 192.0.2.100	198.51.100.100	ICMP	108	0x01f4 (50	64 Echo (ping) request	id=0x0018, seq=353/24833, ttl=64	(no r
	10 2022-08-02 15:46:59.699153	335 192.0.2.100	198.51.100.100	ICMP	102	0x01f4 (50	64 Echo (ping) request	id=0x0018, seq=353/24833, ttl=64	(no r
	11 2022-08-02 15:47:00.723142	541 192.0.2.100	198.51.100.100	ICMP	108	0x01f9 (50	 64 Echo (ping) request 	id=0x0018, seq=354/25089, ttl=64	(no r
	12 2022-08-02 15:47:00.723144	543 192.0.2.100	198.51.100.100	ICMP	102	0x01f9 (50	 64 Echo (ping) request 	id=0x0018, seq=354/25089, ttl=64	(no r
	13 2022-08-02 15:47:01.747162	204 192.0.2.100	198.51.100.100	ICMP	108	0x026e (62	 64 Echo (ping) request 	id=0x0018, seq=355/25345, ttl=64	(no r
	14 2022-08-02 15:47:01.747163	783 192.0.2.100	198.51.100.100	ICMP	102	0x026e (62	 64 Echo (ping) request 	id=0x0018, seq=355/25345, ttl=64	(no r
	15 2022-08-02 15:47:02.771209	952 192.0.2.100	198.51.100.100	ICMP	108	0x02bc (70	64 Echo (ping) request	id=0x0018, seq=356/25601, ttl=64	(no r
	16 2022-08-02 15:47:02.771211	362 192.0.2.100	198.51.100.100	ICMP	102	0x02bc (70	64 Echo (ping) request	id=0x0018, seq=356/25601, ttl=64	(no r
	17 2022-08-02 15:47:03.772258	550 192.0.2.100	198.51.100.100	ICMP	108	0x032f (81	 64 Echo (ping) request 	id=0x0018, seq=357/25857, ttl=64	(no r
	18 2022-08-02 15:47:03.772259	724 192.0.2.100	198.51.100.100	ICMP	102	0x032f (81	 64 Echo (ping) request 	id=0x0018, seq=357/25857, ttl=64	(no r
	19 2022-08-02 15:47:04.791118	519 192.0.2.100	198.51.100.100	ICMP	108	0x040f (10	39) 64 Echo (ping) request	id=0x0018, seq=358/26113, ttl=64	(no r
	20 2022-08-02 15:47:04.791119	721 192.0.2.100	198.51.100.100	ICMP	102	0x040f (10	39) 64 Echo (ping) request	id=0x0018, seq=358/26113, ttl=64	(nor v
<									>
5	Frame 1: 108 bytes on wire (864	bits), 108 bytes	captured (864 bits)	on interfac	e capture_u0	1, i 0000	58 97 bd b9 77 0e 00 50 56 9d	e8 be 89 26 80 0a X ··· w ·· P V ···· &	i++
)	Ethernet II, Src: VMware 9d:e8	be (00:50:56:9d:e8	:be), Dst: Cisco b9:	77:0e (58:9	7:bd:b9:77:0e) 0010	00 00 81 00 00 66 08 00 45 00	00 54 00 12 40 00 ·····f·· E··T··	@·
~	VN-Tag					0020	40 01 4d 9b c0 00 02 64 c6 33	64 64 08 00 9e 67 @·M····d ·3dd··	· g
	1	= Dire	ction: From Bridge			0030	00 18 01 5d e2 46 e9 62 00 00	00 00 c1 a6 0c 00 ···]·F·b ·····	•••
	.0	= Poin	ter: vif_id			0040	00 00 00 00 10 11 12 13 14 15	16 17 18 19 1a 1b	
	00 0000 0000 1010	= Dest	ination: 10			0050	1c 1d 1e 1f 20 21 22 23 24 25	26 27 28 29 2a 20 ···· ! # \$%& ()	-+
	0	= Loop	ed: No 🤞	4		0000	2C 20 2e 2t 30 31 32 33 34 35	30 37 ,/0123 4507	
	0	= Rese	rved: 0	1 I I I					
	00	= Vers	ion: 0						
	000	0000 0000 = Sour	ce: 0						
	Type: 802.1Q Virtual LAN (0x	3100)							
~	802.10 Virtual LAN, PRI: 0, DE	: 0, ID: 102							
	000 = Priori	ty: Best Effort (d	efault) (0)						
	0 = DEI: I	neligible		3					
	0000 0110 0110 = ID: 10	2							
	Type: IPv4 (0x0800)								
)	Internet Protocol Version 4, S	c: 192.0.2.100, Ds	t: 198.51.100.100 🍃						
5	Internet Control Message Proto	ol	4	2					
1									
1						>			

Wählen Sie das zweite Paket aus, und überprüfen Sie die wichtigsten Punkte:

- 1. Nur ICMP-Echoanforderungspakete werden erfasst. Jedes Paket wird erfasst und zweimal angezeigt.
- 2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.
- 3. Der interne Switch fügt den zusätzlichen Port-VLAN-Tag **102 ein**, der die Eingangsschnittstelle Ethernet1/2 identifiziert.

No.	. Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info			^
-	1 2022-08-02 15:46:55.603277760	192.0.2.100	198.51.100.100	ICMP	108 1	0x0012 (18)	64 Echo (ping) 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 (ping) 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 (ping) 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 (ping) 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 (ping) 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 (ping) 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 (ping) 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 (ping) 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 (ping) 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 (ping) 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 (ping) 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 (ping) 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 (ping) 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 (ping) 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 (ping) 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 (ping) 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 (ping) 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 (ping) 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 (ping) 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 (ping) request	id=0x0018, seq=358/26113,	ttl=64 (no r	~
<									>	
>	Frame 2: 102 bytes on wire (816 bit	s), 102 bytes ca	ptured (816 bits) or	interface ca	pture u0 1	, i 0000 58 97	bd b9 77 0e 00 50 56 9d e	8 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_b9:77	:0e (58:97:bd	:b9:77:0e)	0010 08 00	45 00 00 54 00 12 40 00 4	0 01 4d 9b c0 00 ··E··T·	·· @·@·M···	
\sim	802.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 102				0020 02 64	c6 33 64 64 08 00 9e 67 0	0 18 01 5d e2 46 ·d·3dd·	·· ·g· ··] · F	
	000 = Priority: N	Best Effort (defa	ult) (0)			0030 e9 62	00 00 00 00 c1 a6 0c 00 0	0 00 00 00 10 11 ·b·····		
	0 = DEI: Inelig	gible	3			0040 12 13	14 15 16 17 18 19 1a 1b 1	c 1d 1e 1f 20 21	() *·····	
	0000 0110 0110 = ID: 102	-			0050 22 23	24 25 26 27 28 29 2a 20 2	c 2d 2e 2f 30 31 "#\$%& () -+,/01		
	Type: IPv4 (0x0800)					0000 32 33	34 33 36 37	234367		
>	Internet Protocol Version 4, Src: 1	92.0.2.100, Dst:	198.51.100.100							
>	Internet Control Message Protocol		2							

Erklärung

Wenn eine Paketerfassung an einer vorderen Schnittstelle konfiguriert ist, erfasst der Switch

gleichzeitig jedes Paket zweimal:

- Nach dem Einfügen des Port-VLAN-Tags.
- Nach dem Einfügen des VN-Tags.

In der Reihenfolge der Vorgänge wird das VN-Tag zu einem späteren Zeitpunkt eingefügt als das Port-VLAN-Tag. In der Erfassungsdatei wird das Paket mit dem VN-Tag jedoch früher angezeigt als das Paket mit dem Port-VLAN-Tag.

Wenn ein Erfassungsfilter angewendet wird, werden nur die Pakete erfasst, die mit dem Filter in Eingangsrichtung übereinstimmen.

In dieser Tabelle ist die Aufgabe zusammengefasst:

Aufgabe	Erfassu ngspun kt	Internes Port-VLAN in erfassten Paketen	Richtun g	Benutzerfilter	Erfasster Datenverkehr
Konfigurieren und Überprüfen einer Paketerfassung mit einem Filter an der vorderen Schnittstelle "Ethernet1/2"	Etherne t1/2	102	Nur Eingan g	Protokolle: ICMP Quelle: 192.0.2.100 Ziel: 198.51.100.100	ICMP-Echo-Anfragen von H 192.0.2.100 an Host 198.51.100.100

Sammeln von FirePOWER 4100/9300-internen Switch-Erfassungsdateien

FCM

Befolgen Sie diese Schritte auf FCM, um interne Switch-Erfassungsdateien zu sammeln:

1. Klicken Sie auf die Schaltfläche **Sitzung deaktivieren**, um die aktive Aufzeichnung zu beenden:

~										
Overview	Interfaces	Logical Devices	Security Engine	Platform Settings				System T	ools Help	admin
Capture Sess	sion Filter Lis	t								
							C Refresh Capture Session	Delete All Se	issions	
	cap1	Drop Count	: 0	Operational State: up	Buffer Size: 256 M	48	Snap Length: 1518 Bytes			8 🔟
Interface Na	me	Filter		File Size (in bytes)	File Name	Device Name				
Ethernet1/2		None		34700	cap1-ethernet-1-2-0.pcap	ftd1	\overline{A}			

2. Stellen Sie sicher, dass der Betriebsstatus DOWN - Session_Admin_Shut:

Overview Interfaces Logica	l Devices Security Engine	Platform Settings			System Tools Help adm
Capture Session Filter List					
				Pafrash Cardura	Carsing Dalata Al Carsings
			_	O Relian Capture	Joste Al Jessinis
a D cap1	Drop Count: 0	Operational State: DOWN - Session_Admin_Shut	Buffer Size: 256 MB	Snap Length: 1518	Bytes 🥜 🕄 🗄
Interface Name	Filter	File Size (in bytes)	File Name	Device Name	
Ethernet1/2	None	218828	cap1-ethemet-1-2-0.pcap	ftd1	<u>↓</u>

3. Klicken Sie auf Herunterladen, um die Erfassungsdatei herunterzuladen:

Overview Interfaces L	ogical Devices Security Engin	e Platform Settings			System	i Tools Help admin
Capture Session Fiter List						
					C Refresh Capture Session Delete	All Sessions
Cap1	Drop Count: 0	Operational State: DOWN - Session_Admin_Shu	at Buffer Size: 256 MB		Snap Length: 1518 Bytes	282
Interface Name	Filter	File Size (in bytes)	File Name	Device Name		
Ethernet1/2	None	218828	cap1-ethemet-1-2-0.pcap	ftd1	土	

Bei Port-Channel-Schnittstellen wiederholen Sie diesen Schritt für alle Teilnehmer-Schnittstellen.

FXOS-CLI

Befolgen Sie diese Schritte auf der FXOS-CLI, um Erfassungsdateien zu erfassen:

1. Die aktive Erfassung beenden:

```
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
  Laden Sie die Erfassungsdatei aus dem local-mgmt-Befehlsbereich hoch:
```

firepower# connect local-mgmt

1	firepower(l	ocal-mgmt)#	сору	<pre>/packet-capture/session-1/cap1-ethernet-1-2-0.pcap</pre>	?
	ftp:	Dest File	URI		
	http:	Dest File	URI		
	https:	Dest File	URI		
	scp:	Dest File	URI		
	sftp:	Dest File	URI		
	tftp:	Dest File	URI		
	usbdrive:	Dest File	URI		
	volatile:	Dest File	URI		
	workspace:	Dest File	URI		

firepower(local-mgmt)# copy /packet-capture/session-1/cap1-ethernet-1-2-0.pcap
ftp://ftpuser@10.10.10.1/cap1-ethernet-1-2-0.pcap
Password:

Bei Port-Channel-Schnittstellen kopieren Sie die Erfassungsdatei für jede Member-Schnittstelle.

Richtlinien, Einschränkungen und Best Practices für Interner Switch Paketerfassung

Die Richtlinien und Einschränkungen im Zusammenhang mit der internen Switch-Erfassung für Firepower 4100/9300 finden Sie im *Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide* oder im *Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*, Chapter **Troubleshooting**, Abschnitt **Paketerfassung**.

Dies ist die Liste der Best Practices, die auf der Verwendung der Paketerfassung in TAC-Fällen basieren:

- Beachten Sie Richtlinien und Einschränkungen.
- Erfassen Sie Pakete an allen Port-Channel-Mitgliedsschnittstellen, und analysieren Sie alle Erfassungsdateien.
- Verwenden Sie Erfassungsfilter.
- Berücksichtigen Sie die Auswirkungen von NAT auf Paket-IP-Adressen, wenn ein Erfassungsfilter konfiguriert wird.
- Erhöhen oder verringern Sie die **Snap-Linse**, die die Frame-Größe angibt, falls sie vom Standardwert von 1518 Byte abweicht. Eine geringere Größe führt zu einer höheren Anzahl erfasster Pakete und umgekehrt.
- Passen Sie die Puffergröße nach Bedarf an.
- Beachten Sie die **Drop Count** für FCM oder FXOS CLI. Sobald die Puffergrößengrenze erreicht ist, erhöht sich der Zähler für die Verwerfung.
- Verwenden Sie filter!**vntag** in Wireshark, um nur Pakete ohne VN-Tag anzuzeigen. Dies ist nützlich, um VN-markierte Pakete in den Front-Interface-Paketerfassungsdateien auszublenden.
- Verwenden Sie den Filter **frame.number&1** in Wireshark, um nur ungerade Frames anzuzeigen. Dies ist nützlich, um doppelte Pakete in den Backplane-Schnittstellen-Paketerfassungsdateien auszublenden.
- Bei Protokollen wie TCP wendet Wireshark Farbregeln an, die Pakete mit bestimmten Bedingungen in verschiedenen Farben anzeigen. Bei internen Switch-Erfassungen aufgrund doppelter Pakete in Erfassungsdateien kann das Paket farbig dargestellt und falsch-positiv markiert werden. Wenn Sie die Paketerfassungsdateien analysieren und einen beliebigen Filter anwenden, exportieren Sie die angezeigten Pakete in eine neue Datei und öffnen Sie stattdessen die neue Datei.

Konfiguration und Verifizierung auf Sichere Firewall 3100

Im Gegensatz zu Firepower 4100/9300 werden die internen Switch-Erfassungen auf der Secure Firewall 3100 über den Befehl **capture <name> switch** auf der Befehlszeilenschnittstelle der Anwendung konfiguriert. Dabei gibt die **Switch-**Option an, dass die Erfassungen auf dem internen Switch konfiguriert werden.

Dies ist der Befehl capture mit der switch-Option:

> capture cap_sw switch ?

buffer	Configure size of capture buffer, default is 256MB								
ethernet-type	Capture Ethernet packets of a particular type, default is IP								
interface	Capture packets on a specific interface								
ivlan	Inner Vlan								
match	Capture packets based on match criteria								
ovlan	Outer Vlan								
packet-length	Configure maximum length to save from each packet, default is								
	64 bytes								
real-time	Display captured packets in real-time. Warning: using this								
	option with a slow console connection may result in an								
	excessive amount of non-displayed packets due to performance								
	limitations.								
stop	Stop packet capture								
trace	Trace the captured packets								
type	Capture packets based on a particular type								
<cr></cr>									

Allgemeine Schritte für die Konfiguration der Paketerfassung:

1. Geben Sie eine Eingangsschnittstelle an:

Die Switch-Erfassungskonfiguration akzeptiert den **Namen** der Eingangsschnittstelle. Der Benutzer kann die Namen der Datenschnittstellen, den internen Uplink oder die Verwaltungsschnittstellen angeben:

> 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. Geben Sie den Ethernet-Frame-EtherType an. Der Standard-EtherType ist IP. Die **Ethernet**-Optionswerte geben den EtherType an:

```
> capture capsw switch interface inside ethernet-type ?
802.1Q
<0-65535> Ethernet type
arp
ip
ip6
pppoed
pppoes
rarp
sgt
vlan
```

 Geben Sie die Übereinstimmungsbedingungen an. Die Option zum Erfassen von Übereinstimmungen legt die Übereinstimmungskriterien fest:

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

- 4. Geben Sie andere optionale Parameter an, z. B. die Puffergröße, die Paketlänge usw.
- 5. Aktivieren Sie die Erfassung. Der Befehl **no capture <Name> switch stop** aktiviert die Erfassung:

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

- 6. Überprüfen Sie die Erfassungsdetails:
- Der Verwaltungsstatus ist aktiviert, und der Betriebsstatus ist aktiv.
- Größe der Paketerfassungsdatei Pcapsize erhöht sich.
- Die Anzahl der erfassten Pakete in der Ausgabe von show capture <cap_name> ist ungleich null.
- Capture-Pfad PCAPFILE. Die erfassten Pakete werden automatisch im Ordner /mnt/disk0/packet-capture/ gespeichert.
- Erfassungsbedingungen. Die Software erstellt automatisch Erfassungsfilter, die auf Erfassungsbedingungen basieren.

```
> 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
                 enabled
 Admin State:
 Oper State:
                   up
Oper State Reason: Active
Config Success:
                  yes
Config Fail Reason:
Append Flaq:
              overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count:
                  0
Total Physical ports involved in Packet Capture: 1
Physical port:
Slot Id:
                   1
```

Port Id:	1
Pcapfile:	/mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize:	18838
Filter:	capsw-1-1

Packet Capture Filter Info

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

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

7. Stoppen Sie die Erfassung bei Bedarf:

```
> capture capsw switch stop
>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
                 24
Pcapsize:
Filter:
                 capsw-1-1
Packet Capture Filter Info
Name:
                  capsw-1-1
Protocol:
                  0
                 0
Ivlan:
                 205
Ovlan:
Src Ip:
                0.0.0.0
Dest Ip:
                0.0.0.0
                 ::
Src Ipv6:
                 ::
Dest Ipv6:
Src MAC:
                 00:00:00:00:00:00
                00:00:00:00:00:00
Dest MAC:
                 0
Src Port:
Dest Port:
                0
```

Ethertype: 0

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

8. Sammeln Sie die Erfassungsdateien. Befolgen Sie die Schritte im Abschnitt **Sammeln von Dateien zur Erfassung interner Switches der Secure Firewall 3100**.

In Version 7.2 wird die interne Switch-Erfassungskonfiguration auf dem FMC oder FDM nicht unterstützt. Bei der ASA Software-Version 9.18(1) und höher können die internen Switch-Erfassungen in den ASDM-Versionen 7.18.1.x und höher konfiguriert werden.

Diese Szenarien beziehen sich auf häufige Anwendungsfälle der internen Switch-Erfassung für die sichere Firewall 3100.

Paketerfassung an einer physischen oder Port-Channel-Schnittstelle

Verwenden Sie FTD oder ASA CLI, um eine Paketerfassung an der Schnittstelle Ethernet1/1 oder Port-Channel1 zu konfigurieren und zu überprüfen. Beide Schnittstellen enthalten den Namen **if**.

Topologie, Paketfluss und Erfassungspunkte



Konfiguration

Befolgen Sie die folgenden Schritte auf der ASA- oder FTD-CLI, um eine Paketerfassung an der Schnittstelle Ethernet1/1 oder Port-channel1 zu konfigurieren:

1. Überprüfen Sie den Namen:

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

2. Eine Aufzeichnungssitzung erstellen:

> capture capsw switch interface inside

3. Aufzeichnungssitzung aktivieren:

> no capture capsw switch stop Verifizierung

Überprüfen Sie den Namen der Erfassungssitzung, den Verwaltungs- und Betriebsstatus, den Schnittstellensteckplatz und die Kennung. Stellen Sie sicher, dass sich der **Pcapsize**-Wert in Byte erhöht und die Anzahl der erfassten Pakete ungleich null ist:

> show capture	capsw detail	
Packet Capture	info	
Name:	capsw	
Session:	1	
Admin State:	enabled	
Oper State:	up	
Oper State Re	ason: Active	
Config Success	s: yes	
Config Fail Re	eason:	
Append Flag:	overwrite	
Session Mem Us	age: 256	
Session Pcap S	Snap Len: 1518	
Error Code:	0	
Drop Count:	0	
Total Physical Physical port:	ports involved is	n Packet Capture: 1
Slot Id:	1	
Port Id:	1	
Pcapfile:	/mnt/disk0/j	packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize:	12653	
Filter:	capsw-1-1	
Packet Capture	Filter Info	
Name:	capsw-1-1	
Protocol:	0	
Ivlan:	0	
Ovlan:	0	
Src Ip:	0.0.0.0	

Dest Ip:	0.0.0
Src Ipv6:	::
Dest Ipv6:	::
Src MAC:	00:00:00:00:00:00
Dest MAC:	00:00:00:00:00:00
Src Port:	0
Dest Port:	0
Ethertype:	0

Total Physical breakout ports involved in Packet Capture: 0

79 packets captured on disk using switch capture

Reading of capture file from disk is not supported Im Fall von Port-channel1 wird die Erfassung an allen Mitgliedsschnittstellen konfiguriert:

> 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 L	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:	28824
Filter:	capsw-1-4
Packet Capture Filte	er 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	Filter	Info
Name:		Ca	apsw-1-3
Protoc	ol:	0	
Ivlan:		0	
Ovlan:		0	
Src Ip	:	0	.0.0.0
Dest I	p:	0	.0.0.0
Src Ip	vć:	:	:
Dest I	pv6:	:	:
Src MA	.C:	00	0:00:00:00:00:00
Dest M	IAC:	00	0:00:00:00:00:00
Src Po	ort:	0	
Dest P	ort:	0	
Ethert	ype:	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 Die Port-Channel-Member-Schnittstellen können in der FXOS-Befehlszeile **local-mgmt** mit dem Befehl **show port channel summary** überprüft werden:

> co:	nnect fxc	S						
KSEC	-FPR3100-	1 connect local	L-mgmt					
KSEC	-FPR3100-	·1(local-mgmt) :	show port	channel	summa	ry		
Flag	s: D - I	Down P -	Up in po	rt-chann	el (m	embers)		
I -	Individua	al H - Hot-star	ndby (LAC	P only)				
s -	Suspended	l r - Module-1	removed					
S -	Switched	R - Routed						
U - '	Up (port-	-channel)						
M - 1	Not in us	se. Min-links no	ot met					
Grou	p Port-	Type I	Protocol	Member	Ports			
	Channel							
1	Pol(U)	Eth I	LACP	Eth1/3(P)	Eth1/4(P)		
LACP	KeepAliv	ve Timer:						
	Channel	PeerKeepAlive	 CimerFast					
1	Po1(U)	False						
Clus	ter LACP	Status:						
	Channel	ClusterSpanned	d Cluste	rDetach	Clus	terUnitID	ClusterSysID	
1	Po1(U)	False	Fal	se	0		clust	

Um auf FXOS auf ASA zuzugreifen, führen Sie den Befehl **connect fxos admin** aus. Bei Multi-Context führen Sie den Befehl im Admin-Kontext aus.

Erfassungsdateien erfassen

Befolgen Sie die Schritte im Abschnitt Sammeln von Dateien zur Erfassung interner Switches der Secure Firewall 3100.

Analyse der Erfassungsdatei

Öffnen Sie die Erfassungsdateien für Ethernet1/1 mit einer Anwendung zum Lesen der Paketerfassungsdatei. Wählen Sie das erste Paket aus, und überprüfen Sie die Schlüsselpunkte:

- 1. Nur ICMP-Echoanforderungspakete werden erfasst.
- 2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.

No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info	<u>^</u>
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 re
	5 2022-08-07 19:50:10.928245	192.0.2.100	198.51.100.100	ICMP	102	0x9b10 (39696)	64 Echo (ping) request	id=0x0034, seq=5/1280, ttl=64 (no 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 re
	8 2022-08-07 19:50:13.934155	192.0.2.100	198.51.100.100	ICMP	102	0x9b8b (39819)	64 Echo (ping) request	id=0x0034, seq=8/2048, ttl=64 (no re
	9 2022-08-07 19:50:14.932004	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 hytes cant	ured (816 hits)			0000 bc e7 12	34 9a 14 00 50 56 9d e8	be 08 00 45 004P VE.
S E+F	arnet II. Src: VMware 0d:e8:he (00	50:56:0d:08:bo)	Det: Cisco 34:0a:	14 (hc:e7:12:3	(1.00.14)	0010 00 54 9a	10 40 00 40 01 b3 9c c0	00 02 64 c6 33 ·T··@·@· ·····d·3
Tot	ternet Protocol Version 4. Src: 19	.0.2.100. Dst: 1	98.51.100.100			0020 64 64 08	00 c6 91 00 34 00 01 61	17 f0 62 00 00 dd ····· 4 ··a··b··
Int	ternet Control Message Protocol		5015111001100		2	0030 00 00 18	ec 08 00 00 00 00 00 10	11 12 13 14 15
	ternet control hassage motocol					0040 16 17 18	19 1a 1b 1c 1d 1e 1f 20	21 22 23 24 25 !"#\$%
						0050 26 27 28	29 2a 2b 2c 2d 2e 2f 30	31 32 33 34 35 &'()*+,/012345
						0060 36 37 55	55 55 55	670000

Öffnen Sie die Erfassungsdateien für Portchannel1-Mitgliedsschnittstellen. Wählen Sie das erste Paket aus, und überprüfen Sie die wichtigsten Punkte:

- 1. Nur ICMP-Echoanforderungspakete werden erfasst.
- 2. Der ursprüngliche Paket-Header enthält kein VLAN-Tag.

No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info			^
E	1 2022-08-07 20:40:58.657533	192.0.2.100	198.51.100.100	ICMP	102	0x9296 (37526)	64 Echo (ping) request	id=0x0035, seq=1/256, tt	tl=64 (no res	
	2 2022-08-07 20:40:59.658611	192.0.2.100	198.51.100.100	ICMP	102	0x9370 (37744)	64 Echo (ping) request	id=0x0035, seq=2/512, tt	tl=64 (no res	
	3 2022-08-07 20:41:00.655662	192.0.2.100	198.51.100.100	ICMP	102	0x93f0 (37872)	64 Echo (ping) request	id=0x0035, seq=3/768, tt	tl=64 (no res	
	4 2022-08-07 20:41:01.659749	192.0.2.100	198.51.100.100	ICMP	102	0x946f (37999)	64 Echo (ping) request	id=0x0035, seq=4/1024, t	ttl=64 (no r€	
	5 2022-08-07 20:41:02.660624	192.0.2.100	198.51.100.100	ICMP	102	0x94a4 (38052)	64 Echo (ping) request	id=0x0035, seq=5/1280, t	ttl=64 (no r€	
	6 2022-08-07 20:41:03.663226	192.0.2.100	198.51.100.100	ICMP	102	0x952d (38189)	64 Echo (ping) request	id=0x0035, seq=6/1536, t	ttl=64 (no r€	
	7 2022-08-07 20:41:04.661262	192.0.2.100	198.51.100.100	ICMP	102	0x958d (38285)	64 Echo (ping) request	id=0x0035, seq=7/1792, t	ttl=64 (no r€	
	8 2022-08-07 20:41:05.665955	192.0.2.100	198.51.100.100	ICMP	102	0x95d8 (38360)	64 Echo (ping) request	id=0x0035, seq=8/2048, t	ttl=64 (no r€	
	9 2022-08-07 20:41:06.666538	192.0.2.100	198.51.100.100	ICMP	102	0x964b (38475)	64 Echo (ping) request	id=0x0035, seq=9/2304, t	ttl=64 (no r€	
	10 2022-08-07 20:41:07.667298	192.0.2.100	198.51.100.100	ICMP	102	0x972b (38699)	64 Echo (ping) request	id=0x0035, seq=10/2560,	ttl=64 (no r	
	11 2022-08-07 20:41:08.670540	192.0.2.100	198.51.100.100	ICMP	102	0x980a (38922)	64 Echo (ping) request	id=0x0035, seq=11/2816,	ttl=64 (no r	
	12 2022-08-07 20:41:09.668278	192.0.2.100	198.51.100.100	ICMP	102	0x9831 (38961)	64 Echo (ping) request	id=0x0035, seq=12/3072,	ttl=64 (no r	
	13 2022-08-07 20:41:10.672417	192.0.2.100	198.51.100.100	ICMP	102	0x98a2 (39074)	64 Echo (ping) request	id=0x0035, seq=13/3328,	ttl=64 (no r	
	14 2022-08-07 20:41:11.671369	192.0.2.100	198.51.100.100	ICMP	102	0x98f7 (39159)	64 Echo (ping) request	id=0x0035, seq=14/3584,	ttl=64 (no r	
	15 2022-08-07 20:41:12.675462	192.0.2.100	198.51.100.100	ICMP	102	0x99e4 (39396)	64 Echo (ping) request	id=0x0035, seq=15/3840,	ttl=64 (no r	
	16 2022-08-07 20:41:13.674903	192.0.2.100	198.51.100.100	ICMP	102	0x9a84 (39556)	64 Echo (ping) request	id=0x0035, seq=16/4096,	ttl=64 (no r	
	17 2022-08-07 20:41:14.674093	192.0.2.100	198.51.100.100	ICMP	102	0x9af3 (39667)	64 Echo (ping) request	id=0x0035, seq=17/4352,	ttl=64 (no r	
	18 2022-08-07 20:41:15.676904	192.0.2.100	198.51.100.100	ICMP	102	Øx9b8e (39822)	64 Echo (ping) request	id=0x0035, seq=18/4608,	ttl=64 (no r	~
<									>	
>	Frame 1: 102 bytes on wire (816 bits)	, 102 bytes captu	ured (816 bits)			0000 bc e7 12	2 34 9a 2c 00 50 56 9d e8	be 08 00 45 00 ···4·, 1	P V · · · · E ·	
>	Ethernet II, Src: VMware 9d:e8:be (00	:50:56:9d:e8:be),	Dst: Cisco 34:9a:2	c (bc:e7:12:3	4:9a:2c)	0010 00 54 92	96 40 00 40 01 bb 16 c0	00 02 64 c6 33 ·T··@·@	· · · · · · d · 3	
>	Internet Protocol Version 4, Src: 192	.0.2.100, Dst: 19	98.51.100.100		_	0020 64 64 08	8 00 58 a8 00 35 00 01 4d	23 f0 62 00 00 dd · · X · · 9	5 · · M# · b · ·	
>	Internet Control Message Protocol				2	0030 00 00 96	c 8 04 00 00 00 00 00 10	11 12 13 14 15		
	0					0040 16 17 18	3 19 1a 1b 1c 1d 1e 1f 20	21 22 23 24 25	! "#\$%	
						0050 26 27 28	3 29 2a 2b 2c 2d 2e 2f 30	31 32 33 34 35 & ()*+,-	/012345	
						0060 36 37 55	55 55 55	670000		

Erklärung

Die Switch-Erfassungen werden an den Schnittstellen Ethernet1/1 oder Port-Channel1 konfiguriert.

In dieser Tabelle ist die Aufgabe zusammengefasst:

Aufgabe	Erfassung spunkt	Interner Filter	Richtung	Erfasster Datenverkehr
Konfigurieren und Überprüfen der Paketerfassung an der Schnittstelle Ethernet1/1	Ethernet1/ 1	None	Nur Eingang	ICMP-Echo-Anfragen von Host 192.0.2.100 an Host 198.51.100.10
Konfiguration und Verifizierung der Paketerfassung an der Schnittstelle	Ethernet1/ 3	None	Nur Eingang	ICMP-Echo-Anfragen von Host 192.0.2.100 an Host 198.51.100.10

Paketerfassung auf einer Subschnittstelle einer physischen oder Port-Channel-Schnittstelle

Verwenden Sie die FTD- oder ASA-CLI, um eine Paketerfassung an den Subschnittstellen Ethernet1/1.205 oder Port-Channel1.205 zu konfigurieren und zu überprüfen. Beide Subschnittstellen haben den Namen **innen**.



Topologie, Paketfluss und Erfassungspunkte

Konfiguration

Befolgen Sie die folgenden Schritte auf der ASA- oder FTD-CLI, um eine Paketerfassung an der Schnittstelle Ethernet1/1 oder Port-channel1 zu konfigurieren:

1. Überprüfen Sie den Namen:

<pre>> show nameif</pre>		
Interface	Name	Security
Ethernet1/1.205	inside	0
Ethernet1/2	outside	0
Management1/1	diagnostic	0

<pre>> show nameif</pre>		
Interface	Name	Security
Port-channel1.205	inside	0
Ethernet1/2	outside	0
Management1/1	diagnostic	0

2. Eine Aufzeichnungssitzung erstellen:

> capture capsw switch interface inside

3. Aufzeichnungssitzung aktivieren:

> no capture capsw switch stop
Verifizierung

Überprüfen Sie den Namen der Erfassungssitzung, den Verwaltungs- und Betriebsstatus, den Schnittstellensteckplatz und die Kennung. Stellen Sie sicher, dass der **Pcapsize**-Wert in Byte erhöht wird und die Anzahl der erfassten Pakete ungleich null ist:

> show capture caps	w 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 1	Len: 1518
Error Code:	0
Drop Count:	0
Total Physical port:	s 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 Filte	er 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
Dest MAC:	00:00:00:00:00
Src Port:	0
Dest Port:	0
Ethertype:	0

46 packets captured on disk using switch capture

Reading of capture file from disk is not supported In diesem Fall wird ein Filter mit dem äußeren VLAN **Ovlan=205** erstellt und auf die Schnittstelle angewendet.

Im Fall von Port-channel1 wird die Erfassung mit dem Filter **Ovlan=205** auf allen Member-Schnittstellen konfiguriert:

> show capture capsw detail Packet Capture info Name: capsw Session: Admin State: enabled 1 Session: Oper State Reason: Active Config Success: yes Config Fail Reason: Append Flaq: overwrite Session Mem Usage: 256 Session Pcap Snap Len: 1518 Error Code: 0 Drop Count: 0 Total Physical ports involved in Packet Capture: 2 Physical port: Slot Id: 1 Port Id: 4 /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-4-0.pcap Pcapfile: Pcapsize: 23442 Filter: capsw-1-4 Packet Capture Filter Info Name: capsw-1-4 Protocol: 0 Ivlan: 0 205 **Ovlan:** 0.0.0.0 Src Ip: Dest Ip: 0.0.0.0 Src Ipv6: :: Dest Ipv6: :: Src MAC: 00:00:00:00:00:00 00:00:00:00:00:00 Dest MAC: 0 Src Port: 0 Dest Port: Ethertype: 0 Physical port: Slot Id: 1 Port Id: 3 Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-3-0.pcap Pcapsize: 5600 Filter: capsw-1-3 Packet Capture Filter Info Name: capsw-1-3 Protocol: 0 Ivlan: 0 Ovlan: 205

Src Ip:	0.0.0.0
Dest Ip:	0.0.0
Src Ipv6:	::
Dest Ipv6:	::
Src MAC:	00:00:00:00:00:00
Dest MAC:	00:00:00:00:00:00
Src Port:	0
Dest Port:	0
Ethertype:	0

Total Physical breakout ports involved in Packet Capture: 0

49 packet captured on disk using switch capture

Reading of capture file from disk is not supported

Die Port-Channel-Member-Schnittstellen können in der FXOS-Befehlszeile **local-mgmt** mit dem Befehl **show port channel summary** überprüft werden:

> connect fxos

••• KSEC-FPR3100-1 connect local-mgmt KSEC-FPR3100-1(local-mgmt) show portchannel summary P - Up in port-channel (members) Flags: D - Down 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 ------Type Group Port-Protocol Member Ports Channel _____ Pol(U) Eth LACP Eth1/3(P) Eth1/4(P) 1 LACP KeepAlive Timer: _____ Channel PeerKeepAliveTimerFast _____ Pol(U) False 1 Cluster LACP Status: _____ Channel ClusterSpanned ClusterDetach ClusterUnitID ClusterSysID _____ 0 Pol(U) False False 1 clust

Um auf FXOS auf ASA zuzugreifen, führen Sie den Befehl **connect fxos admin** aus. Bei Multi-Context führen Sie diesen Befehl im Admin-Kontext aus.

Erfassungsdateien erfassen

Befolgen Sie die Schritte im Abschnitt Sammeln von Dateien zur Erfassung interner Switches der Secure Firewall 3100.

Analyse der Erfassungsdatei

Öffnen Sie die Erfassungsdateien für Ethernet1/1.205 mit einer Anwendung zum Lesen von Paketerfassungsdateien. Wählen Sie das erste Paket aus, und überprüfen Sie die Schlüsselpunkte:

- 1. Nur ICMP-Echoanforderungspakete werden erfasst.
- 2. Der ursprüngliche Paket-Header hat den VLAN-Tag 205.

No.	Time	Source	Destination	Protocol	Length	IP ID		IP TTL Info							^
E.	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	(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	(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	(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	(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	(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	(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	(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	(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	(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	~
<														>	
> Fr	ame 1: 106 bytes on wire (848 bits)	. 106 bytes capt	ured (848 bits)			0000	bc e7 1	2 34 9a 14	00 50	56 9d e8	be 81 00 00	cd4	·P V····		_
> Et	hernet II, Src: VMware 9d:e8:be (00	:50:56:9d:e8:be)	Dst: Cisco 34:9a:	14 (bc:e7:12:3	4:9a:14)	0010	08 00 4	5 00 00 54	41 1f	40 00 40	01 0c 8e c0	00 ··E··T	A. 0.0.		
~ 86	2.10 Virtual LAN, PRI: 0, DEI: 0, I	D: 205	-			0020	02 64 c	6 33 64 64	08 00	06 67 00	37 00 01 be	2c ·d·3dd	·· ·g·7·	··,	
	000 = Priority: Be	st Effort (defaul	t) (0)			0036	f0 62 0	0 00 00 00	8e fe	03 00 00	00 00 00 10	11 ·b····			
					0046	12 13 1	4 15 16 17	18 19	1a 1b 1c	1d 1e 1f 20	21	•••••••	1.1		
0000 1100 1101 = ID: 205					0056	22 23 2	4 25 26 27	28 29	2a 2b 2c	2d 2e 2f 30	31 "#\$%&"	() *+,	/01		
	Type: IPv4 (0x0800)				2	0066	32 33 3	4 35 36 37	55 55	55 55		234567	00 00		
	Trailer: 55555555														
> Ir	> Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100														
> Ir	ternet Control Message Protocol														
_	0														

Öffnen Sie die Erfassungsdateien für Portchannel1-Mitgliedsschnittstellen. Wählen Sie das erste Paket aus, und überprüfen Sie die wichtigsten Punkte:

- 1. Nur ICMP-Echoanforderungspakete werden erfasst.
- 2. Der ursprüngliche Paket-Header hat den VLAN-Tag 205.

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 r€	
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 r€	
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 r€	
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 r€	
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 capt	ured (848 bits)			0000 bc e7 1	2 34 9a 14 00 50 56 9d e8	be 81 00 00 cd4P V	
> Ethernet II, Src: VMware_9d:e8:be (@	0:50:56:9d:e8:be)	, Dst: Cisco 34:9a:	14 (bc:e7:12:3	4:9a:14)	0010 08 00 4	5 00 00 54 41 1f 40 00 40	01 0c 8e c0 00 ··E··TA·@·@·····	
802.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 205	-			0020 02 64 c	6 33 64 64 08 00 06 67 00	37 00 01 b0 2c ·d·3dd·· ·g·7···,	
000 Briority: B	est Effort (defau	lt) (0)			0030 f0 62 0	0 00 00 00 8e fe 03 00 00	00 00 00 10 11 ·b·····	
0 = DEI: Inelig	ible				0040 12 13 1	4 15 16 17 18 19 1a 1b 1c	1d 1e 1f 20 21	
0000 1100 1101 = ID: 205				-	0050 22 23 2	4 25 26 27 28 29 2a 20 2c	2d 2e 2f 30 31 #\$%& () ~+,/01	
Type: IPv4 (0x0800)				2	0000 32 33 3	4 35 36 37 55 55 55 55	23456700 00	
Trailer: 5555555								
> Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100								
> Internet Control Message Protocol								

Erklärung

Die Switch-Erfassungen werden an den Subschnittstellen Ethernet1/1.205 oder Port-Channel1.205 mit einem Filter konfiguriert, der mit dem äußeren VLAN 205 übereinstimmt.

In dieser Tabelle ist die Aufgabe zusammengefasst:

Aufgabe	Erfassun gspunkt	Interner Filter	Richtun g	Erfasster Datenverkehr
Konfiguration und Verifizierung einer Paketerfassung an der Subschnittstelle Ethernet1/1.205	Ethernet 1/1	Äußeres VLAN 205	Nur Eingan g	ICMP-Echo-Anfragen von Host 192.0.2.100 an Host 198.51.100.
Konfiguration und Verifizierung einer Paketerfassung an der Subschnittstelle	Ethernet 1/3	Äußeres VLAN 205	Nur Eingan	ICMP-Echo-Anfragen von Host 192.0.2.100 an Host 198.51.100.7

Paketerfassung an internen Schnittstellen

Die sichere Firewall verfügt über 2 interne Schnittstellen:

- in_data_uplink1: Verbindet die Anwendung mit dem internen Switch.
- in_mgmt_uplink1 Stellt einen dedizierten Paketpfad für Managementverbindungen wie SSH zur Verwaltungsschnittstelle oder die Verwaltungsverbindung (auch Sftunnel genannt) zwischen dem FMC und dem FTD bereit.

Aufgabe 1

Verwenden Sie FTD oder ASA CLI, um eine Paketerfassung auf der Uplink-Schnittstelle **in_data_uplink1** zu konfigurieren und zu überprüfen.

Topologie, Paketfluss und Erfassungspunkte



Konfiguration

Führen Sie die folgenden Schritte auf ASA oder FTD CLI aus, um eine Paketerfassung auf der Schnittstelle **in_data_uplink1 zu** konfigurieren:

- 1. Eine Aufzeichnungssitzung erstellen:
- > capture capsw switch interface in_data_uplink1
 - 2. Aufzeichnungssitzung aktivieren:

> no capture capsw switch stop
Verifizierung

Überprüfen Sie den Namen der Erfassungssitzung, den Verwaltungs- und Betriebsstatus, den Schnittstellensteckplatz und die Kennung. Stellen Sie sicher, dass der **Pcapsize**-Wert in Byte erhöht wird und die Anzahl der erfassten Pakete ungleich null ist:

> show capture capsw detail Packet Capture info Name: capsw Session: 1 Admin State: enabled Oper State: up Oper State Reason: Active Config Success: yes Config Fail Reason: Append Flag: overwrite Session Mem Usage: 256 Session Pcap Snap Len: 1518 0 Error Code: 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 capsw-1-18 Filter: Packet Capture Filter Info capsw-1-18 Name: Protocol: 0 Tvlan: 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 00:00:00:00:00:00 Dest MAC: 0 Src Port:

Total Physical breakout ports involved in Packet Capture: 0

66 packets captured on disk using switch capture

0 0

Dest Port:

Ethertype:

Reading of capture file from disk is not supported

In diesem Fall wird eine Erfassung auf der Schnittstelle mit der internen ID **18** erstellt, die die in_data_uplink1-Schnittstelle auf der sicheren Firewall 3130 ist. Der Befehl **show portManager switch status** in der FXOS-Befehlszeile **local-mgmt** gibt die Schnittstellen-IDs an:

> connect fxos KSEC-FPR3100-1 connect local-mgmt KSEC-FPR3100-1(local-mgmt) show portmanager switch status Mode Link Speed Duplex Loopback Mode Port Manager Dev/Port -----_____ ____ -----SGMIIUp1GFullNoneSGMIIUp1GFullNoneSGMIIUp1GFullNoneSGMIIUp1GFullNoneSGMIIDown1GHalfNoneSGMIIDown1GHalfNoneSGMIIDown1GHalfNoneSGMIIDown1GHalfNoneSGMIIDown1GHalfNoneSGMIIDown1GHalfNone 0/1Link-Up 0/2 Link-Up 0/3 SGMII Link-Up 0/4 SGMII Link-Up SGMII Mac-Link-Down 0/5SGMII Mac-Link-Down 0/6 Mac-Link-Down 0/7 0/8 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

Um auf FXOS auf ASA zuzugreifen, führen Sie den Befehl **connect fxos admin** aus. Bei Multi-Context führen Sie diesen Befehl im Admin-Kontext aus.

Erfassungsdateien erfassen

Befolgen Sie die Schritte im Abschnitt Sammeln von Dateien zur Erfassung interner Switches der Secure Firewall 3100.

Analyse der Erfassungsdatei

Öffnen Sie die Erfassungsdateien für die Schnittstelle in_data_uplink1 mit einer Anwendung zum Lesen von Paketerfassungsdateien. Überprüfen Sie den Schlüsselpunkt - in diesem Fall werden ICMP-Echoanforderungs- und Echoantwortpakete erfasst. Dies sind die Pakete, die von der Anwendung an den internen Switch gesendet werden.

No.	Time		Source	Destination	Protocol	Length	IP ID	IP TTL Info	<u>^</u>
	1 2022-08-07	22:40:06.685606	192.0.2.100	198.51.100.100	ICMP	102	0x4d93 (19859)	64 Echo (ping) request	id=0x003a, seq=33/8448, ttl=64 (repl
e	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	0x4de8 (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	0x6db2 (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	0x4edc (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	0x6dbf (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	0x6ed5 (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 v
<									>
> Ena	me 1: 102 bytes	s on wire (816 bits), 102 bytes capt	ured (816 bits)			0000 00 50 56	9d e7 50 bc e7 12 34 9a	15 08 00 45 00 ·PV··P·· ·4····E·
> Eth	ernet II. Src:	Cisco 34:9a:15 (bc	:e7:12:34:9a:15).	Dst: VMware 9d:e7:	50 (00:50:56:9	d:e7:50)	0010 00 54 40	93 40 00 40 01 00 1a c0	00 02 64 c6 33 ·TM·@·@· ····d·3
> Int	ernet Protocol	Version 4, Src: 19	2.0.2.100. Dst: 19	98.51.100.100			0020 64 64 08	00 7f 15 00 3a 00 21 39	3f f0 62 00 00 dd · · · • • • 19? · b · ·
> Int	ernet Control M	lessage Protocol					0030 00 00 80	1a 05 00 00 00 00 00 10	11 12 13 14 15
							0040 16 17 18	19 1a 1b 1c 1d 1e 1f 20	21 22 23 24 25 !"#\$%
							0050 26 27 28	29 2a 2b 2c 2d 2e 2f 30	31 32 33 34 35 &'()*+,/012345
							0060 36 37 55	55 55 55	670000

Erklärung

Wenn eine Switch-Erfassung an der Uplink-Schnittstelle konfiguriert ist, werden nur Pakete erfasst, die von der Anwendung an den internen Switch gesendet werden. An die Anwendung gesendete Pakete werden nicht erfasst.

In dieser Tabelle ist die Aufgabe zusammengefasst:

Aufgabe	Erfassung spunkt	Interner Filter	Richtung	Erfasster Datenverkehr
Konfigurieren und Überprüfen einer Paketerfassung an der Uplink- Schnittstelle in_data_uplink1	in_data_u plink1	None	Nur Eingang	ICMP-Echo-Anfragen von Host 192.0.2.100 an Host 198.51.100 ICMP-Echo-Antworten von Host 198.51.100.100 zu Host 192.0.2.

Aufgabe 2

Verwenden Sie FTD oder ASA CLI, um eine Paketerfassung auf der Uplink-Schnittstelle in_mgmt_uplink1 zu konfigurieren und zu überprüfen. Nur die Pakete der Verbindungen auf Verwaltungsebene werden erfasst.

Topologie, Paketfluss und Erfassungspunkte



Konfiguration

Führen Sie die folgenden Schritte auf ASA- oder FTD-CLI aus, um eine Paketerfassung auf der Schnittstelle **in_mgmt_uplink1 zu** konfigurieren:

- 1. Eine Aufzeichnungssitzung erstellen:
- > capture capsw switch interface in_mgmt_uplink1
 - 2. Aufzeichnungssitzung aktivieren:

> no capture capsw switch stop
Verifizierung

Überprüfen Sie den Namen der Erfassungssitzung, den Verwaltungs- und Betriebsstatus, den Schnittstellensteckplatz und die Kennung. Stellen Sie sicher, dass der **Pcapsize**-Wert in Byte

erhöht wird und die Anzahl der erfassten Pakete ungleich null ist:

> show capture capsw detail Packet Capture info Name: capsw Session: 1 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: /mnt/disk0/packet-capture/sess-1-capsw-mgmt-uplink1.pcap 137248 capsw-1 10 Slot Id: Port Id: Pcapfile: Pcapsize: capsw-1-19 Filter: Packet Capture Filter Info Name: capsw-1-19 Protocol: 0 0 Ivlan: Ovlan: 0 0.0.0.0 Src Ip: Dest Ip: 0.0.0.0 Src Ipv6: :: Dest Ipv6: :: Src MAC: 00:00:00:00:00:00 Dest MAC: 00:00:00:00:00:00 Src Port: 0 Dest Port: 0 0 Ethertype:

Total Physical breakout ports involved in Packet Capture: 0

281 packets captured on disk using switch capture

Reading of capture file from disk is not supported

In diesem Fall wird eine Erfassung an der Schnittstelle mit einer internen ID 19 erstellt, die die in_mgmt_uplink1-Schnittstelle auf der sicheren Firewall 3130 ist. Der Befehl show portManager switch status in der FXOS-Befehlszeile local-mgmt gibt die Schnittstellen-IDs an:

> connect fxos

•••

KOHO HDD 2100 1		legel memb
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	$1 \mathrm{G}$	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

Um auf FXOS auf ASA zuzugreifen, führen Sie den Befehl **connect fxos admin** aus. Bei Multi-Context führen Sie diesen Befehl im Admin-Kontext aus.

Erfassungsdateien erfassen

Befolgen Sie die Schritte im Abschnitt Sammeln von Dateien zur Erfassung interner Switches der Secure Firewall 3100.

Analyse der Erfassungsdatei

Öffnen Sie die Erfassungsdateien für die Schnittstelle **in_mgmt_uplink1 mit** einer Anwendung zum Lesen der Paketerfassungsdatei. Überprüfen Sie den Schlüsselpunkt - in diesem Fall werden nur die Pakete der Management-IP-Adresse 192.0.2.200 angezeigt. Beispiele sind SSH-, Sftunneloder ICMP-Echo-Antwort-Pakete. Dies sind die Pakete, die von der Schnittstelle für das Anwendungsmanagement über den internen Switch an das Netzwerk gesendet werden.

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 (470	56) 64 39181 → 8305 [ACK] Seq=61372 Ack=875 Win=1384	Len=1448 TS	
197 2022-08-07 23	:21:45.133385	192.0.2.200	192.0.2.101	TCP	1518	0xb7d1 (470	57) 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 (470	64 Application Data			
199 2022-08-07 23	:21:45.928772	192.0.2.200	192.0.2.100	ICMP	78	0xbd48 (484	64 Echo (ping) reply	id=0x0001, seq=4539/47889	9, ttl=64	
200 2022-08-07 23	:21:45.949024	192.0.2.200	192.0.2.101	TLSv1.2	128	0x4a97 (190	95) 64 Application Data			
201 2022-08-07 23	:21:45.949027	192.0.2.200	192.0.2.101	TCP	70	0x4a98 (190	96) 64 8305 → 58885 [ACK] Seq=21997 Ack=26244 Win=411	16 Len=0 TSv	
202 2022-08-07 23	:21:46.019895	192.0.2.200	192.0.2.101	TLSv1.2	100	0x4a99 (190	97) 64 Application Data			
203 2022-08-07 23	:21:46.019899	192.0.2.200	192.0.2.101	TLSv1.2	96	0x4a9a (190	64 Application Data			
204 2022-08-07 23	:21:46.019903	192.0.2.200	192.0.2.101	TCP	70	0x4a9b (190	99) 64 8305 → 58885 [ACK] Seq=22053 Ack=26274 Win=411	16 Len=0 TSv	
205 2022-08-07 23	:21:46.019906	192.0.2.200	192.0.2.101	TCP	70	0x4a9c (191	30) 64 8305 → 58885 [ACK] Seq=22053 Ack=26300 Win=411	16 Len=0 TSv	
206 2022-08-07 23	:21:46.136415	192.0.2.200	192.0.2.101	TCP	70	0xb7d3 (470	59) 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 (485	 64 Echo (ping) reply 	id=0x0001, seq=4540/48145	5, ttl=64	
208 2022-08-07 23	:21:47.980409	192.0.2.200	192.0.2.100	ICMP	78	0xbdf2 (486	64 Echo (ping) reply	id=0x0001, seq=4541/48401	1, ttl=64	
209 2022-08-07 23	:21:48.406312	192.0.2.200	192.0.2.101	TCP	70	0x4a9d (191	31) 64 8305 → 58885 [ACK] Seq=22053 Ack=26366 Win=411	16 Len=0 TSv	
210 2022-08-07 23	:21:48.903236	192.0.2.200	192.0.2.101	TLSv1.2	747	0x4a9e (191	32) 64 Application Data			
211 2022-08-07 23	:21:48.994386	192.0.2.200	192.0.2.100	ICMP	78	Øxbe48 (487	12) 64 Echo (ping) reply	id=0x0001, seq=4542/48657	7, ttl=64	
212 2022-08-07 23	:21:50.008576	192.0.2.200	192.0.2.100	ICMP	78	Øxbea6 (488	64 Echo (ping) reply	id=0x0001, seq=4543/48913	3, ttl=64	
213 2022-08-07 23	:21:50.140167	192.0.2.200	192.0.2.101	TCP	1518	0xb7d4 (470	50) 64 39181 → 8305 [ACK] Seq=65188 Ack=921 Win=1384	Len=1448 TS	
214 2022-08-07 23	:21:50.140171	192.0.2.200	192.0.2.101	TCP	1518	0xb7d5 (470	51) 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 (470	64 Application Data			
216 2022-08-07 23	:21:51.015884	192.0.2.200	192.0.2.100	ICMP	78	Øxbec1 (488	33) 64 Echo (ping) reply	id=0x0001, seq=4544/49169	9, ttl=64	
217 2022-08-07 23	:21:51.142842	192.0.2.200	192.0.2.101	TCP	70	0xb7d7 (470	53) 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 (488	64 Echo (ping) reply	id=0x0001, seq=4545/49425	5, ttl=64	
219 2022-08-07 23	:21:53.042744	192.0.2.200	192.0.2.100	ICMP	78	0xbf59 (489	35) 64 Echo (ping) reply	id=0x0001, seq=4546/49681	1, ttl=64	
220 2022-08-07 23	:21:53.073144	192.0.2.200	192.0.2.100	SSH	170	Øxad34 (443	 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 (443	41) 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 (191	33) 64 Application Data			
223 2022-08-07 23	:21:54.102899	192.0.2.200	192.0.2.100	ICMP	78	Øxbf63 (489	95) 64 Echo (ping) reply	id=0x0001, seq=4547/49937	7, ttl=64	
224 2022-08-07 23	:21:54.903675	192.0.2.200	192.0.2.101	TCP	70	0x4aa0 (191	34) 64 8305 → 58885 [ACK] Seq=23407 Ack=26424 Win=411	16 Len=0 TSv	
175 2022 00 07 22	.01.55 106700	103 0 3 300	103 0 3 100	TCMD	70	Avhfel (Ana	20) 64 Echo (ning) conly	id-0v0001 con-4540/50103	× ++1-64	- *
> Frame 1: 747 bytes o	on wire (5976 bits), 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: Ci	isco 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 Ve	ersion 4, Src: 192	.0.2.200, Dst: 1	92.0.2.101			0020 02	65 20 71 e6 05 67 1b 2a c5	db e3 6b d4 80 18 ·e q··g·	* · · · k · · ·	
> Transmission Control	l Protocol, Src Po	ort: 8305, Dst Po	rt: 58885, Seq	: 1, Ack: 1, Len: 6	77	0030 10	14 27 cc 00 00 01 01 08 0a	08 76 95 7f 91 02	· · · v · · · ·	
> Transport Layer Secu	urity					0040 3d	41 17 03 03 02 a0 22 6a 01	e0 ff cc 98 f9 af =A·····"	j	
						0050 07	40 75 19 a4 d5 df 64 d8 fe	66 8e 9b cc 8d 2f -@ud		
						0060 92	b2 1a 64 e7 20 36 03 8e 48	02 5a 7c 85 30 d4 ···d·6·	-H-Z -0-	
						0070 Ta	c0 a8 56 08 a0 a7 7e 19 3a	79 b4 15 16 44 99	- KW-	
						0000 00	ch 43 9e 1f fd a7 70 75 e5	6h a4 f8 2h ee 47	U-k-+-G	
						00a0 2f	86 73 8f b1 e1 b5 c6 57 e3	a8 46 0e cb 26 b7 /.s	WF&-	
						00b0 5b	c7 e3 09 54 f3 c1 ff 26 d9	87 ea 51 3d 20 08 [····T···	& · · · Q= ·	
						00c0 16	fd cb f5 4f 91 98 5e 86 15	17 55 68 6f 5d 040	····Uho]·	
						Л			-	~

Erklärung

Wenn eine Switch-Erfassung auf der Management-Uplink-Schnittstelle konfiguriert ist, werden nur von der Anwendungsmanagement-Schnittstelle gesendete Eingangspakete erfasst. Pakete, die für die Verwaltungsschnittstelle der Anwendung bestimmt sind, werden nicht erfasst.

In dieser Tabelle ist die Aufgabe zusammengefasst:

Aufgabe	Erfassung spunkt	Interner Filter	Richtung	Erfasster Datenverkehr
Konfigurieren und Überprüfen einer Paketerfassung auf der Management- Uplink- Schnittstelle	in_mgmt_ uplink1	None	Nur Eingang (von der Managementschnittste Ile zum Netzwerk über den internen Switch)	ICMP-Echoantworten von FTD-Verwaltur IP-Adresse 192.0.2.200 an Host 192.0.2. Sftunnel von FTD-Management-IP-Adress 192.0.2.200 zu FMC-IP-Adresse 192.0.2 SSH von FTD-Management-IP-Adresse 192.0.2.200 an Host 192.0.2.100

Paketerfassungsfilter

Die internen Switch-Paketerfassungsfilter werden auf die gleiche Weise konfiguriert wie die Paketerfassung auf Datenebene. Verwenden Sie **Ethernet-Typ** und **Match-**Optionen, um Filter zu konfigurieren.

Konfiguration

Befolgen Sie die folgenden Schritte auf ASA oder FTD CLI, um eine Paketerfassung mit einem Filter zu konfigurieren, der ARP-Frames oder ICMP-Paketen von Host 198.51.100.100 auf Schnittstelle Ethernet1/1 entspricht:

1. Überprüfen Sie den Namen:

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

2. Erstellen einer Aufzeichnungssitzung für ARP oder ICMP:

> capture capsw switch interface inside ethernet-type arp

> capture capsw switch interface inside match icmp 198.51.100.100 Verifizierung

Überprüfen Sie den Namen der Aufzeichnungssitzung und den Filter. Der Ethertype-Wert ist 2054 im Dezimalformat und 0x0806 im Hexadezimalformat:

> 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 port Physical port:	s involved in Packet Capture: 1						
Slot Id:	1						
Port Id:	1						
Pcapfile:	/mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap						
Pcapsize:	0						
Filter:	capsw-1-1						
Packet Capture Filt	er Info						
Name:	capsw-1-1						
Protocol:	0						
Ivlan:	0						
Ovlan:	0						
Src Ip:	0.0.0.0						
Dest Ip:	0.0.0.0						
Src Ipv6:	::						
Dest Ipv6:	::						
Src MAC:	00:00:00:00:00						
Dest MAC:	00:00:00:00:00						
Src Port:	0						

Total Physical breakout ports involved in Packet Capture: 0

0

Src Port: Dest Port:

Ethertype: 2054

0 packet captured on disk using switch capture

Reading of capture file from disk is not supported Dies ist die Verifizierung des Filters für ICMP. IP-Protokoll 1 ist das ICMP:

> show capture capsw detail

Packet Capture info Name: capsw Session: 1

Admin State:IAdmin State:disabledOper State:downOper State Reason:Session_Admin_ShutConfig Success:yesConfig Fail Reason:Append Flag:Append Flag:overwriteSession Mem Usage:256Session Pcap Snap Len:1518Error Code:0Drop 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
Dest MAC:	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

Erfassen von Dateien für den internen Secure Firewall 3100-Switch

Verwenden Sie die ASA- oder FTD-CLI, um interne Switch-Erfassungsdateien zu erfassen. Auf FTD kann die Erfassungsdatei auch über den CLI-**Kopierbefehl** an Ziele exportiert werden, die über die Daten- oder Diagnoseschnittstellen erreichbar sind.

Alternativ kann die Datei im Expertenmodus nach /**ngfw/var/common** kopiert und über die Option **File Download** vom FMC heruntergeladen werden.

Bei Port-Channel-Schnittstellen müssen Sie sicherstellen, dass die Paketerfassungsdateien von

allen Mitgliedsschnittstellen erfasst werden.

ASA

Führen Sie die folgenden Schritte aus, um interne Switch-Erfassungsdateien in der ASA CLI zu erfassen:

- 1. Erfassung beenden:
- asa# capture capsw switch stop
 - 2. Überprüfen Sie, ob die Aufzeichnungssitzung beendet wurde, und notieren Sie sich den Namen der Aufzeichnungsdatei.

```
asa# show capture capsw detail
Packet Capture info
Name:
                 capsw
Session:
                 1
 Admin State: disabled
Oper State: down
Admin 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
Drop Count:
                  0
Total Physical ports involved in Packet Capture: 1
Slot Id: 1

Port Id: 1

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

Pcapsize: 139826

Filter:
Physical port:
               capsw-1-1
Filter:
Packet Capture Filter Info
          capsw-1-1
Name:
Protocol:
                  0
                  0
Ivlan:
Ovlan:
                  0
                 0.0.0.0
Src Ip:
                 0.0.0.0
Dest Ip:
Src Ipv6:
                  ::
Dest Ipv6:
                  ::
                 00:00:00:00:00:00
Src MAC:
                 00:00:00:00:00:00
Dest MAC:
Src Port:
                  0
                 0
Dest Port:
                 0
Ethertype:
Total Physical breakout ports involved in Packet Capture: 0
886 packets captured on disk using switch capture
Reading of capture file from disk is not supported
```

3. Verwenden Sie den CLI-Befehl copy, um die Datei in Remote-Ziele zu exportieren:

```
asa# copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap ?
cluster: Copy to cluster: file system
              Copy to disk0: file system
disk0:
               Copy to disk1: file system
disk1:
              Copy to flash: file system
flash:
ftp:
               Copy to ftp: file system
running-config Update (merge with) current system configuration
              Copy to scp: file system
scp:
smb:
               Copy to smb: file system
startup-config Copy to startup configuration
system: Copy to system: file system
                Copy to tftp: file system
tftp:
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
```

Führen Sie die folgenden Schritte aus, um interne Switch-Erfassungsdateien auf der FTD-CLI zu erfassen und auf Server zu kopieren, die über Daten- oder Diagnoseschnittstellen erreichbar sind:

1. Rufen Sie die Diagnose-CLI auf:

```
> 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#</pre>

2. Erfassung beenden:

firepower# capture capi switch stop

3. Überprüfen Sie, ob die Aufzeichnungssitzung beendet wurde, und notieren Sie sich den Namen der Aufzeichnungsdatei:

```
firepower# show capture capsw detail
Packet Capture info
Name:
                  capsw
Session:
                  1
Admin State:
                 disabled
 Oper State:
                   down
 Oper State Reason: Session_Admin_Shut
                  yes
Config Success:
Config Fail Reason:
Append Flaq:
              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 H	Filter Info
Name:	capsw-1-1
Protocol:	0
Ivlan:	0
Ovlan:	0
Src Ip:	0.0.0.0
Dest Ip:	0.0.0.0
Src Ipv6:	::
Dest Ipv6:	::
Src MAC:	00:00:00:00:00
Dest MAC:	00:00:00:00:00
Src Port:	0
Dest Port:	0
Ethertype:	0
Total Physical k	preakout ports involved in Packet Capture: 0

886 packets captured on disk using switch capture

Reading of capture file from disk is not supported

4. Verwenden Sie den CLI-Befehl copy, um die Datei in Remote-Ziele zu exportieren.

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

Führen Sie die folgenden Schritte aus, um Erfassungsdateien von FMC über die Option **Dateidownload** zu sammeln:

- 1. Erfassung beenden:
- > capture capsw switch stop
 - 2. Überprüfen Sie, ob die Aufzeichnungssitzung beendet wurde, und notieren Sie den Dateinamen und den vollständigen Pfad der Erfassungsdatei:

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

Wechseln Sie in den Expertenmodus und in den Root-Modus:

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

4. Kopieren Sie die Erfassungsdatei nach /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. Wählen Sie auf FMC Devices > File Download:



6. Wählen Sie das FTD aus, geben Sie den Namen der Erfassungsdatei an, und klicken Sie auf **Herunterladen**:

Firewall Management Center Devices / Troubleshoot / File Download	Analysis Policies	Devices Objects	Integration Depl	oy Q 🚱 🌣 Ø lab_domain \ admin ▼ 🛗 🕴 SECURE
	Device FPR3100-1 File sess-1-capsw-etherne	• It-1-1-0.pcap Back Download		Threat Defense CLI Packet Capture Packet Tracer

Richtlinien, Einschränkungen und Best Practices für die interne Switch-Paketerfassung

Richtlinien und Einschränkungen:

- Mehrere Sitzungen der Switch-Erfassungskonfiguration werden unterstützt, es kann jedoch nur jeweils eine Sitzung der Switch-Erfassung aktiv sein. Der Versuch, zwei oder mehr Aufzeichnungssitzungen zu aktivieren, führt zu dem Fehler "FEHLER: Die Sitzung konnte nicht aktiviert werden, da maximal 1 aktive Paketerfassungssitzung erreicht wurde."
- Die Erfassung eines aktiven Switches kann nicht gelöscht werden.
- Switch-Erfassungen können in der Anwendung nicht gelesen werden. Der Benutzer muss die Dateien exportieren.
- Bestimmte Erfassungsoptionen für die Datenebene wie **Dump, Decodierung, Paketnummer, Trace** und andere werden für Switch-Erfassungen nicht unterstützt.
- Bei Multi-Context-ASA werden die Switch-Erfassungen an Datenschnittstellen in Benutzerkontexten konfiguriert. Die Switch-Erfassungen an den Schnittstellen in_data_uplink1 und in_mgmt_uplink1 werden nur im Admin-Kontext unterstützt.

Dies ist die Liste der Best Practices, die auf der Verwendung der Paketerfassung in TAC-Fällen basieren:

- Beachten Sie Richtlinien und Einschränkungen.
- Verwenden Sie Erfassungsfilter.
- Berücksichtigen Sie die Auswirkungen von NAT auf Paket-IP-Adressen, wenn ein Erfassungsfilter konfiguriert wird.
- Erhöhen oder verringern Sie die **Paketlänge**, die die Frame-Größe angibt, falls sie sich vom Standardwert von 1518 Byte unterscheidet. Eine geringere Größe führt zu einer höheren Anzahl erfasster Pakete und umgekehrt.
- Passen Sie die Puffergröße nach Bedarf an.
- Beachten Sie den **Drop Count** in der Ausgabe des Befehls **show cap <cap_name> detail**. Sobald die Puffergrößengrenze erreicht ist, erhöht sich der Zähler für die Verwerfung.

Zugehörige Informationen

- Firepower 4100/9300 Chassis Manager und FXOS CLI Konfigurationsanleitungen
- <u>Cisco Secure Firewall 3100 Erste Schritte</u>
- Befehlsreferenz für Cisco Firepower 4100/9300 FXOS

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.