Configuración y verificación de capturas internas de switches Firepower y firewall seguro

Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados Antecedentes** Descripción general de alto nivel de la arquitectura del sistema Descripción general de alto nivel de las operaciones internas del switch Flujo de paquetes y puntos de captura Configuración y verificación en Firepower 4100/9300 Captura de paquetes en una interfaz física o de canal de puerto Capturas de paquetes en interfaces de backplane Capturas de paquetes en puertos de aplicaciones y aplicaciones Captura de paquetes en una subinterfaz de una interfaz física o de canal de puerto Filtros de captura de paquetes Recopilación de archivos de captura de switches internos Firepower 4100/9300 Directrices, limitaciones y prácticas recomendadas para la captura de paquetes de switches internos Configuración y verificación en Secure Firewall 3100 Captura de paquetes en una interfaz física o de canal de puerto Captura de paquetes en una subinterfaz de una interfaz física o de canal de puerto Captura de paquetes en interfaces internas Filtros de captura de paquetes Recopilación de archivos de captura de switches internos de Secure Firewall 3100 Directrices, limitaciones y prácticas recomendadas para la captura de paquetes de switches internos Información Relacionada

Introducción

Este documento describe la configuración y verificación de las capturas del switch interno Firepower y Secure Firewall.

Prerequisites

Requirements

Conocimiento básico del producto, análisis de captura.

Componentes Utilizados

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Firewall seguro 31xx
- Firepower 41xx
- Firepower 93xx
- Cisco Secure eXtensible Operating System (FXOS) 2.12.0.x
- Cisco Secure Firewall Threat Defence (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)

Antecedentes

Descripción general de alto nivel de la arquitectura del sistema

Desde la perspectiva del flujo de paquetes, la arquitectura de Firepower 4100/9300 y Secure Firewall 3100 se puede visualizar como se muestra en esta figura:



El chasis incluye estos componentes:

• Switch interno: reenvía el paquete de la red a la aplicación y viceversa. El switch interno está conectado a las interfaces frontales que residen en el módulo de interfaz integrado o los módulos de red externos y se conecta a dispositivos externos, por ejemplo, switches. Algunos

ejemplos de interfaces frontales son Ethernet 1/1, Ethernet 2/4, etc. El "frente" no es una definición técnica fuerte. En este documento, se utiliza para distinguir las interfaces conectadas a dispositivos externos de las interfaces de backplane o uplink.

 Placa base o enlace ascendente: interfaz interna que conecta el módulo de seguridad (SM) al switch interno. Esta tabla muestra las interfaces de placa base en Firepower 4100/9300 y la interfaz de enlace ascendente en Secure Firewall 3100:

| Platform | Número de módulos de seguridad admitidos | Interfaces de backplane/uplink | Interfaces de aplic asignadas |
|---|---|---|--|
| Firepower 4100 (excepto Firepower 4110/4112) | 1 | SM1: Ethernet1/9 Ethernet1/10 | Internal-Data0/0 Internal-Data0/1 |
| Firepower 4110/4112 | 1 | Ethernet1/9 | Internal-Data0/0 |
| Firepower 9300 | 3 | SM1: Ethernet1/9 Ethernet1/10 SM2: Ethernet1/11 Ethernet1/12 SM3: Ethernet1/13 Ethernet1/14 | Internal-Data0/0 Internal-Data0/1 Internal-Data0/0 Internal-Data0/1 Internal-Data0/0 Internal-Data0/1 |
| Firewall seguro 3100 | 1 | SM1: in_data_uplink1 | Internal-Data0/1 |

En el caso de 2 interfaces de placa base por módulo, el switch interno y las aplicaciones de los módulos realizan un equilibrio de carga de tráfico en las 2 interfaces.

- Módulo de seguridad, motor de seguridad o blade: el módulo en el que se instalan aplicaciones como FTD o ASA. Firepower 9300 admite hasta 3 módulos de seguridad.
- Interfaz de aplicación asignada: las aplicaciones, como FTD o ASA, asignan la placa base o las interfaces de enlace ascendente a interfaces internas. En otras palabras, las interfaces de placa base o de enlace ascendente son visibles como interfaces internas en las aplicaciones.
 Utilice el comando show interface detail para verificar las interfaces internas:

```
> 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 State is active
Interface Internal-Data0/1 "", is up, line protocol is up
Control Point Interface States:
Interface Internal-Data0/1 "", is up, line protocol is up
Control Point Interface States:
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
```

Descripción general de alto nivel de las operaciones internas del switch

Firepower 4100/9300

Para tomar una decisión de reenvío, el switch interno utiliza una etiqueta de interfaz VLAN, o etiqueta de puerto VLAN, y una etiqueta de red virtual (VN-tag).

El switch interno utiliza la etiqueta de VLAN de puerto para identificar una interfaz. El switch inserta la etiqueta de VLAN de puerto en cada paquete de ingreso que vino en las interfaces frontales. El sistema configura automáticamente la etiqueta VLAN y no se puede cambiar manualmente. El valor de la etiqueta se puede verificar en el shell de comandos **fxos**:

```
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
```

La etiqueta VN también es insertada por el switch interno y utilizada para reenviar los paquetes a la aplicación. El sistema lo configura automáticamente y no se puede cambiar manualmente.

La etiqueta del puerto VLAN y la etiqueta VN se comparten con la aplicación. La aplicación inserta las respectivas etiquetas VLAN de interfaz de salida y las etiquetas VN en cada paquete. Cuando

el switch interno recibe un paquete de la aplicación en las interfaces de la placa posterior, el switch lee la etiqueta VLAN de la interfaz de egreso y la etiqueta VN, identifica la aplicación y la interfaz de egreso, elimina la etiqueta VLAN del puerto y la etiqueta VN y reenvía el paquete a la red.

Firewall seguro 3100

Al igual que en Firepower 4100/9300, el switch interno utiliza la etiqueta de VLAN de puerto para identificar una interfaz.

La etiqueta del puerto VLAN se comparte con la aplicación. La aplicación inserta las respectivas etiquetas VLAN de interfaz de salida en cada paquete. Cuando el switch interno recibe un paquete de la aplicación en la interfaz de enlace ascendente, el switch lee la etiqueta VLAN de la interfaz de egreso, identifica la interfaz de egreso, elimina la etiqueta VLAN del puerto y reenvía el paquete a la red.

Flujo de paquetes y puntos de captura

Los firewalls Firepower 4100/9300 y Secure Firewall 3100 admiten capturas de paquetes en las interfaces del switch interno.

Esta figura muestra los puntos de captura de paquetes a lo largo de la trayectoria del paquete dentro del chasis y la aplicación:



Los puntos de captura son:

- 1. Punto de captura de entrada de la interfaz frontal del switch interno. Una interfaz frontal es cualquier interfaz conectada a los dispositivos pares, como los switches.
- 2. Punto de captura de ingreso de interfaz de plano de datos
- 3. Punto de captura de Snort
- 4. Punto de captura de salida de interfaz de plano de datos
- 5. Plano posterior interno del switch o punto de captura de entrada de enlace ascendente. Una placa base o una interfaz de enlace ascendente conecta el switch interno a la aplicación.

El switch interno sólo admite capturas de interfaz de ingreso. Es decir, solo se pueden capturar

los paquetes recibidos de la red o de la aplicación ASA/FTD. No se admiten capturas de paquetes de salida.

Configuración y verificación en Firepower 4100/9300

Las capturas internas del switch Firepower 4100/9300 se pueden configurar en Herramientas > Captura de paquetes en FCM o en captura de paquetes de alcance en FXOS CLI. Para obtener una descripción de las opciones de captura de paquetes, consulte la *Guía de configuración del administrador de chasis FXOS de Cisco Firepower 4100/9300* o la *Guía de configuración CLI de FXOS de Cisco Firepower 4100/9300*, capítulo Resolución de problemas, sección Captura de paquetes.

Estos escenarios abarcan casos prácticos comunes de capturas de switches internos Firepower 4100/9300.

Captura de paquetes en una interfaz física o de canal de puerto

Utilice FCM y CLI para configurar y verificar una captura de paquetes en la interfaz Ethernet1/2 o Portchannel1. En el caso de una interfaz de canal de puerto, asegúrese de seleccionar todas las interfaces de miembro físicas.

Topología, flujo de paquetes y puntos de captura



Configuración

FCM

Siga estos pasos en FCM para configurar una captura de paquetes en las interfaces Ethernet1/2 o Portchannel1:

1. Utilice Tools > Packet Capture > Capture Session para crear una nueva sesión de captura:

| 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. Seleccione la interfaz **Ethernet1/2**, proporcione el nombre de sesión y haga clic en **Save and Run** para activar la captura:

| Overview Interfaces Logical Devices Security Engine Platform Settings | | System Tools Help admin |
|---|--|--------------------------|
| Select an instance: ftd1 | | Save and Run Save Cancel |
| ftd1 | Session Name* Cap1 Selected Interfaces Ethernet1/2 | |
| Ethernet/2 | Buffer Size 256 MB v Snap length: 1518 Bytes | |
| Ethernet1/3 | Store Packets Overwrite Append | |
| Ethernet1/1 FTD Ethernet1/10 | Capture Filter Apply Filter Cepture All | |
| Ehenet1/5 (Portchannel1) | | |
| Ethernet1/4 (Portchannel1) | | |

3. En el caso de una interfaz de canal de puerto, seleccione todas las interfaces de miembro físicas, proporcione el nombre de sesión y haga clic en **Guardar y Ejecutar** para activar la captura:

| Overview Interfaces Logical Devices Security Engine Platform Settings | | | | | System Tools Help admin |
|---|---------------------|--------------------------|--------------|---------|-------------------------|
| Select an instance: ftd1 v | | | Save and Run | Save Ca | ncel |
| ftd1 | Session Name* | cap1 | | | |
| | Selected Interfaces | Ethernet1/5, Ethernet1/4 | | | |
| Ethernet1/2 | Buffer Size | 256 MB | | | |
| | Snap length: | 1518 Bytes | | | |
| Ethernet1/3 | Store Packets | Overwrite Append | | | |
| | | | | | |
| Ethernet1/1 | Capture Filter | Apply Filter Capture All | | | |
| Ethernet1/10 | | | | | |
| Ethernet1/5 (Butchannet) | | | | | |
| | | | | | |
| Ethernet1/4 (Portchannel1) | | | | | |
| | | | | | |
| | | | | | |

CLI FXOS

Siga estos pasos en la CLI de FXOS para configurar una captura de paquetes en las interfaces Ethernet1/2 o Portchannel1:

1. Identifique el tipo de aplicación y el identificador:

firepower# scope ssa firepower /ssa # show app-instance Admin State Oper State Running Version Startup Version App Name Identifier Slot ID Deploy Type Turbo Mode Profile Name Cluster State Cluster Role ______ _____ _____ __ ___ Enabled 7.2.0.82 ftd ftd1 1 Online 7.2.0.82 Not Applicable None Native No

2. En el caso de una interfaz de canal de puerto, identifique sus interfaces miembro:

| 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. Crear una sesión de captura: | |

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* # up
firepower /packet-capture/session* # enable
firepower /packet-capture/session* # commit
firepower /packet-capture/session #

Para las interfaces de canal de puerto, se configura una captura independiente para cada interfaz miembro:

```
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 #
Verificación
```

FCM

Verifique el Nombre de la Interfaz, asegúrese de que el Estado Operacional esté activo y que el

Tamaño del Archivo (en bytes) aumente:

| | Overview | Interfaces | Logical Devices | Security Engine | Platform Set | ttings | | | | | System | Tools | Help | admin |
|---|--------------|--------------|-----------------|-----------------|---------------|-----------------|--------------------------|----------|--------------|--------------|---------------|---------|------------|-------|
| Γ | | | | | | | | | | | | | | |
| 1 | Capture Ses | sion Fiter I | ist | | | | | | | | | | | |
| | | | | | | | | | C Refresh Ca | ture Session | Delete All Se | essions | | |
| ľ | • | cap1 | Drop Coun | t: 0 | Operational S | State: up | Buffer Size: 256 M | в | Snap Length: | 518 Bytes | | | 4 5 | |
| | Interface Na | ime | Filter | | File | Size (in bytes) | File Name | Device N | lame | | | | | |
| | Ethernet1/2 | | None | | 2863 | 32 | cap1-ethernet-1-2-0.pcap | ftd1 | | \pm | | | | |

Portchannel1 con interfaces miembro Ethernet1/4 y Ethernet1/5:

| Overview Interfaces Li | Overview Interfaces Logical Devices Security Engine Platform Settings System Tools Help admin | | | | | | | | | | |
|-----------------------------|---|-----------------------|--------------------------|-------------|---------------------------|---------------------|--|--|--|--|--|
| | | | | | | | | | | | |
| Capture Session Filter List | | | | | | | | | | | |
| | | | | | C Refresh Capture Session | Delete All Sessions | | | | | |
| a 🔳 cap1 | Drop Count: 0 | Operational State: up | Buffer Size: 256 MB | | Snap Length: 1518 Bytes | | | | | | |
| Interface Name | Filter | File Size (in bytes) | File Name | Device Name | | | | | | | |
| Ethernet1/S | None | 160 | cap1-ethernet-1-5-0.pcap | ftd1 | 4 | | | | | | |
| Ethernet1/4 | None | 85000 | cap1-ethernet-1-4-0.pcap | ftd1 | ⊻ | | | | | | |

CLI FXOS

Verifique los detalles de la captura en scope packet-capture:

```
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
Canal de puerto 1 con interfaces miembro Ethernet1/4 y 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
```

Recopilar archivos de captura

Siga los pasos de la sección Recopilación de archivos de captura de switch internos de Firepower 4100/9300.

Capturar análisis de archivos

Utilice una aplicación de lector de archivos de captura de paquetes para abrir el archivo de captura para Ethernet1/2. Seleccione el primer paquete y compruebe los puntos clave:

- 1. Solo se capturan los paquetes de solicitud de eco ICMP. Cada paquete se captura y se muestra 2 veces.
- 2. El encabezado del paquete original no tiene la etiqueta VLAN.
- 3. El switch interno inserta la etiqueta adicional del puerto VLAN **102** que identifica la interfaz de ingreso Ethernet1/2.
- 4. El switch interno inserta una etiqueta VN adicional.

| No. Time | Source | Destination | Protocol | Length | PD | IP TTL Info | |
|------------------------------------|-------------------|---------------------|--------------|--------------|----------------|----------------------|--|
| 1 2022-07-13 06:23:58.2850809 | 0 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x9dec (40428) | 64 Echo (ping) reque | st id=0x001a, seq=7/1792, ttl=64 (no response found!) |
| 2 2022-07-13 06:23:58.2850828 | 8 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9dec (40428) | 64 Echo (ping) reque | st id=0x001a, seq=7/1792, ttl=64 (no response found!) |
| 3 2022-07-13 06:23:59.3090488 | 6 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x9ed0 (40656) | 64 Echo (ping) reque | st id=0x001a, seq=8/2048, ttl=64 (no response found!) |
| 4 2022-07-13 06:23:59.3091937 | 1 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9ed0 (40656) | 64 Echo (ping) reque | st id=0x001a, seq=8/2048, ttl=64 (no response found!) |
| 5 2022-07-13 06:24:00.3330541 | 0 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x9f20 (40736) | 64 Echo (ping) reque | st id=0x001a, seq=9/2304, ttl=64 (no response found!) |
| 6 2022-07-13 06:24:00.3330560 | 4 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9f20 (40736) | 64 Echo (ping) reque | st id=0x001a, seq=9/2304, ttl=64 (no response found!) |
| 7 2022-07-13 06:24:01.3571735 | 0 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x9f2d (40749) | 64 Echo (ping) reque | st id=0x001a, seq=10/2560, ttl=64 (no response found!) |
| 8 2022-07-13 06:24:01.3571747 | 8 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9f2d (40749) | 64 Echo (ping) reque | st id=0x001a, seq=10/2560, ttl=64 (no response found!) |
| 9 2022-07-13 06:24:02.3810737 | 1 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x9f88 (40840) | 64 Echo (ping) reque | st id=0x001a, seq=11/2816, ttl=64 (no response found!) |
| 10 2022-07-13 06:24:02.3810749 | 9 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9f88 (40840) | 64 Echo (ping) reque | st id=0x001a, seq=11/2816, ttl=64 (no response found!) |
| 11 2022-07-13 06:24:03.4051990 | 1 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xa077 (41079) | 64 Echo (ping) reque | st id=0x001a, seq=12/3072, ttl=64 (no response found!) |
| 12 2022-07-13 06:24:03.4052002 | 1 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xa077 (41079) | 64 Echo (ping) reque | st id=0x001a, seq=12/3072, ttl=64 (no response found!) |
| 13 2022-07-13 06:24:04.4291556 | 33 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xa10f (41231) | 64 Echo (ping) reque | st id=0x001a, seq=13/3328, ttl=64 (no response found!) |
| 14 2022-07-13 06:24:04.4291568 | 1 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xa10f (41231) | 64 Echo (ping) reque | st id=0x001a, seq=13/3328, ttl=64 (no response found!) |
| 15 2022-07-13 06:24:05.4531566 | 2 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xa16a (41322) | 64 Echo (ping) reque | st id=0x001a, seq=14/3584, ttl=64 (no response found!) |
| 16 2022-07-13 06:24:05.4531580 | 2 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xa16a (41322) | 64 Echo (ping) reque | st id=0x001a, seq=14/3584, ttl=64 (no response found!) |
| 17 2022-07-13 06:24:06.4771276 | 37 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xa1e9 (41449) | 64 Echo (ping) reque | st id=0x001a, seq=15/3840, ttl=64 (no response found!) |
| 18 2022-07-13 06:24:06.4771298 | 9 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xa1e9 (41449) | 64 Echo (ping) reque | st id=0x001a, seq=15/3840, ttl=64 (no response found!) |
| 19 2022-07-13 06:24:07.5012913 | 4 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xa1f6 (41462) | 64 Echo (ping) reque | st id=0x001a, seq=16/4096, ttl=64 (no response found!) |
| 20 2022-07-13 06:24:07.5012930 | 1 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xa1f6 (41462) | 64 Echo (ping) reque | st id=0x001a, seq=16/4096, ttl=64 (no response found!) |
| 21 2022-07-13 06:24:08.5250899 | 6 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xa257 (41559) | 64 Echo (ping) reque | st id=0x001a, seq=17/4352, ttl=64 (no response found!) |
| 22 2022-07-13 06:24:08.5250920 | 8 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xa257 (41559) | 64 Echo (ping) reque | st id=0x001a, seq=17/4352, ttl=64 (no response found!) |
| 23 2022-07-13 06:24:09.5492365 | 0 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xa2a9 (41641) | 64 Echo (ping) reque | st id=0x001a, seq=18/4608, ttl=64 (no response found!) |
| 24 2022-07-13 06:24:09.5492385 | 4 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xa2a9 (41641) | 64 Echo (ping) reque | st id=0x001a, seq=18/4608, ttl=64 (no response found!) |
| 25 2022-07-13 06:24:10.5731101 | 6 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xa345 (41797) | 64 Echo (ping) reque | st id=0x001a, seq=19/4864, ttl=64 (no response found!) |
| 26 2022-07-13 06:24:10.5731125 | 4 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xa345 (41797) | 64 Echo (ping) reque | st id=0x001a, seq=19/4864, ttl=64 (no response found!) |
| 27 2022-07-13 06:24:11.5970860 | 7 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xa349 (41801) | 64 Echo (ping) reque | st id=0x001a, seq=20/5120, ttl=64 (no response found!) |
| 28 2022-07-13 06:24:11.5970881 | 0 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xa349 (41801) | 64 Echo (ping) reque | st id=0x001a, seq=20/5120, ttl=64 (no response found!) |
| 29 2022-07-13 06:24:12.6210610 | 2 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xa3dc (41948) | 64 Echo (ping) reque | st id=0x001a, seq=21/5376, ttl=64 (no response found!) |
| ¢ | | | | | | | |
| > Frame 1: 108 bytes on wire (864 | bits), 108 bytes | captured (864 bits) | on interfac | ce capture u | 0 1, id 0 | | 0000 58 97 bd b9 77 0e 00 50 56 9d e8 be 89 26 80 0a X ··· w · P V ··· & · |
| > Ethernet II, Src: VMware 9d:e8: | e (00:50:56:9d:e8 | tbe), Dst: Cisco b9 | :77:0e (58:9 | 97:bd:b9:77: | 80) | | 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 | = Dire | ction: From Bridge | | | | | 0030 00 1a 00 07 f4 64 ce 62 00 00 00 00 20 a2 07 00d.b |
| .0 | = Poin | ter: vif id | _ | | | | 0840 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b |
| | = Dest | ination: 10 | _ | | | | 0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ···· !"# \$%&'()"+ |
| 0 | = Loop | ed: No | | | | | 0060 2c 2d 2e 2t 30 31 32 33 34 35 36 37 ,/0123 4567 |
| | = Rese | rved: 0 | 4 | | | | |
| 00 | = Vers | ion: 0 | _ | | | | |
| 0000 | 0000 0000 = Sour | ce: 0 | _ | | | | |
| Type: 802.10 Virtual LAN (0x8 | (60) | | | | | | |
| 802.10 Virtual LAN, PRI: 0, DEI | 0, ID: 102 | | | | | | |
| 000 = Priorit | : Best Effort (d | efault) (0) | | | | | |
| 0 = DEI: In | ligible | | 2 | | | | |
| 0000 0110 0110 = ID: 102 | 0 | | 2 | | | | |
| Type: IPv4 (0x0800) | | | | | | | |
| > Internet Protocol Version 4. Sre | : 192.0.2.100. Ds | t: 198.51.100.100 | | | | | |
| > Internet Control Message Protoco | 1 | | 2 | | | | |
| | | | | | | | |
| | | | | | | | |

Seleccione el segundo paquete y verifique los puntos clave:

- 1. Solo se capturan los paquetes de solicitud de eco ICMP. Cada paquete se captura y se muestra 2 veces.
- 2. El encabezado del paquete original no tiene la etiqueta VLAN.
- 3. El switch interno inserta la etiqueta adicional del puerto VLAN **102** que identifica la interfaz de ingreso Ethernet1/2.

| No. | Time | Source | Destination | Protocol | Length | PD | IP TTL Info | |
|------|--|-------------------------|---------------------|---------------|-----------|----------------|-----------------------|---|
| F | 1 2022-07-13 06:23:58.285080930 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x9dec (40428) | 64 Echo (ping) reques | id=0x001a, seq=7/1792, ttl=64 (no response found!) |
| | 2 2022-07-13 06:23:58.285082858 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9dec (40428) | 64 Echo (ping) reques | id=0x001a, seq=7/1792, ttl=64 (no response found!) |
| | 3 2022-07-13 06:23:59.309048886 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x9ed0 (40656) | 64 Echo (ping) reques | id=0x001a, seq=8/2048, ttl=64 (no response found!) |
| | 4 2022-07-13 06:23:59.309193731 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9ed0 (40656) | 64 Echo (ping) reques | t id=0x001a, seq=8/2048, ttl=64 (no response found!) |
| | 5 2022-07-13 06:24:00.333054190 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x9f20 (40736) | 64 Echo (ping) reques | t id=0x001a, seq=9/2304, ttl=64 (no response found!) |
| | 6 2022-07-13 06:24:00.333056014 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9f20 (40736) | 64 Echo (ping) reques | t id=0x001a, seq=9/2304, ttl=64 (no response found!) |
| | 7 2022-07-13 06:24:01.357173530 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x9f2d (40749) | 64 Echo (ping) reques | t id=0x001a, seq=10/2560, ttl=64 (no response found!) |
| | 8 2022-07-13 06:24:01.357174708 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9f2d (40749) | 64 Echo (ping) reques | t id=0x001a, seq=10/2560, ttl=64 (no response found!) |
| | 9 2022-07-13 06:24:02.381073741 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x9f88 (40840) | 64 Echo (ping) reques | id=0x001a, seq=11/2816, ttl=64 (no response found!) |
| | 10 2022-07-13 06:24:02.381074999 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9f88 (40840) | 64 Echo (ping) reques | t id=0x001a, seq=11/2816, ttl=64 (no response found!) |
| | 11 2022-07-13 06:24:03.405199041 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xa077 (41079) | 64 Echo (ping) reques | t id=0x001a, seq=12/3072, ttl=64 (no response found!) |
| | 12 2022-07-13 06:24:03.405200261 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xa077 (41079) | 64 Echo (ping) reques | t id=0x001a, seq=12/3072, ttl=64 (no response found!) |
| | 13 2022-07-13 06:24:04.429155683 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xa10f (41231) | 64 Echo (ping) reques | t id=0x001a, seq=13/3328, ttl=64 (no response found!) |
| | 14 2022-07-13 06:24:04.429156831 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xa10f (41231) | 64 Echo (ping) reques | t id=0x001a, seq=13/3328, ttl=64 (no response found!) |
| | 15 2022-07-13 06:24:05.453156612 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xa16a (41322) | 64 Echo (ping) reques | id=0x001a, seq=14/3584, ttl=64 (no response found!) |
| | 16 2022-07-13 06:24:05.453158052 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xa16a (41322) | 64 Echo (ping) reques | t id=0x001a, seq=14/3584, ttl=64 (no response found!) |
| | 17 2022-07-13 06:24:06.477127687 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xa1e9 (41449) | 64 Echo (ping) reques | t id=0x001a, seq=15/3840, ttl=64 (no response found!) |
| | 18 2022-07-13 06:24:06.477129899 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xa1e9 (41449) | 64 Echo (ping) reques | t id=0x001a, seq=15/3840, ttl=64 (no response found!) |
| | 19 2022-07-13 06:24:07.501291314 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xa1f6 (41462) | 64 Echo (ping) reques | t id=0x001a, seq=16/4096, ttl=64 (no response found!) |
| | 20 2022-07-13 06:24:07.501293041 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xa1f6 (41462) | 64 Echo (ping) reques | t id=0x001a, seq=16/4096, ttl=64 (no response found!) |
| | 21 2022-07-13 06:24:08.525089956 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xa257 (41559) | 64 Echo (ping) reques | id=0x001a, seq=17/4352, ttl=64 (no response found!) |
| | 22 2022-07-13 06:24:08.525092088 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xa257 (41559) | 64 Echo (ping) reques | id=0x001a, seq=17/4352, ttl=64 (no response found!) |
| | 23 2022-07-13 06:24:09.549236500 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xa2a9 (41641) | 64 Echo (ping) reques | t id=0x001a, seq=18/4608, ttl=64 (no response found!) |
| | 24 2022-07-13 06:24:09.549238564 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xa2a9 (41641) | 64 Echo (ping) reques | t id=0x001a, seq=18/4608, ttl=64 (no response found!) |
| | 25 2022-07-13 06:24:10.573110146 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xa345 (41797) | 64 Echo (ping) reques | t id=0x001a, seq=19/4864, ttl=64 (no response found!) |
| | 26 2022-07-13 06:24:10.573112504 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xa345 (41797) | 64 Echo (ping) reques | t id=0x001a, seq=19/4864, ttl=64 (no response found!) |
| | 27 2022-07-13 06:24:11.597086027 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xa349 (41801) | 64 Echo (ping) reques | t id=0x001a, seq=20/5120, ttl=64 (no response found!) |
| | 28 2022-07-13 06:24:11.597088170 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xa349 (41801) | 64 Echo (ping) reques | id=0x001a, seq=20/5120, ttl=64 (no response found!) |
| | 29 2022-07-13 06:24:12.621061022 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xa3dc (41948) | 64 Echo (ping) reques | t id=0x001a, seq=21/5376, ttl=64 (no response found!) |
| < | | | | | | | | |
| 5 E | are 3: 103 butes on wine (016 bit | c) 102 bytes c | antured (016 hits) | on interface | conture u | 0.1. id 0 | | 0000 58 07 hd h0 77 00 00 50 56 0d o8 ho 81 00 00 66 Y |
| | thannat II. Spc: Whoma Odiagiha (| 00:50:56:0d:00: | ha) Det: Circo ba | 77:00 (59:07: | bd:b0:77: | 0_1, 10 0 | | 0010 08 00 45 00 00 54 9d ec 40 00 40 01 af c0 c0 00E.T. 0.0. |
| 1 9 | A2 10 Victual LAN DRT: 0 DET: 0 | ID: 102 | bej, bsc. cisco by. | 11.00 (30.97. | 00.09.77. | ue) | | 0020 02 64 c6 33 64 64 08 00 4e a2 00 1a 00 07 f4 64 ·d·3dd·· N·····d |
| . 01 | and - Priority: F | hest Effort (de | fault) (0) | | | | | 0030 ce 62 00 00 00 00 20 a2 07 00 00 00 00 00 10 11 .b |
| | a - DET: Toolig | sest errore (de | (aurc) (0) | 2 | | | | 0040 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 |
| | 0000 0110 0110 - 10: 102 | siore | | 2 | | | | 0050 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 "#\$%&'() *+,/01 |
| | Type: TPv4 (0v0000) | | | | | | | 0060 32 33 34 35 36 37 234567 |
| T | aternet Protocol Version 4. Src: 1 | 92.0.2.100 Dst | 198.51.100.100 | - | | | | |
| | nternet Control Message Protocol | | . 19019111001100 | 2 | | | | |
| 12 | ternet control heaven for the same from the same | | | - | | | | |

Abra los archivos de captura para las interfaces de miembro Portchannel1. Seleccione el primer paquete y verifique los puntos clave:

1. Solo se capturan los paquetes de solicitud de eco ICMP. Cada paquete se captura y se muestra 2 veces.

- 2. El encabezado del paquete original no tiene la etiqueta VLAN.
- 3. El switch interno inserta una etiqueta de VLAN de puerto adicional **1001** que identifica la interfaz de ingreso Portchannel1.
- 4. El switch interno inserta una etiqueta VN adicional.

| _ | | | | | | | | | | | | _ |
|----------|-------------------------------------|------------------|---------------------|-------------|-----------------|---------|---------|-------------------------|---------------|----------------------------|-----------|---|
| No. | Time | Source | Destination | Protocol | Length | IP ID | | IP TTL Info | | | | ^ |
| F | 1 2022-08-05 23:07:31.865872877 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | Øx322e | (12846) | 64 Echo (ping) reques | t id=0x002d, | seq=245/62720, ttl | =64 (nc | |
| | 2 2022-08-05 23:07:31.865875131 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | Øx322e | (12846) | 64 Echo (ping) reques | t 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) reques | t 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) reques | t 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) reques | t 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) reques | t 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) reques | t id=0x002d, | seq=248/63488, ttl | =64 (nc | |
| | 8 2022-08-05 23:07:34.883051649 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | Øx3373 | (13171) | 64 Echo (ping) reques | t 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) reques | t 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) reques | t 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) reques | t 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) reques | t 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) reques | t 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) reques | t 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) reques | t 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) reques | t 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) reques | t 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) reques | t 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) reques | t id=0x002d, | seq=254/65024, ttl | =64 (nc | ~ |
| < | | | | | | | | | | | > | |
| > Fr | ame 1: 108 bytes on wire (864 bits) | , 108 bytes capt | tured (864 bits) or | n interface | e capture u0 3, | i 0000 | a2 76 | f2 00 00 25 00 50 56 9d | 8 be 89 26 80 | 54 · v · · · % · P V · · · | · · & · T | |
| > E1 | hernet II, Src: VMware_9d:e8:be (00 | :50:56:9d:e8:be) |), Dst: a2:76:f2:00 | 0:00:25 (a2 | 2:76:f2:00:00:2 | 5) 0010 | 00 00 | 81 00 03 e9 08 00 45 00 | 0 54 32 2e 40 | 00 ····· E··1 | 12.0 | |
| VI | I-Tag | | | | | 0020 | 40 01 | 1b 7f c0 00 02 64 c6 33 | 4 64 08 00 1e | d6 @d .3dd | db | |
| | 1 | = Directio | n: From Bridge | | | 0030 | 00 2d | 00 f5 a6 a2 ed 62 00 00 | 0 00 7a 2f 0b | 00 ·-···b ···· | ·z/·· | |
| | .0 | = Pointer: | vif_id | | | 0040 | 00 00 | 00 00 10 11 12 13 14 15 | 6 17 18 19 1a | 1b | | |
| | 00 0000 0101 0100 | = Destinat | ion: 84 | | | 0050 | 1c 1d | 1e 1f 20 21 22 23 24 25 | 6 27 28 29 2a | 20 1"# \$%& | ·()*+ | |
| | 0 | = Looped: | No 4 | | | 0000 | 20 20 | 2e 2T 30 31 32 33 34 35 | 6 37 | ,/0123 456/ | / | |
| | 0 | = Reserved | : 0 | | | | | | | | | |
| | 00 | = Version: | 0 | | | | | | | | | |
| | 0000 0000 | 0000 = Source: | 0 | | | | | | | | | |
| | Type: 802.10 Virtual LAN (0x8100) | | | | | | | | | | | |
| 8 | 2.10 Virtual LAN, PRI: 0, DEI: 0, I | D: 1001 | | | | | | | | | | |
| | 000 Bes | st Effort (defau | lt) (0) | | | | | | | | | |
| | 0 = DEI: Ineligit | ble | | | | | | | | | | |
| | 0011 1110 1001 = ID: 1001 | | | | | | | | | | | |
| | Type: IPv4 (0x0800) | | | | | | | | | | | |
| I | ternet Protocol Version 4, Src: 192 | .0.2.100, Dst: 1 | 198.51.100.100 👝 | | | | | | | | | |
| I | ternet Control Message Protocol | | 2 | | | | | | | | | |
| | | | | | | | | | | | | |

Seleccione el segundo paquete y verifique los puntos clave:

- 1. Solo se capturan los paquetes de solicitud de eco ICMP. Cada paquete se captura y se muestra 2 veces.
- 2. El encabezado del paquete original no tiene la etiqueta VLAN.
- 3. El switch interno inserta una etiqueta de VLAN de puerto adicional **1001** que identifica la interfaz de ingreso Portchannel1.

| No | p. Time | Source | Destination | Protocol | Length | PD | | Ib. | TTL Info | | | | | | | ^ |
|----|---------------------------------------|-------------------|---------------------|---------------|------------|----------|---------|-------|----------|--------|----------|-------------|---------------|----------|-----|---|
| C | 1 2022-08-05 23:07:31.865872877 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x322e | (12846) | | 64 Echo | (ping) | request | id=0x002d, | seq=245/62720 | , ttl=64 | (nc | |
| | 2 2022-08-05 23:07:31.865875131 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | Øx322e | (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 cap | ture u0 3, | i 0000 | a2 76 | f2 06 | 00 25 | 90 50 | 56 9d e8 | be 81 00 03 | e9 ·v···%·F | 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 06 | 00 54 | 32 2e | 40 00 40 | 01 1b 7f ce | 000 ··E··T2. | @·@····· | | |
| 4 | 802.10 Virtual LAN, PRI: 0, DEI: 0, 1 | ID: 1001 | | | | 0020 | 02 64 | C6 33 | 64 64 | 98 99 | 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 | 7a 2f | 0b 00 00 | 00 00 00 10 | 11 ·b····z/ | | 1 | |
| ш | 0 = DEI: Ineligi | ble | 3 | | | 0040 | 12 13 | 14 15 | 6 16 17 | 18 19 | 1a 1b 1c | 1d 1e 1f 20 | 21 | | 1 | |
| ш | 0011 1110 1001 = ID: 1001 | | | | | 0050 | 22 23 | 24 25 | 26 27 | 28 29 | 2a 2b 2c | 2d 2e 2† 30 | 31 "#\$%&"() | *+,/01 | i. | |
| ш | Type: IPv4 (0x0800) | | | | | 0000 | 32 33 | 34 33 | 30 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 | | | | | | | | | | | | | |
| н | | | | | | | | | | | | | | | | |

Explicación

Cuando se configura una captura de paquetes en una interfaz frontal, el switch captura simultáneamente cada paquete dos veces:

- Después de la inserción de la etiqueta de VLAN de puerto.
- Después de la inserción de la etiqueta VN.

En el orden de las operaciones, la etiqueta VN se inserta en una etapa posterior a la inserción de la etiqueta VLAN del puerto. Sin embargo, en el archivo de captura, el paquete con la etiqueta VN se muestra antes que el paquete con la etiqueta de puerto VLAN.

Esta tabla resume la tarea:

| Tarea | Punto de captura | VLAN de puerto interno en paquetes capturados | Dirección: | Tráfico capturado |
|--|------------------------------------|---|-----------------|---|
| Configurar y verificar una captura de paquetes en la interfaz Ethernet1/2 | Ethernet1/ 2 | 102 | Solo entrada | Solicitudes de eco ICMP del hos 192.0.2.100 al host 198.51.100.1 |
| Configure y verifique una captura de paquetes en la interfaz Portchannel1 con las interfaces miembro Ethernet1/4 y Ethernet1/5 | Ethernet1/ 4 Ethernet1/ 5 | 1001 | Solo entrada | Solicitudes de eco ICMP del hos 192.0.2.100 al host 198.51.100.1 |

Capturas de paquetes en interfaces de backplane

Utilice FCM y CLI para configurar y verificar una captura de paquetes en interfaces de placa base.

Topología, flujo de paquetes y puntos de captura



Configuración

FCM

Siga estos pasos en FCM para configurar capturas de paquetes en interfaces de backplane:

1. Utilice Tools > Packet Capture > Capture Session para crear una nueva sesión de captura:

| Overview Interfaces Logical Devices Security Engine Platform Settings | I Tools Help admin | |
|---|--------------------|----------------------|
| | Packet Capture | Troubleshooting Logs |
| Capture Session Filter List | | |
| C Refresh | Capture Session De | ete All Sessions |
| No Session available | | |

2. Para capturar paquetes en todas las interfaces de backplane, seleccione la aplicación y, a continuación, Todos los puertos de backplane en la lista desplegable Capturar en. También puede elegir la interfaz de backplane específica. En este caso, están disponibles las interfaces de placa base Ethernet1/9 y Ethernet1/10. Proporcione el Nombre de la Sesión y haga clic en Guardar y Ejecutar para activar la captura:

| Overview Interfaces Logical Devices Security Engine I | Platform Settings | | System loois Help admin |
|---|----------------------------------|---|--|
| Select an instance: ftd1 v | | | Save and Run Save Cancel |
| ftd1 | | Session Name* | capi |
| Ethemet1/2 | | Selected Interfaces Buffer Size | None 256 MB V |
| | | Snap length: Store Packets Capture On | 1518 system Overwrite Append Al Badobine Ports |
| Ethernet1/3 | ETD Ethernet1/9, Ethernet1/10 | Capture Filter | ftd Ethernet1/9 Ethernet1/10 Al Backplane Ports |
| Ethernet1/1 | | | |
| 1 | | | |

CLI FXOS

Siga estos pasos en la CLI de FXOS para configurar las capturas de paquetes en las interfaces de la placa posterior:

1. Identifique el tipo de aplicación y el identificador:

| 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 | | | | | | | | | | | |
|---|-------------------|---------------------|---------------------|-------------------------------|---------------|----------|--|--|--|--|--|
| ftd Native | ftd1 No | 1 | Enabled Not Appl | Online icable None | - 7.2.0.82 | 7.2.0.82 | | | | | |
| 2. Crea | ir una sesió | n de captura | a: | | | | | | | | |
| firepower# | scope pack | et-capture | | | | | | | | | |
| firepower | /packet-cap | ture # creat | e session c | ap1 | | | | | | | |
| firepower | /packet-cap | ture/sessior | 1* # create | phy-port Eth1/9 | | | | | | | |
| firepower | /packet-cap | ture/sessior | /phy-port* | # set app ftd | | | | | | | |
| firepower | /packet-cap | ture/sessior | /phy-port* | <pre># set app-identif;</pre> | ier ftd1 | | | | | | |
| firepower | /packet-cap | ture/sessior | /phy-port* | # up | | | | | | | |
| firepower | /packet-cap | ture/sessior | n* # create | phy-port Eth1/10 | | | | | | | |
| firepower | /packet-cap | ture/sessior | n/phy-port* | # set app ftd | | | | | | | |

```
firepower /packet-capture/session/phy-port* # set app-identifier ftd1
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # enable
firepower /packet-capture/session* # commit
firepower /packet-capture/session #
Verificación
```

FCM

Verifique el **Nombre de la Interfaz**, asegúrese de que el **Estado Operacional** esté activo y que el **Tamaño del Archivo (en bytes)** aumente:

| Overview | Interfaces | Logical Devices | Security Engine | Platform Settings | | | | System Tools Help admin |
|------------------------|-------------|-----------------|-----------------|-----------------------|---------------------|-------------------------|---------------------------|-------------------------|
| | | | | | | | | |
| Capture Ses | ssion Fiter | List | | | | | | |
| | | | | | | | C Refresh Capture Session | Delete Al Sessions |
| 🔺 💽 cap1 Drop Count: 0 | | | it: 0 | Operational State: up | Buffer Siz | Snap Length: 1518 Bytes | | |
| Interface N | ame | Filter | | File Size (in bytes) | File Name | Device N | lame | |
| Ethernet1/10 | D | None | | 194352 | cap1-ethernet-1-10 | -0.pcap ftd1 | 1 | |
| Ethernet1/9 | | None | | 286368 | cap1-ethernet-1-9-0 | 0.pcap ftd1 | | |
| <u> </u> | | | | | - | | | |

CLI FXOS

Verifique los detalles de la captura en scope packet-capture:

```
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
```

Siga los pasos de la sección Recopilación de archivos de captura de switch internos de Firepower 4100/9300.

Capturar análisis de archivos

Utilice una aplicación de lector de archivos de captura de paquetes para abrir los archivos de captura. En el caso de más de una interfaz de backplane, asegúrese de abrir todos los archivos de captura para cada interfaz de backplane. En este caso, los paquetes se capturan en la interfaz Ethernet1/9 de la placa de interconexiones.

Seleccione el primer y el segundo paquete y verifique los puntos clave:

- 1. Cada paquete de solicitud de eco ICMP se captura y se muestra 2 veces.
- 2. El encabezado del paquete original no tiene la etiqueta VLAN.
- 3. El switch interno inserta la etiqueta adicional del puerto VLAN **103** que identifica la interfaz de salida Ethernet1/3.
- 4. El switch interno inserta una etiqueta VN adicional.

| No. | Time | See | urce 0 | Destination | Protocol | Length | PD | | IP TTL Info | | | | | | | | |
|-----|--------------------|----------------------|------------------|--------------------|----------------|-----------|----------|--------|-------------|--------|---------|------------------|-------------|-----------|-----------|-------------------|-------------------|
| | 1 2022-07-14 20: | 20:36.513854256 19 | 2.0.2.100 1 | 198.51.100.100 | ICMP | 108 | 0x5990 (| 22928) | 64 Echo | (ping) | request | id=0x0001, | seq=15/38 | 10, ttl=6 | 54 (no r | response found!) | |
| | 2 2022-07-14 20: | 20:36.513857289 19 | 02.0.2.100 1 | 198.51.100.100 | ICMP | 108 | 0x5990 (| 22928) | 64 Echo | (ping) | request | id=0x0001, | seq=15/384 | 10, ttl=6 | 64 (rep] | ly in 3) | |
| | 3 2022-07-14 20: | 20:36.514117394 19 | 8.51.100.100 1 | 192.0.2.100 | ICMP | 108 | Øxcc2c (| 52268) | 64 Echo | (ping) | reply | id=0x0001, | seq=15/384 | 10, ttl=6 | i4 (requ | uest in 2) | |
| | 4 2022-07-14 20: | 20:36.514119312 19 | 8.51.100.100 1 | 192.0.2.100 | ICMP | 108 | Øxcc2c (| 52268) | 64 Echo | (ping) | reply | id=0x0001, | seq=15/38/ | 0, ttl=6 | 54 | | |
| | 5 2022-07-14 20: | 20:37.537723822 19 | 2.0.2.100 1 | 198.51.100.100 | ICMP | 108 | 0x5a00 (| 23848) | 64 Echo | (ping) | request | id=0x0001, | seq=16/40 | 6, ttl=6 | i4 (no r | response found!) | |
| | 6 2022-07-14 20: | 20:37.537726588 19 | 2.0.2.100 1 | 198.51.100.100 | ICMP | 108 | 0x5a00 (| 23040) | 64 Echo | (ping) | request | id=0x0001, | seq=16/40 | 6, ttl=6 | i4 (rep) | ly in 7) | |
| | 7 2022-07-14 20: | 20:37.538046165 19 | 8.51.100.100 1 | 92.0.2.100 | ICMP | 108 | Øxcc9b (| 52379) | 64 Echo | (ping) | reply | id=0x0001 | seg=16/40 | 6, ttl=6 | 4 (reg | uest in 6) | |
| | 8 2022-07-14 20: | 20:37.538048311 19 | 8.51.100.100 1 | 92.0.2.100 | ICMP | 108 | exceph (| 52379) | 64 Echo | (ping) | reply | id=0x0001 | seg=16/40 | 6. ttl=f | 14 | | |
| | 9 2022-07-14 20: | 20:38.561776064 19 | 2.0.2.100 1 | 98.51.100.100 | TCMP | 108 | exsah7 (| 23223) | 64 Echo | (ning) | request | id=0x0001 | seg=17/43 | 2. ttl=f | 4 (no r | response found!) | |
| | 10 2022-07-14 201 | 20:30 561770310 10 | 2 0 2 100 1 | 09 51 100 100 | TCMP | 100 | OvSab7 (| 22222) | 64 Echo | (ping) | request | id=0x0001 | seq=17/43 | 2 ++1-4 | A (con] | ly in 11) | |
| | 11 2022-07-14 201 | 20.30.501770310 19 | 0 51 100 100 1 | 02 0 2 100 | TCMP | 100 | Overet (| 52420) | 64 Echo | (ping) | canly | id-0x0001 | seq=17/43 | 2 ++1-4 | A (read | upst in 10) | |
| | 12 2022-07-14 201 | 20.30.502040200 19 | 0 51 100 100 1 | 192.0.2.100 | TCMD | 100 | Oxecc4 (| 52420) | 64 Echo | (ping) | cooly | id-0x0001 | seq=17/43 | 2, 111-0 | in (requ | uest in 10) | |
| | 12 2022-07-14 20. | 20.30.502050555 19 | 0.01.100.100 1 | 192.0.2.100 | TCHP | 100 | Outher (| 22420) | 64 Echo | (ping) | repry | id-0x0001 | seq=17/45 | 12, ttl=0 | 4 / 100 1 | assesses foundly | |
| | 15 2022-07-14 20: | 20:39.383677643 19 | 2.0.2.100 1 | 198.51.100.100 | TCHP | 100 | Outhac (| 23300) | 64 Echo | (ping) | request | id-0x0001, | Seq=10/400 | 0, ttl-t | | response roundi) | |
| | 14 2022-07-14 20: | 20:39.585678455 19 | 2.0.2.100 1 | 198.51.100.100 | ICMP | 108 | 0X5046 (| 23366) | 64 Echo | (ping) | request | 1d=0x0001, | seq=18/464 | 18, ttl=e | sa (rep. | 1y 1n 15) | |
| | 15 2022-07-14 20: | 20:39.585936554 19 | 8.51.100.100 1 | 192.0.2.100 | ICMP | 108 | excasa (| 52621) | 64 Echo | (ping) | reply | 1d=0x0001, | seq=18/464 | 18, ttl=6 | 64 (requ | uest in 14) | |
| | 16 2022-07-14 20: | 20:39.585937900 19 | 8.51.100.100 1 | 192.0.2.100 | ICMP | 108 | 0xcd8d (| 52621) | 64 Echo | (ping) | reply | id=0x0001, | seq=18/46 | 18, ttl=6 | 54 | | |
| | 17 2022-07-14 20: | 20:40.609804804 19 | 02.0.2.100 1 | 198.51.100.100 | ICMP | 108 | 0x5b7b (| 23419) | 64 Echo | (ping) | request | id=0x0001, | seq=19/48 | 4, ttl=6 | 54 (no r | response found!) | |
| | 18 2022-07-14 20: | 20:40.609807618 19 | 92.0.2.100 1 | 198.51.100.100 | ICMP | 108 | 0x5b7b (| 23419) | 64 Echo | (ping) | request | id=0x0001, | seq=19/48 | 4, ttl=6 | 64 (rep) | ly in 19) | |
| | 19 2022-07-14 20: | 20:40.610179685 19 | 8.51.100.100 1 | 192.0.2.100 | ICMP | 108 | Øxcd8f (| 52623) | 64 Echo | (ping) | reply | id=0x0001, | seq=19/48 | i4, ttl=6 | i4 (requ | uest in 18) | |
| | 20 2022-07-14 20: | 20:40.610181944 19 | 8.51.100.100 1 | 192.0.2.100 | ICMP | 108 | Øxcd8f (| 52623) | 64 Echo | (ping) | reply | id=0x0001, | seq=19/48 | i4, ttl≕6 | 54 | | |
| | 21 2022-07-14 20: | 20:41.633805153 19 | 92.0.2.100 1 | 198.51.100.100 | ICMP | 108 | 0x5b7e (| 23422) | 64 Echo | (ping) | request | id=0x0001, | seq=20/513 | 0, ttl=0 | i4 (no r | response found!) | |
| | 22 2022-07-14 20: | 20:41.633806997 19 | 02.0.2.100 1 | 198.51.100.100 | ICMP | 108 | 0x5b7e (| 23422) | 64 Echo | (ping) | request | id=0x0001, | seq=20/513 | 0, ttl=0 | i4 (rep] | ly in 23) | |
| | 23 2022-07-14 20: | 20:41.634084102 19 | 8.51.100.100 1 | 192.0.2.100 | ICMP | 108 | 0xce36 (| 52790) | 64 Echo | (ping) | reply | id=0x0001, | seq=20/513 | 0, ttl=0 | 4 (requ | uest in 22) | |
| | 24 2022-07-14 20:3 | 20:41.634085368 19 | 8.51.100.100 1 | 192.0.2.100 | ICMP | 108 | Oxce36 (| 52790) | 64 Echo | (ping) | reply | id=0x0001, | seq=20/513 | 0, ttl=0 | 54 | | |
| | 25 2022-07-14 20:3 | 20:42.657709898 19 | 2.0.2.100 1 | 198.51.100.100 | ICMP | 108 | 0x5bf0 (| 23536) | 64 Echo | (ping) | request | id=0x0001, | seq=21/53 | 6, ttl=6 | 64 (no r | response found!) | |
| | 26 2022-07-14 20: | 20:42.657711660 19 | 2.0.2.100 1 | 198.51.100.100 | ICMP | 108 | 0x5bf0 (| 23536) | 64 Echo | (ping) | request | id=0x0001 | seg=21/53 | 6, ttl=6 | 4 (rep) | ly in 27) | |
| | 27 2022-07-14 20: | 20:42.657980675 19 | 8.51.100.100 1 | 92.0.2.100 | ICMP | 108 | Oxce49 (| 52809) | 64 Echo | (ping) | reply | id=0x0001 | seg=21/53 | 6. ttl=6 | 4 (regu | uest in 26) | |
| | 28 2022-07-14 20: | 20:42.657981971 19 | 8.51.100.100 1 | 92.0.2.100 | ICMP | 108 | Oxce49 (| 52809) | 64 Echo | (ping) | reply | id=0x0001 | seg=21/53 | 6. ttl=6 | 14 | , | |
| | 29 2822-87-14 28: | 20:43.681736697 19 | 2.0.2.100 1 | 98.51.100.100 | ICMP | 108 | 0x5c52 (| 23634) | 64 Echo | (ping) | request | id=0x0001. | seg=22/56 | 2. ttl=6 | 54 (no r | response found!) | |
| | | | | | | **** | ensess (| | | (P | edacae | | and writes. | | | | |
| < | | | | | | | | | | | | | | | | | |
| > F | rame 1: 108 bytes | on wire (864 bits), | , 108 bytes cap | ptured (864 bits) | on interface o | apture_u0 | 8, id 0 | | | | 0 | 000 00 50 | 56 9d e7 56 | 58 97 | bd b9 7 | 77 2d 89 26 00 00 | -PV - PX |
| > E | thernet II, Src: C | isco_b9:77:2d (58:9 | 97:bd:b9:77:2d) |), Dst: VMware_9d: | 7:50 (00:50:5 | 6:9d:e7:5 | 60) | | | | 0 | 010 00 0a | 81 00 00 6 | 08 00 | 45 00 0 | 00 54 59 90 40 00 | ·····g·· E··TY·@· |
| ٧V | N-Tag | | | | | | | | | | 0 | 020 40 01 | f4 1c c0 0 | 02 64 | c6 33 (| 64 64 08 00 22 68 | @·····d ·3dd··*h |
| | 0 | | = Directi | on: To Bridge | | | | | | | 0 | 030 00 01 | 00 Of 89 7. | d0 62 | 00 00 0 | 00 00 b3 d7 09 00 | ·····z·b ····· |
| н | .0 | | = Pointer | : vif_id | | | | | | | 0 | 848 88 88 | 00 00 10 1 | 12 13 | 14 15 1 | 16 17 18 19 1a 1b | 18. 4001/18 |
| | | | = Destina | tion: 0 | | | | | | | | 050 1c 1d | 10 11 20 2 | 22 23 | 24 25 2 | 26 27 28 29 28 20 | |
| н | | 0 | = Looped: | No | A | | | | | | | 868 2C 2d | 2e 2f 30 3 | 32 33 | 34 35 3 | 36 37 | ,/0123 4567 |
| | | | = Reserve | d: 0 | 4 I | | | | | | | | | | | | |
| н | | | = Version | : 0 | | | | | | | | | | | | | |
| н | | | 1010 = Source: | 10 | | | | | | | | | | | | | |
| н | Type: 802.10 Vir | tual LAN (0x8100) | acate - pour cer | | | | | | | | | | | | | | |
| 5 | 10 Victual LAN | PRI: A DEL: A TO | 103 | | | | | | | | | | | | | | |
| • | 000 | = Deigeity: Back | t Effort (dafa | (0) | | | | | | | | | | | | | |
| Т | | - Off, Teoligibl | le | 011) (0) | | | | | | | | | | | | | |
| Т | | Der: Ineligio. | TG. | | 5 | | | | | | | | | | | | |
| Т | 0000 0110 0 | 111 - 10: 105 | | | | | | | | | | | | | | | |
| J. | Type: 19V4 (0x08 | 00) | | 100 51 100 100 | _ | | | | | | | | | | | | |
| 1 | nternet Protocol V | rersion 4, Src: 192. | .0.2.100, Dst: | 198.51.100.100 | | | | | | | | | | | | | |
| 2 I | nternet Control Me | issage Protocol | | | 2 | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |

| No. | Time | Source | Destination | Protocol | Length | IP ID | | IP TTL Info | | | | | | | |
|-----|-------------------------------------|-----------------|---------------------|----------|-------------------|---------|---------|-------------|--------|---------|--------------------|----------------|---------|------------------------|-----------------------|
| - | 1 2022-07-14 20:20:36.513854256 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x5990 | (22928) | 64 Echo | (ping) | request | id=0x0001 | , seq=15/3840, | ttl=64 | (no response found!) | |
| | 2 2022-07-14 20:20:36.513857289 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x5990 | (22928) | 64 Echo | (ping) | request | id=0x0001 | , seq=15/3840, | ttl=64 | (reply in 3) | |
| | 3 2022-07-14 20:20:36.514117394 | 198.51.100.10 | 9 192.0.2.100 | ICMP | 108 | 0xcc2c | (52268) | 64 Echo | (ping) | reply | id=0x0001 | , seq=15/3840, | ttl=64 | (request in 2) | |
| | 4 2022-07-14 20:20:36.514119312 | 198.51.100.10 | 0 192.0.2.100 | ICMP | 108 | Øxcc2c | (52268) | 64 Echo | (ping) | reply | id=0x0001 | , seq=15/3840, | ttl=64 | | |
| | 5 2022-07-14 20:20:37.537723822 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x5a00 | (23040) | 64 Echo | (ping) | request | id=0x0001 | , seq=16/4096, | ttl=64 | (no response found!) | |
| | 6 2022-07-14 20:20:37.537726588 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x5a00 | (23040) | 64 Echo | (ping) | request | id=0x0001 | , seq=16/4096, | ttl=64 | (reply in 7) | |
| | 7 2022-07-14 20:20:37.538046165 | 198.51.100.100 | 9 192.0.2.100 | ICMP | 108 | 0xcc9b | (52379) | 64 Echo | (ping) | reply | id=0x0001 | , seq=16/4096, | ttl=64 | (request in 6) | |
| | 8 2022-07-14 20:20:37.538048311 | 198.51.100.100 | 9 192.0.2.100 | ICMP | 108 | 0xcc9b | (52379) | 64 Echo | (ping) | reply | id=0x0001 | , seq=16/4096, | ttl=64 | | |
| | 9 2022-07-14 20:20:38.561776064 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x5ab7 | (23223) | 64 Echo | (ping) | request | id=0x0001 | , seq=17/4352, | tt1=64 | (no response found!) | |
| | 10 2022-07-14 20:20:38.561778310 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x5ab7 | (23223) | 64 Echo | (ping) | request | id=0x0001 | , seq=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 | 0xccc4 | (52420) | 64 Echo | (ping) | reply | id=0x0001 | , seq=17/4352, | ttl=64 | (request in 10) | |
| | 12 2022-07-14 20:20:38.562050333 | 198.51.100.10 | 0 192.0.2.100 | ICMP | 108 | 0xccc4 | (52420) | 64 Echo | (ping) | reply | id=0x0001 | , seq=17/4352, | ttl=64 | | |
| | 13 2022-07-14 20:20:39.585677043 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x5b46 | (23366) | 64 Echo | (ping) | request | id=0x0001 | , seq=18/4608, | ttl=64 | (no response found!) | |
| | 14 2022-07-14 20:20:39.585678455 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x5b46 | (23366) | 64 Echo | (ping) | request | id=0x0001 | , seq=18/4608, | ttl=64 | (reply in 15) | |
| | 15 2022-07-14 20:20:39.585936554 | 198.51.100.100 | 0 192.0.2.100 | ICMP | 108 | 0xcd8d | (52621) | 64 Echo | (ping) | reply | id=0x0001 | , seq=18/4608, | ttl=64 | (request in 14) | |
| | 16 2022-07-14 20:20:39.585937900 | 198.51.100.100 | 9 192.0.2.100 | ICMP | 108 | 0xcd8d | (52621) | 64 Echo | (ping) | reply | id=0x0001 | , seq=18/4608, | ttl=64 | | |
| | 17 2022-07-14 20:20:40.609804804 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x5b7b | (23419) | 64 Echo | (ping) | request | id=0x0001 | , seq=19/4864, | ttl=64 | (no response found!) | |
| | 18 2022-07-14 20:20:40.609807618 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x5b7b | (23419) | 64 Echo | (ping) | request | id=0x0001 | , seq=19/4864, | tt1=64 | (reply in 19) | |
| | 19 2022-07-14 20:20:40.610179685 | 198.51.100.10 | 3 192.0.2.100 | ICMP | 108 | 0xcd8f | (52623) | 64 Echo | (ping) | reply | id=0x0001 | , seq=19/4864, | ttl=64 | (request in 18) | |
| | 20 2022-07-14 20:20:40.610181944 | 198.51.100.10 | 0 192.0.2.100 | ICMP | 108 | 0xcd8f | (52623) | 64 Echo | (ping) | reply | id=0x0001 | , seq=19/4864, | ttl=64 | | |
| | 21 2022-07-14 20:20:41.633805153 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x5b7e | (23422) | 64 Echo | (ping) | request | id=0x0001 | , seq=20/5120, | tt1=64 | (no response found!) | |
| | 22 2022-07-14 20:20:41.633806997 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x5b7e | (23422) | 64 Echo | (ping) | request | id=0x0001 | , seq=20/5120, | tt1=64 | (reply in 23) | |
| | 23 2022-07-14 20:20:41.634084102 | 198.51.100.100 | 0 192.0.2.100 | ICMP | 108 | Øxce36 | (52790) | 64 Echo | (ping) | reply | id=0x0001 | , seq=20/5120, | tt1=64 | (request in 22) | |
| | 24 2022-07-14 20:20:41.634085368 | 198.51.100.100 | 9 192.0.2.100 | ICMP | 108 | 0xce36 | (52790) | 64 Echo | (ping) | reply | id=0x0001 | , seq=20/5120, | tt1=64 | | |
| | 25 2022-07-14 20:20:42.657709898 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x5bf0 | (23536) | 64 Echo | (ping) | request | id=0x0001 | , seq=21/5376, | tt1=64 | (no response found!) | |
| | 26 2022-07-14 20:20:42.657711660 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0x5bf0 | (23536) | 64 Echo | (ping) | request | 1d=0x0001 | , seq=21/5376, | tt1=64 | (reply in 27) | |
| | 27 2022-07-14 20:20:42.657980675 | 198.51.100.100 | 3 192.0.2.100 | ICMP | 108 | 0xce49 | (52809) | 64 Echo | (ping) | reply | 1d=0x0001 | , seq=21/5376, | tt1=64 | (request in 26) | |
| | 28 2022-07-14 20:20:42.657981971 | 198.51.100.100 | 3 192.0.2.100 | ICMP | 108 | Øxce49 | (52809) | 64 Echo | (ping) | reply | 1d=0x0001 | , seq=21/5376, | tt1=64 | (| |
| | 29 2022-07-14 20:20:43.681736697 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0X5C52 | (23634) | 64 Echo | (ping) | request | 1d=0x0001 | , seq=22/5632, | tt1=64 | (no response tound!) | |
| < | | | | | | | | | | | | | | | |
| > | Frame 2: 108 bytes on wire (864 bit | s), 108 bytes (| captured (864 bits) |) on int | terface capture_u | 0_8, id | 0 | | | 6 | 000 00 50 | 56 9d e7 50 5 | 8 97 bo | 1 b9 77 2d 89 26 00 00 | ·PV ··PX · ··w ··& ·· |
| > | Ethernet II, Src: Cisco b9:77:2d (5 | 8:97:bd:b9:77: | 2d), Dst: VMware 9 | d:e7:50 | (00:50:56:9d:e7: | 50) | | | | 6 | 9910 99 9 a | 81 00 00 67 0 | 8 00 45 | 5 00 00 54 59 90 40 00 | ····g·· E··TY·@· |
| 1 | VN-Tag | | | | | | | | | 6 | 9928 49 91 | f4 1c c0 00 0 | 2 64 ct | 5 33 64 64 08 00 22 68 | @d -3dd"h |
| | 0 | = Direc | tion: To Bridge | | | | | | | | 0030 00 01 | 00 0f 89 7a d | 0 62 00 | 00 00 00 b3 d7 09 00 | ·····z·b |
| | .0 | = Point | er: vif_id | | | | | | | | 0040 00 00 | 10 16 20 21 2 | 2 13 14 | 15 16 17 18 19 1a 10 | 1"# 678'/*+ |
| | | = Desti | nation: 0 | | | | | | | | 1050 1C 10 | 2e 2f 30 31 3 | 2 33 3/ | 35 36 37 | |
| | ···· ··· ··· ··· ··· 0 ···· | = Loope | d: No | 4 | | | | | | | | | | | , |
| | 0 | = Reser | ved: 0 | | | | | | | | | | | | |
| | 00 | = Versi | on: 0 | | | | | | | | | | | | |
| | 0000 000 | 00 1010 = Sourc | e: 10 | | | | | | | | | | | | |
| | Type: 802.1Q Virtual LAN (0x8100) |) | | | | | | | | | | | | | |
| M | 802.1Q Virtual LAN, PRI: 0, DEI: 0, | ID: 103 | | | | | | | | | | | | | |
| н | 000 = Priority: E | Best Effort (de | fault) (0) | | | | | | | | | | | | |
| н | 0 = DEI: Inelig | lple | | 3 | | | | | | | | | | | |
| | 0000 0110 0111 = ID: 103 | | | - | | | | | | | | | | | |
| Ш | Type: IPv4 (0x0800) | | | | | | | | | | | | | | |
| Р | Internet Protocol Version 4, Src: 1 | 92.0.2.100, DS | t: 198.51.100.100 | 2 | | | | | | | | | | | |
| 2 | Internet Control Message Protocol | | | 2 | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |

Seleccione el tercer y el cuarto paquetes y verifique los puntos clave:

- 1. Cada respuesta de eco ICMP se captura y se muestra 2 veces.
- 2. El encabezado del paquete original no tiene la etiqueta VLAN.
- 3. El switch interno inserta la etiqueta adicional del puerto VLAN **102** que identifica la interfaz de salida Ethernet1/2.
- 4. El switch interno inserta una etiqueta VN adicional.

| _ | | | | | | | | |
|----------|---------------------------------------|----------------------------------|------------------|------------|----------------|-------------------|--------|--|
| No. | Time S | Source Destination | Protocol | Length 1 | P D | IP TTL Info | | |
| - | 1 2022-07-14 20:20:36.513854256 1 | 192.0.2.100 198.51.100.100 | ICMP | 108 0 | 0x5990 (22928) | 64 Echo (ping) re | equest | id=0x0001, seq=15/3840, ttl=64 (no response found!) |
| | 2 2022-07-14 20:20:36.513857289 1 | 192.0.2.100 198.51.100.100 | ICMP | 108 | 1x5998 (22928) | 64 Echo (ning) re | equest | id=0x0001, seg=15/3840, ttl=64 (reply in 3) |
| 4 | 3 2022-07-14 20:20:36,514117394 1 | 198,51,100,100 192,0,2,100 | ICMP | 108 1 6 | axcc2c (52268) | 64 Echo (ping) re | eply | id=0x0001, seg=15/3840, ttl=64 (request in 2) |
| Г | 4 2022-07-14 20:20:36.514119312 1 | 198.51.100.100 192.0.2.100 | ICMP | 108 6 | axcc2c (52268) | 64 Echo (ping) re | eply | id=0x0001, seg=15/3840, ttl=64 |
| | 5 2022-07-14 20:20:37 537723822 1 | 192 8 2 188 198 51 188 188 | TCMP | 108 | av5a00 (23040) | 64 Echo (ning) re | equest | id=0x0001, seq=16/4006, ttl=64 (no response foundl) |
| | 6 2022-07-14 20:20:37 537726588 1 | 102 0 2 100 108 51 100 100 | TCMD | 108 6 | av5200 (23040) | 64 Echo (ping) re | equest | id=0x0001, seq=16/4006, ttl=64 (renly in 7) |
| | 7 2022-07-14 20:20:37:537720508 1 | 109 51 100 100 100 0 2 100 | TCMD | 100 0 | weenh (53370) | 64 Echo (ping) re | anly | id-0x0001, seq-16/4006, ttl-64 (repry 107) |
| | / 2022-07-14 20.20.37.538040105 1 | | TCHP | 100 0 | (52375) | GA Echo (ping) re | epty | 10=0x0001, seq=10/4050, tt1=04 (request 10 0) |
| | 8 2022-07-14 20:20:37.538048311 1 | 198.51.100.100 192.0.2.100 | ICMP | 108 6 | xccap (223/9) | 64 Echo (ping) re | epty | 10=0x0001, seq=16/4096, ttl=64 |
| | 9 2022-07-14 20:20:38.561776064 1 | 192.0.2.100 198.51.100.100 | ICMP | 108 6 | 9X5ab7 (23223) | 64 Echo (ping) re | equest | 10=0X0001, seq=17/4352, tt1=64 (no response round!) |
| | 10 2022-07-14 20:20:38.561778310 1 | 192.0.2.100 198.51.100.100 | ICMP | 108 6 | 3x5ab7 (23223) | 64 Echo (ping) re | equest | 1d=0x0001, seq=17/4352, tt1=64 (reply in 11) |
| | 11 2022-07-14 20:20:38.562048288 1 | 198.51.100.100 192.0.2.100 | ICMP | 108 0 | 9xccc4 (52420) | 64 Echo (ping) re | eply | 1d=0x0001, seq=17/4352, ttl=64 (request in 10) |
| | 12 2022-07-14 20:20:38.562050333 1 | 198.51.100.100 192.0.2.100 | ICMP | 108 0 | 0xccc4 (52420) | 64 Echo (ping) re | eply : | id=0x0001, seq=17/4352, ttl=64 |
| | 13 2022-07-14 20:20:39.585677043 1 | 192.0.2.100 198.51.100.100 | ICMP | 108 0 | 0x5b46 (23366) | 64 Echo (ping) re | equest | id=0x0001, seq=18/4608, ttl=64 (no response found!) |
| | 14 2022-07-14 20:20:39.585678455 1 | 192.0.2.100 198.51.100.100 | ICMP | 108 0 | 3x5b46 (23366) | 64 Echo (ping) re | equest | id=0x0001, seq=18/4608, ttl=64 (reply in 15) |
| | 15 2022-07-14 20:20:39.585936554 1 | 198.51.100.100 192.0.2.100 | ICMP | 108 0 | excd8d (52621) | 64 Echo (ping) re | eply : | id=0x0001, seq=18/4608, ttl=64 (request in 14) |
| | 16 2022-07-14 20:20:39.585937900 1 | 198.51.100.100 192.0.2.100 | ICMP | 108 6 | excd8d (52621) | 64 Echo (ping) re | eply | id=0x0001, seq=18/4608, ttl=64 |
| | 17 2022-07-14 20:20:40.609804804 1 | 192.0.2.100 198.51.100.100 | ICMP | 108 0 | ax5b7b (23419) | 64 Echo (ping) re | equest | id=0x0001, seg=19/4864, ttl=64 (no response found!) |
| | 18 2022-07-14 20:20:40.609807618 1 | 192.0.2.100 198.51.100.100 | ICMP | 108 0 | ax5b7b (23419) | 64 Echo (ping) re | equest | id=0x0001, seg=19/4864, ttl=64 (reply in 19) |
| | 19 2022-07-14 20:20:40.610179685 1 | 198.51.100.100 192.0.2.100 | ICMP | 108 6 | axcd8f (52623) | 64 Echo (ping) re | eply | id=0x0001, seg=19/4864, ttl=64 (request in 18) |
| | 20 2022-07-14 20:20:40.610181944 1 | 198.51.100.100 192.0.2.100 | TCMP | 108 6 | axcd8f (52623) | 64 Echo (ping) re | eply | id=0x0001, seg=19/4864, ttl=64 |
| | 21 2022-07-14 20:20:41.633805153 1 | 192.0.2.100 198.51.100.100 | TCMP | 108 6 | ax5b7e (23422) | 64 Echo (ping) re | equest | id=8x8881, seq=28/5128, ttl=64 (no response found1) |
| | 22 2022-07-14 20:20:41:055005155 1 | 102 0 2 100 100 51 100 100 | TCMD | 100 0 | ysh7a (22422) | 64 Echo (ping) re | aquast | id=0x0001, seq=20/5120, ttl=64 (nolv in 22) |
| | 22 2022-07-14 20:20:41.033000997 1 | 100 51 100 100 100 0 2 100 | TCHP | 100 0 | x507e (25422) | 64 Echo (ping) re | equest | id-0x0001, seq-20/5120, ttl-64 (repry 10 25) |
| | 25 2022-07-14 20:20:41.054004102 1 | 198.51.100.100 192.0.2.100 | TCHP | 100 0 | 5xceso (52790) | ou Echo (ping) re | epty | 10=0x0001, Seq=20/5120, ttl=04 (request 10 22) |
| | 24 2022-07-14 20:20:41.634085368 1 | 198.51.100.100 192.0.2.100 | ICMP | 108 0 | axce36 (52790) | 64 Echo (ping) re | epty | 10=0X0001, seq=20/5120, tt1=64 |
| | 25 2022-07-14 20:20:42.657709898 1 | 192.0.2.100 198.51.100.100 | ICMP | 108 0 | 9X5010 (23536) | 64 Echo (ping) re | equest | 10=0X0001, seq=21/53/6, tt1=64 (no response found!) |
| | 26 2022-07-14 20:20:42.657711660 1 | 192.0.2.100 198.51.100.100 | ICMP | 108 € | 0x5bf0 (23536) | 64 Echo (ping) re | equest | id=0x0001, seq=21/5376, ttl=64 (reply in 27) |
| | 27 2022-07-14 20:20:42.657980675 1 | 198.51.100.100 192.0.2.100 | ICMP | 108 0 | 0xce49 (52809) | 64 Echo (ping) re | eply | id=0x0001, seq=21/5376, ttl=64 (request in 26) |
| | 28 2022-07-14 20:20:42.657981971 1 | 198.51.100.100 192.0.2.100 | ICMP | 108 0 | 9xce49 (52809) | 64 Echo (ping) re | eply | id=0x0001, seq=21/5376, ttl=64 |
| | 29 2022-07-14 20:20:43.681736697 1 | 192.0.2.100 198.51.100.100 | ICMP | 108 6 | 3x5c52 (23634) | 64 Echo (ping) re | equest | id=0x0001, seq=22/5632, ttl=64 (no response found!) |
| ć | | | | | | | | |
| | Frame 3, 400 butes an user (064 bits) | and huter contured (ord hite) | on intenfore c | | | | | 00 00 50 56 0d of ha 59 07 hd ha 77 0a 90 36 00 00 |
| 0 | Frame 5: 108 bytes on wire (864 bits) |), 108 bytes captured (864 bits) | on incertace c | apcure_uo_ | 8, 10 0 | | 00 | 10 00 00 00 00 00 00 00 00 00 00 00 00 0 |
| _ | Ethernet 11, Src: C1SCO 09:77:00 (58: | :97:0d:09:77:0e), DSt: VMware 90 | 1:68:06 (00:20:2 | 6:90:e8:De |) | | 00. | 20 40 01 c1 80 c6 33 64 64 c0 00 02 64 00 00 2a 68 03ddd.*b |
| 1 | VN-Tag | | | | | | 00. | 30 00 01 01 00 00 35 04 04 00 00 02 04 00 00 28 00 g |
| I | 0 | = Direction: To Bridge | | | | | 00. | 40 00 00 00 00 10 11 12 13 14 15 16 17 18 10 1a 1h |
| I | .0 | <pre> = Pointer: vif_id</pre> | | | | | 00 | 50 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b !"# \$1\$*'()"+ |
| I | 0000 0000 0000 | = Destination: 0 | | | | | 00 | 68 2c 2d 2e 2f 30 31 32 33 34 35 36 37/0123 4567 |
| I | ···· ··· ··· ··· ··· 0 ···· | = Looped: No | 41 | | | | | , ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, |
| I | | = Reserved: 0 | - I | | | | | |
| I | | = Version: 0 | | | | | | |
| I | 0000 0000 | 1010 = Source: 10 | | | | | | |
| I | Type: 802.1Q Virtual LAN (0x8100) | | | | | | | |
| 4 | 802.10 Virtual LAN, PRI: 0, DEI: 0, 1 | ID: 102 | | | | | | |
| I | 000 Priority: Re | st Effort (default) (0) | | | | | | |
| I | | ble | 2 | | | | | |
| 1 | 0000 0110 0110 - TO: 102 | | 2 | | | | | |
| 1 | Tunoi Thuế (0x0000) | | | | | | | |
| J | Tetennet Bostesel Vension 4 Ensi 109 | E E1 100 100 Drt. 103 0 3 100 | _ | | | | | |
| 1 | Internet Protocol Version 4, Src: 198 | 5.51.100.100, DSt: 192.0.2.100 | 2 | | | | | |
| 2 | Internet control Message Protocol | | 4 | | | | | |

Explicación

Cuando se configura una captura de paquetes en una interfaz de backplane, el switch captura simultáneamente cada paquete dos veces. En este caso, el switch interno recibe paquetes que ya están etiquetados por la aplicación en el módulo de seguridad con la etiqueta de VLAN de puerto y la etiqueta VPN. La etiqueta VLAN identifica la interfaz de salida que el chasis interno utiliza para reenviar los paquetes a la red. La etiqueta VLAN 103 en los paquetes de solicitud de eco ICMP identifica Ethernet1/3 como la interfaz de salida, mientras que la etiqueta VLAN 102 en los paquetes de respuesta de eco ICMP identifica Ethernet1/2 como la interfaz de salida. El switch interno quita la etiqueta VN y la etiqueta VLAN de la interfaz interna antes de que los paquetes se reenvíen a la red.

Esta tabla resume la tarea:

| Tarea | Punto de captura | VLAN de puerto interno en paquetes capturados | Direcci ón: | Tráfico capturado |
|---|------------------------------------|---|---------------------|--|
| Configuración y verificación de capturas de paquetes en interfaces de backplane | Interfac es de backpla ne | 102 103 | Solo entrad a | Solicitudes de eco ICMP del ho 192.0.2.100 al host 198.51.100 Respuestas de eco ICMP del h 198.51.100.100 al host 192.0.2 |

Capturas de paquetes en puertos de aplicaciones y aplicaciones

Las capturas de paquetes de puertos de aplicaciones o aplicaciones siempre se configuran en las interfaces de la placa de interconexiones y, además, en las interfaces frontales si el usuario especifica la dirección de captura de la aplicación.

Hay principalmente 2 casos prácticos:

- Configure las capturas de paquetes en las interfaces de la placa de interconexiones para los paquetes que salen de una interfaz frontal específica. Por ejemplo, configure las capturas de paquetes en la interfaz Ethernet1/9 de la placa de interconexiones para los paquetes que salen de la interfaz Ethernet1/2.
- Configure capturas simultáneas de paquetes en una interfaz frontal específica y en las interfaces de la placa posterior. Por ejemplo, configure capturas simultáneas de paquetes en la interfaz Ethernet1/2 y en la interfaz de placa de interconexiones Ethernet1/9 para paquetes que salgan de la interfaz Ethernet1/2.

Esta sección abarca ambos casos prácticos.

Tarea 1

Utilice FCM y CLI para configurar y verificar una captura de paquetes en la interfaz de la placa posterior. Se capturan los paquetes para los que el puerto de aplicación Ethernet1/2 se identifica como la interfaz de salida. En este caso, se capturan las respuestas ICMP.

Topología, flujo de paquetes y puntos de captura



Configuración

FCM

Siga estos pasos en FCM para configurar una captura de paquetes en la aplicación FTD y el puerto Ethernet1/2 de la aplicación:

1. Utilice Tools > Packet Capture > Capture Session para crear una nueva sesión de captura:

| 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 | | |

 Seleccione la aplicación Ethernet1/2 en la lista desplegable Application Port y seleccione Egress Packet en Application Capture Direction. Proporcione el Nombre de la Sesión y haga clic en Guardar y Ejecutar para activar la captura:

| Overview Interfaces Logical Devices Security Engine | Platform Settings | | | System Too | ols Help a | admin |
|---|---------------------------|--|--------------------------|------------|------------|-------|
| Select an instance: ftd1 | | Save an | and Run Save | Cancel | | |
| ftd1 | | Session Name* cap1 | | | | |
| Ethernet1/2 | | Selected Interfaces None Buffer Size 256 MB Snap length: 1518 | ♥ Bytes | | | |
| Ethernet1/3 | | Store Packets Overwrite Ap Capture On ftd Application Port Ethernet1/2 | Append V | | | |
| | Ethernet1/9, Ethernet1/10 | Application Capture Direction All Packets Egres Capture Filter Cap | ess Packet apture All | | | |
| Ethernet1/1 | | | | | | |
| | | | | | | |

CLI FXOS

Siga estos pasos en la CLI de FXOS para configurar las capturas de paquetes en las interfaces de la placa posterior:

1. Identifique el tipo de aplicación y el identificador:

| firepower# | scope ss | a | | | | | |
|-------------|-----------------|-------------------|---------------------------|---------|--------------|----------------|-------------------|
| firepower | /ssa# sh | low app-ins | tance | | | | |
| App Name | Identifi | er Slot ID | Admin Stat | e Oper | State | Running Versio | n Startup Version |
| Deploy Typ | e Turbo M | Node Profil | e Name Cluster | State | Cluster R | ole | |
| | | | | | | | |
| ftd | ftd1 | 1 | Enabled | Onlin | e | 7.2.0.82 | 7.2.0.82 |
| Native | No | | Not App | licable | None | | |
| 2 Crea | ar una ses | sión de car | otura: | | | | |
| | | | | | | | |
| | | | | | | | |
| firepower# | scope pa | cket-captu | re | | | | |
| firepower | /packet-c | apture # c | reate session | cap1 | | | |
| firepower | /packet-c | apture/ses | sion* # create | app-po | rt 1 112 Et | hernet1/2 ftd | |
| firepower | /packet-c | apture/ses | <pre>sion/app-port*</pre> | # set | app-identif: | ier ftd1 | |
| firepower | /packet-c | apture/ses | <pre>sion/app-port*</pre> | # set | filter "" | | |
| firepower | /packet-c | apture/ses | <pre>sion/app-port*</pre> | # set | subinterfac | e 0 | |
| firepower | /packet-c | apture/ses | <pre>sion/app-port*</pre> | # up | | | |
| firepower | /packet-c | apture/ses | sion* # commit | | | | |
| firepower | /packet-c | apture/ses | sion # | | | | |
| Verificació | ón | | | | | | |

FCM

Verifique el **Nombre de la Interfaz**, asegúrese de que el **Estado Operacional** esté activo y que el **Tamaño del Archivo (en bytes)** aumente:

| ſ | Overview | Interfaces | Logical Devices | Security Engine | Platform Setti | ngs | | | | | | System | Tools H | elp adm | iin |
|---|-------------|----------------|-----------------|-----------------|-----------------|---------------|--------------------------|-----|-----------|------------------|-------------|--------------|----------|---------|----------|
| | | | | | | | | | | | | | | | |
| ſ | Capture Ses | sion Fiter Lis | t | | | | | | | | | | | | |
| | | | | | | | | | c | Refresh Capt | ure Session | Delete All S | Sessions | | |
| ſ | | cap1 | Drop Count: | 0 | Operational Sta | ate: up | Buffer Size: 256 | мв | 5 | nap Length: 1518 | Bytes | | | | <u>.</u> |
| Ì | Interface N | ame | Filter | | File Si | ze (in bytes) | File Name | De | vice Name | | | | | | |
| | Ethernet1/2 | - Ethernet1/10 | None | | 576 | | cap1-vethernet-1175.pcap | ftd | 1 | | \pm | | | | |
| | Ethernet1/2 | - Ethernet1/9 | None | | 4360 | | cap1-vethemet-1036.pcap | ftd | 11 | | ⊻ | | | | |

CLI FXOS

Verifique los detalles de la captura en scope packet-capture:

```
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:
```

Recopilar archivos de captura

Siga los pasos de la sección Recopilación de archivos de captura de switch internos de Firepower 4100/9300.

Capturar análisis de archivos

Utilice una aplicación de lector de archivos de captura de paquetes para abrir los archivos de captura. En el caso de varias interfaces de backplane, asegúrese de abrir todos los archivos de captura para cada interfaz de backplane. En este caso, los paquetes se capturan en la interfaz Ethernet1/9 de la placa de interconexiones.

Seleccione el primer y el segundo paquete y verifique los puntos clave:

- 1. Cada respuesta de eco ICMP se captura y se muestra 2 veces.
- 2. El encabezado del paquete original no tiene la etiqueta VLAN.
- 3. El switch interno inserta la etiqueta adicional del puerto VLAN **102** que identifica la interfaz de salida Ethernet1/2.
- 4. El switch interno inserta una etiqueta VN adicional.

| No. Time | Source | Destination | Protocol | Length | PD | IP TTL Info | |
|--|--|--|--|---|--|--|--|
| 1 2022-08-01 10:03:22.231237959 | 198.51.100.100 | 192.0.2.100 | 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 | 8X4303 (17331) | 64 ECHO (ping) reply | 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 | id=0x0012, seq=8/2048, ttl=64 |
| 17 2022-08-01 10:03:30.378795204 | 198.51.100.100 | 192.0.2.100 | ICMP | 108 | 0x4597 (17815) | 64 Echo (ping) reply | id=0x0012, seq=9/2304, ttl=64 |
| 18 2022-08-01 10:03:30.378798172 | 198.51.100.100 | 192.0.2.100 | ICMP | 108 | 0x4597 (17815) | 64 Echo (ping) reply | id=0x0012, seq=9/2304, 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 (18842) | 64 Echo (ping) reply | 1d=0x0012, seq=10/2560, tt1=64 |
| 21 2022-08-01 10:03:32.426693254 | 198.51.100.100 | 192.0.2.100 | ICMP | 108 | 0x468a (18058) | 64 Echo (ping) reply | 1d=0x0012, seq=11/2816, tt1=64 |
| 22 2022-08-01 10:03:32.420093091 | 198.51.100.100 | 192.0.2.100 | ICHP | 100 | 0X4003 (10038) | e4 Ecuo (brug) Lebrà | 10=0X0012, Seq=11/2010, CC1=04 |
| ¢ | | | | | | | |
| > Frame 1: 108 bytes on wire (864 bit | s), 108 bytes ca | otured (864 bits) | on interface | capture u | 0 8. id 0 | | 0000 00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00 ·PV···X· ··w··&·· |
| > Ethernet II, Src: Cisco b9:77:0e (| 8:97: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 42 f8 00 00 ·····f·· E··TB··· |
| VN-Tag | | | , | | | | 0020 40 01 4a b5 c6 33 64 64 c0 00 02 64 00 00 90 04 @J3ddd |
| 0 | = Direct | ion: To Bridge | | | | | 0030 00 12 00 01 dd a4 e7 62 00 00 00 e3 0d 09 00 ·····b ·····b |
| .0 | = Pointer | r: vif_id | | | | | 0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 10 |
| 0000 0000 0000 | = Destin | ation: 0 | | | | | 0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 |
| ···· ··· ··· ··· ··· 0··· ··· ·· | = Looped: | : No | 41 | | | | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, |
| 0 | = Reserve | ed: 0 | | | | | |
| | ·· ···· = Version | n: 0 | | | | | |
| 0000 00 | 00 1010 = Source: | : 10 | | | | | |
| Type: 802.10 Virtual LAN (0x8100 |) | | | | | | |
| 802.1Q Virtual LAN, PRI: 0, DEI: 0, | ID: 102 | | | | | | |
| 000 = Priority: | Best Effort (deta | ault) (0) | 2 | | | | |
| 0 = DEI: Ineli | gible | | 3 | | | | |
| 0000 0110 0110 = ID: 102 | | | - | | | | |
| Type: IPv4 (0x0800) | | | _ | | | | |
| Internet Protocol Version 4, Src: 1 | 98.51.100.100, D | st: 192.0.2.100 | 2 | | | | |
| Internet Control Message Protocol | | | 2 | | | | |
| | | | _ | | | | |
| | | | | | | | |
| | 6 | Providence in the second | and and | 1.000 | | | |
| No. Time | Source | Destination | Protocol | Length | PD | PTTL Mo | 14 mm 2 mm 2 / 25 (12 - 52 - 52 - 52 - 52 - 52 - 52 - 52 - |
| No. Time 1 2022-08-01 10:03:22.231237959 2 2022 08-01 10:03:22.231237959 | Source 198.51.100.100 | Destination 192.0.2.100 | Protocol ICMP | Length 108 | PD 0x42f8 (17144) | PTTL 100 64 Echo (ping) reply | id-0x0012, seq=1/256, ttl=64 |
| No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:22.231239747 | Source 198.51.100.100 198.51.100.100 | Destination 192.0.2.100 192.0.2.100 192.0.2.100 | Protocol ICMP ICMP | Length 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) | ₽TTL №0 64 Echo (ping) reply 64 Echo (ping) reply na Echo (ping) reply | id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 |
| No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:23.232244769 4 2022-08-01 10:03:23.232244753 | Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 | Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 | Protocol ICMP ICMP ICMP ICMP | Length 108 1 108 1 108 1 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x4303 (17331) 0x4303 (17331) | PTTL 140 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 |
| No. Time 1 2022-08-01 10:03:22,231237959 2 2022-08-01 10:03:22,231239747 3 2022-08-01 10:03:22,232244769 4 2022-08-01 10:03:23,232244753 5 2022-08-01 10:03:24,23240793981 | Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 | Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 | Protocol ICMP ICMP ICMP ICMP ICMP | Length 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x4305 (17331) 0x43b3 (17331) 0x445c (17502) | PTTL 140 64 Echo (ping) reply 64 Echo (ping) reply 64 Echo (ping) reply 64 Echo (ping) reply 64 Echo (ping) reply | id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 |
| No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237979 3 2022-08-01 10:03:23.23224779 4 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:24.234705981 6 2022-08-01 10:03:24.2347653981 | 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 ICMP | Length 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x4303 (17331) 0x43b3 (17331) 0x445e (17502) 0x445e (17502) | PTTL 200 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=3/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64 |
| Ho. Time 1 2022-08-01 10:03:22.211237959 2 2022-08-01 10:03:23.232244769 4 2022-08-01 10:03:23.232244769 5 2022-08-01 10:03:24.242753 5 2022-08-01 10:03:24.242470961 6 2022-08-01 10:03:25.252672449 | 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 1 108 108 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x4303 (17331) 0x445e (17502) 0x445e (17502) 0x445e (17502) | PTTL 100 64 Echo (ping) reply 64 Echo (ping) reply 04 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 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64 |
| Ins. Time 1 2022-08-01 10:03:22.21237959 2 2022-08-01 10:03:22.23123747 3 2022-08-01 10:03:23.232244763 5 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:24.234706751 6 2022-08-01 10:03:24.234706751 7 2022-08-01 10:03:25.258672449 8 2022-08-01 10:03:25.258572449 | Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 | Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 | Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP | Length 108 1 108 1 1 | PD 0x42f8 (17144) 0x42f8 (17144) 0x4303 (17331) 0x4456 (17502) 0x4456 (17502) 0x4464 (17508) 0x4464 (17508) | PTR 196 64 Echo (ping) reply 64 Echo (ping) reply | id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/256, 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=3/71024, ttl=64 id=0x0012, seq=4/1024, ttl=64 |
| No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 3 3022-08-01 10:03:22.231237959 4 2022-08-01 10:03:22.231237753 5 2022-08-01 10:03:24.23247059 7 2022-08-01 10:03:24.234703961 7 2022-08-01 10:03:25.258572409 8 2022-08-01 10:03:25.25857249 9 2022-08-01 10:03:26.23263169 | 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 | Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP | Length 108 1 108 1 1 | PD 0x42f8 (17144) 0x4305 (17331) 0x4305 (17331) 0x445e (17502) 0x445e (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) | PTL 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=3/1024, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=4/1024, ttl=64 |
| Ime Time 1 2022-08-01 10:03:22,23123959 2 2022-08-01 10:03:22,231239747 3 3022-08-01 10:03:23,232244769 5 2022-08-01 10:03:23,232244753 5 202-08-01 10:03:24,23470391 6 2022-08-01 10:03:25,2586744651 7 202-08-01 10:03:25,2586744661 9 2022-08-01 10:03:26,228663169 10 2022-08-01 10:03:26,282663169 10 202-08-01 10:03:26,282663169 | 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 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 | Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP | Length 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x4305 (1731) 0x4352 (17502) 0x44545 (17502) 0x44645 (17508) 0x4464 (17508) 0x4463 (17603) 0x4463 (17603) | P TL b6 64 Echo (ping) reply 64 Echo (ping) reply | id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 |
| Ho. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.23123747 3 2022-08-01 10:03:23.232244705 5 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:24.234706751 7 2022-08-01 10:03:24.234706751 7 2022-08-01 10:03:25.258672449 8 2022-08-01 10:03:25.258572451 9 2022-08-01 10:03:26.282663169 10 2022-08-01 10:03:27.366751681 11 2022-08-01 10:03:27.366671694 | 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 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 | Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP | Length 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x4305 (17331) 0x43b3 (17331) 0x4456 (17502) 0x4454 (17502) 0x4464 (17508) 0x4464 (17508) 0x4463 (17603) 0x4463 (17603) | PTL 166 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 65 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=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=3/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 |
| No. Time 1 2022-08-01 10:03:22.21237959 2 2022-08-01 10:03:23.232244760 4 4022-08-01 10:03:23.232244760 5 2020-08-01 10:03:23.232244760 6 2022-08-01 10:03:24.23470501 7 022-08-01 10:03:25.25872440 8 2022-08-01 10:03:25.258672461 9 202-08-01 10:03:25.258672461 9 202-08-01 10:03:27.3066716378 10 2022-08-01 10:03:27.3066716378 12 2022-08-01 10:03:27.3066716374 | Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 | Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 | Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP | 108 108 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x42b3 (17331) 0x43b3 (17331) 0x445c (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17603) 0x44c3 (17603) 0x44c7 (17639) 0x467 (17639) | PTL 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=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=6/1356, ttl=64 id=0x0012, seq=6/1356, ttl=64 |
| Ime Time 1 2022-08-01 10:03:22.231239759 2 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:23.232244769 4 2022-08-01 10:03:23.232244753 5 2022-08-01 10:03:24.2347096751 7 7022-08-01 10:03:25.2586724601 8 2022-08-01 10:03:25.258672461 9 2022-08-01 10:03:25.258672461 9 2022-08-01 10:03:27.36674737 10 202-08-01 10:03:27.306767164 12 2022-08-01 10:03:27.306674764 12 2022-08-01 10:03:27.306674764 12 2022-08-01 10:03:27.306674764 | Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 | Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 | Protocol ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP | Length 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x43b3 (17331) 0x43b3 (17331) 0x43b5 (17502) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17639) 0x467 (17639) 0x4667 (17639) | P TL b6 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 64 Echo (ping) reply | id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/256, 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=3/708, ttl=64 id=0x0012, seq=3/128, ttl=64 id=0x0012, seq=3/128, ttl=64 id=0x0012, seq=3/128, ttl=64 id=0x0012, seq=3/136, ttl=64 id=0x0012, seq=3/136, ttl=64 id=0x0012, seq=3/136, ttl=64 id=0x0012, seq=3/136, ttl=64 id=0x0012, seq=3/1372, ttl=64 |
| No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.21239747 3 3022-08-01 10:03:22.21239747 4 2022-08-01 10:03:22.23224750 5 2022-08-01 10:03:24.234703981 6 2022-08-01 10:03:25.25872440 7 2020-08-01 10:03:25.25872440 9 2020-08-01 10:03:26.232666183 10 2022-08-01 10:03:27.306674641 9 2020-08-01 10:03:27.366746618 11 2022-08-01 10:03:27.366746743 12 2022-08-01 10:03:27.36674764378 13 2022-08-01 10:03:27.36674764378 13 2022-08-01 10:03:27.36674764378 13 202-08-01 10:03:27.36674764378 13 202-08-01 10:03:27.36674378 13 202-08-01 10:03:27.36674378 13 202-08-01 10:03:27.36674378 13 202-08-01 10:03:27.33066475153 | 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 | 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 | Length 108 1 108 1 109 10 100 100 100 100 100 100 100 10000000 | PD 0x42f8 (17144) 0x42f8 (17144) 0x42b3 (17331) 0x43b3 (17331) 0x4454 (17502) 0x4454 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x4459 (17744) 0x4559 (17744) | PTL 166 64 Echo (ping) reply 64 Echo (ping) reply 64 Echo (ping) reply 65 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=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=5/136, ttl=64 id=0x0012, seq=5/137, ttl=64 id=0x0012, seq=7/1722, ttl=64 |
| He. Time 1 2022-08-01 10:03:22.21239759 2 2022-08-01 10:03:23.23224769 3 2022-08-01 10:03:23.232247763 5 2022-08-01 10:03:23.232247763 5 2022-08-01 10:03:24.2347096751 7 2022-08-01 10:03:25.258672406 9 2022-08-01 10:03:25.258672406 9 2022-08-01 10:03:27.306671694 12 2022-08-01 10:03:27.306674778 12 2022-08-01 10:03:27.306674778 13 2022-08-01 10:03:27.306674778 14 2022-08-01 10:03:27.3065743951 12 2022-08-01 10:03:27.3065743951 14 2022-08-01 10:03:27.306574395 15 202-08-01 10:03:27.306574395 14 2022-08-01 10:03:27.306574395 15 2022-08-01 10:03:27.306574395 16 2022-08-01 10:03:27.306574395 16 2022-08-01 10:03:27.306574395 16 | Source 198, 51, 100, 100 198, 51, 100, 100 | Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 | Protocol ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP | Length 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x4395 (17144) 0x4395 (17141) 0x4395 (17151) 0x4456 (17502) 0x4456 (17502) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4467 (17639) 0x4467 (17749) 0x4559 (17744) 0x4555 (17744) | P TL b6 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 68 Echo (ping) reply 68 Echo (ping) reply 69 Echo (ping) reply 60 Echo (ping | id-0x0012, seq-1/256, ttl=64 id-0x0012, seq-1/256, ttl=64 id-0x0012, seq-2/512, ttl=64 id-0x0012, seq-2/512, ttl=64 id-0x0012, seq-3/768, ttl=64 id-0x0012, seq-3/768, ttl=64 id-0x0012, seq-3/768, ttl=64 id-0x0012, seq-3/1280, ttl=64 id-0x0012, seq-3/1280, ttl=64 id-0x0012, seq-5/1280, ttl=64 id-0x0012, seq-5/1280, ttl=64 id-0x0012, seq-5/1360, ttl=64 id-0x0012, seq-5/1360, ttl=64 id-0x0012, seq-5/1360, 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 |
| Ime 1 2022-08-01 10:03:22,231239759 2 2022-08-01 10:03:22,231239747 3 2022-08-01 10:03:23,232244769 4 2022-08-01 10:03:23,232244753 5 2022-08-01 10:03:24,23479391 6 2022-08-01 10:03:24,2347096751 7 2022-08-01 10:03:25,2586724601 9 2022-08-01 10:03:26,2386761694 10 2022-08-01 10:03:27,306671694 12 2022-08-01 10:03:28,3306667153 13 2022-08-01 10:03:28,330667153 15 2022-08-01 10:03:28,3306667153 16 2022-08-01 10:03:28,33066615153 16 2022-08-01 10:03:28,33066615153 16 2022-08-01 10:03:28,33066615153 16 2022-08-01 10:03:28,33066615153 16 2022-08-01 10:03:28,3306645153 16 2022-08-01 10:03:28,3306645153 16 2022-08-01 10:03:28,3306545153 16 <td< td=""><td>Source 198, 51, 100, 100 198, 51, 100, 100</td><td>Destination 192, 0, 2, 100 192, 0, 100 192, 0, 100 192, 0, 100 192, 0, 100 192, 0, 100</td><td>Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP</td><td>Length 108 1 108 1 109 100 100 100 100 100 100 100 100 100</td><td>PD 0x42f8 (17144) 0x42f8 (17144) 0x4305 (17331) 0x4353 (17331) 0x4456 (17502) 0x4454 (17502) 0x4464 (17508) 0x4644 (17508) 0x4644 (17639) 0x4647 (17639) 0x4647 (17639) 0x4647 (17639) 0x4550 (17744) 0x4555 (17747) 0x4553 (17747)</td><td>PTL b6 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 68 Echo (ping) reply 69 Echo (ping) reply 60 Echo (ping)</td><td>id-0x0012, seq-1/256, ttl=64 id-0x0012, seq-2/512, ttl=64 id-0x0012, seq-2/512, ttl=64 id-0x0012, seq-2/512, ttl=64 id-0x0012, seq-3/768, 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-5/1380, ttl=64 id-0x0012, seq-5/1380, ttl=64 id-0x0012, seq-5/1380, ttl=64 id-0x0012, seq-5/1380, ttl=64 id-0x0012, seq-5/1380, ttl=64 id-0x0012, seq-3/192, ttl=64 id-0x0012, seq-3/192, ttl=64 id-0x0012, seq-3/2048, ttl=64 id-0x001</td></td<> | 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 ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP | Length 108 1 108 1 109 100 100 100 100 100 100 100 100 100 | PD 0x42f8 (17144) 0x42f8 (17144) 0x4305 (17331) 0x4353 (17331) 0x4456 (17502) 0x4454 (17502) 0x4464 (17508) 0x4644 (17508) 0x4644 (17639) 0x4647 (17639) 0x4647 (17639) 0x4647 (17639) 0x4550 (17744) 0x4555 (17747) 0x4553 (17747) | PTL b6 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 68 Echo (ping) reply 69 Echo (ping) reply 60 Echo (ping) | 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-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-5/1380, ttl=64 id-0x0012, seq-5/1380, ttl=64 id-0x0012, seq-5/1380, ttl=64 id-0x0012, seq-5/1380, ttl=64 id-0x0012, seq-5/1380, ttl=64 id-0x0012, seq-3/192, ttl=64 id-0x0012, seq-3/192, ttl=64 id-0x0012, seq-3/2048, ttl=64 id-0x001 |
| No. Time 1 2022-08-01 10:03:22.21239759 2 2022-08-01 10:03:23.232244769 4 4022-08-01 10:03:23.232244769 4 4022-08-01 10:03:23.232244769 5 202-08-01 10:03:24.2347953 5 202-08-01 10:03:25.2587249 7 202-08-01 10:03:25.2587249 9 202-08-01 10:03:25.2587249 9 202-08-01 10:03:25.2587249 9 202-08-01 10:03:26.28266183 11 2022-08-01 10:03:27.306671694 12 202-08-01 10:03:27.306671694 12 202-08-01 10:03:27.306745375 13 202-08-01 10:03:27.306745375 14 202-08-01 10:03:27.306745375 15 202-08-01 10:03:27.306745375 15 202-08-01 10:03:27.306745375 16 202-08-01 10:03:27.30674575 16 202-08-01 10:03:27.30674575 16 202-08-01 | Source 198, 51, 100, 100 198, 51, 100, 100 | Destination 192.0.2.100 192.0 | Protocol ICNP ICNP ICNP 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) 0x42f8 (17144) 0x43b3 (17331) 0x4454 (17502) 0x4454 (17502) 0x4454 (17503) 0x4464 (17508) 0x4464 (17508) 0x4464 (17639) 0x4467 (17639) 0x467 (17639) 0x467 (17749) 0x4559 (17744) 0x4559 (17747) 0x4597 (17815) | PTL 166 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 68 Echo (ping) reply 68 Echo (ping) reply 68 Echo (ping) reply 69 Echo (ping) reply 60 Echo (ping | id=0x0012, seq=1/256, tt]=64 id=0x0012, seq=1/256, tt]=64 id=0x0012, seq=2/512, tt]=64 id=0x0012, seq=2/512, tt]=64 id=0x0012, seq=3/768, tt]=64 id=0x0012, seq=4/1024, tt]=64 id=0x0012, seq=4/1024, tt]=64 id=0x0012, seq=5/1280, tt]=64 id=0x0012, seq=5/1280, tt]=64 id=0x0012, seq=5/1280, tt]=64 id=0x0012, seq=5/136, tt]=64 id=0x0012, seq=5/136, tt]=64 id=0x0012, seq=5/136, tt]=64 id=0x0012, seq=7/1792, tt]=64 id=0x0012, seq=3/2048, tt]=64 id=0x001 |
| Ho. Time 1 2022-08-01 10:03:22.231239759 2 2022-08-01 10:03:23.232247753 3 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:24.2347090751 7 2022-08-01 10:03:25.2586724861 9 2022-08-01 10:03:25.2586724861 9 2022-08-01 10:03:27.306671694 10 2022-08-01 10:03:27.306674787 10 2022-08-01 10:03:27.306674781 10 2022-08-01 10:03:27.306674781 12 2022-08-01 10:03:27.306674781 12 202-08-01 10:03:29.35495061 15 2022-08-01 10:03:29.3549507151 15 2022-08-01 10:03:29.354950761 17 2022-08-01 10:03:29.3549759311 16 2022-08-01 10:03:29.3549759311 16 2022-08-01 10:03:29.3549759311 17 202-08-01 10:03:29.3549759311 17<202- | Source 198, 51, 100, 100 198, 51, 100, 100 | Destruction 192, 0, 2, 100 192, 0, 2, 100 1 | Protocol ICMP | Length 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17144) 0x43b3 (17331) 0x43b5 (17502) 0x4456 (17502) 0x4456 (17503) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (1763) 0x467 (1763) 0x467 (17742) 0x4550 (17744) 0x4553 (17747) 0x4553 (17747) 0x4597 (17815) 0x4697 (17815) | PTL b6 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 67 Echo (ping) reply 68 Echo (ping) reply 68 Echo (ping) reply 69 Echo (ping) reply 60 Echo (ping) | id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=7/1256, ttl=64 id=0x0012, seq=7/512, ttl=64 id=0x0012, seq=7/512, ttl=64 id=0x0012, seq=4/768, 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=4/1124, ttl=64 id=0x0012, seq=4/2144, ttl=64 id=0 |
| No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.21239747 3 3022-08-01 10:03:22.23224750 4 2022-08-01 10:03:22.23224750 5 2022-08-01 10:03:24.234703961 6 2022-08-01 10:03:24.234703961 7 2022-08-01 10:03:25.258672496 9 2020-08-01 10:03:25.258672496 9 2020-08-01 10:03:26.232666183 11 2022-08-01 10:03:27.366674378 13 2022-08-01 10:03:27.36667164378 13 2022-08-01 10:03:28.3306667153 15 2022-08-01 10:03:28.330667153 16 202-08-01 10:03:03.738795171 16 202-08-01 10:03:03.738795172 16 202-08-01 10:03:03.738795172 18 202-08-01 10:03:03.738795172 18 202-08-01 10:03:03.738795172 18 202-08-01 10:03:03.738795172 2022-08-01 | Source 198, 51, 100, 100 198, 51, 100, 100 | Destination 192, 0, 2, 100 192, 0, 100 192, 0, 100 192, 0, 2, 100 192, 0, 2, 100 192, 0, | Protocol ICMP | Length 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x4305 (17331) 0x43b5 (17331) 0x4456 (17502) 0x4454 (17502) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x4550 (17744) 0x4555 (17747) 0x4597 (17815) 0x4677 (18042) | PTL b6 64 Echo (ping) reply 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 68 Echo (ping) reply 68 Echo (ping) reply 68 Echo (ping) reply 69 Echo (ping) reply 60 Echo (ping) | id-exe012, seq-1/256, ttl=64 id=exe012, seq-2/512, ttl=64 id=exe012, seq-2/512, ttl=64 id=exe012, seq-2/512, ttl=64 id=exe012, seq-3/768, ttl=64 id=exe012, seq-3/768, ttl=64 id=exe012, seq-4/1024, ttl=64 id=exe012, seq-5/1280, ttl=64 id=exe012, seq-5/1280, ttl=64 id=exe012, seq-5/136, ttl=64 id=exe012, seq-5/136, ttl=64 id=exe012, seq-5/136, ttl=64 id=exe012, seq-5/136, ttl=64 id=exe012, seq-5/136, ttl=64 id=exe012, seq-8/2048, ttt=64 id=exe012, |
| Ho. Time 1 2022-08-01 10:03:22.21239759 2 2032-08-01 10:03:23.232244769 4 4022-08-01 10:03:23.232244769 5 202-08-01 10:03:23.232244769 6 4022-08-01 10:03:24.2347930 5 202-08-01 10:03:25.2587249 7 202-08-01 10:03:25.2587249 9 202-08-01 10:03:25.2587249 9 202-08-01 10:03:26.28266163 11 2022-08-01 10:03:27.30667478 12 202-08-01 10:03:27.30667478 13 202-08-01 10:03:27.30667478 14 202-08-01 10:03:27.306574781 15 202-08-01 10:03:27.306574781 16 202-08-01 10:03:27.306574781 16 202-08-01 10:03:27.306574781 16 202-08-01 10:03:27.305795931 16 202-08-01 10:03:27.305795724 18 202-08-01 10:03:21.402774775 21 202-08-01 | Source 198, 51, 100, 100 198, 51, 100, 100 | Destination 192.0.2.100 192.0 | Protocol ICMP IC | Length 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x4395 (17144) 0x4395 (17141) 0x4395 (17582) 0x4456 (17582) 0x4454 (17588) 0x4464 (17588) 0x4464 (17589) 0x4467 (17589) 0x4467 (17639) 0x4467 (17639) 0x4675 (17744) 0x4555 (17747) 0x4555 (17747) 0x4557 (17815) 0x4677 (18042) 0x4676 (18042) | PTL b6 64 Echo (ping) reply 64 Echo (ping) reply | id-0x0012, seq-1/256, ttl=64 id-0x0012, seq-1/256, ttl=64 id-0x0012, seq-2/512, ttl=64 id-0x0012, seq-2/512, ttl=64 id-0x0012, seq-3/768, ttl=64 id-0x0012, seq-3/768, ttl=64 id-0x0012, seq-3/768, ttl=64 id-0x0012, seq-3/1280, ttl=64 id-0x0012, seq-3/1280, ttl=64 id-0x0012, seq-5/1280, ttl=64 id-0x0012, seq-5/2048, ttl=64 id-0x0012, seq-5/2048, ttl=64 id-0x0012, seq-5/2046, ttl=64 id-0x0012, seq-10/2560, ttl=64 id-0x0012, seq-10/2560, ttl=64 |
| Ho. Time 1 2022-08-01 10:03:22.231239759 2 2022-08-01 10:03:23.232247753 3 2022-08-01 10:03:23.232247753 5 202-08-01 10:03:23.232247753 5 202-08-01 10:03:24.23470981 6 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:27.306671641 10 202-08-01 10:03:27.306671641 12 2022-08-01 10:03:28.3306646775 13 2022-08-01 10:03:29.354959331 15 2022-08-01 10:03:29.354959331 16 2022-08-01 10:03:03.738952441 16 2022-08-01 10:03:03.7389594741 17 2022-08-01 10:03:03.7389594712 19 2022-08-01 10:03:03:14.042774775 10 2022-08-01 10:03:31.40274775 20 2022-08-01 10:03:31.402744755 10 | Source 198, 51, 100, 100 198, 51, 100, 100 | Destination 192.0.2.100 192.0 | Protocol ICMP IC | Length 108 1 108 1 1 | PD 0x42f8 (17144) 0x42f8 (17144) 0x43b3 (17331) 0x43b3 (17331) 0x445e (17502) 0x445e (17502) 0x4454 (17508) 0x44c4 (17508) 0x44c4 (17508) 0x44c4 (17639) 0x44c7 (17639) 0x44c7 (17639) 0x4556 (17744) 0x4555 (17744) 0x4555 (17747) 0x4557 (17741) 0x4597 (17815) 0x4597 (18042) 0x4632 (18058) | PTL b6 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 64 Echo (ping) reply | id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=7/256, 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=3/768, ttl=64 id=0x0012, seq=3/7128, ttl=64 id=0x0012, seq=3/7128, ttl=64 id=0x0012, seq=3/7128, ttl=64 id=0x0012, seq=3/7128, ttl=64 id=0x0012, seq=3/7138, ttl=64 id=0x0012, seq=3/7138, ttl=64 id=0x0012, seq=3/7192, ttl=64 id=0x0012, seq=3/7192, ttl=64 id=0x0012, seq=3/284, ttl=64 id=0x0012, seq=3/284, ttl=64 id=0x0012, seq=3/284, ttl=64 id=0x0012, seq=3/2184, ttl=64 id=0x0012, seq=3/2304, ttl=64 id=0x0012 |
| No. Time 1 2022-08-01 10:03:22.21237959 2 2022-08-01 10:03:23.232244769 4 4022-08-01 10:03:23.232244769 4 4022-08-01 10:03:23.232244769 5 602-08-01 10:03:24.242470391 5 602-08-01 10:03:25.25872490 7 7022-08-01 10:03:25.25872490 9 7022-08-01 10:03:25.25872490 9 7022-08-01 10:03:25.25872491 9 7022-08-01 10:03:27.306671694 12 7022-08-01 10:03:27.306671694 12 7022-08-01 10:03:27.306671694 12 7022-08-01 10:03:27.306771573 14 7022-08-01 10:03:27.306774578 16 7022-08-01 10:03:27.306774578 17 7022-08-01 10:03:27.324266995204 18 7022-08-01 10:03:27.2426697524 19 7022-08-01 10:03:27.2426697524 19 7022-08-01 10:03:27.2426697524 20 | Source 198, 51, 100, 100 198, 51, 100, 100 | Destruction 192.0.2.100 192.0 | Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP | Length 108 108 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x4305 (17144) 0x4305 (17141) 0x4350 (1731) 0x4452 (17502) 0x4454 (17508) 0x4454 (17508) 0x4454 (17508) 0x4454 (17508) 0x4454 (17508) 0x4454 (17508) 0x4454 (17508) 0x4455 (17744) 0x4555 (17744) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4572 (18042) 0x4674 (18058) 0x4684 (18058) | P TL b6 64 Echo (ping) reply 64 Echo (ping) reply | id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/52, 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 id=0x0012, seq=3/128, ttl=64 id=0x0012, seq=3/128, ttl=64 id=0x0012, seq=3/136, ttl=64 id=0x0012, seq=3/136, ttl=64 id=0x0012, seq=3/128, ttl=64 id=0x0012, seq=3/128, ttl=64 id=0x0012, seq=3/284, ttl=64 id=0x00 |
| No. Time 1 2022-08-01 10:03:22.21239759 2 2022-08-01 10:03:23.23224769 3 3022-08-01 10:03:23.232247753 5 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:24.2347096751 7 7022-08-01 10:03:25.2586724061 9 2022-08-01 10:03:25.2586724061 9 2022-08-01 10:03:27.306671694 12 2022-08-01 10:03:27.306674787 14 2022-08-01 10:03:27.306674787 14 2022-08-01 10:03:27.306574787 17 2022-08-01 10:03:27.306574787 18 2022-08-01 10:03:27.306574787 19 202-08-01 10:03:27.306574787 16 2022-08-01 10:03:27.30571644 19 2022-08-01 10:03:27.30571644 19 202-08-01 10:03:27.30571644 19 202-08-01 10:03:27.30571644 19 202-08-01 10:03:27.3057164478 19 <t< td=""><td>Source 198, 51, 100, 100 198, 51, 100, 100 198,</td><td>Destination 192.0.2.100 192.0</td><td>Protocol ICMP IC</td><td>Length 108 108 108 108 108 108 108 108 108 108</td><td>PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17144) 0x43b3 (17331) 0x43b5 (17502) 0x4456 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (1763) 0x4467 (1763) 0x467 (1763) 0x467 (1774) 0x4556 (17744) 0x4556 (17744) 0x4555 (17747) 0x4555 (17747) 0x4553 (17747) 0x4597 (17815) 0x4697 (18042) 0x468a (18042) 0x468a (18058) 0x468a (18058)</td><td>PTL b6 64 Echo (ping) reply 64 Echo (ping) reply</td><td>id-0x0012, seq-1/256, ttl=64 id-0x0012, seq-2/52, ttl=64 id-0x0012, seq-2/512, ttl=64 id-0x0012, seq-2/512, ttl=64 id-0x0012, seq-2/512, ttl=64 id-0x0012, seq-2/1024, ttl=64 id-0x0012, seq-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-3/1792, ttl=64 id-0x0012, seq-3/1792, ttl=64 id-0x0012, seq-3/1792, ttl=64 id-0x0012, seq-3/1792, ttl=64 id-0x0012, seq-3/1920, ttl=64 id-0x0012, seq-3/2040, ttl=64 id-0x0012, seq-10/2560, ttl=64 id-0x0012, seq-11/2816, ttl=64</td></t<> | Source 198, 51, 100, 100 198, | Destination 192.0.2.100 192.0 | Protocol ICMP IC | Length 108 108 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17144) 0x43b3 (17331) 0x43b5 (17502) 0x4456 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (1763) 0x4467 (1763) 0x467 (1763) 0x467 (1774) 0x4556 (17744) 0x4556 (17744) 0x4555 (17747) 0x4555 (17747) 0x4553 (17747) 0x4597 (17815) 0x4697 (18042) 0x468a (18042) 0x468a (18058) 0x468a (18058) | PTL b6 64 Echo (ping) reply 64 Echo (ping) reply | id-0x0012, seq-1/256, ttl=64 id-0x0012, seq-2/52, ttl=64 id-0x0012, seq-2/512, ttl=64 id-0x0012, seq-2/512, ttl=64 id-0x0012, seq-2/512, ttl=64 id-0x0012, seq-2/1024, ttl=64 id-0x0012, seq-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-3/1792, ttl=64 id-0x0012, seq-3/1792, ttl=64 id-0x0012, seq-3/1792, ttl=64 id-0x0012, seq-3/1792, ttl=64 id-0x0012, seq-3/1920, ttl=64 id-0x0012, seq-3/2040, ttl=64 id-0x0012, seq-10/2560, ttl=64 id-0x0012, seq-11/2816, ttl=64 |
| Ho. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 3 3022-08-01 10:03:22.231237753 5 2022-08-01 10:03:22.232247753 5 2022-08-01 10:03:22.232247753 5 2022-08-01 10:03:22.232247753 7 2022-08-01 10:03:25.258572406 9 2022-08-01 10:03:25.258572406 9 2022-08-01 10:03:27.3066716378 11 2022-08-01 10:03:27.3066743778 12 2022-08-01 10:03:27.3066743778 13 2022-08-01 10:03:27.3065716417 14 2022-08-01 10:03:27.3065745731 16 2022-08-01 10:03:27.3065716417 17 202-08-01 10:03:27.30559511 16 2022-08-01 10:03:31.3037959224 18 2022-08-01 10:03:31.402772217 20 202-08-01 10:03:32.426693254 22 2022-08-01 10:03:32.426695591 2 722-08-01 10:03:32.426695591 2 722-08-01 10:03:32.426695591 | Source 198.51,100.100 198.51 | Destination 192.0.2.100 192.0 | Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP | Length 108 108 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x4305 (1731) 0x4305 (1731) 0x4356 (17502) 0x4454 (17508) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17503) 0x4467 (17503) 0x4467 (17639) 0x4457 (17639) 0x4457 (17744) 0x4555 (17744) 0x4557 (17744) 0x4557 (17745) 0x4597 (17815) 0x4597 (17815) 0x4673 (18042) 0x468a (18058) 0x468a (18058) | PTL b6 64 Echo (ping) reply 64 Echo (ping) reply | id=0x0012, seq=1/256, tt]=64 id=0x0012, seq=2/512, tt]=64 id=0x0012, seq=2/512, tt]=64 id=0x0012, seq=2/512, tt]=64 id=0x0012, seq=4/1024, tt]=64 id=0x0012, seq=4/1024, tt]=64 id=0x0012, seq=4/1024, tt]=64 id=0x0012, seq=4/136, tt]=64 id=0x0012, seq=4/136, tt]=64 id=0x0012, seq=4/136, tt]=64 id=0x0012, seq=4/136, tt]=64 id=0x0012, seq=4/136, tt]=64 id=0x0012, seq=4/136, tt]=64 id=0x0012, seq=3/2048, tt]=64 id=0x0012, seq=3/2166, tt]=64 id=0x0012, seq=11/2816, tt]=64 id=0x0012, seq=11/2816, tt]=64 id=0x0012, seq=11/2816, tt]=64 id=0x0012, seq=11/2816, tt]=64 id=0x0012, seq=11/2816, tt]=64 id=0x0012, seq=11/2816, tt]=64 00 00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00fr = -TB |
| <pre>Hb. Time 1 2022-08-01 10:03;22.21123759 2 2032-08-01 10:01;32.221123759 2 2032-08-01 10:03;23.232244769 4 4022-08-01 10:03;23.232244769 4 4022-08-01 10:03;23.232244769 5 2022-08-01 10:03;24.2347090751 7 7022-08-01 10:03;25.2586724861 9 2032-08-01 10:03;25.2586724861 9 2032-08-01 10:03;26.28266168 11 2022-08-01 10:03;26.28266168 11 2022-08-01 10:03;26.28266168 11 2022-08-01 10:03;27.30667478 13 3022-08-01 10:03;27.30657159 13 42022-08-01 10:03;27.30657159 14 2022-08-01 10:03;20.378795931 16 2032-08-01 10:03;20.378795284 18 4022-08-01 10:03;20.378795284 18 4022-08-01 10:03;21.40272217 20 2022-08-01 10:03;21.402724775 21 2022-08-01 10:03;21.402724775 22 2022-08-01 10:03;21.402724775 22 2022-08-01 10:03;21.402695691 </pre> | Source 198, 51, 100, 100 198, | Destruction 192.0.2.100 192.0 | Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP | Length 108 108 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17144) 0x4395 (1752) 0x4395 (1752) 0x445e (17502) 0x445e (17502) 0x4462 (17508) 0x4462 (17603) 0x4462 (17603) 0x4467 (1763) 0x467 (1763) 0x467 (1763) 0x4673 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4568 (18042) 0x468a (18058) 0x468a (18058) | PTL b6 64 Echo (ping) reply 64 Echo (ping) reply | id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/7128, ttl=64 id=0x0012, seq=3/7128, ttl=64 id=0x0012, seq=3/7192, 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=13/2560, ttl=64 id=0x0012, seq=13/266, ttl=64 id=0x0012, seq=3/266, dt |
| No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.21239747 3 3022-08-01 10:03:22.23224759 5 2022-08-01 10:03:22.23224759 5 2022-08-01 10:03:22.23224759 7 2022-08-01 10:03:22.23224759 8 2022-08-01 10:03:25.25857240 9 202-08-01 10:03:25.25857240 9 202-08-01 10:03:25.25857240 9 202-08-01 10:03:25.25857240 9 202-08-01 10:03:27.36657604 9 202-08-01 10:03:27.3665764378 11 2022-08-01 10:03:28.330664753 12 2022-08-01 10:03:28.33066755331 14 2022-08-01 10:03:28.33066755331 15 2022-08-01 10:03:28.3306675531 16 2022-08-01 10:03:28.3306675531 17 2022-08-01 10:03:28.3306675531 18 2022-08-01 10:03:28.3306675531 19 202-08-01 10:03:28.3306675531 19 202-08-01 10:03:28.33066755931 10 20:28-08-01 10:03:28.3306675531 20 202-08-01 10:03:31.4027757752 <t< td=""><td>Source 198.51,100.100 198.51</td><td>Destination 192.0.2.100 192.0</td><td>Protect ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP</td><td>Length 108 108 108 108 108 108 108 108 108 108</td><td>PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (1734) 0x43b3 (17331) 0x445e (17502) 0x445e (17502) 0x4464 (17508) 0x44c3 (17603) 0x44c4 (17603) 0x44c4 (17639) 0x44c7 (17639) 0x44c7 (17639) 0x4556 (17744) 0x4556 (17744) 0x4555 (17747) 0x4557 (17845) 0x4577 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058)</td><td>PTL b6 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 68 Echo (ping) reply 69 Echo (ping) reply 60 Echo (ping)</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=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/108, 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=3/236, ttl=64 id=0x0012, seq=3/248, ttl=64 id=0x0012, seq=3/236, ttl=64 id=0x0012, seq=3/248, 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 | Protect ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP | Length 108 108 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (1734) 0x43b3 (17331) 0x445e (17502) 0x445e (17502) 0x4464 (17508) 0x44c3 (17603) 0x44c4 (17603) 0x44c4 (17639) 0x44c7 (17639) 0x44c7 (17639) 0x4556 (17744) 0x4556 (17744) 0x4555 (17747) 0x4557 (17845) 0x4577 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058) | PTL b6 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 68 Echo (ping) reply 69 Echo (ping) reply 60 Echo (ping) | 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 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/108, 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=3/236, ttl=64 id=0x0012, seq=3/248, ttl=64 id=0x0012, seq=3/236, ttl=64 id=0x0012, seq=3/248, ttl=64 id=0x0012, seq=11/2816, ttl=64 |
| Hb. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:23.232244769 4 4022-08-01 10:03:23.232244769 4 4022-08-01 10:03:23.232244769 5 202-08-01 10:03:23.232244769 6 2022-08-01 10:03:23.232244769 7 202-08-01 10:03:23.232244753 5 202-08-01 10:03:25.2586724861 9 202-08-01 10:03:25.2586724861 9 202-08-01 10:03:27.306671694 12 2022-08-01 10:03:27.306671694 12 202-08-01 10:03:27.306671694 12 202-08-01 10:03:27.306671694 12 202-08-01 10:03:27.30674378 16 202-08-01 10:03:27.30674378 16 202-08-01 10:03:27.30674378 16 202-08-01 10:03:27.30674378 16 202-08-01 10:03:27.426693501 17 202-08-01 10:03:27.42669524 2 2022-08-01 | Source 198.51,100.100 198.51 | Destruction 192.0.2.100 192.0 | Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP | Length 108 108 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x4305 (17144) 0x4305 (17141) 0x4356 (17502) 0x4456 (17502) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x467 (17639) 0x4555 (17744) 0x4553 (17747) 0x4553 (17747) 0x4597 (17815) 0x4597 (17815) 0x4674 (18042) 0x4668 (18058) 0x4668 (18058) | PTL b6 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 68 Echo (ping) reply 68 Echo (ping) reply 69 Echo (ping) reply 60 Echo (ping) reply 60 Echo (ping) reply 60 Echo (ping) reply 60 Echo (ping) | id-0x0012, seq-1/256, ttl=64 id-0x0012, seq-2/52, 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 id-0x0012, seq-3/768, ttl=64 id-0x0012, seq-3/7128, ttl=64 id-0x0012, seq-5/1280, ttl=64 id-0x0012, seq-5/2048, ttl=64 id-0x0012, seq-5/2048, ttl=64 id-0x0012, seq-5/2048, ttl=64 id-0x0012, seq-5/2048, ttl=64 id-0x0012, seq-13/216, ttl=64 id-0x0012, seq-13/216, ttl=64 id-0x0012, seq-11/2816, ttl=10, ttl=10, ttl=10, ttl=10, ttl=10 |
| No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 3 202-08-01 10:03:22.231237959 3 202-08-01 10:03:22.231237959 4 2022-08-01 10:03:24.234703981 6 2022-08-01 10:03:24.234703981 6 2022-08-01 10:03:25.258672409 9 2022-08-01 10:03:25.2586724061 9 2022-08-01 10:03:25.2586724061 9 2022-08-01 10:03:27.306671604 10 2022-08-01 10:03:27.306671641 11 2022-08-01 10:03:27.366767153 15 2022-08-01 10:03:27.3549367061 16 2022-08-01 10:03:27.35493670531 16 2022-08-01 10:03:27.35493670531 17 2022-08-01 10:03:27.35493670531 18 2022-08-01 10:03:27.345493704 18 2022-08-01 10:03:27.3454936704 19 2022-08-01 10:03:27.345493704 18 2022-08-01 10:03:27.345493724 20 202-08-01 10:03:27.426693254 22 2022-08-01 10:03:27.426693254 22 2022-08-01 10:03:27.426695691 <tr< td=""><td>Source 198.51.100.100 198.51</td><td>Destruction 192.0.2.100 192.0</td><td>Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP</td><td>Length 108 108 108 108 108 108 108 108 108 108</td><td>PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17144) 0x4395 (1752) 0x4395 (1752) 0x4456 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (1763) 0x467 (1763) 0x467 (1763) 0x467 (17747) 0x4553 (17747) 0x4553 (17747) 0x4597 (17815) 0x4697 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058) 0x468a (18058)</td><td>PTL b6 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 68 Echo (ping) reply 68 Echo (ping) reply 69 Echo (ping) reply 60 Echo (ping)</td><td>id=0x0012, seq=1/256, tt]=64 id=0x0012, seq=7/1256, tt]=64 id=0x0012, seq=7/512, tt]=64 id=0x0012, seq=7/102, tt]=64 id=0x0012, seq=7/1024, tt]=64 id=0x0012, seq=7/2048, tt]=64 id=0x0012, seq=7/2048, tt]=64 id=0x0012, seq=10/2560, tt]=64 id=0x0012, seq=11/2816, tt]=64 id=0x0012, seq=112</td></tr<> | Source 198.51.100.100 198.51 | Destruction 192.0.2.100 192.0 | Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP | Length 108 108 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17144) 0x4395 (1752) 0x4395 (1752) 0x4456 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (1763) 0x467 (1763) 0x467 (1763) 0x467 (17747) 0x4553 (17747) 0x4553 (17747) 0x4597 (17815) 0x4697 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058) 0x468a (18058) | PTL b6 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 68 Echo (ping) reply 68 Echo (ping) reply 69 Echo (ping) reply 60 Echo (ping) | id=0x0012, seq=1/256, tt]=64 id=0x0012, seq=7/1256, tt]=64 id=0x0012, seq=7/512, tt]=64 id=0x0012, seq=7/102, tt]=64 id=0x0012, seq=7/1024, tt]=64 id=0x0012, seq=7/2048, tt]=64 id=0x0012, seq=7/2048, tt]=64 id=0x0012, seq=10/2560, tt]=64 id=0x0012, seq=11/2816, tt]=64 id=0x0012, seq=112 |
| No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 3 3022-08-01 10:03:22.231237753 5 2022-08-01 10:03:22.232247753 5 2022-08-01 10:03:22.232247753 5 2022-08-01 10:03:22.232247753 7 2022-08-01 10:03:22.232247753 8 2022-08-01 10:03:25.2585724061 9 2022-08-01 10:03:25.2585724061 9 2022-08-01 10:03:27.3066716378 11 2022-08-01 10:03:27.306674378 12 2022-08-01 10:03:27.306571641 12 2022-08-01 10:03:27.306571641 12 2022-08-01 10:03:27.306571641 12 2022-08-01 10:03:27.306571641 14 2022-08-01 10:03:379.35935704 16 2022-08-01 10:03:31.402772217 20 202-08-01 10:03:32.426695691 20 202-08-01 10:03:32.426695691 20 202-08-01 10:03:32.426695691 20 202-08-01 10:03:32.426695691 20 202-08-01 10:03:32.426695691 20 202-08-01 10:03:32.426695691 | Source 198.51.100.100 198.51 | Destruction 192.0.2.100 192.0 | Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP | Length 108 108 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x4305 (1731) 0x4305 (1731) 0x4364 (17502) 0x4454 (17502) 0x4464 (17508) 0x4464 (17508) 0x4462 (17503) 0x4467 (17539) 0x4467 (17639) 0x4467 (17639) 0x4673 (17744) 0x4553 (17744) 0x4553 (17744) 0x4557 (17815) 0x4677 (18042) 0x4678 (18058) 0x468a (18058) 0x468a (18058) | PTL b6 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 68 Echo (ping) reply 69 Echo (ping) reply 60 Echo (ping) | id-exx012, seq-1/256, tt]=64 id-exx012, seq-2/512, tt]=64 id-exx012, seq-2/512, tt]=64 id-exx012, seq-2/512, tt]=64 id-exx012, seq-3/768, tt]=64 id-exx012, seq-4/1024, tt]=64 id-exx012, seq-4/2046, tt]=64 id-exx012, seq-4/2046, tt]=64 id-exx012, seq-4/2046, tt]=64 id-exx012, seq-4/2046, tt]=64 id-exx012, seq-11/2816, tt]=64 id-exx012, seq-11, seq-11, seq-11, seq-11, seq-11, seq- |
| Hb. Time 1 2022-08-01 10:03:22.21239759 2 2022-08-01 10:03:23.232244769 4 4022-08-01 10:03:23.232244769 4 4022-08-01 10:03:23.232244769 5 202-08-01 10:03:23.232244769 6 4022-08-01 10:03:23.232244769 7 202-08-01 10:03:25.2587240 9 202-08-01 10:03:25.258724861 9 202-08-01 10:03:26.282666183 11 202-08-01 10:03:27.306674781 12 202-08-01 10:03:27.306674781 13 202-08-01 10:03:27.306674781 14 202-08-01 10:03:20.378959131 16 202-08-01 10:03:20.378795172 19 202-08-01 10:03:21.402772177 21 202-08-01 10:03:21.402774775 21 202-08-01 10:03:21.426695691 | Source 198.51.100.100 198.51 | Destruction 192.0.2.100 192.0 | Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP | Length 108 108 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17144) 0x4395 (1752) 0x4395 (1752) 0x4456 (17502) 0x4456 (17503) 0x4462 (17603) 0x4462 (17603) 0x4467 (1763) 0x4467 (1763) 0x4467 (1763) 0x4672 (17744) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4573 (18042) 0x4668 (18058) 0x4668 (18058) | PTL b6 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=2/5128, ttl=64 1d=0x0012, seq=2/2048, ttl=64 1d=0x0012, seq=2/2048, ttl=64 1d=0x0012, seq=2/2048, ttl=64 1d=0x0012, seq=2/2048, ttl=64 1d=0x0012, seq=1/2560, ttl=64 1d=0x0012, seq=1/2816, ttl=64 1d=0x0012, seq=1/2816, ttl=64 1d=0x0012, seq=1/1/2816, ttl=64 |
| No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.212329747 3 3022-08-01 10:03:22.23224759 4 2022-08-01 10:03:22.23224753 5 2022-08-01 10:03:24.23470396 7 2022-08-01 10:03:25.25867240 8 2022-08-01 10:03:25.25867240 9 202-08-01 10:03:25.25867240 9 202-08-01 10:03:25.25867240 9 202-08-01 10:03:25.25867240 9 202-08-01 10:03:26.232666183 11 2022-08-01 10:03:27.36674074 13 2022-08-01 10:03:28.330667153 14 2022-08-01 10:03:28.330667153 15 2022-08-01 10:03:12.42569311 16 202-08-01 10:03:13.037879172 16 202-08-01 10:03:11.402727217 20 202-08-01 10:03:12.426693254 12 2022-08-01 10:03:12.426693254 22 2022-08-01 10:03:32.426695691 20 702-08-01 10:03:32.426695591 20 702-08-01 10:03:32.426695591 20 702-08-01 10:03:32.426695591 20 702-08-01 </td <td>Source 198.51,100.100 198.51</td> <td>Destination 192.0.2.100 192.0</td> <td>Protect ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP</td> <td>Length 108 108 108 108 108 108 108 108</td> <td>PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17141) 0x43b3 (17331) 0x43b5 (17502) 0x4454 (17502) 0x4454 (17508) 0x4464 (17508) 0x4464 (17608) 0x4467 (17639) 0x4467 (17639) 0x467 (17639) 0x467 (17747) 0x4555 (17747) 0x4555 (17747) 0x4557 (17842) 0x4682 (18058) 0x468a (18058) 0x468a (18058) 0x468a (18058)</td> <td>PTL b6 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 68 Echo (ping) reply 68 Echo (ping) reply 69 Echo (ping) reply 60 Echo (ping)</td> <td>id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=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 id=0x0012, seq=3/108, ttl=64 id=0x0012, seq=3/128, 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=10/2560, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x00012, seq=11/2816, ttl=64</td> | Source 198.51,100.100 198.51 | Destination 192.0.2.100 192.0 | Protect ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP | Length 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17141) 0x43b3 (17331) 0x43b5 (17502) 0x4454 (17502) 0x4454 (17508) 0x4464 (17508) 0x4464 (17608) 0x4467 (17639) 0x4467 (17639) 0x467 (17639) 0x467 (17747) 0x4555 (17747) 0x4555 (17747) 0x4557 (17842) 0x4682 (18058) 0x468a (18058) 0x468a (18058) 0x468a (18058) | PTL b6 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 68 Echo (ping) reply 68 Echo (ping) reply 69 Echo (ping) reply 60 Echo (ping) | id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=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 id=0x0012, seq=3/108, ttl=64 id=0x0012, seq=3/128, 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=10/2560, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x00012, seq=11/2816, ttl=64 |
| K. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:23.232244769 4 4022-08-01 10:03:23.232244769 4 4022-08-01 10:03:23.232244769 5 5022-08-01 10:03:23.232244769 6 602-08-01 10:03:23.232244769 7 022-08-01 10:03:25.258724801 9 020-08-01 10:03:25.258724861 9 020-08-01 10:03:27.306671694 12 2022-08-01 10:03:27.306671694 12 1202-08-01 10:03:27.306671694 12 1202-08-01 10:03:27.306671694 12 2022-08-01 10:03:27.30674378 16 020-08-01 10:03:27.30674378 16 020-08-01 10:03:27.30674378 16 020-08-01 10:03:27.30674378 16 020-08-01 10:03:27.30674378 16 020-08-01 10:03:27.426693501 16 020-08-01 10:03:27.426693242 2 2022-08-01 | Source 198.51.100.100 198.51 | Destruction 192.0.2.100 192.0 | Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP | Length 108 108 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x4305 (17144) 0x4305 (17141) 0x4356 (17502) 0x4456 (17502) 0x4456 (17503) 0x4467 (17503) 0x4467 (17633) 0x4467 (17633) 0x4467 (17639) 0x4556 (17744) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4597 (17815) 0x4597 (17815) 0x4674 (18042) 0x4668 (18058) 0x4668 (18058) | PTL b6 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 68 Echo (ping) reply 69 Echo (ping) reply 60 Echo (ping) | id-exx012, seq-1/256, ttl=64 id-exx012, seq-2/52, ttl=64 id-exx012, seq-2/512, ttl=64 id-exx012, seq-2/512, ttl=64 id-exx012, seq-3/768, ttl=64 id-exx012, seq-4/1024, ttl=64 id-exx012, seq-4/1024, ttl=64 id-exx012, seq-5/1280, ttl=64 id-exx012, seq-6/1536, ttl=64 id-exx012, seq-6/1536, ttl=64 id-exx012, seq-6/1536, ttl=64 id-exx012, seq-6/1536, ttl=64 id-exx012, seq-6/1536, ttl=64 id-exx012, seq-7/1722, ttl=64 id-exx012, seq-7/1722, ttl=64 id-exx012, seq-8/2048, ttl=64 id-exx012, seq-9/2040, ttl=64 id-exx012, seq-9/2040, ttl=64 id-exx012, seq-9/2104, ttl=64 id-exx012, seq-9/2104, ttl=64 id-exx012, seq-11/2816, |
| No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 3 202-08-01 10:03:22.231237959 4 2022-08-01 10:03:22.231237959 5 2022-08-01 10:03:24.234703981 6 4 2022-08-01 10:03:24.234703981 6 4 2022-08-01 10:03:25.258672406 9 2022-08-01 10:03:25.258672406 9 2022-08-01 10:03:25.258672406 9 2022-08-01 10:03:25.258672406 9 2022-08-01 10:03:27.36667163 11 2022-08-01 10:03:27.36667164 12 2022-08-01 10:03:27.36667153 13 2022-08-01 10:03:27.354935706 14 2022-08-01 10:03:27.3549357031 16 622-08-01 10:03:27.354935704 18 2022-08-01 10:03:21.40277757 20 202-08-01 10:03:21.4027803752 18 2022-08-01 10:03:21.402780375 19 2022-08-01 10:03:21.402780375 20 202-08-01 10:03:21.402780375 21 2022-08-01 10:03:21.426693254 22 2022-08-01 10:03:21.2426695691 | Source 198.51.100.100 198.51 | Destruction 192.0.2.100 192.0 | Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP | Length 108 108 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17144) 0x4395 (17502) 0x43b6 (17502) 0x4456 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17603) 0x4467 (1763) 0x467 (1763) 0x467 (1763) 0x467 (17747) 0x4555 (17744) 0x4553 (17747) 0x4597 (17815) 0x4597 (17815) 0x4682 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058) 0x468a (18058) | PTL b6 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 68 Echo (ping) reply 68 Echo (ping) reply 69 Echo (ping) reply 60 Echo (ping) | 10-0x0012, seq-1/256, ttl=64 10-0x0012, seq-2/512, ttl=64 10-0x0012, seq-2/512, ttl=64 10-0x0012, seq-3/766, ttl=64 10-0x0012, seq-3/7102, ttl=64 10-0x0012, seq-3/7128, ttl=64 10-0x0012, seq-3/7129, ttl=64 10-0x0012, seq-10/7560, ttl=64 10-0x0012, seq-11/2816, ttl |
| K. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 3 3022-08-01 10:03:22.232247753 5 2022-08-01 10:03:24.232247753 5 2022-08-01 10:03:24.2324709 8 2022-08-01 10:03:24.23247953 7 2022-08-01 10:03:25.2585724061 9 2022-08-01 10:03:25.2585724061 9 2022-08-01 10:03:25.2585724061 9 2022-08-01 10:03:25.2585724061 9 2022-08-01 10:03:25.2585724061 12 2022-08-01 10:03:27.3066716378 13 2022-08-01 10:03:27.306674378 13 2022-08-01 10:03:27.306674378 13 2022-08-01 10:03:27.306571641 16 2022-08-01 10:03:27.306571641 17 2022-08-01 10:03:27.306571641 18 2022-08-01 10:03:20.373798172 19 2022-08-01 10:03:20.4266935931 16 2022-08-01 10:03:20.426695591 17 2022-08-01 10:03:21.426695591 18 2022-08-01 10:03:21.426695591 20 2022-08-01 10:03:2.426695591 20 2022-08-01 10:03:2.426695591 20 2022-08-01 10:03:2.426695591 20 2022-08-01 10:03:2.426695591 20 2022-08-01 10:03:2.426695591 20 2022-08-01 10:03:2.426695591 21 2022-08-01 10:03:2.426695591 </td <td>Source 198.51.100.100 198.51</td> <td>Destruction 192.0.2.100 192.0</td> <td>Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP</td> <td>Length 108 108 108 108 108 108 108 108 108 108</td> <td>PD 0x42f8 (17144) 0x42f8 (17144) 0x4305 (17141) 0x4305 (17502) 0x445e (17502) 0x445e (17503) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4674 (17639) 0x46753 (17744) 0x4553 (17744) 0x4553 (17744) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4577 (18042) 0x4674 (18058) 0x468a (18058) 0x468a (18058)</td> <td>PTL b6 64 Echo (ping) reply 64 Echo (ping)</td> <td>id-exx012, seq-1/256, tt]=64 id-exx012, seq-2/52, tt]=64 id-exx012, seq-2/512, tt]=64 id-exx012, seq-3/768, tt]=64 id-exx012, seq-3/768, tt]=64 id-exx012, seq-4/1024, tt]=64 id-exx012, seq-4/1026, tt]=64 id-exx012, seq-4/1026, tt]=64 id-exx012, seq-4/2046, tt]=64 id-exx012, seq-4/2046, tt]=64 id-exx012, seq-4/2046, tt]=64 id-exx012, seq-4/2046, tt]=64 id-exx012, seq-14/2816, tt]=64 id-exx012, seq-11/2816, tt]=64 id-exx012, seq-11/2816</td> | Source 198.51.100.100 198.51 | Destruction 192.0.2.100 192.0 | Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP | Length 108 108 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x4305 (17141) 0x4305 (17502) 0x445e (17502) 0x445e (17503) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4674 (17639) 0x46753 (17744) 0x4553 (17744) 0x4553 (17744) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4577 (18042) 0x4674 (18058) 0x468a (18058) 0x468a (18058) | PTL b6 64 Echo (ping) reply 64 Echo (ping) | id-exx012, seq-1/256, tt]=64 id-exx012, seq-2/52, tt]=64 id-exx012, seq-2/512, tt]=64 id-exx012, seq-3/768, tt]=64 id-exx012, seq-3/768, tt]=64 id-exx012, seq-4/1024, tt]=64 id-exx012, seq-4/1026, tt]=64 id-exx012, seq-4/1026, tt]=64 id-exx012, seq-4/2046, tt]=64 id-exx012, seq-4/2046, tt]=64 id-exx012, seq-4/2046, tt]=64 id-exx012, seq-4/2046, tt]=64 id-exx012, seq-14/2816, tt]=64 id-exx012, seq-11/2816, tt]=64 id-exx012, seq-11/2816 |
| K. Time 1 2022-08-01 10:03:22.231239759 2 2022-08-01 10:03:22.231239759 2 3022-08-01 10:03:22.231239759 3 302-08-01 10:03:22.231239759 4 3022-08-01 10:03:22.2324759 5 2022-08-01 10:03:24.234703981 6 7022-08-01 10:03:24.23470551 7 7022-08-01 10:03:25.258672406 9 7022-08-01 10:03:25.258672406 9 7022-08-01 10:03:25.258672406 10 7022-08-01 10:03:25.258672406 10 7022-08-01 10:03:27.306671604 12 7022-08-01 10:03:27.306671604 13 7022-08-01 10:03:27.306671604 14 7022-08-01 10:03:29.554936706 17 7022-08-01 10:03:12,9.3549936706 17 7022-08-01 10:03:13,403779572217 2 7022-08-01 10:03:13,40277775 2 7022-08-01 10:03:13,40272217 2 7022-08-01 10:03:13,40272217 2 7022-08-01 10:03:13,40274775 2 7022-08-01 10:03:13,40274775 2 7022-08-01 10:03:13,40274775 2 7022-08-01 10:03:13,40274775 2 7022-08-01 10:03:13,40274775 2 7022-08-01 10:03:13,40274775 2 7022-08-01 10:03:13,40274775 2 7022-08-01 10:03:13,40274775 2 7022-08-01 10:03:13,4027669501 | Source 198.51.100.100 198.51 | Destruction 192.0.2.100 192.0 | Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP | Length 108 108 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17144) 0x4395 (1752) 0x4356 (1752) 0x4456 (17502) 0x4456 (17503) 0x4462 (17633) 0x4462 (17633) 0x4467 (17633) 0x4467 (17633) 0x4467 (17633) 0x44553 (17744) 0x4553 (17744) 0x4553 (17744) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4568 (18042) 0x468a (18058) 0x468a (18058) | PTL b6 64 Echo (ping) reply 64 Echo (ping) reply | 10-0x0012, seq-1/256, ttl-64 10-0x0012, seq-2/512, ttl-64 10-0x0012, seq-2/512, ttl-64 10-0x0012, seq-2/512, ttl-64 10-0x0012, seq-2/512, ttl-64 10-0x0012, seq-3/768, ttl-64 10-0x0012, seq-3/768, ttl-64 10-0x0012, seq-3/1024, ttl-64 10-0x0012, seq-3/2045, ttl-64 10-0x0012, seq-11/2816, |
| Ko. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 3 3022-08-01 10:03:22.232247753 5 2022-08-01 10:03:24.23240769 7 2022-08-01 10:03:24.23240753 5 2022-08-01 10:03:24.23240769 8 7022-08-01 10:03:25.25867240 9 7022-08-01 10:03:25.25867240 9 7022-08-01 10:03:25.25867240 9 7022-08-01 10:03:26.282666183 11 7022-08-01 10:03:27.30667160 12 2022-08-01 10:03:27.30657160 14 2022-08-01 10:03:28.330667137 15 2022-08-01 10:03:28.330667137 16 2022-08-01 10:03:28.330667137 17 202-08-01 10:03:27.30571604 18 2022-08-01 10:03:28.330667152 2 2022-08-01 10:03:32.426693254 2 2 2022-08-01 10:03:32.426695691 VH-Tag | Source 198.51.100.100 198.51 | Destination 192.0.2.100 192.0 | Protocol ICMP | Length 108 108 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x4305 (1731) 0x4305 (1731) 0x4364 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17509) 0x4455 (17744) 0x4555 (17744) 0x4557 (17744) 0x4557 (17744) 0x4597 (17815) 0x4677 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058) | PTL b6 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 68 Echo (ping) reply 69 Echo (ping) reply 60 Echo (ping) | id=0x0012, seq=1/256, tl=64 id=0x0012, seq=2/512, tl=64 id=0x0012, seq=2/512, tl=64 id=0x0012, seq=2/512, tl=64 id=0x0012, seq=3/768, tl=64 id=0x0012, seq=4/1024, tl=64 id=0x0012, seq=4/1024, tl=64 id=0x0012, seq=4/136, tl=64 id=0x0012, seq=4/136, tl=64 id=0x0012, seq=4/136, tl=64 id=0x0012, seq=4/136, tl=64 id=0x0012, seq=4/136, tl=64 id=0x0012, seq=3/2304, tl=64 id=0x0012, seq=13/2816, tl=64 id=0x0012, seq=11/2816, tl=6 |
| <pre>No. Trme 1 2022-08-01 10:03:22.21237959 2 2022-08-01 10:03:22.21239747 3 2022-08-01 10:03:23.232244769 4 4022-08-01 10:03:23.232244769 4 4022-08-01 10:03:23.232244769 6 2022-08-01 10:03:25.258672480 8 2022-08-01 10:03:25.258672480 9 2022-08-01 10:03:25.258672481 1 2022-08-01 10:03:25.258672481 1 2022-08-01 10:03:27.306674378 13 2022-08-01 10:03:27.306674378 13 2022-08-01 10:03:27.306674378 13 2022-08-01 10:03:27.306674378 13 2022-08-01 10:03:27.306674378 13 2022-08-01 10:03:27.30674378 13 2022-08-01 10:03:27.30674378 13 2022-08-01 10:03:27.30674378 13 2022-08-01 10:03:27.30674378 13 2022-08-01 10:03:27.32674775 22 2022-08-01 10:03:21.40277217 20 2022-08-01 10:03:21.4027724775 22 2022-08-01 10:03:22.426695691 </pre> | Source 198.51.100.100 198.51 | Destruction 192.0.2.100 192.0 | Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP | Length 108 108 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17144) 0x4395 (1752) 0x4356 (1752) 0x4456 (17502) 0x4456 (17503) 0x4462 (17633) 0x4467 (17633) 0x4467 (17633) 0x4467 (17633) 0x4467 (17633) 0x4672 (17744) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4573 (18042) 0x4668 (18058) 0x4668 (18058) | PTL b6 64 Echo (ping) reply 64 Echo (ping) reply | 10 00 50 55 50 <td< td=""></td<> |
| Ko. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 3 3022-08-01 10:03:22.232247753 5 3022-08-01 10:03:22.232247753 5 3022-08-01 10:03:22.232247753 7 2022-08-01 10:03:22.232247753 7 2022-08-01 10:03:22.232247753 9 2022-08-01 10:03:22.23224769 9 2022-08-01 10:03:25.258572404 9 2022-08-01 10:03:25.258572404 9 2022-08-01 10:03:25.258572404 12 2022-08-01 10:03:27.306671604 12 2022-08-01 10:03:27.306671647378 13 2022-08-01 10:03:28.3306674378 14 2022-08-01 10:03:28.3306674378 15 2022-08-01 10:03:28.330667153 16 2022-08-01 10:03:28.330667153 17 2022-08-01 10:03:28.330667153 18 2022-08-01 10:03:11.402727217 2 2022-08-01 10:03:13.40272217 2 2022-08-01 10:03:13.40272217 2 2022-08-01 10:03:13.40274752 2 2022-08-01 10:03:13.40274752 2 7 2022-08-01 10:03:13.40274752 2 7 2022-08-01 10:03:13.40274752 9 0 | Source 198.51.100.100 198.51 | Destination 192.0.2.100 192.0 | Protect ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP | Length 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17144) 0x43b3 (1731) 0x43b3 (1731) 0x43b3 (1752) 0x4454 (17502) 0x4464 (17508) 0x4464 (17603) 0x4467 (1763) 0x4467 (1763) 0x467 (1763) 0x467 (1774) 0x4555 (17744) 0x4555 (17747) 0x4557 (17845) 0x4574 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058) 0x468a (18058) | PTL b6 64 Echo (ping) reply 64 Echo (ping) | 1d=0x0012, seq=1/256, ttl=64 1d=0x0012, seq=2/512, ttl=64 1d=0x0012, seq=2/512, 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=3/108, ttl=64 1d=0x0012, seq=3/108, ttl=64 1d=0x0012, seq=3/128, ttl=64 1d=0x0012, seq=3/128, ttl=64 1d=0x0012, seq=3/128, ttl=64 1d=0x0012, seq=3/128, ttl=64 1d=0x0012, seq=3/2048, ttl=64 1d=0x0012, seq=10/2560, ttl=64 1d=0x0012, seq=11/2816, ttl=64 |
| Ke. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 3 2022-08-01 10:03:22.323244769 4 4022-08-01 10:03:23.232244769 4 4022-08-01 10:03:23.232244769 5 2022-08-01 10:03:23.232244769 8 2022-08-01 10:03:23.232244769 8 2022-08-01 10:03:25.2586724861 9 2022-08-01 10:03:25.2586724861 9 2022-08-01 10:03:25.2586724861 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 10:03:27.306671694 12 2022-08-01 10:03:27.306671694 12 2022-08-01 10:03:27.306671694 12 2022-08-01 10:03:27.30674378 16 2022-08-01 10:03:27.30674378 16 2022-08-01 10:03:27.30674378 17 2022-08-01 10:03:27.325493704 18 2022-08-01 10:03:21.40277217 2 2022-08-01 10:03:21.402774775 21 2022-08-01 10:03:21.402774775 21 2022-08-01 10:03:21.402774775 21 2022-08-01 10:03:21.402774775 21 2022-08-01 10:03:21.402774775 21 2022-08-01 10:03:21.402774775 21 2022-08-01 10:03:21.402774775 21 2022-08-01 10:03:21.4027771775 | Source 198.51.100.100 198.51 | Destruction 192.0.2.100 192.0 | Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP | Length 108 108 108 108 108 108 108 108 108 108 | P.D 0x42f8 (17144) 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17144) 0x43f8 (17144) 0x43f8 (17144) 0x43f8 (17141) 0x43f8 (17582) 0x4454 (17580) 0x4445 (17582) 0x4445 (17683) 0x4445 (17683) 0x4445 (17763) 0x4455 (17744) 0x4555 (17747) 0x4553 (17747) 0x4553 (17747) 0x4674 (18058) 0x468a (18058) 0x468a (18058) 0x468a (18058) 0x468a (18058) | PTL b6 64 Echo (ping) reply 64 Echo (ping) | id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=4/2048, ttl=64 id=0x0012, seq=1/2166, ttl=64 id=0x0012, seq=1/2166, ttl=64 id=0x0012, seq=1/1/2816, ttl=64 |
| K. Time 1 2022-08-01 10:03:22.23123759 2 2022-08-01 10:03:22.23123759 3 202-08-01 10:03:22.23123759 4 2022-08-01 10:03:22.23224750 5 2022-08-01 10:03:24.23470386 6 4 2022-08-01 10:03:24.23470398 7 2022-08-01 10:03:24.23470398 8 2022-08-01 10:03:25.258672406 9 2022-08-01 10:03:25.258672406 9 2022-08-01 10:03:25.258672406 10 2022-08-01 10:03:25.258672406 10 2022-08-01 10:03:27.306671604 12 2022-08-01 10:03:27.30667163 13 2022-08-01 10:03:27.30667163 13 2022-08-01 10:03:27.30667163 14 2022-08-01 10:03:12, 354975031 16 6022-08-01 10:03:13.0.378795172 17 2022-08-01 10:03:13.0.3787957241 18 2022-08-01 10:03:11.402772717 20 202-08-01 10:03:11.40272217 20 202-08-01 10:03:12.42669354 22 2022-08-01 10:03:12.426695691 0 | Source 198.51.100.100 199.51.100.100 199.51 | Destruction 192.0.2.100 192.0 | Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP | Length 108 108 108 108 108 108 108 108 108 108 | PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17144) 0x4395 (1752) 0x4356 (1752) 0x4456 (17502) 0x4456 (17503) 0x4464 (17508) 0x4464 (17508) 0x4464 (1763) 0x4467 (1763) 0x467 (1763) 0x467 (1774) 0x4555 (17744) 0x4555 (17744) 0x4558 (17742) 0x4688 (18042) 0x4688 (18058) 0x4688 (18058) 0x | PTL b6 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 68 Echo (ping) reply 68 Echo (ping) reply 69 Echo (ping) reply 60 Echo (ping) | 10-0x0012, seq-1/256, ttl-64 10-0x0012, seq-2/512, ttl-64 10-0x0012, seq-2/512, ttl-64 10-0x0012, seq-3/768, ttl-64 10-0x0012, seq-3/768, ttl-64 10-0x0012, seq-3/7102, ttl-64 10-0x0012, seq-3/7048, ttl-64 10-0x0012, seq-3/7048, ttl-64 10-0x0012, seq-10/7560, ttl-64 10-0x0012, seq-10/7560, ttl-64 10-0x0012, seq-11/2816, ttl-64 10-0x0012, seq-11/2816 |

Explicación

En este caso, Ethernet1/2 con la etiqueta VLAN de puerto 102 es la interfaz de salida para los paquetes de respuesta de eco ICMP.

Cuando la dirección de captura de la aplicación se establece en **Egress** en las opciones de captura, los paquetes con la etiqueta de VLAN de puerto 102 en el encabezado Ethernet se capturan en las interfaces de placa base en la dirección de ingreso.

Esta tabla resume la tarea:

| Tarea | Punto de captura | VLAN de puerto interno en paquetes capturados | Direcció n: | Tráfico capturado |
|---|-------------------------------|---|-----------------|---|
| Configurar y verificar capturas en la aplicación y el puerto de aplicación Ethernet1/2 | Interfaces de backplane | 102 | Solo entrada | Respuestas de eco ICMP del 198.51.100.100 al host 192.0. |

Tarea 2:

Utilice FCM y CLI para configurar y verificar una captura de paquetes en la interfaz de la placa de interconexiones y la interfaz Ethernet1/2 frontal.

Las capturas de paquetes simultáneas se configuran en:

- Interfaz frontal: se capturan los paquetes con el puerto VLAN 102 en la interfaz Ethernet1/2. Los paquetes capturados son solicitudes de eco ICMP.
- Interfaces de placa base: se capturan los paquetes para los que Ethernet1/2 se identifica como la interfaz de salida o los paquetes con el puerto VLAN 102. Los paquetes capturados son respuestas de eco ICMP.

Topología, flujo de paquetes y puntos de captura



Configuración

FCM

Siga estos pasos en FCM para configurar una captura de paquetes en la aplicación FTD y el puerto Ethernet1/2 de la aplicación:

1. Utilice Tools > Packet Capture > Capture Session para crear una nueva sesión de captura:

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

2. Seleccione la aplicación FTD, Ethernet1/2, en la lista desplegable Application Port y

seleccione All Packets en la Application Capture Direction. Proporcione el Nombre de la Sesión y haga clic en Guardar y Ejecutar para activar la captura:

| Overview Interfaces Logical Devices Security Engine Platform Settings | | System Tools Help admin |
|---|---|--------------------------|
| Select an instance: ftd1 ¥ | | Save and Run Save Cancel |
| ftd1 | Session Name* Cap1 | |
| | Selected Interfaces None | |
| Ethernet1/2 | Buffer Size 256 MB | |
| | Snap length: 1518 Bytes | |
| | Store Packets Overwrite Append | |
| | Capture On ftd 🗸 | |
| Ethernet1/3 | Application Port Ethernet1/2 | |
| Ethernet1/9, Ethernet1/10 | Application Capture Direction All Packets Egress Packet | |
| | Capture Filter Apply Filter Capture All | |
| | | |
| Ethernet1/1 | | |
| | | |
| | | |

CLI FXOS

Siga estos pasos en la CLI de FXOS para configurar las capturas de paquetes en las interfaces de la placa posterior:

1. Identifique el tipo de aplicación y el identificador:

firepower# scope ssa firepower /ssa# show app-instance Admin State Oper State Running Version Startup Version App Name Identifier Slot ID Deploy Type Turbo Mode Profile Name Cluster State Cluster Role _____ _____ **ftd1** 1 Enabled Online 7.2.0.82 7.2.0.82 ftd Native No Not Applicable None 2. Crear una sesión de captura: 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

Verificación

FCM

Verifique el **Nombre de la Interfaz**, asegúrese de que el **Estado Operacional** esté activo y que el **Tamaño del Archivo (en bytes)** aumente:

| Overview Interfaces Lo | ogical Devices Security Engine F | Platform Settings | | | | System Te | ools Hel | ip admin |
|-----------------------------|----------------------------------|-----------------------|--------------------------|-------------|-------------------------|-----------|-------------|----------|
| | | | | | | | | |
| Capture Session Filter List | | | | | | | | |
| | | | | | | Refresh | Capture Ses | ssion De |
| Cap1 | Drop Count: 0 | Operational State: up | Buffer Size: 256 MB | | Snap Length: 1518 Bytes | | | |
| Interface Name | Filter | File Size (in bytes) | File Name | Device Name | | | | |
| Ethernet1/2 | None | 95040 | cap1-ethernet-1-2-0.pcap | ftd1 | * | | | |
| Ethernet1/2 - Ethernet1/10 | None | 368 | cap1-vethernet-1175.pcap | ftd1 | * | | | |
| Ethernet1/2 - Ethernet1/9 | None | 13040 | cap1-vethernet-1036.pcap | ftd1 | Ł | | | |

CLI FXOS

Verifique los detalles de la captura en scope packet-capture:

```
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
```

Siga los pasos de la sección Recopilación de archivos de captura de switch internos de Firepower 4100/9300.

Capturar análisis de archivos

Utilice una aplicación de lector de archivos de captura de paquetes para abrir los archivos de captura. En el caso de varias interfaces de backplane, asegúrese de abrir todos los archivos de captura para cada interfaz de backplane. En este caso, los paquetes se capturan en la interfaz Ethernet1/9 de la placa de interconexiones.

Abra el archivo de captura para la interfaz Ethernet1/2, seleccione el primer paquete y verifique los puntos clave:

- 1. Solo se capturan los paquetes de solicitud de eco ICMP. Cada paquete se captura y se muestra 2 veces.
- 2. El encabezado del paquete original no tiene la etiqueta VLAN.
- 3. El switch interno inserta la etiqueta adicional del puerto VLAN **102** que identifica la interfaz de ingreso Ethernet1/2.
- 4. El switch interno inserta una etiqueta VN adicional.

| No. | Time | Source | Destination | Protocol | Length | PD | IP TTL Info | |
|-----|-------------------------------------|-------------------|---------------------|---------------|------------|----------------|----------------------|---|
| E | 1 2022-08-01 11:33:19.070693081 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xc009 (49161) | 64 Echo (ping) reque | it id=0x0013, seq=1/256, ttl=64 (no response found!) |
| | 2 2022-08-01 11:33:19.070695347 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xc009 (49161) | 64 Echo (ping) reque | <pre>it id=0x0013, seq=1/256, ttl=64 (no response found!)</pre> |
| | 3 2022-08-01 11:33:19.071217121 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 8XC889 (49161) | 64 ECNO (ping) reque | t id=0x0013, seq=1/256, ttl=64 (no response found!) |
| | 4 2022-08-01 11:33:19.071218458 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xc009 (49161) | 64 Echo (ping) reque | <pre>it id=0x0013, seq=1/256, ttl=64 (no response found!)</pre> |
| | 5 2022-08-01 11:33:20.072036625 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xc0ae (49326) | 64 Echo (ping) reque | <pre>it id=0x0013, seq=2/512, ttl=64 (no response found!)</pre> |
| | 6 2022-08-01 11:33:20.072038399 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xc0ae (49326) | 64 Echo (ping) reque | <pre>st id=0x0013, seq=2/512, ttl=64 (no response found!)</pre> |
| | 7 2022-08-01 11:33:21.073266030 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xc167 (49511) | 64 Echo (ping) reque | it 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) reque | it id=0x0013, seg=3/768, ttl=64 (no response found!) |
| | 9 2022-08-01 11:33:22.074576640 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xc175 (49525) | 64 Echo (ping) reque | st id=0x0013, seg=4/1024, ttl=64 (no response found!) |
| | 10 2022-08-01 11:33:22.074578010 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xc175 (49525) | 64 Echo (ping) reque | st 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) reque | st 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) reque | st id=0x0013, seq=5/1280, ttl=64 (no response found!) |
| | 13 2022-08-01 11:33:24.081839490 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xc211 (49681) | 64 Echo (ping) reque | st 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) reque | st id=0x0013, seq=6/1536, ttl=64 (no response found!) |
| | 15 2022-08-01 11:33:25.105806249 | 192.0.2.100 | 198,51,100,100 | ICMP | 108 | 0xc2e2 (49890) | 64 Echo (ping) reque | st 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) reque | st 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) reque | st 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) reque | st 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) reque | st id=0x0013, seg=9/2304, ttl=64 (no response found!) |
| | 20 2022-08-01 11:33:27.153830201 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xc476 (50294) | 64 Echo (ping) reque | st 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) reque | it 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) reque | it 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) reque | it 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) reque | it 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) reque | st 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 | ICMP | 102 | 0xc585 (50565) | 64 Echo (ping) reque | st id=0x0013, seg=12/3072, ttl=64 (no response found!) |
| | 27 2022-08-01 11:33:31.249828955 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xc618 (50712) | 64 Echo (ping) reque | st id=0x0013, seg=13/3328, ttl=64 (no response found!) |
| | 28 2022-08-01 11:33:31.249831121 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xc618 (50712) | 64 Echo (ping) reque | st id=0x0013, seg=13/3328, ttl=64 (no response found!) |
| | 29 2022-08-01 11:33:32.273867960 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xc64f (50767) | 64 Echo (ping) reque | st id=0x0013, seg=14/3584, ttl=64 (no response found!) |
| < | | | | | | | 0 0 1 | |
| 5 | Frame 1: 108 bytes on wire (864 bit | ts) 109 hytes ca | ntured (864 hits) c | n interface c | enture ue | 1 14 0 | | aaaa 58 97 hd h9 77 ac aa 58 56 9d c8 he 89 26 88 aa X |
| Ľ. | Ethernet II. Src: Whare 9d:e8:he (| (00:50:56:9d:e8:h | e). Dst: Cisco h9:7 | 7:0e (58:97:b | 1:h9:77:00 | 1, 10 0 | | 0010 00 00 81 00 00 66 08 00 45 00 00 54 c0 09 40 00 ·····f·· E··T··A· |
| ú | VN-Tag | 0015015015010010 | en osti eistö osti | (50.57.10 | | ., | | 0020 40 01 8d a3 c0 00 02 64 c6 33 64 64 08 00 8d 7c @·····d ·3dd··· |
| | 1 | = Directi | ion: Ecom Bridge | | | | | 0030 00 13 00 01 f2 b9 e7 62 00 00 00 cb 7f 06 00bb |
| | .0 | = Pointer | vif id | | | | | 0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b |
| | | = Destina | tion: 10 | | | | | 0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ···· !"# \$%&'()*+ |
| | | = Looped: | No | 4 | | | | 0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,/0123 4567 |
| | | = Reserve | di 0 | • • | | | | |
| | | = Version | 1: 0 | | | | | |
| | 0000 00 | 00 0000 = Source: | 0 | | | | | |
| | Type: 802.10 Virtual LAN (0x8100 |) | | | | | | |
| J | 802.10 Virtual LAN, PRI: 0, DEI: 0. | ID: 102 | | | | | | |
| | 000 = Priority: | Rest Effort (defa | ult) (0) | | | | | |
| | | gible | | 2 | | | | |
| | 0000 0110 0110 = ID: 102 | 0 | | 2 I . | | | | |
| | Type: IPv4 (0x0800) | | | | | | | |
| | Internet Protocol Version 4. Src: 1 | 192.0.2.100, Dst: | 198,51,100,100 | | | | | |
| 5 | Internet Control Message Protocol | , | | 2 | | | | |
| | 0 | | | | | | | |

Seleccione el segundo paquete y verifique los puntos clave:

- 1. Solo se capturan los paquetes de solicitud de eco ICMP. Cada paquete se captura y se muestra 2 veces.
- 2. El encabezado del paquete original no tiene la etiqueta VLAN.
- 3. El switch interno inserta la etiqueta adicional del puerto VLAN **102** que identifica la interfaz de ingreso Ethernet1/2.

| No | Time | Source | Destination | Protocol | Length | PD | IP TTL INfo | | |
|----|-------------------------------------|-------------------|---------------------|----------------|----------|----------------|--------------------|---------|--|
| r. | 1 2022-08-01 11:33:19.070693081 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 1 | 0xc009 (49161) | 64 Echo (ping) rec | quest i | d=0x0013, seq=1/256, ttl=64 (no response found!) |
| | 2 2022-08-01 11:33:19.070695347 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xc009 (49161) | 64 Echo (ping) red | quest i | d=0x0013, seq=1/256, ttl=64 (no response found!) |
| | 3 2022-08-01 11:33:19.071217121 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xc009 (49161) | 64 Echo (ping) rec | quest i | d=0x0013, seq=1/256, ttl=64 (no response found!) |
| | 4 2022-08-01 11:33:19.071218458 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xc009 (49161) | 64 Echo (ping) red | quest i | d=0x0013, seq=1/256, ttl=64 (no response found!) |
| | 5 2022-08-01 11:33:20.072036625 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xc0ae (49326) | 64 Echo (ping) rec | quest i | d=0x0013, seq=2/512, ttl=64 (no response found!) |
| | 6 2022-08-01 11:33:20.072038399 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xc0ae (49326) | 64 Echo (ping) red | quest i | d=0x0013, seq=2/512, ttl=64 (no response found!) |
| | 7 2022-08-01 11:33:21.073266030 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xc167 (49511) | 64 Echo (ping) rec | quest i | d=0x0013, seq=3/768, ttl=64 (no response found!) |
| | 8 2022-08-01 11:33:21.073268327 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xc167 (49511) | 64 Echo (ping) rec | quest i | d=0x0013, seq=3/768, ttl=64 (no response found!) |
| | 9 2022-08-01 11:33:22.074576640 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xc175 (49525) | 64 Echo (ping) rec | quest i | d=0x0013, seq=4/1024, ttl=64 (no response found!) |
| | 10 2022-08-01 11:33:22.074578010 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xc175 (49525) | 64 Echo (ping) rec | quest i | d=0x0013, seq=4/1024, ttl=64 (no response found!) |
| | 11 2022-08-01 11:33:23.075779089 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xc208 (49672) | 64 Echo (ping) rec | quest i | d=0x0013, seq=5/1280, ttl=64 (no response found!) |
| | 12 2022-08-01 11:33:23.075781513 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xc208 (49672) | 64 Echo (ping) rec | quest i | d=0x0013, seq=5/1280, ttl=64 (no response found!) |
| | 13 2022-08-01 11:33:24.081839490 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xc211 (49681) | 64 Echo (ping) rec | quest i | d=0x0013, seq=6/1536, ttl=64 (no response found!) |
| | 14 2022-08-01 11:33:24.081841386 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xc211 (49681) | 64 Echo (ping) rec | quest i | d=0x0013, seq=6/1536, ttl=64 (no response found!) |
| | 15 2022-08-01 11:33:25.105806249 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xc2e2 (49890) | 64 Echo (ping) rec | quest i | d=0x0013, seq=7/1792, ttl=64 (no response found!) |
| | 16 2022-08-01 11:33:25.105807895 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xc2e2 (49890) | 64 Echo (ping) rec | quest i | d=0x0013, seq=7/1792, ttl=64 (no response found!) |
| | 17 2022-08-01 11:33:26.129836278 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xc3b4 (50100) | 64 Echo (ping) rec | quest i | d=0x0013, seq=8/2048, ttl=64 (no response found!) |
| | 18 2022-08-01 11:33:26.129838114 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xc3b4 (50100) | 64 Echo (ping) rec | quest i | d=0x0013, seq=8/2048, ttl=64 (no response found!) |
| | 19 2022-08-01 11:33:27.153828653 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xc476 (50294) | 64 Echo (ping) rec | quest i | d=0x0013, seq=9/2304, ttl=64 (no response found!) |
| | 20 2022-08-01 11:33:27.153830201 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xc476 (50294) | 64 Echo (ping) rec | quest i | d=0x0013, seq=9/2304, ttl=64 (no response found!) |
| | 21 2022-08-01 11:33:28.177847175 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xc516 (50454) | 64 Echo (ping) rec | quest i | d=0x0013, seq=10/2560, ttl=64 (no response found!) |
| | 22 2022-08-01 11:33:28.177849075 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xc516 (50454) | 64 Echo (ping) red | quest i | d=0x0013, seq=10/2560, ttl=64 (no response found!) |
| | 23 2022-08-01 11:33:29.201804760 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xc578 (50552) | 64 Echo (ping) red | quest i | d=0x0013, seq=11/2816, ttl=64 (no response found!) |
| | 24 2022-08-01 11:33:29.201806488 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xc578 (50552) | 64 Echo (ping) red | quest i | d=0x0013, seq=11/2816, ttl=64 (no response found!) |
| | 25 2022-08-01 11:33:30.225834765 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xc585 (50565) | 64 Echo (ping) red | quest i | d=0x0013, seq=12/3072, ttl=64 (no response found!) |
| | 26 2022-08-01 11:33:30.225836835 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xc585 (50565) | 64 Echo (ping) red | quest i | d=0x0013, seq=12/3072, ttl=64 (no response found!) |
| | 27 2022-08-01 11:33:31.249828955 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xc618 (50712) | 64 Echo (ping) red | quest i | d=0x0013, seq=13/3328, ttl=64 (no response found!) |
| | 28 2022-08-01 11:33:31.249831121 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xc618 (50712) | 64 Echo (ping) red | quest i | d=0x0013, seq=13/3328, ttl=64 (no response found!) |
| | 29 2022-08-01 11:33:32.273867960 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 | 0xc64f (50767) | 64 Echo (ping) rec | quest i | d=0x0013, seq=14/3584, ttl=64 (no response found!) |
| < | | | | | | | | | |
| > | Frame 2: 102 bytes on wire (816 bit | s), 102 bytes ca | ptured (816 bits) o | n interface ca | pture_u | 0_1, id 0 | | 0000 | 58 97 bd b9 77 0e 00 50 56 9d e8 be 81 00 00 66 Xw.P Vf |
| > | Ethernet II, Src: VMware 9d:e8:be (| 00:50:56:9d:e8:b | e), Dst: Cisco b9:7 | 7:0e (58:97:bd | :b9:77:0 | 0e) | | 0010 | 08 00 45 00 00 54 c0 09 40 00 40 01 8d a3 c0 00 ··E··T·· @·@···· |
| × | 802.1Q Virtual LAN, PRI: 0, DEI: 0, | ID: 102 | | | | | | 0020 | 02 64 c6 33 64 64 08 00 8d 7c 00 13 00 01 f2 b9 ·d·3dd··· |
| | 000 = Priority: H | Best Effort (defa | ult) (0) | | | | | 0030 | e7 62 00 00 00 00 cb 7f 06 00 00 00 00 00 10 11 ·b····· |
| | 0 = DEI: Ineli | gible | | 5 1 | | | | 0040 | 12 13 14 15 16 17 18 19 1a 16 1c 1d 1e 1f 20 21 |
| | 0000 0110 0110 = ID: 102 | | | | | | | 0050 | 22 23 24 23 20 27 28 29 28 20 20 20 20 20 21 30 31 #\$M& () **,*./01 32 33 34 35 36 37 334567 |
| | Type: IPv4 (0x0800) | | | | | | | | 52 55 54 55 50 57 254307 |
| > | Internet Protocol Version 4, Src: 1 | 92.0.2.100, Dst: | 198.51.100.100 🖉 | | | | | | |
| | Internet Control Message Protocol | | 4 | | | | | | |
| 11 | | | | | | | | | |
| 1 | | | | | | | | | |

Abra el archivo de captura para la interfaz Ethernet1/9, seleccione el primer y el segundo paquete y verifique los puntos clave:

- 1. Cada respuesta de eco ICMP se captura y se muestra 2 veces.
- 2. El encabezado del paquete original no tiene la etiqueta VLAN.
- 3. El switch interno inserta la etiqueta adicional del puerto VLAN **102** que identifica la interfaz de salida Ethernet1/2.
- 4. El switch interno inserta una etiqueta VN adicional.

| No. | Time | Source | Destination | Protocol | Length | 2P 3D | 3P TTL 3nfo | |
|------|------------------------------------|-------------------|---------------------|----------------|------------|----------------|----------------------|---|
| | 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 | 0x4f27 (20263) | 64 Echo (ping) reply | id=0x0013, seq=1/256, ttl=64 |
| | 3 2022-08-01 11:33:20.072677302 | 198.51.100.100 | 192.0.2.100 | ICMP | 108 | 0X4110 (20475) | et cono (brug) rebrà | id=0x0013, seq=2/512, ttl=64 |
| | 4 2022-08-01 11:33:20.072679384 | 198.51.100.100 | 192.0.2.100 | ICMP | 108 | 0x4ffb (20475) | 64 Echo (ping) reply | id=0x0013, seq=2/512, ttl=64 |
| | 5 2022-08-01 11:33:21.073913640 | 198.51.100.100 | 192.0.2.100 | ICMP | 108 | 0x50ac (20652) | 64 Echo (ping) reply | id=0x0013, seq=3/768, ttl=64 |
| | 6 2022-08-01 11:33:21.073915690 | 198.51.100.100 | 192.0.2.100 | ICMP | 108 | 0x50ac (20652) | 64 Echo (ping) reply | id=0x0013, seq=3/768, ttl=64 |
| | 7 2022-08-01 11:33:22.075239381 | 198.51.100.100 | 192.0.2.100 | ICMP | 108 | 0x513e (20798) | 64 Echo (ping) reply | id=0x0013, seq=4/1024, ttl=64 |
| | 8 2022-08-01 11:33:22.075241491 | 198.51.100.100 | 192.0.2.100 | ICMP | 108 | 0x513e (20798) | 64 Echo (ping) reply | id=0x0013, seq=4/1024, ttl=64 |
| | 9 2022-08-01 11:33:23.076447152 | 198.51.100.100 | 192.0.2.100 | ICMP | 108 | 0x51c9 (20937) | 64 Echo (ping) reply | id=0x0013, seq=5/1280, ttl=64 |
| | 10 2022-08-01 11:33:23.076449303 | 198.51.100.100 | 192.0.2.100 | ICMP | 108 | 0x51c9 (20937) | 64 Echo (ping) reply | id=0x0013, seq=5/1280, ttl=64 |
| | 11 2022-08-01 11:33:24.082407896 | 198.51.100.100 | 192.0.2.100 | ICMP | 108 | 0x528e (21134) | 64 Echo (ping) reply | id=0x0013, seq=6/1536, ttl=64 |
| | 12 2022-08-01 11:33:24.082410099 | 198.51.100.100 | 192.0.2.100 | ICMP | 108 | 0x528e (21134) | 64 Echo (ping) reply | id=0x0013, seq=6/1536, ttl=64 |
| | 13 2022-08-01 11:33:25.106382424 | 198.51.100.100 | 192.0.2.100 | ICMP | 108 | 0x52af (21167) | 64 Echo (ping) reply | id=0x0013, seq=7/1792, ttl=64 |
| | 14 2022-08-01 11:33:25.106384549 | 198.51.100.100 | 192.0.2.100 | ICMP | 108 | 0x52af (21167) | 64 Echo (ping) reply | id=0x0013, seq=7/1792, ttl=64 |
| | 15 2022-08-01 11:33:26.130437851 | 198.51.100.100 | 192.0.2.100 | ICMP | 108 | 0x53a6 (21414) | 64 Echo (ping) reply | id=0x0013, seg=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, seg=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, seg=9/2304, ttl=64 |
| | 18 2022-08-01 11:33:27.154400198 | 198.51.100.100 | 192.0.2.100 | ICMP | 108 | 0x5446 (21574) | 64 Echo (ping) reply | id=0x0013, seg=9/2304, ttl=64 |
| | 19 2022-08-01 11:33:28,178469866 | 198,51,100,100 | 192.0.2.100 | ICMP | 108 | 0x5493 (21651) | 64 Echo (ping) reply | id=0x0013, seg=10/2560, ttl=64 |
| | 20 2022-08-01 11:33:28,178471810 | 198,51,100,100 | 192.0.2.100 | ICMP | 108 | 0x5493 (21651) | 64 Echo (ping) reply | id=0x0013, seg=10/2560, ttl=64 |
| | 21 2022-08-01 11:33:29.202395869 | 198.51.100.100 | 192.0.2.100 | ICMP | 108 | 0x54f4 (21748) | 64 Echo (ping) reply | id=0x0013, seg=11/2816, ttl=64 |
| | 22 2022-08-01 11:33:29,202398067 | 198,51,100,100 | 192.0.2.100 | ICMP | 108 | 0x54f4 (21748) | 64 Echo (ping) reply | id=0x0013, seg=11/2816, ttl=64 |
| | 23 2022-08-01 11:33:30.226398735 | 198.51.100.100 | 192.0.2.100 | ICMP | 108 | 0x5526 (21798) | 64 Echo (ping) reply | id=0x0013, seg=12/3072, ttl=64 |
| | 24 2022-08-01 11:33:30.226401017 | 198.51.100.100 | 192.0.2.100 | ICMP | 108 | 0x5526 (21798) | 64 Echo (ping) reply | id=0x0013, seg=12/3072, ttl=64 |
| | 25 2022-08-01 11:33:31,250387808 | 198,51,100,100 | 192.0.2.100 | ICMP | 108 | 0x55f2 (22002) | 64 Echo (ping) reply | id=0x0013, seg=13/3328, ttl=64 |
| | 26 2022-08-01 11:33:31.250389971 | 198,51,100,100 | 192.0.2.100 | ICMP | 108 | 0x55f2 (22002) | 64 Echo (ping) reply | id=0x0013, seg=13/3328, ttl=64 |
| | 27 2022-08-01 11:33:32.274416011 | 198.51.100.100 | 192.0.2.100 | ICMP | 108 | 0x5660 (22112) | 64 Echo (ping) reply | id=0x0013, seg=14/3584, ttl=64 |
| | 28 2022-08-01 11:33:32.274418229 | 198,51,100,100 | 192.0.2.100 | ICMP | 108 | 0x5660 (22112) | 64 Echo (ping) reply | id=0x0013, seg=14/3584, ttl=64 |
| | 29 2022-08-01 11:33:33,298397657 | 198,51,100,100 | 192.0.2.100 | ICMP | 108 | 0x56e7 (22247) | 64 Echo (ping) reply | id=0x0013, seg=15/3840, ttl=64 |
| < | | | | | | (| (12.6) (12.6) (12.6) | |
| > En | ame 1: 108 bytes on wire (864 bit | s). 108 bytes ca | ntured (864 bits) o | n interface ca | nture u0 | 8. id 0 | | 8888 00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00 - PV - X w - & |
| 5 Et | hernet II. Src: Cisco h9:77:0e (5) | 8:97:hd:h9:77:0e |). Dst: Wheare 9d:e | the (00:50:56 | ·9d·e8·he |) | | 0010 00 0a 81 00 00 66 08 00 45 00 00 54 4f 27 00 00f. ETO' |
| VI | I-Tag | 01571001051777100 | i oser maare sare | 100 (00150150 | 1.501COTOC | / | | 0020 40 01 3e 86 c6 33 64 64 c0 00 02 64 00 00 95 7c @.>3ddd |
| | ê | = Directi | on: To Bridge | | | | | 0030 00 13 00 01 f2 b9 e7 62 00 00 00 cb 7f 06 00bb |
| | .0 | = Pointer | vif id | | | | | 0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b |
| | | = Destina | tion: 0 | | | | | 0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ···· !"# \$%&"()"+ |
| | | = Looned: | No | | | | | 0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,/0123 4567 |
| | | = Reserve | d: 0 | | | | | |
| | | - Version | 1.0 | | | | | |
| | | 0 1010 = Source: | 10 | | | | | |
| | Type: 802.10 Virtual LAN (0x8100) | | ** | | | | | |
| V 88 | 2.10 Virtual LAN, PRI: 0, DEI: 0. | ID: 102 | | | | | | |
| | 000 Priority: R | lest Effort (defa | ult) (0) | | | | | |
| | | ible | | | | | | |
| | 0000 0110 0110 = ID: 102 | | | ' | | | | |
| | Type: IPv4 (0x0800) | | | | | | | |
| > In | ternet Protocol Version 4, Src: 1 | 98.51.100.100. D | st: 192.0.2.100 | | | | | |
| > In | ternet Control Message Protocol | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

| No. Time | Source | Destination | Protocol | Length | PD | IP TTL Info | _ | |
|--|------------------|---------------------|----------------|-----------|----------------|---------------------|------|---|
| 1 2022-08-01 11:33:19.071512698 | 198.51.100.100 | 192.0.2.100 | ICMP | 108 - | 0x4f27 (20263) | 64 Echo (ping) rep | 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) rep. | 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 (20475) | 64 ECRO (ping) rep. | 1y | 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 (28475) | 64 Echo (ping) rep | ly : | 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) rep | ly : | 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) rep. | 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) rep | ly : | 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) rep. | ly | 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) rep | ly : | 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) rep | ly : | 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) rep | ly : | 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) rep | ly : | 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) rep | ly : | 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) rep | ly : | 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) rep | ly : | 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) rep | ly : | 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) rep | ly : | 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) rep | ly : | 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) rep | ly : | 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) rep | ly : | 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) rep | ly : | 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) rep | ly : | 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) rep | ly : | 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) rep | 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) rep | ly : | 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) rep | ly | 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) rep | ly | 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) rep | ly | 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) rep | ly : | id=0x0013, seq=15/3840, ttl=64 |
| < | | | | | | | | |
| > Frame 2: 108 bytes on wire (864 bits | s), 108 bytes ca | ptured (864 bits) o | n interface ca | pture_u0_ | 8, id 0 | | 0000 | ∂ 00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00 ·PV···X· ··w··&·· |
| > Ethernet II, Src: Cisco b9:77:0e (58 | 8:97:bd:b9:77:0e |), Dst: VMware 9d:e | 8:be (00:50:56 | :9d:e8:be | 2) | | 0010 | 00 0a 81 00 00 66 08 00 45 00 00 54 4f 27 00 00 ·····f·· E··TO'·· |
| ✓ VN-Tag | | | | | | | 0020 | 40 01 3e 86 c6 33 64 64 c0 00 02 64 00 00 95 7c @·>··3dd ···d··· |
| 0 | = Directi | on: To Bridge | | | | | 0030 | 00 13 00 01 f2 b9 e7 62 00 00 00 cb 7f 06 00bb |
| .0 | = Pointer | : vif_id | | | | | | 10 00 00 00 10 11 12 13 14 15 16 17 18 19 18 10 |
| 00 0000 0000 0000 | = Destina | tion: 0 | | | | | 0050 | 20 2d 2a 2f 2a 2f 2a 21 22 23 24 25 26 27 26 29 2a 20 |
| 0 | = Looped: | No 🧹 | 11 | | | | | , -1,0125 4507 |
| 0 | = Reserve | d: 0 | · I | | | | | |
| | = Version | : 0 | | | | | | |
| 0000 000 | 0 1010 = Source: | 10 | | | | | | |
| Type: 802.1Q Virtual LAN (0x8100) | | | | | | | | |
| ✓ 802.1Q Virtual LAN, PRI: 0, DEI: 0, | ID: 102 | | | | | | | |
| 000 = Priority: B | est Effort (defa | ult) (0) | | | | | | |
| 0 = DEI: Inelig | ible | | 5 1 | | | | | |
| 0000 0110 0110 = ID: 102 | | | | | | | | |
| Type: IPv4 (0x0800) | | | | | | | | |
| > Internet Protocol Version 4, Src: 19 | 98.51.100.100, D | st: 192.0.2.100 🍃 | | | | | | |
| > Internet Control Message Protocol | | (| 4 | | | | | |
| | | | | | | | | |

Explicación

Si se selecciona la opción **All Packets** en la **Application Capture Direction**, se configuran 2 capturas de paquetes simultáneas relacionadas con el puerto Ethernet1/2 de la aplicación seleccionada: una captura en la interfaz Ethernet1/2 frontal y una captura en interfaces de backplane seleccionadas.

Cuando se configura una captura de paquetes en una interfaz frontal, el switch captura simultáneamente cada paquete dos veces:

- Después de la inserción de la etiqueta de VLAN de puerto.
- Después de la inserción de la etiqueta VN.

En el orden de las operaciones, la etiqueta VN se inserta en una etapa posterior a la inserción de la etiqueta VLAN del puerto. Sin embargo, en el archivo de captura, el paquete con la etiqueta VN se muestra antes que el paquete con la etiqueta de puerto VLAN. En este ejemplo, la etiqueta VLAN 102 en los paquetes de solicitud de eco ICMP identifica Ethernet1/2 como la interfaz de ingreso.

Cuando se configura una captura de paquetes en una interfaz de backplane, el switch captura simultáneamente cada paquete dos veces. El switch interno recibe paquetes que ya están etiquetados por la aplicación en el módulo de seguridad con la etiqueta de VLAN de puerto y la etiqueta VN. La etiqueta de VLAN de puerto identifica la interfaz de salida que el chasis interno utiliza para reenviar los paquetes a la red. En este ejemplo, la etiqueta VLAN 102 en los paquetes de respuesta de eco ICMP identifica Ethernet1/2 como la interfaz de salida.

El switch interno quita la etiqueta VN y la etiqueta VLAN de la interfaz interna antes de que los paquetes se reenvíen a la red.

Esta tabla resume la tarea:

| | captura | interno en paquetes capturados | : | |
|---|-------------------------------|--------------------------------|-----------------|--|
| Configurar y verificar capturas en la aplicación y el | Interfaces de backplane | 102 | Solo entrada | Respuestas de eco ICMP del 198.51.100.100 al host 192.0.2.100 |
| puerto de aplicación Ethernet1/2 | Interfaz Ethernet1/2 | 102 | Solo entrada | Solicitudes de eco ICMP del l 192.0.2.100 al host 198.51.100.100 |

Captura de paquetes en una subinterfaz de una interfaz física o de canal de puerto

Utilice FCM y CLI para configurar y verificar una captura de paquetes en la subinterfaz Ethernet1/2.205 o en la subinterfaz de canal de puerto Portchannel1.207. Las subinterfaces y capturas en las subinterfaces sólo se admiten para la aplicación FTD en modo contenedor. En este caso, se configura una captura de paquetes en Ethernet1/2.205 y Portchannel1.207.

Topología, flujo de paquetes y puntos de captura



Configuración

FCM

Siga estos pasos en FCM para configurar una captura de paquetes en la aplicación FTD y el puerto Ethernet1/2 de la aplicación:

1. Utilice Tools > Packet Capture > Capture Session para crear una nueva sesión de captura:

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

2. Seleccione la instancia de aplicación específica ftd1, la subinterfaz Ethernet1/2.205, proporcione el nombre de sesión y haga clic en **Guardar y Ejecutar** para activar la captura:

| Select an instance: ftd1 Y | | | Save and Run Save Cancel |
|---|---------------------|--|---|
| Subinterface selection Ethermet1/2.205 Ethermet1/2.206 Subinterfaces(2) Ethermet1/2 | | Session Name* Selected Interfaces Buffer Size Snap length: Store Packets | Cap1 Ethernet1/2.205 256 MB 1518 Overwrite Append |
| Ethernet1/1 | FTD Ethernet1/10 | Capture Filter | Apply Filter Cepture All |

3. En el caso de una subinterfaz de canal de puerto, debido al ID de bug de Cisco, las subinterfaces <u>CSCvq3119</u> no son visibles en FCM. Utilice la CLI de FXOS para configurar capturas en subinterfaces de canal de puerto.

CLI FXOS

Siga estos pasos en FXOS CLI para configurar una captura de paquetes en las subinterfaces Ethernet1/2.205 y Portchannel1.207:

1. Identifique el tipo de aplicación y el identificador:

| firepower# firepower | scope /ssa # | ssa show app-inst | ance | | | | | | |
|---|--|----------------------|---------|--------------|----------|----------|--|--|--|
| App Name | App Name Identifier Slot ID Admin State Oper State Running Version Startup Version | | | | | | | | |
| Deploy Type | Deploy Type Turbo Mode Profile Name Cluster State Cluster Role | | | | | | | | |
| | | | | | | | | | |
| ftd | ftd1 | 1 | Enabled | Online | 7.2.0.82 | 7.2.0.82 | | | |
| Container | No | RP20 | Not App | licable None | | | | | |
| ftd | ftd2 | 1 | Enabled | Online | 7.2.0.82 | 7.2.0.82 | | | |
| Container | No | RP20 | Not App | licable None | | | | | |
| 2. En el caso de una interfaz de canal de puerto, identifique sus interfaces miembro: | | | | | | | | | |

```
firepower# connect fxos
<output skipped>
firepower(fxos)# show port-channel summary
Flags: D - Down P - Up in port-channel (members)
I - Individual H - Hot-standby (LACP only)
s - Suspended r - Module-removed
S - Switched R - Routed
```

```
U - Up (port-channel)

M - Not in use. Min-links not met

Group Port- Type Protocol Member Ports

Channel

1 Pol(SU) Eth LACP Eth1/3(P) Eth1/3(P)
```

3. Crear una sesión de captura:

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
firepower /packet-capture/session #

Para subinterfaces de canal de puerto, cree una captura de paquetes para cada interfaz miembro de canal de puerto:

```
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 #
```

Verificación

FCM

Verifique el **Nombre de la Interfaz**, asegúrese de que el **Estado Operacional** esté activo y que el **Tamaño del Archivo (en bytes)** aumente:

| Overview | Interfaces | Logical Devices Se | curity Engine | Platform Settings | | | | | | | | | System Tools | Help admin |
|---------------|------------------|--------------------|---------------|-------------------|-----------|----------------------|---|-------------------------|----------|-------------|---------------------|-----------------|--------------------|------------|
| | | | | | | | | | | | | | | |
| Capture Ses | sion Filter List | | | | | | | | | | | | | |
| | | | | | | | | | | | C Re | capture Session | Delete All Session | 6 |
| • | cap1 | Dr | op Count: 0 | | Operation | nal State: up | | Buffer Size | : 256 MB | | Snap Length: 1518 B | tes | | .8.8 |
| Interface Na | me | | Filter | | | File Size (in bytes) | | File Name | | Device Name | | | | |
| Ethernet1/2.3 | 105 | | None | | | 233992 | | cap1-ethemet-1-2-0.pcap | | ftd1 | | * | | |
| | | | | | | | • | | | | | | | |

Las capturas de subinterfaz de canal de puerto configuradas en la CLI de FXOS también son visibles en FCM; sin embargo, no se pueden editar:

| Overview Interfac | ces Logical Devices Security Engine | Platform Settings | | | | System Tools | Help admin |
|-------------------|-------------------------------------|-----------------------|--------------------------|---------------|-------------------------|--------------------|------------|
| | | | | | | | |
| Capture Session R | ter List | | | | | | |
| | | | | | Capture Session | Delete Al Sessions | 9 |
| in i cap1 | Drop Count: 0 | Operational State: up | Buffer Size: 256 HB | | Snap Length: 1518 Bytes | | 480 |
| Interface Name | Filter | File Size (in bytes) | File Name | Device Name | | | |
| Ethernet1/4.207 | None | 624160 | cap1-ethernet-1-4-0.pcap | Not available | | | |
| Ethernet1/3.207 | None | 160 | cap1-ethernet-1-3-0.pcap | Not available | * | | |
| | | | | | | | |
| | | | | | | | |

CLI FXOS

Verifique los detalles de la captura en scope packet-capture:

```
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
Canal de puerto 1 con interfaces miembro Ethernet1/3 y 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

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
```

Recopilar archivos de captura

Siga los pasos de la sección Recopilación de archivos de captura de switch internos de Firepower 4100/9300.

Capturar análisis de archivos

Utilice una aplicación de lector de archivos de captura de paquetes para abrir el archivo de captura. Seleccione el primer paquete y verifique los puntos clave:

- 1. Solo se capturan los paquetes de solicitud de eco ICMP. Cada paquete se captura y se muestra 2 veces.
- 2. El encabezado del paquete original tiene la etiqueta VLAN 205.
- 3. El switch interno inserta la etiqueta adicional del puerto VLAN **102** que identifica la interfaz de ingreso Ethernet1/2.
- 4. El switch interno inserta una etiqueta VN adicional.

| No. | Time | Source | Destination | Protocol | Length | 1P 1D | IP TTL Info | | | | |
|-----|------------------------------------|-------------------|---------------------|----------------|-----------|--------------|-----------------------------|-------------|-------|---|--|
| F | 1 2022-08-04 07:21:56.993302102 | 192.0.2.100 | 198.51.100.100 | ICMP | 112 | 0x9574 (3826 | 64 Echo | (ping) requ | est i | 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 (3826 | 64 Echo | (ping) requ | est i | 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 (3955 | 64 Echo | (ping) requ | est i | 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 (3955 | 64 Echo | (ping) requ | est i | 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 (3961 | 64 Echo | (ping) requ | est i | 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 (3961 | 64 Echo | (ping) requ | est i | 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 (3973 | 64 Echo | (ping) requ | est i | 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 (3973 | 64 Echo | (ping) requ | est i | 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 (3995 | 64 Echo | (ping) requ | est i | 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 (3995 | 64 Echo | (ping) requ | est i | 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 (4013 | 64 Echo | (ping) requ | est i | 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 (4013 | 64 Echo | (ping) requ | est i | 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 (4032 | 64 Echo | (ping) requ | est i | 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 (4032 | 64 Echo | (ping) requ | est i | 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 (4035 | 64 Echo | (ping) requ | est i | 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 (4035 | 64 Echo | (ping) requ | est 1 | 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 (4045 | 5) 64 Echo | (ping) requ | est i | 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 (4845 | 5) 64 Echo | (ping) requ | est 1 | 1d=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 (4055 | 64 Echo | (ping) requ | est i | 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 (4055 | 64 Echo | (ping) requ | est 1 | 1d=0x0022, seq=18/4608, tt1=64 (no response found!) | |
| | 21 2022-08-04 07:22:15.365941588 | 192.0.2.100 | 198.51.100.100 | ICMP | 112 | 0x9efb (4069 | 64 Echo | (ping) requ | est i | 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 | 0x9etb (4069 | 64 Echo | (ping) requ | est 1 | 1d=0x0022, seq=19/4864, tt1=64 (no response found!) | |
| | 23 2022-08-04 07:22:16.389973843 | 192.0.2.100 | 198.51.100.100 | ICMP | 112 | 0x9fe8 (4093 | 5) 64 Echo | (ping) requ | est 1 | 1d=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 | 0x9te8 (4093 | 5) 64 Echo | (ping) requ | est 1 | 1d=0x0022, seq=20/5120, tt1=64 (no response found!) | |
| | 25 2022-08-04 07:22:17.413936452 | 192.0.2.100 | 198.51.100.100 | ICMP | 112 | 0x3079 (4108 | 1) 64 Echo | (ping) requ | est 1 | 1d=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 (4108 | 1) 64 Echo | (ping) requ | est 1 | 1d=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 (4124 | 5) 64 ECNO | (ping) requ | est 1 | 10=0x0022, seq=22/5632, tt1=64 (no response found) | |
| < | | | | | | | | | | | |
| > F | rame 1: 112 bytes on wire (896 bit | s), 112 bytes ca | ptured (896 bits) o | n interface ca | pture_u0_ | 1, id 0 | | | 0000 | 0 a2 76 f2 00 00 1b 00 50 56 9d e8 be 89 26 80 54 ··································· | |
| > E | thernet II, Src: VMware 9d:e8:be (| 00:50:56:9d:e8:b | e), Dst: a2:76:f2:0 | 0:00:1b (a2:76 | :f2:00:00 | :1b) | | | 0010 | 0 00 00 81 00 00 66 81 00 00 cd 08 00 45 00 00 54 ·····f·· ····E··T | |
| ~ V | N-Tag | | | | | | | | 0020 | 0 95 74 40 00 40 01 b8 38 c0 00 02 64 c6 33 64 64 ·t@·@··8 ···d·3dd | |
| | 1 | = Directi | on: From Bridge | | | | | | 0030 | 0 08 00 eb 95 00 22 00 01 88 73 eb 62 00 00 00 00 ····· ··· ·············· | |
| | .0 | = Pointer | : vif_id | | | | | | 0040 | | |
| н | 00 0000 0101 0100 | = Destina | tion: 84 | . | | | | | 0050 | 0 18 19 18 10 10 10 10 10 17 20 21 22 23 24 25 26 27 | |
| | ···· ··· ··· ··· ··· 0 ···· ·· | = Looped: | No 🧹 | 11 | | | | | 0000 | 20 29 28 20 20 20 20 20 20 21 30 32 32 33 54 33 30 37 () +,, 01234307 | |
| н | | = Reserve | d: 0 | · I | | | | | | | |
| | 00 | = Version | : 0 | | | | | | | | |
| н | 0000 00 | 00 0000 = Source: | 0 | | | | | | | | |
| L | Type: 802.1Q Virtual LAN (0x8100 |) | | | | | | | | | |
| × 8 | 02.1Q Virtual LAN, PRI: 0, DEI: 0, | ID: 102 | | | | | | | | | |
| | 000 = Priority: | Best Effort (defa | ult) (0) | | | | | | | | |
| н | 0 = DEI: Ineli | gible | | 3 1 | | | | | | | |
| | 0000 0110 0110 = ID: 102 | | | | | | | | | | |
| L | Type: 802.1Q Virtual LAN (0x8100 |) | | | | | | | | | |
| × 8 | 02.1Q Virtual LAN, PRI: 0, DEI: 0, | ID: 205 | | | | | | | | | |
| Г | 000 = Priority: | Best Effort (defa | ult) (0) | | | | | | | | |
| | 0 = DEI: Ineli | gible | | | | | | | | | |
| Т | 0000 1100 1101 = ID: 205 | | | | | | | | | | |
| 1 | Type: IPv4 (0x0800) | | 4 | - | | | | | | | |
| > 1 | nternet Protocol Version 4, Src: 1 | 192.0.2.100, Dst: | 198.51.100.100 | | | | | | | | |
| > 1 | nternet Control Message Protocol | | | | | | | | | | |
| L | | | | | | | | | | | |
| | | | | | | | | | | | |

Seleccione el segundo paquete y verifique los puntos clave:

- 1. Solo se capturan los paquetes de solicitud de eco ICMP. Cada paquete se captura y se muestra 2 veces.
- 2. El encabezado del paquete original tiene la etiqueta VLAN 205.

| Ν | o. Time | Source | Destination | Protocol | Length | 1P 1D | IP TTL Info | | |
|----|---------------------------------------|-------------------------------|---------------------|----------------|------------|----------------|-------------------|--------|--|
| | - 1 2022-08-04 07:21:56.993302102 | 192.0.2.100 | 198.51.100.100 | ICMP | 112 | 0x9574 (38260) | 64 Echo (ping) 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 | equest | 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, seg=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, seg=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, seg=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, seg=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, seg=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, seg=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, seg=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, seg=15/3840, ttl=64 (no response found!) |
| | 15 2022-08-04 07:22:12.325936521 | 192.0.2.100 | 198.51.100.100 | ICMP | 112 | 0x9da2 (40354) | 64 Echo (ping) re | equest | id=0x0022, seg=16/4096, ttl=64 (no response found!) |
| | 16 2022-08-04 07:22:12.325937895 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9da2 (40354) | 64 Echo (ping) re | equest | id=0x0022, seg=16/4096, ttl=64 (no response found!) |
| | 17 2022-08-04 07:22:13.326988040 | 192.0.2.100 | 198.51.100.100 | ICMP | 112 | 0x9e07 (40455) | 64 Echo (ping) re | equest | id=0x0022, seg=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 | equest | id=0x0022, seg=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 | equest | id=0x0022, seg=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 | equest | 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 | equest | 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 | equest | 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!) |
| < | | | | | | 1 1 | | | and the first of the state |
| E | France 2, 102 butes an using (016 bit | (a) 102 butes as | atured (016 bits) a | . intenfore e | | 1 14 0 | | | 23 76 £3 00 00 1h 00 50 . 56 0d 00 ho 01 00 00 cd |
| | Thereat II for theread diethe | (00.E0.EC.Od.og.b | ptured (816 01ts) 0 | n interface ca | ipture_ue_ | 1, 10 0 | | 000 | 0 02 76 72 00 00 10 00 50 50 50 90 68 06 81 00 00 Cu V V V V |
| 1 | 202 to Vintural LAN, DOT, O, DOT, O | 101.3013019010810 | e), Ust: az:/0.12.0 | 0.00.10 (az.m | 5112100100 | | | 002 | 0 02 64 66 33 64 64 08 00 eb 95 00 22 00 01 88 73 |
| 1 | Sozilų virtuai LAN, PKI: 0, DEI: 0 | , 10: 205 Doct Iffort (dof | with) (0) | | | | | 003 | eb 62 00 00 00 00 d9 9d 00 00 00 00 00 10 11 ·b····· |
| н | o privi tech | aible | aure) (o) | | | | | 004 | 0 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 |
| Е | 0000 1100 1101 - IO: 305 | RIDIG | | | | | | 005 | 0 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 "#\$%&'() *+,/01 |
| Е | Tuno: Tout (0x0000) | | | 2 | | | | 006 | /0 32 33 34 35 36 37 234567 |
| 1. | Internet Destacel Version A Secu | 103 0 3 100 0/11 | 109 51 100 100 | | | | | | |
| Ľ | Internet Control Message Protocol | 192.0.2.100, DSC: | 198.31.100.100 | | | | | | |
| Ľ | internet control Pessage Protocol | | | | | | | | |

Ahora abra los archivos de captura para Portchannel1.207. Seleccione el primer paquete y verifique los puntos clave

- 1. Solo se capturan los paquetes de solicitud de eco ICMP. Cada paquete se captura y se muestra 2 veces.
- 2. El encabezado del paquete original tiene la etiqueta VLAN 207.
- 3. El switch interno inserta una etiqueta de VLAN de puerto adicional **1001** que identifica la interfaz de ingreso Portchannel1.
- 4. El switch interno inserta una etiqueta VN adicional.

| No. Time | Source | Destination | Protocol | Length | PD | 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, seq=7/1792, ttl=255 (no response found!) |
| 16 2022-08-04 08:18:24.576408585 | 192.168.247.100 | 192.168.247.102 | ICMP | 118 | 0x60a5 (24741) | 255 Echo (ping) re | quest | id=0x007b, seq=7/1792, ttl=255 (no response found!) |
| 17 2022-08-04 08:18:24.576885643 | 192.168.247.100 | 192.168.247.102 | ICMP | 128 | 0x60a6 (24742) | 255 Echo (ping) re | quest | id=0x007b, seq=8/2048, ttl=255 (no response found!) |
| 18 2022-08-04 08:18:24.576886561 | 192.168.247.100 | 192.168.247.102 | ICMP | 118 | 0x60a6 (24742) | 255 Echo (ping) re | quest | id=0x007b, seq=8/2048, ttl=255 (no response found!) |
| 19 2022-08-04 08:18:24.577394328 | 192.168.247.100 | 192.168.247.102 | ICMP | 128 | 0x60a7 (24743) | 255 Echo (ping) re | quest | id=0x007b, 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, seq=9/2304, ttl=255 (no response found!) |
| 21 2022-08-04 08:18:24.577987632 | 192.168.247.100 | 192.168.247.102 | ICMP | 128 | 0x60a8 (24744) | 255 Echo (ping) re | quest | 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) re | quest | id=0x007b, seq=10/2560, ttl=255 (no response found!) |
| 23 2022-08-04 08:18:24.578448781 | 192.168.247.100 | 192.168.247.102 | ICMP | 128 | 0x60a9 (24745) | 255 Echo (ping) re | quest | 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) 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 | ICMP | 128 | 0x60aa (24746) | 255 Echo (ping) re | quest | id=0x007b, seq=12/3072, ttl=255 (no response found!) |
| 26 2822-88-84 88:18:24.578988897 | 192.168.247.100 | 192.168.247.102 | ICMP | 118 | 0x60aa (24746) | 255 Echo (ping) re | quest | id=0x007b, seg=12/3072, ttl=255 (no response found!) |
| 27 2022-08-04 08:18:24.579426962 | 192.168.247.100 | 192.168.247.102 | ICMP | 128 | 0x60ab (24747) | 255 Echo (ping) re | quest | id=0x007b, seq=13/3328, ttl=255 (no response found!) |
| 6 | | | | | | | | and the first of the state |
| h Forme 1, 100 butes on vice (1004 bits | 1 100 hutor com | hund (1034 bits) or | . Interface c | | 2 14 0 | | | 22 76 62 00 00 10 00 17 df d6 oc 00 00 26 00 2d |
| Sthemat II free Gissa devasion (00) | s), 128 bytes cap | Curea (1024 Dits) or | interface ca | apture_ue | _3, 10 0 | | 0000 | a2 70 12 00 00 10 00 17 01 00 00 00 00 00 00 00 00 00 00 00 00 |
| Pethernet II, SPC: CISCO detected (ed. | 17:01:00:ec:00), | DSt: a2:70:12:00:00 | 5.1C (az:/6.17 | 2:00:00:1 | -) | | 0020 | 60 9e 00 00 ff 01 ea dd c0 a8 f7 64 c0 a8 f7 66 ` |
| vn-rag | - Direction | . Foon Doidgo | | | | | 0030 | 08 00 e5 c8 00 7b 00 00 00 00 00 02 4d 8c 4a 78 ·····{····N·Jx |
| | - Deleter | i From Britage | | | | | 0040 | ab cd |
| 00 0000 0011 1101 | - Destination | V17_10 | | | | | 0050 | ab cd |
| | - Learnada A | 011. 01 | A | | | | 0060 | ab cd |
| | - Recorded: N | 0 | 7 I | | | | 0070 | ab cd |
| | - Version | 0 | | | | | | |
| | = version. | 0 | | | | | | |
| Turner 000 10 Winters 1 111 (0:0100) | 0000 = Source: e | | | | | | | |
| Type: 802.10 VIrtual LAN (0X8100) | 1001 | | _ | | | | | |
| W 802.10 VIFtual LAN, PRI: 0, DEI: 0, 1 | at ffant (dafau) | (a) | | | | | | |
| oco = priority: Be | st errort (deraul | (0) | 2 | | | | | |
| | 016 | | 2 | | | | | |
| 0011 1110 1001 = 10: 1001 | | | | | | | | |
| Type: 802.10 Virtual LAN (0X8100) | 10: 207 | | _ | | | | | |
| ADD | et Effort (defou) | +) (0) | | | | | | |
| 000 = Priority: Be | st errort (défaul | () (0) | | | | | | |
| | 016 | | _ | | | | | |
| Turos Vout (202020) | | | 21 | | | | | |
| Tetepnet Desteral Version (free to | 160 347 100 00 | 103 169 347 103 | - | | | | | |
| Internet Protocol Version 4, SFC: 19, | 2.108.247.100, DS | . 192.108.247.102 | | | | | | |
| Thernet control Message Protocol | | | | | | | | |
| - | | | | | | | | |
| | | | | | | | - | |

Seleccione el segundo paquete y verifique los puntos clave:

- 1. Solo se capturan los paquetes de solicitud de eco ICMP. Cada paquete se captura y se muestra 2 veces.
- 2. El encabezado del paquete original tiene la etiqueta VLAN 207.

| | o. Time | Source | Destination | Protocol | Length | PD | IP TTL Info | |
|---|---------------------------------------|-------------------|----------------------|--------------|-------------|----------------|-------------------------|--|
| | 1 2022-08-04 08:18:24.572548869 | 192.168.247.100 | 192.168.247.102 | ICMP | 128 | 0x609e (24734) | 255 Echo (ping) request | d=0x007b, seq=0/0, ttl=255 (no response found!) |
| | 2 2022-08-04 08:18:24.572550073 | 192.168.247.100 | 192.168.247.102 | ICMP | 118 | 0x609e (24734) | 255 Echo (ping) request | d=0x007b, seq=0/0, ttl=255 (no response found!) |
| | 3 2022-08-04 08:18:24.573286630 | 192.168.247.100 | 192.168.247.102 | ICMP | 128 | 0x609f (24735) | 255 Echo (ping) request | id=0x007b, seq=1/256, ttl=255 (no response found!) |
| | 4 2022-08-04 08:18:24.573287640 | 192.168.247.100 | 192.168.247.102 | ICMP | 118 | 0x609f (24735) | 255 Echo (ping) request | id=0x007b, seq=1/256, ttl=255 (no response found!) |
| | 5 2022-08-04 08:18:24.573794751 | 192.168.247.100 | 192.168.247.102 | ICMP | 128 | 0x60a0 (24736) | 255 Echo (ping) request | id=0x007b, seq=2/512, ttl=255 (no response found!) |
| | 6 2022-08-04 08:18:24.573795748 | 192.168.247.100 | 192.168.247.102 | ICMP | 118 | 0x60a0 (24736) | 255 Echo (ping) request | id=0x007b, seq=2/512, ttl=255 (no response found!) |
| | 7 2022-08-04 08:18:24.574368638 | 192.168.247.100 | 192.168.247.102 | ICMP | 128 | 0x60a1 (24737) | 255 Echo (ping) request | id=0x007b, seq=3/768, ttl=255 (no response found!) |
| | 8 2022-08-04 08:18:24.574369574 | 192.168.247.100 | 192.168.247.102 | ICMP | 118 | 0x60a1 (24737) | 255 Echo (ping) request | id=0x007b, seq=3/768, ttl=255 (no response found!) |
| | 9 2022-08-04 08:18:24.574914512 | 192.168.247.100 | 192.168.247.102 | ICMP | 128 | 0x60a2 (24738) | 255 Echo (ping) request | id=0x007b, seq=4/1024, ttl=255 (no response found!) |
| | 10 2022-08-04 08:18:24.574915415 | 192.168.247.100 | 192.168.247.102 | ICMP | 118 | 0x60a2 (24738) | 255 Echo (ping) request | id=0x007b, seq=4/1024, ttl=255 (no response found!) |
| | 11 2022-08-04 08:18:24.575442569 | 192.168.247.100 | 192.168.247.102 | ICMP | 128 | 0x60a3 (24739) | 255 Echo (ping) request | id=0x007b, seq=5/1280, ttl=255 (no response found!) |
| | 12 2022-08-04 08:18:24.575443601 | 192.168.247.100 | 192.168.247.102 | ICMP | 118 | 0x60a3 (24739) | 255 Echo (ping) request | id=0x007b, seq=5/1280, ttl=255 (no response found!) |
| | 13 2022-08-04 08:18:24.575918119 | 192.168.247.100 | 192.168.247.102 | ICMP | 128 | 0x60a4 (24740) | 255 Echo (ping) request | id=0x007b, seq=6/1536, ttl=255 (no response found!) |
| | 14 2022-08-04 08:18:24.575919057 | 192.168.247.100 | 192.168.247.102 | ICMP | 118 | 0x60a4 (24740) | 255 Echo (ping) request | id=0x007b, seq=6/1536, ttl=255 (no response found!) |
| | 15 2022-08-04 08:18:24.576407671 | 192.168.247.100 | 192.168.247.102 | ICMP | 128 | 0x60a5 (24741) | 255 Echo (ping) request | id=0x007b, seq=7/1792, ttl=255 (no response found!) |
| | 16 2022-08-04 08:18:24.576408585 | 192.168.247.100 | 192.168.247.102 | ICMP | 118 | 0x60a5 (24741) | 255 Echo (ping) request | id=0x007b, seq=7/1792, ttl=255 (no response found!) |
| | 17 2022-08-04 08:18:24.576885643 | 192.168.247.100 | 192.168.247.102 | ICMP | 128 | 0x60a6 (24742) | 255 Echo (ping) request | id=0x007b, seq=8/2048, ttl=255 (no response found!) |
| | 18 2022-08-04 08:18:24.576886561 | 192.168.247.100 | 192.168.247.102 | ICMP | 118 | 0x60a6 (24742) | 255 Echo (ping) request | id=0x007b, seq=8/2048, ttl=255 (no response found!) |
| | 19 2022-08-04 08:18:24.577394328 | 192.168.247.100 | 192.168.247.102 | ICMP | 128 | 0x60a7 (24743) | 255 Echo (ping) request | id=0x007b, seq=9/2304, ttl=255 (no response found!) |
| | 20 2022-08-04 08:18:24.577395234 | 192.168.247.100 | 192.168.247.102 | ICMP | 118 | 0x60a7 (24743) | 255 Echo (ping) request | id=0x007b, seq=9/2304, ttl=255 (no response found!) |
| | 21 2022-08-04 08:18:24.577987632 | 192.168.247.100 | 192.168.247.102 | ICMP | 128 | 0x60a8 (24744) | 255 Echo (ping) request | id=0x007b, seq=10/2560, ttl=255 (no response found!) |
| | 22 2022-08-04 08:18:24.577989290 | 192.168.247.100 | 192.168.247.102 | ICMP | 118 | 0x60a8 (24744) | 255 Echo (ping) request | id=0x007b, seq=10/2560, ttl=255 (no response found!) |
| | 23 2022-08-04 08:18:24.578448781 | 192.168.247.100 | 192.168.247.102 | ICMP | 128 | 0x60a9 (24745) | 255 Echo (ping) request | id=0x007b, seq=11/2816, ttl=255 (no response found!) |
| | 24 2022-08-04 08:18:24.578449909 | 192.168.247.100 | 192.168.247.102 | ICMP | 118 | 0x60a9 (24745) | 255 Echo (ping) request | id=0x007b, seq=11/2816, ttl=255 (no response found!) |
| | 25 2022-08-04 08:18:24.578900043 | 192.168.247.100 | 192.168.247.102 | ICMP | 128 | 0x60aa (24746) | 255 Echo (ping) request | id=0x007b, seq=12/3072, ttl=255 (no response found!) |
| L | 26 2022-08-04 08:18:24.578900897 | 192.168.247.100 | 192.168.247.102 | ICMP | 118 | 0x60aa (24746) | 255 Echo (ping) request | id=0x007b, seq=12/3072, ttl=255 (no response found!) |
| | 27 2022-08-04 08:18:24.579426962 | 192.168.247.100 | 192.168.247.102 | ICMP | 128 | 0x60ab (24747) | 255 Echo (ping) request | id=0x007b, seq=13/3328, ttl=255 (no response found!) |
| 4 | | | | | | | | |
| | Frame 2: 118 bytes on wire (944 bits) | , 118 bytes capt | ured (944 bits) on : | interface ca | pture u0 3, | id 0 | 0000 | a2 76 f2 00 00 1c 00 17 df d6 ec 00 81 00 00 cf ·v····· |
| | Ethernet II, Src: Cisco d6:ec:00 (00: | 17:df:d6:ec:00), | Dst: a2:76:f2:00:00 | 1:1c (a2:76: | f2:00:00:10 | :) | 0010 | 08 00 45 00 00 64 60 9e 00 00 ff 01 ea dd c0 a8 ···E··d`· ····· |
| • | 802.10 Virtual LAN, PRI: 0, DEI: 0, 1 | D: 207 | | | | | 0020 | f7 64 c0 a8 f7 66 08 00 e5 c8 00 7b 00 00 00 00 ·d···f·· ···{··· |
| L | 000 Be Priority: Be | st Effort (defaul | t) (0) | | | | 0030 | 00 02 4d 8c 4a 78 ab cd ab cd ab cd ab cd ab cd ··M·Jx······ |
| L | 0 = DEI: Ineligi | ble | | | | | 0040 | ab cd |
| L | 0000 1100 1111 = ID: 207 | | | 21 | | | 0050 | ab cd |
| Е | Type: IPv4 (0x0800) | | | - 1 | | | 0060 | ab cd |
| | Internet Protocol Version 4, Src: 192 | 168.247.100, Dst | : 192.168.247.102 | | | | 0070 | |
| | Internet Control Message Protocol | | | | | | | |
| Е | | | | | | | | |
| | | | | | | | | |

Explicación

Cuando se configura una captura de paquetes en una interfaz frontal, el switch captura simultáneamente cada paquete dos veces:

- Después de la inserción de la etiqueta de VLAN de puerto.
- Después de la inserción de la etiqueta VN.

En el orden de las operaciones, la etiqueta VN se inserta en una etapa posterior a la inserción de la etiqueta VLAN del puerto. Sin embargo, en el archivo de captura, el paquete con la etiqueta VN se muestra antes que el paquete con la etiqueta de puerto VLAN. Además, en el caso de las subinterfaces, en los archivos de captura, cada segundo paquete no contiene la etiqueta de VLAN de puerto.

Esta tabla resume la tarea:

| Tarea | Punto de captura | VLAN de puerto interno en paquetes capturados | Direcció n: | Tráfico capturado |
|--|------------------------------------|---|-----------------|--|
| Configurar y verificar una captura de paquetes en la subinterfaz Ethernet1/2.205 | Ethernet1/ 2.205 | 102 | Solo entrada | Solicitudes de eco ICMP del hos 192.0.2.100 al host 198.51.100. |
| Configure y verifique una captura de paquetes en la subinterfaz Portchannel1 con las interfaces miembro Ethernet1/3 y Ethernet1/4 | Ethernet1/ 3 Ethernet1/ 4 | 1001 | Solo entrada | Solicitudes de eco ICMP de 192.168.207.100 al host 192.168.207.102 |

Filtros de captura de paquetes

Utilice FCM y CLI para configurar y verificar una captura de paquetes en la interfaz Ethernet1/2 con un filtro.

Topología, flujo de paquetes y puntos de captura



Configuración

FCM

Siga estos pasos en FCM para configurar un filtro de captura para los paquetes de solicitud de eco ICMP del host 192.0.2.100 al host 198.51.100.100 y aplicarlo a la captura de paquetes en la interfaz Ethernet1/2:

- 1. Utilice Tools > Packet Capture > Filter List > Add Filter para crear un filtro de captura.
- 2. Especifique el **Nombre de filtro, Protocolo, IPv4 de origen, IPv4 de destino** y haga clic en **Guardar:**
| Overview Interfa | aces Logical Devices Se | curity Engine Platf | orm Settings | | | | | | | | | System Tools | Help admin |
|------------------|-------------------------|---------------------|--------------|--------------|-------------------|-------------|---------------------|----------|------------|------------|-----------|--------------|------------|
| | | | | | | | | | | | | | |
| Capture Session | lter List | | | | | | | | | | | | _ |
| Filter List | | | | | | | | | | | | Ad | d Filter |
| Filter Name | | From | 10-5 | | Те | | | Protocol | Inner vlan | Outer vlan | EtherType | | |
| filter_icmp | 00:00:00:00:00:00 | 192.0.2.100 | 11 | 0 | 00:00:00:00:00:00 | 192.0.2.100 | 11 | 0 | 1 | 0 | 0 | 0 | /8 |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | Edit Packe | t Filter | | | () X | | | | | |
| | | | | 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 | | _ | | | | | |
| | | | | MAC | 0 | Port | | | | | | | |
| | | | | PAG. | 00:00:00:00:00:00 | HAC | 00:00:00:00:00:00:0 | Canad | | | | | |
| | | | | | | | Save | Cancel | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |

3. Utilice Tools > Packet Capture > Capture Session para crear una nueva sesión de captura:

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

4. Seleccione Ethernet1/2, proporcione el **nombre de sesión**, aplique el filtro de captura y haga clic en **Guardar y ejecutar** para activar la captura:

| Overview Interfaces Logical Devices Security Engine Platform Settings | Syr | stem Tools Help admin |
|---|---|-----------------------|
| Select an instance: ftd1 💌 | Save and Run Save Cancel | |
| ftd1 | Session Name* cap1 | |
| | Selected Interfaces Ethernet1/2 | |
| themet/2 | Buffer Size 256 MB 🗸 | |
| | Snap length: 1518 Bytes | |
| | Store Packets Overwrite Append | |
| | | |
| Ethemeti/3 | Capture Filter Apply Filter Capture All | |
| Ethernet1/9, Ethernet1/10 | | |
| | Appry fitter_kmp V IS Ethemet1/2 V | |
| | | |
| Ethernet1/1 | | |
| | | |
| | | |
| | | |

CLI FXOS

Siga estos pasos en la CLI de FXOS para configurar las capturas de paquetes en las interfaces de la placa posterior:

1. Identifique el tipo de aplicación y el identificador:

Identifier Slot ID Admin State Oper State Running Version Startup Version App Name Deploy Type Turbo Mode Profile Name Cluster State Cluster Role _____ ftd ftd1 1 Enabled Online 7.2.0.82 7.2.0.82 Not Applicable None Native No 2. Identifique el número de protocolo IP en https://www.iana.org/assignments/protocol-

numbers/protocol-numbers.xhtml. En este caso, el número de protocolo ICMP es 1.

3. Cree una sesión de captura:

```
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 #
```

Verificación

FCM

Verifique el **Nombre de la Interfaz**, asegúrese de que el **Estado Operacional** esté activo y que el **Tamaño del Archivo (en bytes)** aumente:

| Overview Interf | Overview Interfaces Logical Devices Security Engine Platform Settings Svatem Tools Help admin | | | | | | | | | | | | |
|-----------------|---|-------------|------|------|-------------------|----------------|------|------|----------|------------|------------|-----------|-----|
| | | | | | | | | | | | | | |
| Capture Session | Filter List | | | | | | | | | | | | |
| Filter List | Filter List Ad Filter | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| Filter Name | | From | | | | То | | | Protocol | Inner vlan | Outer vian | EtherType | |
| | MAC | IPv4 | IPv6 | Port | MAC | IPv4 | IPv6 | Port | | | | | |
| 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 |

Verifique el nombre de la interfaz, el **filtro**, asegúrese de que el **estado operativo** esté activo y el **tamaño del archivo (en bytes)** aumente en **Herramientas > Captura de paquetes > Sesión de captura**:

| Overview Interfaces | ogical Devices Security Engir | e Platform Settings | | | | | System Tools Help admin |
|-----------------------------|-------------------------------|----------------------|--------------------------|-------------|---------------------|---------------------------|-------------------------|
| | | | | | | | |
| Capture Session Filter List | : | | | | | | |
| | | | | | | C Refresh Capture Session | Delete All Sessions |
| 🔺 🗻 cap1 | Drop Count: 0 | | Operational State: up | | Buffer Size: 256 MB | Snap Length: 1518 Bytes | |
| Interface Name | Filter | File Size (in bytes) | File Name | Device Name | | | |
| Ethernet1/2 | filter_icmp | 84340 | cap1-ethernet-1-2-0.pcap | ftd1 | * | | |

CLI FXOS

Verifique los detalles de la captura en scope packet-capture:

```
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
Recopilar archivos de captura
```

Siga los pasos de la sección Recopilación de archivos de captura de switch internos de Firepower 4100/9300.

Capturar análisis de archivos

Utilice una aplicación de lector de archivos de captura de paquetes para abrir el archivo de captura. Seleccione el primer paquete y compruebe los puntos clave

- 1. Solo se capturan los paquetes de solicitud de eco ICMP. Cada paquete se captura y se muestra 2 veces.
- 2. El encabezado del paquete original no tiene la etiqueta VLAN.
- 3. El switch interno inserta la etiqueta adicional del puerto VLAN **102** que identifica la interfaz de ingreso Ethernet1/2.
- 4. El switch interno inserta una etiqueta VN adicional.

| No. Time | Source | Destination | Protocol | Length | PD | IP TTL Info | | ^ |
|---------------------------------------|-------------------|---------------------|---------------|------------|----------------|-----------------------------|---------------------------|----------------|
| 1 2022-08-02 15:46:55.603277760 | 192.0.2.100 | 198.51.100.100 | ICMP | 108 - | 0x0012 (18) | 64 Echo (ping) request | id=0x0018, seq=349/23809, | ttl=64 (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 1: 108 bytes on wire (864 bit | ts), 108 bytes ca | ptured (864 bits) o | n interface c | apture_u0_ | 1, i 0000 58 9 | 7 bd b9 77 0e 00 50 56 9d e | 8 be 89 26 80 0a X···w·· | P V····&·· |
| > Ethernet II, Src: VMware 9d:e8:be (| (00:50:56:9d:e8:b | e), Dst: Cisco b9:7 | 7:0e (58:97:b | d:b9:77:0e |) 0010 00 0 | 0 81 00 00 66 08 00 45 00 0 | 00 54 00 12 40 00 ·····f· | · E··T··@· |
| ✓ VN-Tag | | | | | 0020 40 0 | 1 4d 9b c0 00 02 64 c6 33 0 | 64 64 08 00 9e 67 @·M···· | d ·3dd···g |
| 1 | = Directi | ion: From Bridge | | | 0030 00 1 | 8 01 5d e2 46 e9 62 00 00 0 | 00 00 c1 a6 0c 00 ···]·F· | b |
| .0 | = Pointer | ·: vif_id | | | 0040 00 0 | 0 00 00 10 11 12 13 14 15 1 | 6 17 18 19 1a 1b | |
| 00 0000 0000 1010 | = Destina | ation: 10 | | | 0050 1c 1 | d 1e 1f 20 21 22 23 24 25 2 | 26 27 28 29 2a 2b ···· !" | # \$%&`()"+ |
| 0 0 | = Looped: | No 4 | | | 0000 2C 2 | a ze zt 30 31 32 33 34 35 : | ,/012 | 3 4567 |
| 0 | = Reserve | ed: 0 | | | | | | |
| | = Version | n: 0 | | | | | | |
| 0000 00 | 00 0000 = Source: | 0 | | | | | | |
| Type: 802.1Q Virtual LAN (0x8100 |) | | | | | | | |
| 802.1Q Virtual LAN, PRI: 0, DEI: 0 | , ID: 102 | | | | | | | |
| 000 = Priority: | Best Effort (defa | ault) (0) | | | | | | |
| 0 = DEI: Ineli | gible | 3 | | | | | | |
| 0000 0110 0110 = ID: 102 | - | _ | | | | | | |
| Type: IPv4 (0x0800) | | | | | | | | |
| > Internet Protocol Version 4, Src: 1 | 192.0.2.100, Dst: | 198.51.100.100 | | | | | | |
| > Internet Control Message Protocol | | 2 | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| < | | | | | > | | | |

Seleccione el segundo paquete y verifique los puntos clave:

- 1. Solo se capturan los paquetes de solicitud de eco ICMP. Cada paquete se captura y se muestra 2 veces.
- 2. El encabezado del paquete original no tiene la etiqueta VLAN.
- 3. El switch interno inserta la etiqueta adicional del puerto VLAN **102** que identifica la interfaz de ingreso Ethernet1/2.

| No. | Time | Source | Destination | Protocol | Length | IP ID | IP TTL Info | | ^ |
|--------|----------------------------------|-------------------|---------------------|----------------|------------|----------------|-------------------------|---------------------------|------------------|
| _ 1 | 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 |
| 1 | 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 |
| 1 3 | 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 | 1 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 | 5 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 | 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 | 3 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 |
| 16 | 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 | 1 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 | 2 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 | 3 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 | 1 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 | 5 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 | 5 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 | 7 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 | 3 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 |
| 26 | 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 🗸 |
| < | | | | | | | | | > |
| > Fran | me 2: 102 bytes on wire (816 bit | s), 102 bytes ca | ptured (816 bits) o | n interface ca | pture u0 1 | , i 0000 58 97 | bd b9 77 0e 00 50 56 9d | e8 be 81 00 00 66 X···w· | •P V·····f |
| > Ethe | ernet II, Src: VMware 9d:e8:be (| 00:50:56:9d:e8:b | e), Dst: Cisco b9:7 | 7:0e (58:97:bd | :b9:77:0e | 0010 08 00 | 45 00 00 54 00 12 40 00 | 40 01 4d 9b c0 00 ··E··T | ···@·@·M···· |
| ✓ 802. | .1Q Virtual LAN, PRI: 0, DEI: 0, | ID: 102 | | | | 0020 02 64 | c6 33 64 64 08 00 9e 67 | 00 18 01 5d e2 46 ·d·3dd | ··· ·g···]·F |
| 0 | 00 = Priority: 1 | Best Effort (defa | ult) (0) | | | 0030 e9 62 | 00 00 00 00 c1 a6 0c 00 | 00 00 00 00 10 11 ·b···· | |
| | 0 = DEI: Inelig | gible | 3 | | | 0040 12 13 | 14 15 16 17 18 19 1a 1b | 1c 1d 1e 1f 20 21 | ······ |
| | 0000 0110 0110 = ID: 102 | | - | | | 0050 22 23 | 24 25 26 27 28 29 2a 2b | 2c 2d 2e 2f 30 31 "#\$%&" | () *+,/01 |
| Т | ype: IPv4 (0x0800) | | | | | 0000 32 33 | 34 33 30 37 | 234567 | |
| > Inte | ernet Protocol Version 4, Src: 1 | | | | | | | | |
| > Inte | ernet Control Message Protocol | 2 | | | | | | | |
| | | | | | | | | | |

Explicación

Cuando se configura una captura de paquetes en una interfaz frontal, el switch captura simultáneamente cada paquete dos veces:

- Después de la inserción de la etiqueta de VLAN de puerto.
- Después de la inserción de la etiqueta VN.

En el orden de las operaciones, la etiqueta VN se inserta en una etapa posterior a la inserción de la etiqueta VLAN del puerto. Sin embargo, en el archivo de captura, el paquete con la etiqueta VN se muestra antes que el paquete con la etiqueta de puerto VLAN.

Cuando se aplica un filtro de captura, sólo se capturan los paquetes que coinciden con el filtro en la dirección de entrada.

Esta tabla resume la tarea:

| Tarea | Punto de captura | VLAN de puerto interno en paquetes capturados | Direcci ón: | Filtro de usuario | Tráfico capturado |
|---|------------------------|---|-----------------|--|---|
| Configure y verifique una captura de paquetes con un filtro en la interfaz Ethernet1/2 frontal | Etherne t1/2 | 102 | Solo entrada | Protocolo: ICMP Fuente: 192.0.2.100 Destino: 198.51.100.100 | Solicitudes de eco ICMP de 192.0.2.100 al host 198.51.100.100 |

Recopilación de archivos de captura de switches internos Firepower 4100/9300

FCM

Siga estos pasos en FCM para recopilar archivos de captura de switch internos:

1. Haga clic en el botón **Disable Session** para detener la captura activa:

| Overview | Interfaces | Logical Devices | Security Engine | Platform Settings | | | | System | Tools | Help | admin |
|--------------|-----------------|-----------------|-----------------|-----------------------|--------------------------|-------------|-------------------------|-----------|----------|------|-------|
| | | | | | | | | | | | |
| Capture Ses | sion Filter Lis | t | | | | | | | | | |
| | | | | | | | Capture Session | Delete Al | Sessions | | |
| | cap1 | Drop Coun | t: 0 | Operational State: up | Buffer Size: 256 MB | | Snap Length: 1518 Bytes | | | | 8.0 |
| Interface Na | ame | Filter | | File Size (in bytes) | File Name | Device Name | | | | | |
| Ethernet1/2 | | None | | 34700 | cap1-ethernet-1-2-0.pcap | ftd1 | ¥ | | | | |

2. Asegúrese de que el estado operativo sea DOWN - Session_Admin_Shut:

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

3. Haga clic en **Descargar** para descargar el archivo de captura:

| Overview | Interfaces | Logical Devices | Security Engine | Platform | n Settings | | | | System | Tools | Help | admin |
|-------------|-----------------|-----------------|-----------------|----------|--|-------------------------|-------------|------------------------|----------|------------|------|-------|
| | | | | | | | | | | | | |
| Capture Ses | ssion Fiter Lis | it | | | | | | | | | | |
| | | | | | | | | C Refresh Capture Sess | Delete A | d Sessions | | |
| | cap1 | Drop Coun | t: 0 | Operat | ional State: DOWN - Session_Admin_Shut | Buffer Size: 256 MB | | Snap Length: 1518 Byte | 15 | | 1 | 8 🔟 |
| Interface N | ame | Filter | | | File Size (in bytes) | File Name | Device Name | | | | | |
| Ethernet1/2 | | None | | | 218828 | cap1-ethemet-1-2-0.pcap | ftd1 | 土 | | | | |
| | | | | | | | | | | | | |

En el caso de las interfaces de canal de puerto, repita este paso para cada interfaz miembro.

CLI FXOS

Siga estos pasos en la CLI de FXOS para recopilar los archivos de captura:

1. Detener la captura activa:

```
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
  Cargue el archivo de captura desde el alcance del comando local-mgmt:
```

```
firepower# connect local-mgmt
firepower(local-mgmt)# copy /packet-capture/session-1/cap1-ethernet-1-2-0.pcap ?
ftp: Dest File URI
          Dest File URI
http:
          Dest File URI
https:
          Dest File URI
scp:
sftp:
          Dest File URI
          Dest File URI
tftp:
usbdrive: Dest File URI
volatile: Dest File URI
workspace: Dest File URI
firepower(local-mgmt)# copy /packet-capture/session-1/cap1-ethernet-1-2-0.pcap
ftp://ftpuser@10.10.10.1/cap1-ethernet-1-2-0.pcap
```

Password:

En el caso de las interfaces de canal de puerto, copie el archivo de captura para cada interfaz miembro.

Directrices, limitaciones y prácticas recomendadas para Switch interno Captura de paquete

Para conocer las pautas y limitaciones relacionadas con la captura de switches internos

Firepower 4100/9300, consulte la *Guía de configuración de Cisco Firepower 4100/9300 FXOS Chassis Manager* o la *Guía de configuración de Cisco Firepower 4100/9300 FXOS CLI*, capítulo **Resolución de problemas**, sección *Captura de paquetes*.

Esta es la lista de prácticas recomendadas basadas en el uso de la captura de paquetes en casos de TAC:

- Tenga en cuenta las directrices y limitaciones.
- Capture paquetes en todas las interfaces miembro del canal de puerto y analice todos los archivos de captura.
- Utilice filtros de captura.
- Considere el impacto de NAT en las direcciones IP de paquetes cuando se configura un filtro de captura.
- Aumente o reduzca la **lente de ajuste** que especifica el tamaño de trama en caso de que difiera del valor predeterminado de 1518 bytes. Un tamaño menor da como resultado un mayor número de paquetes capturados y viceversa.
- Ajuste el tamaño del búfer según sea necesario.
- Tenga en cuenta el **Recuento de caídas** en FCM o FXOS CLI. Una vez alcanzado el límite de tamaño del búfer, el contador de conteo de caídas aumenta.
- Utilice el filtro **!vntag** en Wireshark para mostrar sólo los paquetes sin la etiqueta VN. Esto es útil para ocultar paquetes etiquetados VN en los archivos de captura de paquetes de la interfaz frontal.
- Utilice el filtro **frame.number&1** de Wireshark para mostrar sólo fotogramas impares. Esto es útil para ocultar los paquetes duplicados en los archivos de captura de paquetes de la interfaz de la placa de interconexiones.
- En el caso de protocolos como TCP, Wireshark aplica de forma predeterminada reglas de coloración que muestran paquetes con condiciones específicas en diferentes colores. En el caso de las capturas de switch internas debido a paquetes duplicados en los archivos de captura, el paquete se puede colorear y marcar de manera falsa positiva. Si analiza los archivos de captura de paquetes y aplica cualquier filtro, exporte los paquetes mostrados a un nuevo archivo y abra el nuevo archivo.

Configuración y verificación en Firewall seguro 3100

A diferencia de Firepower 4100/9300, las capturas del switch interno en Secure Firewall 3100 se configuran en la interfaz de línea de comandos de la aplicación mediante el comando **capture** <**name>switch**, donde la opción **switch** especifica que las capturas se configuran en el switch interno.

Este es el comando capture con la opción switch:

| <pre>> capture cap_s</pre> | w 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> | |

Los pasos generales para la configuración de la captura de paquetes son los siguientes:

1. Especifique una interfaz de ingreso:

La configuración de captura del switch acepta el **nombre** de interfaz de ingreso **si**. El usuario puede especificar nombres de interfaces de datos, enlaces ascendentes internos o las interfaces de administración:

> 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. Especifique la trama Ethernet EtherType. El EtherType predeterminado es IP. Los valores de la opción **ethernet-type** especifican el EtherType:

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

 Especifique las condiciones de coincidencia. La opción capture match especifica los criterios de coincidencia:

```
> capture capsw switch interface inside match ?
 <0-255> Enter protocol number (0 - 255)
ah
eigrp
esp
gre
 icmp
iстрб
 igmp
 igrp
 ip
 ipinip
 ipsec
         Mac-address filter
mac
nos
 ospf
рср
pim
```

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

> show capture capsw

- 4. Especifique otros parámetros opcionales como el tamaño del búfer, la longitud del paquete, etc.
- 5. Habilite la captura. El comando no capture <name> switch stop activa la captura:

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

27 packet captured on disk using switch capture

6. Verifique los detalles de la captura:

- El estado administrativo es activado, y el estado operativo es activo y activo.
- El tamaño del archivo de captura de paquetes Pcapsize aumenta.
- El número de paquetes capturados en la salida de show capture <cap_name> no es cero.
- Ruta de captura Pcapfile. Los paquetes capturados se guardan automáticamente en la carpeta /mnt/disk0/packet-capture/.
- Condiciones de captura. El software crea automáticamente filtros de captura basados en condiciones de captura.

```
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 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
                /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapfile:
 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 |
| 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 packet captured on disk using switch capture Reading of capture file from disk is not supported

7. Detenga las capturas cuando sea necesario:

```
> capture capsw switch stop
>show capture capsw detail
Packet Capture info
 Name:
                   capsw
                 1
Session:
 Admin State:
                 disabled
 Oper State:
                  down
 Oper State Reason: Session_Admin_Shut
Config Success: yes
Config Fail Reason:
Append Flag:
                 overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
                 0
Drop Count:
Total Physical ports involved in Packet Capture: 1
Physical port:
Slot Id:
                  1
Port Id:
                 1
Pcapfile:
                 /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize:
                  24
Filter:
                  capsw-1-1
Packet Capture Filter Info
Name:
                 capsw-1-1
Protocol:
                 0
Ivlan:
                 0
                 205
Ovlan:
Src Ip:
                 0.0.0.0
Dest Ip:
                  0.0.0.0
Src Ipv6:
                  ::
Dest Ipv6:
                  ::
                 00:00:00:00:00:00
Src MAC:
Dest MAC:
                 00:00:00:00:00:00
Src Port:
                  0
Dest Port:
                  0
Ethertype:
                  0
Total Physical breakout ports involved in Packet Capture: 0
```

0 packet captured on disk using switch capture

Reading of capture file from disk is not supported

8. Recopile los archivos de captura. Siga los pasos de la sección **Recopilación de los archivos de captura interna del switch Secure Firewall 3100**.

En la versión 7.2, la configuración de captura de switch interno no es compatible con FMC o FDM. En el caso del software ASA versión 9.18(1) y posteriores, las capturas internas del switch se pueden configurar en las versiones 7.18.1.x y posteriores de ASDM.

Estos escenarios abarcan casos prácticos comunes de capturas de switches internos de Secure Firewall 3100.

Captura de paquetes en una interfaz física o de canal de puerto

Utilice el FTD o ASA CLI para configurar y verificar una captura de paquetes en la interfaz Ethernet1/1 o Portchannel1. Ambas interfaces tienen el nombre if **inside**.

Topología, flujo de paquetes y puntos de captura



Configuración

Siga estos pasos en ASA o FTD CLI para configurar una captura de paquetes en la interfaz Ethernet1/1 o Port-channel1:

1. Verifique el nombre si:

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

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

2. Crear una sesión de captura:

> capture capsw switch interface inside

3. Habilitar la sesión de captura:

> no capture capsw switch stop Verificación

Verifique el nombre de la sesión de captura, el estado operativo y administrativo, la ranura de interfaz y el identificador. Asegúrese de que el valor de **Pcapsize** en bytes aumente y el número de paquetes capturados no sea cero:

| <pre>> show capture</pre> | capsw detail |
|----------------------------------|--|
| Packet Capture | info |
| Name: | capsw |
| Session: | 1 |
| Admin State: | enabled |
| Oper State: | up |
| Oper State Re | ason: Active |
| Config Success | : yes |
| Config Fail Re | ason: |
| Append Flag: | overwrite |
| Session Mem Us | age: 256 |
| Session Pcap S | nap Len: 1518 |
| Error Code: | 0 |
| Drop Count: | 0 |
| Total Physical Physical port: | ports involved in Packet Capture: 1 |
| Slot Id: | 1 |
| Port Id: | |
| Pcapfile: | /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap |
| Pcapsize: | 12653 |
| Filter: | capsw-1-1 |
| Packet Capture | Filter Info |
| Name: | capsw-1-1 |
| Protocol: | 0 |
| Ivlan: | 0 |
| Ovlan: | 0 |
| Src Ip: | 0.0.0 |
| 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 En el caso del canal de puerto 1, la captura se configura en todas las interfaces miembro:

> show capture capsw detail Packet Capture info Name: capsw Session: 1 Admin State: enabled Oper State: up Oper State Reason: Active Config Success: yes Config Fail Reason: Append Flag: overwrite Session Mem Usage: 256 Session Pcap Snap Len: 1518 Error Code: 0 Drop Count: 0 Total Physical ports involved in Packet Capture: 2 Physical port: Slot Id: 1 Port Id: 4 Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-4-0.pcap Pcapsize: 28824 Filter: capsw-1-4 Packet Capture Filter Info Name: capsw-1-4 Protocol: 0 0 Ivlan: Ovlan: 0 Src Ip: 0.0.0.0 0.0.0.0 Dest Ip: Src Ipv6: :: Dest Ipv6: :: 00:00:00:00:00:00 Src MAC: 00:00:00:00:00:00 Dest MAC: 0 Src Port: Dest Port: 0 Ethertype: 0 Physical port: 1 Slot Id: Port Id: 3 Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-3-0.pcap Pcapsize: 18399 Filter: capsw-1-3 Packet Capture Filter Info Name: capsw-1-3 Protocol: 0 0 Ivlan: 0 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 Dest MAC: 00:00:00:00:00:00

| Src Port: | 0 |
|------------|---|
| Dest Port: | 0 |
| Ethertype: | 0 |

Total Physical breakout ports involved in Packet Capture: 0

56 packet captured on disk using switch capture

Reading of capture file from disk is not supported

Las interfaces de miembro de canal de puerto se pueden verificar en el shell de comandos FXOS **local-mgmt** mediante el comando **show portchannel summary**:

> connect fxos

| ••• | | | | | | | | |
|-------|--|------------|------------|--------------|-----------|--|--|--|
| KSEC- | <pre>KSEC-FPR3100-1 connect local-mgmt</pre> | | | | | | | |
| KSEC- | <pre>KSEC-FPR3100-1(local-mgmt) show portchannel summary</pre> | | | | | | | |
| Flags | 'lags: D - Down P - Up in port-channel (members) | | | | | | | |
| I - 1 | Individual H | I - Hot-st | andby (LAC | P only) | | | | |
| s - 5 | Suspended r | r - Module | -removed | | | | | |
| s - s | Switched F | R - Routed | | | | | | |
| U - U | Jp (port-char | nel) | | | | | | |
| M – 1 | Not in use. M | lin-links | not met | | | | | |
| | | | | | | | | |
| Group | p Port- | Туре | Protocol | Member Ports | | | | |
| | Channel | | | | | | | |
| | | | | | | | | |
| 1 | Pol(U) | Eth | LACP | Eth1/3(P) | Eth1/4(P) | | | |
| | | | | | | | | |
| LACP | KeepAlive Ti | .mer: | | | | | | |
| | | | | | | | | |
| | Channel Pee | erKeepAliv | eTimerFast | | | | | |

Chamler FeerkeepArivernmerFast
1 Pol(U) False
Cluster LACP Status:
Channel ClusterSpanned ClusterDetach ClusterUnitID ClusterSysID

1 Pol(U) False False 0 clust

Para acceder al FXOS en ASA, ejecute el comando **connect fxos admin**. En el caso de multicontexto, ejecute el comando en el contexto de administración.

Recopilar archivos de captura

Siga los pasos de la sección **Recopilación de los archivos de captura interna del switch Secure Firewall 3100**.

Capturar análisis de archivos

Utilice una aplicación de lector de archivos de captura de paquetes para abrir los archivos de captura para Ethernet1/1. Seleccione el primer paquete y compruebe los puntos clave:

- 1. Solo se capturan los paquetes de solicitud de eco ICMP.
- 2. El encabezado del paquete original no tiene la etiqueta VLAN.

| No. | Time | Source | Destination | Protocol | Length | PD | IP TTL Info | <u>^</u> |
|-----|-------------------------------------|-------------------|---------------------|--------------|-------------|----------------|---------------------------|--|
| - | 1 2022-08-07 19:50:06.925768 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9a10 (39440) | 64 Echo (ping) request | id=0x0034, seq=1/256, ttl=64 (no res |
| | 2 2022-08-07 19:50:07.921684 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9a3a (39482) | 64 Echo (ping) request | id=0x0034, seq=2/512, ttl=64 (no res |
| | 3 2022-08-07 19:50:08.924468 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9aa6 (39590) | 64 Echo (ping) request | id=0x0034, seq=3/768, ttl=64 (no res |
| | 4 2022-08-07 19:50:09.928484 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9afe (39678) | 64 Echo (ping) request | id=0x0034, seq=4/1024, ttl=64 (no re |
| | 5 2022-08-07 19:50:10.928245 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9b10 (39696) | 64 Echo (ping) request | id=0x0034, seq=5/1280, ttl=64 (no re |
| | 6 2022-08-07 19:50:11.929144 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9b34 (39732) | 64 Echo (ping) request | id=0x0034, seq=6/1536, ttl=64 (no r€ |
| | 7 2022-08-07 19:50:12.932943 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9b83 (39811) | 64 Echo (ping) request | id=0x0034, seq=7/1792, ttl=64 (no r∈ |
| | 8 2022-08-07 19:50:13.934155 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9b8b (39819) | 64 Echo (ping) request | id=0x0034, seq=8/2048, ttl=64 (no 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 re |
| | 10 2022-08-07 19:50:15.937143 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9cc6 (40134) | 64 Echo (ping) request | id=0x0034, seq=10/2560, ttl=64 (no r |
| | 11 2022-08-07 19:50:16.934848 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9d68 (40296) | 64 Echo (ping) request | id=0x0034, seq=11/2816, ttl=64 (no r |
| | 12 2022-08-07 19:50:17.936908 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9ded (40429) | 64 Echo (ping) request | id=0x0034, seq=12/3072, ttl=64 (no r |
| | 13 2022-08-07 19:50:18.939584 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9e5a (40538) | 64 Echo (ping) request | id=0x0034, seq=13/3328, ttl=64 (no r |
| | 14 2022-08-07 19:50:19.941262 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9efb (40699) | 64 Echo (ping) request | id=0x0034, seq=14/3584, ttl=64 (no r |
| | 15 2022-08-07 19:50:20.940716 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9f50 (40784) | 64 Echo (ping) request | id=0x0034, seq=15/3840, ttl=64 (no r |
| | 16 2022-08-07 19:50:21.940288 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9fe4 (40932) | 64 Echo (ping) request | id=0x0034, seq=16/4096, ttl=64 (no r |
| | 17 2022-08-07 19:50:22.943302 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xa031 (41009) | 64 Echo (ping) request | id=0x0034, seq=17/4352, ttl=64 (no r |
| | 18 2022-08-07 19:50:23.944679 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0xa067 (41063) | 64 Echo (ping) request | id=0x0034, seq=18/4608, ttl=64 (no r 🗸 |
| < | | | | | | | | > |
| 5 | Frame 1: 102 bytes on wire (816 bit | s), 102 bytes cap | tured (816 bits) | | | 0000 bc e7 1 | 2 34 9a 14 00 50 56 9d e8 | be 08 00 45 00 ···4···P V····E· |
| > | Ethernet II, Src: VMware 9d;e8;be (| 00:50:56:9d:e8:be |), Dst: Cisco 34:9a | :14 (bc:e7:1 | 2:34:9a:14) | 0010 00 54 9 | a 10 40 00 40 01 b3 9c c0 | 00 02 64 c6 33 ·T··@·@· ····d·3 |
| 5 | Internet Protocol Version 4, Src: 1 | 92.0.2.100. Dst: | 198.51.100.100 | | 2 | 0020 64 64 6 | 8 00 c6 91 00 34 00 01 61 | 17 f0 62 00 00 dd ·····4 ··a··b·· |
| > | Internet Control Message Protocol | ,, | | | 2 | 0030 00 00 1 | 8 ec 08 00 00 00 00 00 10 | 11 12 13 14 15 |
| 6 | U U | | | | | 0040 16 17 1 | 8 19 1a 1b 1c 1d 1e 1f 20 | 21 22 23 24 25 !"#\$% |
| | | | | | | 0050 26 27 2 | 8 29 2a 2b 2c 2d 2e 2f 30 | 31 32 33 34 35 &'()*+,/012345 |
| | | | | | | 0060 36 37 5 | 5 55 55 55 | 670000 |
| | | | | | | | | |

Abra los archivos de captura para las interfaces de miembro Portchannel1. Seleccione el primer paquete y verifique los puntos clave:

- 1. Solo se capturan los paquetes de solicitud de eco ICMP.
- 2. El encabezado del paquete original no tiene la etiqueta VLAN.

| No | . Time | Source | Destination | Protocol | Length | PD | IP TTL Info | | ^ |
|----|--------------------------------------|-------------------|---------------------|----------------|----------|----------------|-------------------------|--|-----|
| C | 1 2022-08-07 20:40:58.657533 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9296 (37526) | 64 Echo (ping) request | id=0x0035, seq=1/256, ttl=64 (no re | s |
| | 2 2022-08-07 20:40:59.658611 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x9370 (37744) | 64 Echo (ping) request | id=0x0035, seq=2/512, ttl=64 (no re | s |
| | 3 2022-08-07 20:41:00.655662 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x93f0 (37872) | 64 Echo (ping) request | id=0x0035, seq=3/768, ttl=64 (no re | s |
| | 4 2022-08-07 20:41:01.659749 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x946f (37999) | 64 Echo (ping) request | id=0x0035, seq=4/1024, ttl=64 (no 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, ttl=64 (no r | • |
| | 6 2022-08-07 20:41:03.663226 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x952d (38189) | 64 Echo (ping) request | id=0x0035, seq=6/1536, ttl=64 (no r | • |
| | 7 2022-08-07 20:41:04.661262 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x958d (38285) | 64 Echo (ping) request | id=0x0035, seq=7/1792, ttl=64 (no r | e |
| | 8 2022-08-07 20:41:05.665955 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x95d8 (38360) | 64 Echo (ping) request | id=0x0035, seq=8/2048, ttl=64 (no 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, ttl=64 (no r | e |
| | 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 | 0x9b8e (39822) | 64 Echo (ping) request | id=0x0035, seq=18/4608, ttl=64 (no | r ~ |
| < | | | | | | | | > | |
| > | Frame 1: 102 bytes on wire (816 bits |), 102 bytes capt | ured (816 bits) | | | 0000 bc e7 12 | 34 9a 2c 00 50 56 9d e8 | be 08 00 45 00 ····4·, ·P V·····E· | |
| > | Ethernet II, Src: VMware 9d:e8:be (0 | 0:50:56:9d:e8:be) | , Dst: Cisco 34:9a: | 2c (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: 19 | 2.0.2.100, Dst: 1 | 98.51.100.100 | | - | 0020 64 64 08 | 00 58 a8 00 35 00 01 4d | 23 f0 62 00 00 dd · · X · · 5 · · M# · b · · | |
| > | Internet Control Message Protocol | | | | 2 | 0030 00 00 9e | c8 04 00 00 00 00 00 10 | 11 12 13 14 15 | |
| | | | | | | 0040 16 17 18 | 19 1a 1b 1c 1d 1e 1f 20 | 21 22 23 24 25!"#\$% | |
| | | | | | | 0050 26 27 28 | 29 2a 2b 2c 2d 2e 2f 30 | 31 32 33 34 35 & ()*+,/012345 | |
| | | | | | | 0060 36 37 55 | 55 55 55 | 670000 | |
| | | | | | | | | | |

Explicación

Las capturas del switch se configuran en las interfaces Ethernet1/1 o Portchannel1.

Esta tabla resume la tarea:

| Tarea | Punto de captura | Filtro interno | Direcció n: | Tráfico capturado |
|---|------------------------------------|-------------------|-----------------|--|
| Configurar y verificar una captura de paquetes en la interfaz Ethernet1/1 | Ethernet1/ 1 | Ninguno | Solo entrada | Solicitudes de eco ICMP del host 192.0.2.100 al host 198.51.100.100 |
| Configure y verifique una captura de paquetes en la interfaz Portchannel1 con las interfaces miembro Ethernet1/3 y Ethernet1/4 | Ethernet1/ 3 Ethernet1/ 4 | Ninguno | Solo entrada | Solicitudes de eco ICMP del host 192.0.2.100 al host 198.51.100.100 |

Captura de paquetes en una subinterfaz de una interfaz física o de canal de puerto

Utilice el FTD o ASA CLI para configurar y verificar una captura de paquetes en las subinterfaces Ethernet1/1.205 o Portchannel1.205. Ambas subinterfaces tienen el nombre if **inside**.

Topología, flujo de paquetes y puntos de captura



Configuración

Siga estos pasos en ASA o FTD CLI para configurar una captura de paquetes en la interfaz Ethernet1/1 o Port-channel1:

1. Verifique el nombre si:

| <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. Crear una sesión de captura: | | | | | | |

> capture capsw switch interface inside3. Habilitar la sesión de captura:

Verificación

Verifique el nombre de la sesión de captura, el estado operativo y administrativo, la ranura de interfaz y el identificador. Asegúrese de que el valor de **Pcapsize** en bytes aumente y el número de paquetes capturados no sea cero:

| > show capture caps | w detail |
|---------------------|--|
| Packet Capture info |) |
| Name: | capsw |
| Session: | 1 |
| Admin State: | enabled |
| Oper State: | up |
| Oper State Reason | 1: Active |
| Config Success: | yes |
| Config Fail Reason | 1: |
| Append Flag: | overwrite |
| Session Mem Usage: | 256 |
| Session Pcap Snap | Len: 1518 |
| Error Code: | 0 |
| Drop Count: | 0 |
| Total Physical port | s involved in Packet Capture: 1 |
| Physical port: | |
| Slot Id: | 1 |
| Port Id: | |
| Pcapfile: | /mnt/diskU/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap |
| Pcapsize: | 6360 |
| Filter: | capsw-1-1 |
| Packet Capture Filt | er Info |
| Name: | capsw-1-1 |
| Protocol: | 0 |
| Ivlan: | 0 |
| Ovlan: | 205 |
| Src Ip: | 0.0.0 |
| Dest Ip: | 0.0.0.0 |
| Src Ipv6: | :: |
| Dest Ipv6: | :: |
| Src MAC: | 00:00:00:00:00 |
| Dest MAC: | 00:00:00:00:00 |
| Src Port: | 0 |
| Dest Port: | 0 |
| Ethertype: | 0 |
| Total Physical brea | akout ports involved in Packet Capture: 0 |

46 packets captured on disk using switch capture

Reading of capture file from disk is not supported En este caso, se crea un filtro con la VLAN externa **Ovlan=205** y se aplica a la interfaz.

En el caso del Port-channel1, la captura con un filtro **Ovlan=205** se configura en todas las interfaces miembro:

```
> 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: 0 Drop Count: Total Physical ports involved in Packet Capture: 2 Physical port: Slot Id: 1 Port Id: 4 Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-4-0.pcap Pcapsize: 23442 Filter: capsw-1-4 Packet Capture Filter Info Name: capsw-1-4 0 Protocol: 0 Ivlan: 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 00:00:00:00:00:00 Dest MAC: Src Port: 0 Dest Port: 0 Ethertype: 0 Physical port: Slot Id: 1 Port Id: 3 /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-3-0.pcap Pcapfile: Pcapsize: 5600 Filter: capsw-1-3 Packet Capture Filter Info Name: capsw-1-3 Protocol: 0 Ivlan: 0 Ovlan: 205 0.0.0.0 Src Ip: Dest Ip: 0.0.0.0 Src Ipv6: :: :: Dest Ipv6: Src MAC: 00:00:00:00:00:00 00:00:00:00:00:00 Dest MAC: Src Port: 0 Dest Port: 0 0 Ethertype:

Total Physical breakout ports involved in Packet Capture: 0

49 packet captured on disk using switch capture

Reading of capture file from disk is not supported Las interfaces de miembro de canal de puerto se pueden verificar en el shell de comandos FXOS

local-mgmt mediante el comando show portchannel summary:

> connect fxos KSEC-FPR3100-1 connect local-mgmt KSEC-FPR3100-1(local-mgmt) show portchannel summary Flags: D - Down P - Up in port-channel (members) I - Individual H - Hot-standby (LACP only) s - Suspended r - Module-removed S - Switched R - Routed U - Up (port-channel) M - Not in use. Min-links not met _____ Group Port-Type Protocol Member Ports Channel _____ Pol(U) Eth LACP Eth1/3(P) Eth1/4(P) 1 LACP KeepAlive Timer: _____ Channel PeerKeepAliveTimerFast _____ False 1 Pol(U) Cluster LACP Status: _____ Channel ClusterSpanned ClusterDetach ClusterUnitID ClusterSvsID _____ 1 Pol(U) False False 0 clust

Para acceder al FXOS en ASA, ejecute el comando **connect fxos admin**. En el caso de multicontexto, ejecute este comando en el contexto de administración.

Recopilar archivos de captura

Siga los pasos de la sección **Recopilación de los archivos de captura interna del switch Secure Firewall 3100**.

Capturar análisis de archivos

Utilice una aplicación de lector de archivos de captura de paquetes para abrir los archivos de captura para Ethernet1/1.205. Seleccione el primer paquete y compruebe los puntos clave:

- 1. Solo se capturan los paquetes de solicitud de eco ICMP.
- 2. El encabezado del paquete original tiene la etiqueta VLAN 205.

| No. Time | | Source | Destination | Protocol | Length | IP ID | IP TTL Info | | ^ |
|--|-------------------------|-------------------|--------------------|---------------|------------|---------------|--------------------------|--|---|
| _ 1 2022- | 8-07 21:21:01.607187 | 192.0.2.100 | 198.51.100.100 | ICMP | 106 | 0x411f (16671 |) 64 Echo (ping) req | est id=0x0037, seq=1/256, ttl=64 (no res | |
| 2 2022- | 8-07 21:21:02.609418 | 192.0.2.100 | 198.51.100.100 | ICMP | 106 | 0x413a (16698 |) 64 Echo (ping) req | est id=0x0037, seq=2/512, ttl=64 (no res | |
| 3 2022- | 8-07 21:21:03.610671 | 192.0.2.100 | 198.51.100.100 | ICMP | 106 | 0x421a (16922 |) 64 Echo (ping) req | est id=0x0037, seq=3/768, ttl=64 (no res | |
| 4 2022- | 8-07 21:21:04.609160 | 192.0.2.100 | 198.51.100.100 | ICMP | 106 | 0x426c (17004 |) 64 Echo (ping) req | est id=0x0037, seq=4/1024, ttl=64 (no re | |
| 5 2022- | 8-07 21:21:05.609409 | 192.0.2.100 | 198.51.100.100 | ICMP | 106 | 0x4310 (17168 |) 64 Echo (ping) req | est id=0x0037, seq=5/1280, ttl=64 (no re | |
| 6 2022- | 8-07 21:21:06.611847 | 192.0.2.100 | 198.51.100.100 | ICMP | 106 | 0x43df (17375 |) 64 Echo (ping) req | est id=0x0037, seq=6/1536, ttl=64 (no re | |
| 7 2022- | 8-07 21:21:07.616688 | 192.0.2.100 | 198.51.100.100 | ICMP | 106 | 0x44d3 (17619 |) 64 Echo (ping) req | est id=0x0037, seq=7/1792, ttl=64 (no r€ | |
| 8 2022- | 8-07 21:21:08.618023 | 192.0.2.100 | 198.51.100.100 | ICMP | 106 | 0x4518 (17688 |) 64 Echo (ping) req | est id=0x0037, seq=8/2048, ttl=64 (no re | |
| 9 2022- | 8-07 21:21:09.619326 | 192.0.2.100 | 198.51.100.100 | ICMP | 106 | 0x453d (17725 |) 64 Echo (ping) req | est id=0x0037, seq=9/2304, ttl=64 (no r€ | |
| 10 2022- | 8-07 21:21:10.616696 | 192.0.2.100 | 198.51.100.100 | ICMP | 106 | 0x462b (17963 |) 64 Echo (ping) req | est id=0x0037, seq=10/2560, ttl=64 (no r | |
| 11 2022- | 8-07 21:21:11.621629 | 192.0.2.100 | 198.51.100.100 | ICMP | 106 | 0x4707 (18183 |) 64 Echo (ping) req | est id=0x0037, seq=11/2816, ttl=64 (no r | |
| 12 2022- | 8-07 21:21:12.619309 | 192.0.2.100 | 198.51.100.100 | ICMP | 106 | 0x474b (18251 |) 64 Echo (ping) req | est id=0x0037, seq=12/3072, ttl=64 (no r | |
| 13 2022- | 8-07 21:21:13.620168 | 192.0.2.100 | 198.51.100.100 | ICMP | 106 | 0x4781 (18305 |) 64 Echo (ping) req | est id=0x0037, seq=13/3328, ttl=64 (no r | |
| 14 2022- | 8-07 21:21:14.623169 | 192.0.2.100 | 198.51.100.100 | ICMP | 106 | 0x4858 (18520 |) 64 Echo (ping) req | est id=0x0037, seq=14/3584, ttl=64 (no r | |
| 15 2022- | 8-07 21:21:15.622497 | 192.0.2.100 | 198.51.100.100 | ICMP | 106 | 0x4909 (18697 |) 64 Echo (ping) req | est id=0x0037, seq=15/3840, ttl=64 (no r | |
| 16 2022- | 8-07 21:21:16.626226 | 192.0.2.100 | 198.51.100.100 | ICMP | 106 | 0x490b (18699 |) 64 Echo (ping) req | est id=0x0037, seq=16/4096, ttl=64 (no r | |
| 17 2022- | 8-07 21:21:17.629363 | 192.0.2.100 | 198.51.100.100 | ICMP | 106 | 0x4932 (18738 |) 64 Echo (ping) req | est id=0x0037, seq=17/4352, ttl=64 (no r | |
| 18 2022- | 8-07 21:21:18.626651 | 192.0.2.100 | 198.51.100.100 | ICMP | 106 | 0x4a05 (18949 |) 64 Echo (ping) req | est id=0x0037, seq=18/4608, ttl=64 (no r | ~ |
| < | | | | | | | | > | |
| > Frame 1: 100 | bytes on wire (848 bits |), 106 bytes cap | tured (848 bits) | | | 0000 bc e | 7 12 34 9a 14 00 50 56 9 | e8 be 81 00 00 cd ···4···P V····· | |
| Ethernet II, | Src: VMware_9d:e8:be (0 | 0:50:56:9d:e8:be | , Dst: Cisco_34:9a | :14 (bc:e7:12 | :34:9a:14) | 0010 08 0 | 0 45 00 00 54 41 1f 40 0 | 40 01 0c 8e c0 00 ··E··TA· @·@····· | |
| ✓ 802.10 Virtu | al LAN, PRI: 0, DEI: 0, | ID: 205 | | | | 0020 02 6 | 4 c6 33 64 64 08 00 06 6 | 00 37 00 01 b0 2c ·d·3dd·· ·g·7···, | |
| 000 | = Priority: B | est Effort (defau | lt) (0) | | | 0030 10 6 | 2 00 00 00 00 8e fe 03 0 | 00 00 00 00 10 11 ·b····· | |
| 0 | = DEI: Inelig | ible | | | | 0040 12 1 | 3 14 15 16 17 18 19 1a 1 | 1c 1d 1e 1f 20 21 | |
| 0000 | 1100 1101 = ID: 205 | | | | 2 | 0050 22 2 | 3 24 25 26 27 28 29 28 2 | 2C 20 2e 2T 30 31 #\$4& () -+,/01 | |
| Type: IPv | Туре: IРv4 (0х0800) 2 | | | | | 0000 32 3 | 5 54 55 50 57 55 55 55 5 | 25456700 00 | |
| Trailer: 5555555 | | | | | | | | | |
| Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100 | | | | | | | | | |
| > Internet Cor | trol Message Protocol | | | | | | | | |
| | | | | | | | | | |

Abra los archivos de captura para las interfaces de miembro Portchannel1. Seleccione el primer paquete y verifique los puntos clave:

- 1. Solo se capturan los paquetes de solicitud de eco ICMP.
- 2. El encabezado del paquete original tiene la etiqueta VLAN 205.

| No. | Time | Source | Destination | Protocol | Length | IP ID | IP TTL Info | ^ | 4 |
|--------|--|-------------------|---------------------|----------------|-----------|----------------|---------------------------|--|---|
| Г | 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 | 4 |
| | 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 | 1 |
| | 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 | 1 |
| | 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€ | 1 |
| | 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€ | 1 |
| | 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€ | 1 |
| | 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€ | 1 |
| | 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€ | 1 |
| | 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€ | 1 |
| | 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 | 1 |
| | 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 | 1 |
| | 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 | 1 |
| | 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 | 1 |
| | 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 | 1 |
| | 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 | 1 |
| | 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 | 4 |
| | 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 | 1 |
| | 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 🗸 | ł |
| < | | | | | | | | > | 4 |
| > | Frame 1: 106 bytes on wire (848 bits |), 106 bytes capt | ured (848 bits) | | | 0000 bc e7 12 | 2 34 9a 14 00 50 56 9d e8 | be 81 00 00 cd 4 P V | 1 |
| > | Ethernet II, Src: VMware 9d:e8:be (0 | 0:50:56:9d:e8:be | , Dst: Cisco 34:9a: | 14 (bc:e7:12:3 | 34:9a:14) | 0010 08 00 49 | 5 00 00 54 41 1f 40 00 40 | 01 0c 8e c0 00 ··E··TA·@·@····· | |
| \sim | 802.10 Virtual LAN, PRI: 0, DEI: 0, | ID: 205 | - | | · · · · | 0020 02 64 c6 | 5 33 64 64 08 00 06 67 00 | 37 00 01 b0 2c ·d·3dd·· ·g·7···, | |
| | 000 Be | est Effort (defau | lt) (0) | | | 0030 f0 62 00 | 00000008efe 030000 | 00 00 00 10 11 ·b····· | |
| | 0 = DEI: Ineligible | | | | | | 15 16 17 18 19 1a 1b 1c | 1d 1e 1f 20 21 ! | |
| | 0000 1100 1101 = ID: 205 | | | | | 0050 22 23 24 | 1 25 26 27 28 29 2a 2b 2c | 2d 2e 2f 30 31 "#\$%&'() *+,/01 | |
| | Type: IPv4 (0x0800) 2 | | | | | 0060 32 33 34 | 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 | | | | | | | | 1 |
| > | Internet Control Message Protocol | | | | | | | | |
| | 0 | | | | | | | | 1 |

Explicación

Las capturas del switch se configuran en las subinterfaces Ethernet1/1.205 o Portchannel1.205 con un filtro que coincide con la VLAN externa 205.

Esta tabla resume la tarea:

| Tarea | Punto de captura | Filtro interno | Direcci ón: | Tráfico capturado |
|--|------------------------------------|------------------------|-----------------|--|
| Configurar y verificar una captura de paquetes en la subinterfaz Ethernet1/1.205 | Ethernet 1/1 | VLAN externa 205 | Solo entrada | Solicitudes de eco ICMP del host 192.0.2.100 al host 198.51.100.1 |
| Configure y verifique una captura de paquetes en la subinterfaz Portchannel1.205 con las interfaces miembro Ethernet1/3 y Ethernet1/4 | Ethernet 1/3 Ethernet 1/4 | VLAN externa 205 | Solo entrada | Solicitudes de eco ICMP del host 192.0.2.100 al host 198.51.100.1 |

Captura de paquetes en interfaces internas

Secure Firewall tiene 2 interfaces internas:

- in_data_uplink1: conecta la aplicación al switch interno.
- in_mgmt_uplink1 proporciona una trayectoria de paquete dedicada para las conexiones de administración, tales como SSH a la interfaz de administración, o la conexión de administración, también conocida como sftunnel, entre el FMC y el FTD.

Tarea 1

Utilice el FTD o la CLI ASA para configurar y verificar una captura de paquetes en la interfaz de enlace ascendente **in_data_uplink1**.

Topología, flujo de paquetes y puntos de captura



Configuración

Siga estos pasos en ASA o FTD CLI para configurar una captura de paquetes en la interfaz **in_data_uplink1**:

- 1. Crear una sesión de captura:
- > capture capsw switch interface in_data_uplink1
 - 2. Habilitar la sesión de captura:

> no capture capsw switch stop
Verificación

Verifique el nombre de la sesión de captura, el estado operativo y administrativo, la ranura de interfaz y el identificador. Asegúrese de que el valor de **Pcapsize** en bytes aumente y el número de paquetes capturados no sea cero:

> show capture capsw detail
Packet Capture info
Name: capsw
Session: 1

Admin State: enabled Oper State: up Oper State Reason: Active Config Success: yes Config Fail Reason: Append Flag: overwrite Session Mem Usage: 256 Session Pcap Snap Len: 1518 Error Code: 0 0 Drop Count: Total Physical ports involved in Packet Capture: 1 Physical port: Slot Id: 1 Port Id: 18 /mnt/disk0/packet-capture/sess-1-capsw-data-uplink1.pcap Pcapfile: 7704 Pcapsize: Filter: capsw-1-18 Packet Capture Filter Info Name: capsw-1-18 Protocol: 0 0 Ivlan: 0 Ovlan: Src Ip: 0.0.0.0 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: 0 Src Port: Dest Port: 0 Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

66 packets captured on disk using switch capture

Reading of capture file from disk is not supported

En este caso, se crea una captura en la interfaz con un ID interno **18** que es la interfaz in_data_uplink1 en Secure Firewall 3130. El comando **show portmanager switch status** en el shell de comandos FXOS **local-mgmt** muestra los ID de la interfaz:

> connect fxos

...

| KSEC-FPR3100 | 0-1 connect loca | 1-mgmt | | | | |
|--------------|------------------|----------|---------|----------|---------------|---------------|
| KSEC-FPR3100 |)-1(local-mgmt) | show por | tmanage | r switch | status | |
| Dev/Port | Mode | Link | Speed | Duplex | Loopback Mode | Port Manager |
| | | | | | | |
| 0/1 | SGMII | Up | 1G | Full | None | Link-Up |
| 0/2 | SGMII | Up | 1G | Full | None | Link-Up |
| 0/3 | SGMII | Up | 1G | Full | None | Link-Up |
| 0/4 | SGMII | Up | 1G | Full | None | Link-Up |
| 0/5 | SGMII | Down | 1G | Half | None | Mac-Link-Down |
| 0/6 | SGMII | Down | 1G | Half | None | Mac-Link-Down |
| 0/7 | SGMII | Down | 1G | Half | None | Mac-Link-Down |
| 0/8 | SGMII | Down | 1G | Half | None | Mac-Link-Down |
| 0/9 | 1000_BaseX | Down | 1G | Full | None | Link-Down |
| 0/10 | 1000_BaseX | Down | 1G | Full | None | Link-Down |
| 0/11 | 1000_BaseX | Down | 1G | Full | None | Link-Down |
| 0/12 | 1000_BaseX | Down | 1G | Full | None | Link-Down |

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

Para acceder al FXOS en ASA, ejecute el comando **connect fxos admin**. En el caso de multicontexto, ejecute este comando en el contexto de administración.

Recopilar archivos de captura

Siga los pasos de la sección **Recopilación de los archivos de captura interna del switch Secure Firewall 3100**.

Capturar análisis de archivos

Utilice una aplicación de lector de archivos de captura de paquetes para abrir los archivos de captura para la interfaz in_data_uplink1. Compruebe el punto clave: en este caso, se capturan los paquetes de solicitud de eco ICMP y de respuesta de eco. Estos son los paquetes enviados desde la aplicación al switch interno.

| No. | Time | | Source | Destination | Protocol | Length | IP ID | IP TTL Info | | | | ^ |
|------|-----------------|--------------------|----------------|-----------------------|----------------|-------------|---------------|-------------------------------|--------------|---------------------|-------------------|---|
| | 1 2022-08-07 | 22:40:06.685606 | 192.0.2.100 | 198.51.100.100 | ICMP | 102 | 0x4d93 (19859 |) 64 Echo (ping) r | equest id=0> | 003a, seq=33/8448 | , ttl=64 (repl | |
| e | 2 2022-08-07 | 22:40:06.685615 | 198.51.100.3 | 100 192.0.2.100 | ICMP | 102 | 0x6cdc (27868 |) 64 Echo (ping) r | eply id=0x | 003a, seq=33/8448 | , ttl=64 (requ | |
| | 3 2022-08-07 | 22:40:07.684219 | 192.0.2.100 | 198.51.100.100 | TCMD | 102 | 0x4de8 (19944 |) 64 Echo (ping) r | equest id=0 | 003a, 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) r | eply id=0x | 003a, 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) r | equest id=0 | 003a, seq=35/8960 | , ttl=64 (repl | |
| | 6 2022-08-07 | 22:40:08.690806 | 198.51.100.3 | 100 192.0.2.100 | ICMP | 102 | 0x6dbf (28095 |) 64 Echo (ping) r | eply id=0x | 003a, 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) r | equest id=0 | 003a, 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) r | eply id=0x | 003a, 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) r | equest id=0 | :003a, seq=37/9472 | , ttl=64 (repl | |
| | 10 2022-08-07 | 22:40:10.692272 | 198.51.100.3 | 100 192.0.2.100 | ICMP | 102 | 0x6ed5 (28373 |) 64 Echo (ping) r | eply id=0x | 003a, 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) r | equest id=0> | :003a, 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) r | eply id=0 | :003a, 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) r | equest id=0 | :003a, 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) r | eply id=0 | :003a, 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) r | equest id=0 | 003a, seq=40/1024 | a, ttl=64 (rep | |
| | 16 2022-08-07 | 22:40:13.697327 | 198.51.100.3 | 100 192.0.2.100 | ICMP | 102 | 0x703e (28734 |) 64 Echo (ping) r | eply id=0> | 003a, seq=40/1024 | ð, 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) r | equest id=0 | 003a, seq=41/1049 | 5, 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) r | eply id=0 | 003a, seq=41/1049 | 5, ttl=64 (rec | ~ |
| < | | | | | | | | | | | > | |
| > Fr | ame 1: 102 byte | s on wire (816 bit | s), 102 bytes | captured (816 bits) | | | 0000 00 5 | 3 56 9d e7 50 bc e7 12 | 34 9a 15 08 | 00 45 00 · PV · · P | ·· ·4····E· | |
| > Et | hernet II, Src: | Cisco_34:9a:15 (b | c:e7:12:34:9a: | 15), Dst: VMware_9d:e | 7:50 (00:50:50 | 6:9d:e7:50) | 0010 00 5 | 1 4d 93 40 00 <u>40 01</u> 06 | 1a c0 00 02 | 64 c6 33 ·TM·@· | @d-3 | |
| > In | ternet Protocol | Version 4, Src: 1 | 92.0.2.100, Ds | t: 198.51.100.100 | | | 0020 64 6 | 1 08 00 7f 15 00 3a 00 | 21 39 3f f0 | 62 00 00 dd | ··· · 19? · b · · | |
| > In | ternet Control | Message Protocol | | | | | 0030 00 0 | 9 8b 1a 05 00 00 00 00 | 00 10 11 12 | 13 14 15 | | |
| | | | | | | | 0040 16 1 | 7 18 19 1a 1b 1c 1d 1e | 1f 20 21 22 | 23 24 25 | !"#\$% | |
| | | | | | | | 0050 26 2 | 7 28 29 2a 2b 2c 2d 2e | 21 30 31 32 | 33 34 35 & ()*+ | ,/012345 | |
| | | | | | | | 0000 36 3 | 20 20 20 20 20 | | 670000 | | |
| | | | | | | | | | | | | |

Explicación

Cuando se configura una captura de switch en la interfaz de enlace ascendente, solo se capturan

los paquetes enviados desde la aplicación al switch interno. Los paquetes enviados a la aplicación no se capturan.

Esta tabla resume la tarea:

| Tarea | Punto de captura | Filtro interno | Direcció n: | Tráfico capturado |
|---|---------------------|-------------------|-----------------|--|
| Configure y verifique una captura de paquetes en la interfaz de enlace ascendente in_data_uplink1 | in_data_u plink1 | Ninguno | Solo entrada | Solicitudes de eco ICMP del host 192.0.2.100 al host 198.51.100.1 Respuestas de eco ICMP del hos 198.51.100.100 al host 192.0.2.1 |

Tarea 2:

Utilice el FTD o la CLI de ASA para configurar y verificar una captura de paquetes en la interfaz de enlace ascendente **in_mgmt_uplink1**. Sólo se capturan los paquetes de las conexiones del plano de administración.

Topología, flujo de paquetes y puntos de captura



Configuración

Siga estos pasos en ASA o FTD CLI para configurar una captura de paquetes en la interfaz in_mgmt_uplink1:

- 1. Crear una sesión de captura:
- > capture capsw switch interface in_mgmt_uplink1
 - 2. Habilitar la sesión de captura:

> no capture capsw switch stop
Verificación

Verifique el nombre de la sesión de captura, el estado operativo y administrativo, la ranura de interfaz y el identificador. Asegúrese de que el valor de **Pcapsize** en bytes aumente y el número de paquetes capturados no sea cero:

> show capture capsw detail Packet Capture info Name: capsw Session: 1 Admin State: enabled Oper State: up Oper State Reason: Active Config Success: yes Config Fail Reason: Append Flag: overwrite Session Mem Usage: 256 Session Pcap Snap Len: 1518 Error Code: 0 0 Drop Count: Total Physical ports involved in Packet Capture: 1 Physical port: Slot Id: 1 Port Id: 19 /mnt/disk0/packet-capture/sess-1-capsw-mgmt-uplink1.pcap 137248 Pcapfile: Pcapsize: capsw-1-19 Filter: Packet Capture Filter Info Name: capsw-1-19 Protocol: 0 0 Tvlan: 0 Ovlan: 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: 0 Src Port:

Total Physical breakout ports involved in Packet Capture: 0

281 packets captured on disk using switch capture

0

0

Dest Port:

Ethertype:

Reading of capture file from disk is not supported

En este caso, se crea una captura en la interfaz con un ID interno 19 que es la interfaz in_mgmt_uplink1 en Secure Firewall 3130. El comando show portmanager switch status en el shell de comandos FXOS local-mgmt muestra los ID de la interfaz:

| > connect fr | KOS | | | | | |
|------------------------------|------------------|----------|----------|----------|---------------|---------------|
| | | 1 | | | | |
| KSEC-FPR3100 KSEC-FPR3100 |)-1 (local-mgmt) | show por | rtmanage | r switch | status | |
| Dev/Port | Mode | Link | Speed | Duplex | Loopback Mode | Port Manager |
| 0/1 | SGMII | Up | 1G | Full | None | Link-Up |
| 0/2 | SGMII | Up | 1G | Full | None | Link-Up |
| 0/3 | SGMII | Up | 1G | Full | None | Link-Up |
| 0/4 | SGMII | Up | 1G | Full | None | Link-Up |
| 0/5 | SGMII | Down | 1G | Half | None | Mac-Link-Down |
| 0/6 | SGMII | Down | 1G | Half | None | Mac-Link-Down |
| 0/7 | SGMII | Down | 1G | Half | None | Mac-Link-Down |
| 0/8 | SGMII | Down | 1G | Half | None | Mac-Link-Down |

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

Para acceder al FXOS en ASA, ejecute el comando **connect fxos admin**. En el caso de multicontexto, ejecute este comando en el contexto de administración.

Recopilar archivos de captura

Siga los pasos de la sección Recopilación de archivos de captura de switches internos de Secure Firewall 3100.

Capturar análisis de archivos

Utilice una aplicación de lector de archivos de captura de paquetes para abrir los archivos de captura para la interfaz **in_mgmt_uplink1**. Verifique el punto clave; en este caso, sólo se muestran los paquetes de la dirección IP de administración 192.0.2.200. Algunos ejemplos son SSH, Sftunnel o paquetes de respuesta de eco ICMP. Estos son los paquetes enviados desde la interfaz de administración de aplicaciones a la red a través del switch interno.

| No. Time | Source | Destination | Protocol | Length | IP ID | IP TTL Info |
|---|-------------------|--------------------|----------------|---------|----------------|--|
| 196 2022-08-07 23:21:45.133362 | 192.0.2.200 | 192.0.2.101 | TCP | 1518 | 0xb7d0 (47056) | 64 39181 → 8305 [ACK] Seq=61372 Ack=875 Win=1384 Len=1448 TS |
| 197 2022-08-07 23:21:45.133385 | 192.0.2.200 | 192.0.2.101 | TCP | 1518 | 0xb7d1 (47057) | 64 39181 → 8305 [ACK] Seq=62820 Ack=875 Win=1384 Len=1448 TS |
| 198 2022-08-07 23:21:45.133388 | 192.0.2.200 | 192.0.2.101 | TLSv1.2 | 990 | 0xb7d2 (47058) | 64 Application Data |
| 199 2022-08-07 23:21:45.928772 | 192.0.2.200 | 192.0.2.100 | ICMP | 78 | 0xbd48 (48456) | 64 Echo (ping) reply id=0x0001, seq=4539/47889, ttl=64 |
| 200 2022-08-07 23:21:45.949024 | 192.0.2.200 | 192.0.2.101 | TLSv1.2 | 128 | 0x4a97 (19095) | 64 Application Data |
| 201 2022-08-07 23:21:45.949027 | 192.0.2.200 | 192.0.2.101 | TCP | 70 | 0x4a98 (19096) | 64 8305 → 58885 [ACK] Seq=21997 Ack=26244 Win=4116 Len=0 TSv |
| 202 2022-08-07 23:21:46.019895 | 192.0.2.200 | 192.0.2.101 | TLSv1.2 | 100 | 0x4a99 (19097) | 64 Application Data |
| 203 2022-08-07 23:21:46.019899 | 192.0.2.200 | 192.0.2.101 | TLSv1.2 | 96 | 0x4a9a (19098) | 64 Application Data |
| 204 2022-08-07 23:21:46.019903 | 192.0.2.200 | 192.0.2.101 | TCP | 70 | 0x4a9b (19099) | 64 8305 → 58885 [ACK] Seq=22053 Ack=26274 Win=4116 Len=0 TSv |
| 205 2022-08-07 23:21:46.019906 | 192.0.2.200 | 192.0.2.101 | TCP | 70 | 0x4a9c (19100) | 64 8305 → 58885 [ACK] Seq=22053 Ack=26300 Win=4116 Len=0 TSv |
| 206 2022-08-07 23:21:46.136415 | 192.0.2.200 | 192.0.2.101 | TCP | 70 | 0xb7d3 (47059) | 64 39181 → 8305 [ACK] Seq=65188 Ack=921 Win=1384 Len=0 TSval |
| 207 2022-08-07 23:21:46.958148 | 192.0.2.200 | 192.0.2.100 | ICMP | 78 | Øxbd9e (48542) | 64 Echo (ping) reply id=0x0001, seq=4540/48145, ttl=64 |
| 208 2022-08-07 23:21:47.980409 | 192.0.2.200 | 192.0.2.100 | ICMP | 78 | Øxbdf2 (48626) | 64 Echo (ping) reply id=0x0001, seq=4541/48401, ttl=64 |
| 209 2022-08-07 23:21:48.406312 | 192.0.2.200 | 192.0.2.101 | TCP | 70 | 0x4a9d (19101) | 64 8305 → 58885 [ACK] Seq=22053 Ack=26366 Win=4116 Len=0 TSv |
| 210 2022-08-07 23:21:48.903236 | 192.0.2.200 | 192.0.2.101 | TLSv1.2 | 747 | 0x4a9e (19102) | 64 Application Data |
| 211 2022-08-07 23:21:48.994386 | 192.0.2.200 | 192.0.2.100 | ICMP | 78 | Øxbe48 (48712) | 64 Echo (ping) reply id=0x0001, seq=4542/48657, ttl=64 |
| 212 2022-08-07 23:21:50.008576 | 192.0.2.200 | 192.0.2.100 | ICMP | 78 | Øxbea6 (48806) | 64 Echo (ping) reply id=0x0001, seq=4543/48913, ttl=64 |
| 213 2022-08-07 23:21:50.140167 | 192.0.2.200 | 192.0.2.101 | TCP | 1518 | 0xb7d4 (47060) | 64 39181 → 8305 [ACK] Seq=65188 Ack=921 Win=1384 Len=1448 TS |
| 214 2022-08-07 23:21:50.140171 | 192.0.2.200 | 192.0.2.101 | TCP | 1518 | 0xb7d5 (47061) | 64 39181 → 8305 [ACK] Seq=66636 Ack=921 Win=1384 Len=1448 TS |
| 215 2022-08-07 23:21:50.140175 | 192.0.2.200 | 192.0.2.101 | TLSv1.2 | 990 | 0xb7d6 (47062) | 64 Application Data |
| 216 2022-08-07 23:21:51.015884 | 192.0.2.200 | 192.0.2.100 | ICMP | 78 | Øxbec1 (48833) | 64 Echo (ping) reply id=0x0001, seg=4544/49169, ttl=64 |
| 217 2022-08-07 23:21:51.142842 | 192.0.2.200 | 192.0.2.101 | TCP | 70 | 0xb7d7 (47063) | 64 39181 → 8305 [ACK] Seg=69004 Ack=967 Win=1384 Len=0 TSval |
| 218 2022-08-07 23:21:52.030118 | 192.0.2.200 | 192.0.2.100 | ICMP | 78 | 0xbf02 (48898) | 64 Echo (ping) reply id=0x0001, seq=4545/49425, ttl=64 |
| 219 2022-08-07 23:21:53.042744 | 192.0.2.200 | 192.0.2.100 | ICMP | 78 | 0xbf59 (48985) | 64 Echo (ping) reply id=0x0001, seg=4546/49681, ttl=64 |
| 220 2022-08-07 23:21:53.073144 | 192.0.2.200 | 192.0.2.100 | SSH | 170 | 0xad34 (44340) | 64 Server: Encrypted packet (len=112) |
| 221 2022-08-07 23:21:53.194906 | 192.0.2.200 | 192.0.2.100 | TCP | 64 | Øxad35 (44341) | 64 22 → 53249 [ACK] Seg=1025 Ack=881 Win=946 Len=0 |
| 222 2022-08-07 23:21:53.905480 | 192.0.2.200 | 192.0.2.101 | TLSv1.2 | 747 | 0x4a9f (19103) | 64 Application Data |
| 223 2022-08-07 23:21:54.102899 | 192.0.2.200 | 192.0.2.100 | ICMP | 78 | Øxbf63 (48995) | 64 Echo (ping) reply id=0x0001, seg=4547/49937, ttl=64 |
| 224 2022-08-07 23:21:54.903675 | 192.0.2.200 | 192.0.2.101 | TCP | 70 | 0x4aa0 (19104) | 64 8305 → 58885 [ACK] Seg=23407 Ack=26424 Win=4116 Len=0 TSV |
| 115 1011 00 07 12·11·55 126700 | 103 0 3 300 | 102 0 2 100 | TCMD | 70 | avhfe1 (10000) | 64 Echo (ning) conly id-avaaat con-4540/50103 ++1-64 |
| < | | | | | | > |
| > Frame 1: 747 bytes on wire (5976 bits |), 747 bytes capt | ured (5976 bits) | | | 0000 a4 53 0 | e 11 38 2a bc e7 12 34 9a 00 08 00 45 00 ·S··8*·· ·4····E· |
| > Ethernet II, Src: Cisco_34:9a:00 (bc: | e7:12:34:9a:00), | Dst: Cisco_11:38:2 | a (a4:53:0e:11 | :38:2a) | 0010 02 d9 4 | a 3d 40 00 40 06 68 b4 c0 00 02 c8 c0 00 ···J=@·@·h····· |
| > Internet Protocol Version 4, Src: 192 | .0.2.200, Dst: 19 | 2.0.2.101 | | | 0020 02 65 20 | 0 71 e6 05 67 1b 2a c5 db e3 6b d4 80 18 ·e q··g· *···k··· |
| > Transmission Control Protocol, Src Po | rt: 8305, Dst Por | t: 58885, Seq: 1, | Ack: 1, Len: 6 | 77 | 0030 10 14 2. | 7 CC 00 00 01 01 08 0a 08 76 95 77 91 02 |
| > Transport Layer Security | | | | | 0040 30 41 1. | 7 03 03 02 d0 22 0d 01 00 TT CC 98 T9 at =A J. |
| | | | | | 0050 07 40 7 | a 64 e7 20 36 03 8e 48 02 5a 7c 85 30 d4d. 6H.7].0. |
| | | | | | 0070 fa c0 at | 8 56 b8 ad a7 7e 19 3a c1 9c 4b 57 6e e8 |
| | | | | | 0080 be ef 9 | 5 22 84 c1 c1 9d 9f 24 78 b4 15 1c 44 0e" |
| | | | | | 0090 ea cb 43 | 3 9e 1f fd a7 70 75 e5 6b a4 f8 2b ee 47 ···C····p u·k··+·G |
| | | | | | 00a0 2f 86 7 | 3 8f b1 e1 b5 c6 57 e3 a8 46 0e cb 26 b7 /·s···· W··F··&· |
| | | | | | 00b0 5b c7 e | 3 09 54 f3 c1 ff 26 d9 87 ea 51 3d 20 08 [···T··· &···Q= · |
| | | | | | 00c0 16 fd cl | b f5 4f 91 98 5e 86 15 17 55 68 6f 5d 04 ····O··^ ···Uho]· |
| | | | | | | |

Explicación

Cuando se configura una captura de switch en la interfaz de link ascendente de administración, solo se capturan los paquetes de ingreso enviados desde la interfaz de administración de aplicaciones. Los paquetes destinados a la interfaz de administración de aplicaciones no se capturan.

Esta tabla resume la tarea:

| Tarea | Punto de captura | Filtro interno | Dirección: | Tráfico capturado |
|--|---------------------|-------------------|--|--|
| Configurar y verificar una captura de paquetes en la interfaz de link ascendente de administración | in_mgmt_ uplink1 | Ninguno | Solo entrada (desde la interfaz de gestión hasta la red a través del switch interno) | Respuestas de eco ICMP de la dirección administración de FTD 192.0.2.200 al ho 192.0.2.100 Sftunnel de la dirección IP de gestión de 192.0.2.200 a la dirección IP de FMC 192.0.2.101 SSH desde la dirección IP de administrat de FTD 192.0.2.200 al host 192.0.2.100 |

Filtros de captura de paquetes

Los filtros de captura de paquetes de switch internos se configuran de la misma manera que las capturas del plano de datos. Utilice las opciones **ethernet-type** y **match** para configurar los filtros.

Configuración

Siga estos pasos en ASA o FTD CLI para configurar una captura de paquetes con un filtro que coincida con las tramas ARP o los paquetes ICMP del host 198.51.100.100 en la interfaz Ethernet1/1:

1. Verifique el nombre si:

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

2. Cree una sesión de captura para ARP o ICMP:

> capture capsw switch interface inside ethernet-type arp

> capture capsw switch interface inside match icmp 198.51.100.100
Verificación

Verifique el nombre de la sesión de captura y el filtro. El valor Ethertype es **2054** en decimal y **0x0806** en hexadecimal:

| > show capture caps | w 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 | 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: | 0 |
| Filter: | capsw-1-1 |
| Packet Capture Filt | er Info |

| racket capture | FIICEI INIO |
|----------------|-------------------|
| Name: | capsw-1-1 |
| Protocol: | 0 |
| Ivlan: | 0 |
| Ovlan: | 0 |
| Src Ip: | 0.0.0.0 |
| Dest Ip: | 0.0.0.0 |
| Src Ipv6: | :: |
| Dest Ipv6: | :: |
| Src MAC: | 00:00:00:00:00:00 |
| Dest MAC: | 00:00:00:00:00:00 |
| Src Port: | 0 |
| Dest Port: | 0 |
| Ethertype: | 2054 |

0 packet captured on disk using switch capture

Reading of capture file from disk is not supported Esta es la verificación del filtro para ICMP. El protocolo IP 1 es el ICMP:

> show capture capsw detail

Packet Capture info
Name: capsw

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

Total Physical ports involved in Packet Capture: 1

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

Packet Capture Filter Info

| Name: | capsw-1-1 | |
|------------|----------------|--|
| Protocol: | 1 | |
| Ivlan: | 0 | |
| Ovlan: | 0 | |
| Src Ip: | 198.51.100.100 | |
| Dest Ip: | 0.0.0 | |
| Src Ipv6: | :: | |
| Dest Ipv6: | :: | |
| Src MAC: | 00:00:00:00:00 | |
| 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

Recopilación de archivos de captura de switches internos de Secure Firewall 3100

Utilice ASA o FTD CLI para recopilar archivos de captura de switch internos. En FTD, el archivo de captura también se puede exportar mediante el comando CLI **copy** a destinos accesibles a través de las interfaces de datos o diagnóstico.

Como alternativa, el archivo se puede copiar a **/ngfw/var/common** en modo experto y descargarse de FMC mediante la opción **File Download**.

En el caso de las interfaces de canal de puerto, asegúrese de recopilar los archivos de captura de

paquetes de todas las interfaces miembro.

ASA

Siga estos pasos en para recopilar archivos de captura de switch internos en ASA CLI:

- 1. Detener la captura:
- asa# capture capsw switch stop
 - 2. Compruebe que la sesión de captura se ha detenido y anote el nombre del archivo de captura.

```
asa# show capture capsw detail
Packet Capture info
Name:
                 capsw
Session:
                 1
Admin State: disabled
Oper State: down
 Oper State Reason: Session_Admin_Shut
Config Success: yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count:
                0
Total Physical ports involved in Packet Capture: 1
Physical port:
Slot Id:
                1
Port Id:
              1
/mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
139826
                1
 Pcapfile:
Pcapsize:
Filter:
                 capsw-1-1
Packet Capture Filter Info
       capsw-1-1
Name:
                0
Protocol:
Ivlan:
                0
                0
Ovlan:
                0.0.0.0
Src Ip:
Dest Ip:
                0.0.0.0
Src Ipv6:
                 ::
Dest Ipv6:
                  ::
                00:00:00:00:00:00
Src MAC:
                00:00:00:00:00:00
Dest MAC:
Src Port:
                0
Dest Port:
                 0
                0
Ethertype:
Total Physical breakout ports involved in Packet Capture: 0
886 packets captured on disk using switch capture
Reading of capture file from disk is not supported
```

3. Utilice el comando CLI copy para exportar el archivo a destinos remotos:

```
asa# copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap ?
cluster: Copy to cluster: file system
disk0:
              Copy to disk0: file system
disk1:
              Copy to disk1: file system
flash:
              Copy to flash: file system
ftp: Copy to ftp: file system
running-config Update (merge with) current system configuration
scp:
               Copy to scp: file system
smb:
              Copy to smb: file system
startup-config Copy to startup configuration
system: Copy to system: file system
tftp:
              Copy to tftp: file system
asa# copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap tftp://198.51.100.10/
Source filename [/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap]?
Destination filename [sess-1-capsw-ethernet-1-1-0.pcap]?
Copy in progress...C
139826 bytes copied in 0.532 secs
FTD
```

Siga estos pasos para recopilar los archivos de captura de switch internos en la CLI de FTD y copiarlos en servidores accesibles a través de interfaces de datos o diagnóstico:

1. Vaya a la CLI de diagnóstico:

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Click 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> enable
Password: <-- Enter
firepower#
2. Detener la captura:
```

2. Detener la captura.

```
firepower# capture capi switch stop
```

 Verifique que la sesión de captura se haya detenido y anote el nombre del archivo de captura:

| Packet Capture infoName:capswSession:1Admin State:disabledOper State:downOper State:downOper State Reason:Session_Admin_ShutConfig Success:yesConfig Fail Reason:yesAppend Flag:overwriteSession Mem Usage:256Session Pcap Snap Len:1518Error Code:0Orop Count:0Vorop Count:0Port Id:1Port Id:1Pcapfile:/mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap | firepower# show capt | cure capsw detail |
|---|-----------------------------|--|
| Name:capswSession:1Admin State:disabledOper State:downOper State Reason:Session_Admin_ShutConfig Success:yesConfig Fail Reason:yesConfig Fail Reason:overwriteSession Mem Usage:256Session Pcap Snap Len:1518Error Code:0Dorp Count:0Fortal Physical port:involved in Packet Capture:Slot Id:1Port Id:1Pcapfile:/mt/disk0/packet-capture/sess-1-capsw-ethernet-1-0.pcap | Packet Capture info | |
| Session:1Admin State:disabledOper State:downOper State Reason:Session_Admin_ShutConfig Success:yesConfig Fail Reason:overwriteAppend Flag:overwriteSession Mem Usage:256Session Pcap Snap Len:1518Error Code:0Drop Count:0Total Physical portsinvolved in Packet Capture:Slot Id:1Port Id:1Pcapfile:/mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap | Name: | capsw |
| Admin State:disabledOper State:downOper State Reason:Session_Admin_ShutConfig Success:yesConfig Fail Reason:overwriteAppend Flag:overwriteSession Mem Usage:256Session Pcap Snap Len:1518Error Code:0Drop Count:0Total Physical port:involved in Packet Capture:Slot Id:1Port Id:1Pcapfile:/mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap | Session: | 1 |
| Oper State:downOper State Reason:Session_Admin_ShutConfig Success:yesConfig Fail Reason:overwriteAppend Flag:overwriteSession Mem Usage:256Session Pcap Snap Len:1518Error Code:0Drop Count:0Otal Physical port:involved in Packet Capture:Slot Id:1Port Id:1Pcapfile:/mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-10.pcap | Admin State: | disabled |
| Oper State Reason: Session_Admin_ShutConfig Success:yesConfig Fail Reason:Append Flag:overwriteSession Mem Usage:256Session Pcap Snap Len:1518Error Code:0Drop Count:0OOOOProst Id:1Port Id:1Pcapfile:/mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-10.pcap | Oper State: | down |
| 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-1-10.pcap | Oper State Reason: | Session_Admin_Shut |
| 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 | Config Success: | yes |
| 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 | Config Fail Reason: | |
| 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 | Append Flag: | overwrite |
| 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 | Session Mem Usage: | 256 |
| 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 | Session Pcap Snap I | Len: 1518 |
| 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 | Error Code: | 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 | Drop Count: | 0 |
| Physical port: Slot Id: 1 Port Id: 1 Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap | Total Dhygigal ports | involved in Dacket Capture: 1 |
| Slot Id: 1 Port Id: 1 Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap | Devaiant port | s involved in Facket Capture. I |
| Port Id: 1 Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap | Slot Id. | 1 |
| Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap | Dort Id: | 1 |
| rcapille: /mil/disku/packel-capture/sess-1-capsw-ethernet-1-1-U.pcap | Port Iu. | / / / / / / / / / / / / / / / / / / / |
| | PCapIIIe: | /mnt/disku/packet-capture/sess-1-capsw-ethernet-1-1-U.pcap |

| Pcapsize: | 139826 |
|---------------------|-------------------|
| 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: | 00:00:00:00:00:00 |
| Dest MAC: | 00:00:00:00:00:00 |
| Src Port: | 0 |
| Dest Port: | 0 |
| Ethertype: | 0 |
| | |

Total Physical breakout ports involved in Packet Capture: 0

886 packets captured on disk using switch capture

Reading of capture file from disk is not supported

4. Utilice el comando CLI copy para exportar el archivo a destinos remotos.

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

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

Siga estos pasos en para recopilar archivos de captura de FMC mediante la opción **File Download**:

- 1. Detener la captura:
- > capture capsw switch stop
 - 2. Verifique que la sesión de captura esté detenida y observe el nombre del archivo y la ruta completa del archivo de captura:

```
> show capture capsw detail
Packet Capture info
Name: capsw
Session: 1
Admin State: disabled
Oper State: down
```

Oper State Reason: Session_Admin_Shut Config Success: yes Config Fail Reason: Append Flag: overwrite Session Mem Usage: 256 Session Pcap Snap Len: 1518 Error Code: 0 Drop Count: 0 Total Physical ports involved in Packet Capture: 1 Physical port: Slot Id: 1 Port Id: 1 /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
139826 Pcapfile: Pcapsize: Filter: capsw-1-1 Packet Capture Filter Info Name: capsw-1-1 0 Protocol: 0 Ivlan: Ovlan: 0 0.0.0.0 Src Ip: Dest Ip: 0.0.0.0 Src Ipv6: :: Dest Ipv6: :: 00:00:00:00:00:00 Src MAC: 00:00:00:00:00:00 Dest MAC: Src Port: 0 0 Dest Port: 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. Vaya al modo experto y cambie al modo raíz:

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

4. Copie el archivo de captura en /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 ls -1 /ngfw/var/common/sess*
-rwxr-xr-x 1 root admin 139826 Aug 7 20:14 /ngfw/var/common/sess-1-capsw-ethernet-1-1-0.pcap
-rwxr-xr-x 1 root admin 24 Aug 6 21:58 /ngfw/var/common/sess-1-capsw-ethernet-1-3-0.pcap

En FMC elija Devices > File Download:



6. Elija el FTD, proporcione el nombre del archivo de captura y haga clic en Descargar:

| Firewall Management Center Devices / Troubleshoot / File Download | Analysis Policies | Devices Objects | Integration D | Deploy Q 🚱 🌣 🕲 lab_domain \ admin v 时 escor SECURE |
|--|---|-------------------------------|---------------|---|
| | Device FPR3100-1 File sess-1-capsw-etherne | t-1-1-0.pcap Back Download | | Threat Defense CLI Packet Capture Packet Tracer |
| | | | | |

Directrices, limitaciones y prácticas recomendadas para la captura de paquetes de switches internos

Directrices y limitaciones:

- Se admiten varias sesiones de configuración de captura de switch, pero solo una sesión de captura de switch puede estar activa a la vez. Un intento de habilitar 2 o más sesiones de captura produce un error "ERROR: Error al habilitar la sesión, ya que se alcanzó el límite máximo de 1 sesiones de captura de paquetes activas".
- No se puede eliminar una captura de switch activa.
- Las capturas del switch no se pueden leer en la aplicación. El usuario debe exportar los archivos.
- Ciertas opciones de captura del plano de datos como dump, decode, packet-number, trace y otras no se soportan para las capturas del switch.
- En el caso de ASA multicontexto, las capturas del switch en las interfaces de datos se configuran en contextos de usuario. Las capturas del switch en las interfaces in_data_uplink1 e in_mgmt_uplink1 se soportan solamente en el contexto de administración.

Esta es la lista de prácticas recomendadas basadas en el uso de la captura de paquetes en casos de TAC:

- Tenga en cuenta las directrices y limitaciones.
- Utilice filtros de captura.
- Considere el impacto de NAT en las direcciones IP de paquetes cuando se configura un filtro de captura.
- Aumente o disminuya la **longitud del paquete** que especifica el tamaño de trama, en caso de que difiera del valor predeterminado de 1518 bytes. Un tamaño menor da como resultado un mayor número de paquetes capturados y viceversa.
- Ajuste el tamaño del búfer según sea necesario.
- Tenga en cuenta el comando Drop Count en el resultado del comando show cap
 <cap_name>detail. Una vez alcanzado el límite de tamaño del búfer, el contador de conteo de caídas aumenta.

Información Relacionada

- Guías de configuración de Firepower 4100/9300 Chassis Manager y FXOS CLI
- Guía de inicio de Cisco Secure Firewall 3100
- <u>Referencia de Comandos de Cisco Firepower FXOS 4100/9300</u>

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).