

Configuration et vérification du pare-feu sécurisé et des captures de commutateur interne Firepower

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Présentation générale de l'architecture système](#)

[Présentation générale du fonctionnement des commutateurs internes](#)

[Flux de paquets et points de capture](#)

[Configuration et vérification sur Firepower 4100/9300](#)

[Capture de paquets sur une interface physique ou Port Channel](#)

[Captures de paquets sur les interfaces de fond de panier](#)

[Captures de paquets sur les ports des applications et des applications](#)

[Capture de paquets sur une sous-interface d'une interface physique ou Port Channel](#)

[Filtres de capture de paquets](#)

[Collecter les fichiers de capture du commutateur interne Firepower 4100/9300](#)

[Recommandations, limites et meilleures pratiques pour la capture de paquets de commutateur interne](#)

[Configuration et vérification sur Secure Firewall 3100](#)

[Capture de paquets sur une interface physique ou Port Channel](#)

[Capture de paquets sur une sous-interface d'une interface physique ou Port Channel](#)

[Capture de paquets sur des interfaces internes](#)

[Filtres de capture de paquets](#)

[Collecter les fichiers de capture internes du commutateur Secure Firewall 3100](#)

[Recommandations, limites et meilleures pratiques pour la capture de paquets de commutateur interne](#)

[Informations connexes](#)

Introduction

Ce document décrit la configuration et la vérification de la puissance de feu, ainsi que les captures internes du commutateur Secure Firewall.

Conditions préalables

Conditions requises

Connaissances de base du produit, analyse de capture.

Components Used

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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

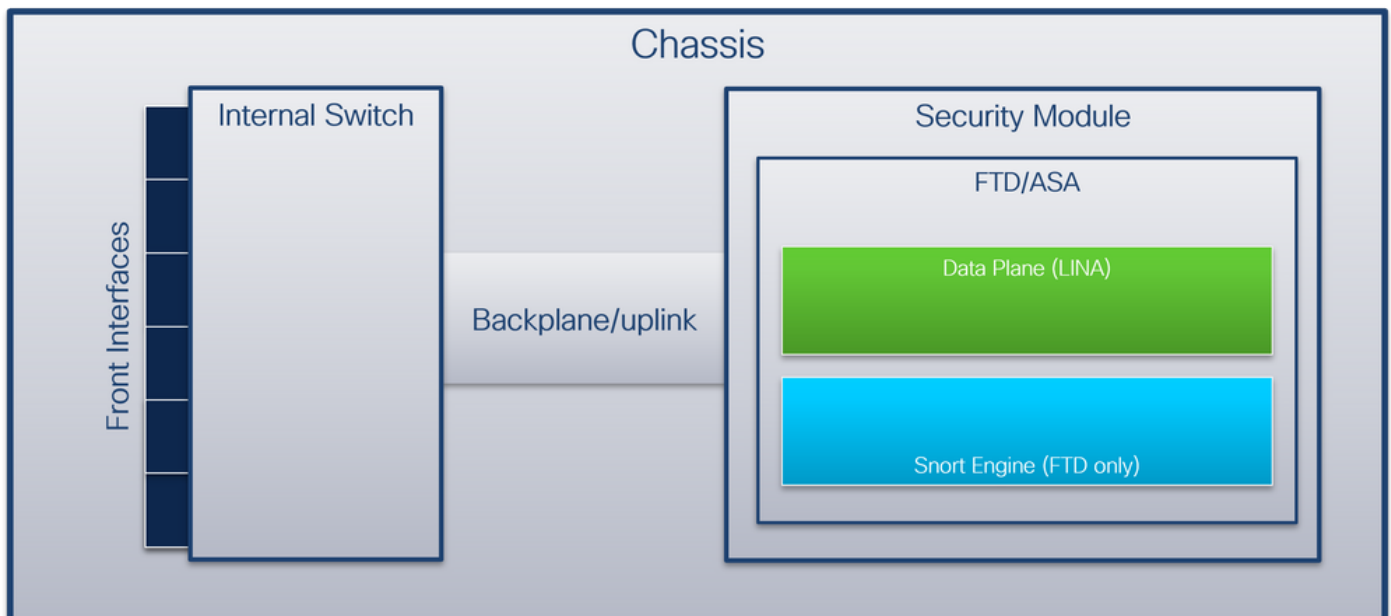
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Pare-feu sécurisé 31xx
- Firepower 41xx
- Firepower 93xx
- Système d'exploitation extensible sécurisé Cisco (FXOS) 2.12.0.x
- Cisco Secure Firewall Threat Defense (FTD) 7.2.0.x
- Cisco Secure Firewall Management Center (FMC) 7.2.0.x
- Cisco Secure Firewall Device Manager (FDM) 7.2.0.x
- Appareil de sécurité adaptatif (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>)

Informations générales

Présentation générale de l'architecture système

Du point de vue du flux de paquets, l'architecture des pare-feu Firepower 4100/9300 et Secure Firewall 3100 peut être visualisée comme illustré dans cette figure :



Le châssis comprend les composants suivants :

- **Commutateur interne** - transfère le paquet du réseau à l'application et vice versa. Le commutateur interne est connecté aux **interfaces avant** qui résident sur le module d'interface intégré ou les modules de réseau externes et se connectent à des périphériques externes, par

exemple, des commutateurs. Ethernet 1/1, Ethernet 2/4, etc. sont des exemples d'interfaces avant. Le « front » n'est pas une définition technique forte. Dans ce document, il est utilisé pour distinguer les interfaces connectées aux périphériques externes des interfaces de fond de panier ou de liaison ascendante.

- **Fond de panier ou liaison ascendante** - interface interne qui connecte le module de sécurité (SM) au commutateur interne. Ce tableau présente les interfaces de fond de panier sur Firepower 4100/9300 et les interfaces de liaison ascendante sur Secure Firewall 3100 :

Plateforme	Nombre de modules de sécurité pris en charge	Interfaces fond de panier/liaison ascendante	Interfaces d'applications mappées
Firepower 4100 (sauf Firepower 4110/4112)	1	SM1 : Ethernet1/9 Ethernet1/10	Internal-Data0/0 Données internes0/1
Firepower 4110/4112	1	Ethernet1/9	Internal-Data0/0 Internal-Data0/0 Données internes0/1
Firepower 9300	3	SM1 : Ethernet1/9 Ethernet1/10 SM2 : Ethernet1/11 Ethernet1/12 SM3 : Ethernet1/13 Ethernet1/14	Internal-Data0/0 Données internes0/1 Internal-Data0/0 Données internes0/1
Pare-feu sécurisé 3100	1	SM1 : in_data_uplink1	Données internes0/1

Dans le cas de 2 interfaces de fond de panier par module, le commutateur interne et les applications sur les modules effectuent un équilibrage de charge de trafic sur les 2 interfaces.

- **Module de sécurité, moteur de sécurité ou lame** - module dans lequel sont installées des applications telles que FTD ou ASA. Firepower 9300 prend en charge jusqu'à 3 modules de sécurité.
- **Interface d'application mappée** - les applications, telles que FTD ou ASA, mappent le fond de panier ou les interfaces de liaison ascendante aux interfaces internes. En d'autres termes, les interfaces de fond de panier ou de liaison ascendante sont visibles en tant qu'interfaces internes dans les applications.

Utilisez la commande **show interface detail** pour vérifier les interfaces internes :

```
> show interface detail | grep Interface
Interface Internal-Control0/0 "ha_ctl_nlp_int_tap", is up, line protocol is up
Control Point Interface States:
  Interface number is 6
  Interface config status is active
  Interface state is active
Interface Internal-Data0/0 "", is up, line protocol is up
Control Point Interface States:
  Interface number is 2
  Interface config status is active
```

```

Interface state is active
Interface Internal-Data0/1 "", is up, line protocol is up
Control Point Interface States:
  Interface number is 3
  Interface config status is active
  Interface state is active
Interface Internal-Data0/2 "nlp_int_tap", is up, line protocol is up
Control Point Interface States:
  Interface number is 4
  Interface config status is active
  Interface state is active
Interface Internal-Data0/3 "ccl_ha_nlp_int_tap", is up, line protocol is up
Control Point Interface States:
  Interface number is 5
  Interface config status is active
  Interface state is active
Interface Internal-Data0/4 "cmi_mgmt_int_tap", is up, line protocol is up
Control Point Interface States:
  Interface number is 7
  Interface config status is active
  Interface state is active
Interface Port-channel6.666 "", is up, line protocol is up
Interface Ethernet1/1 "diagnostic", is up, line protocol is up
Control Point Interface States:
  Interface number is 8
  Interface config status is active
  Interface state is active

```

Présentation générale du fonctionnement des commutateurs internes

Firepower 4100/9300

Pour prendre une décision de transmission, le commutateur interne utilise une **étiquette VLAN d'interface**, ou **étiquette VLAN de port**, et une étiquette **réseau virtuel (étiquette VLAN)**.

L'étiquette VLAN du port est utilisée par le commutateur interne pour identifier une interface. Le commutateur insère l'étiquette VLAN de port dans chaque paquet entrant qui est venu sur les interfaces avant. La balise VLAN est automatiquement configurée par le système et ne peut pas être modifiée manuellement. La valeur de balise peut être vérifiée dans l'interpréteur de commandes **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

```


L'étiquette VN est également insérée par le commutateur interne et utilisée pour transférer les paquets à l'application. Il est automatiquement configuré par le système et ne peut pas être modifié manuellement.

L'étiquette VLAN du port et l'étiquette VLAN sont partagées avec l'application. L'application insère les étiquettes VLAN d'interface de sortie respectives et les étiquettes VLAN dans chaque paquet. Lorsqu'un paquet provenant de l'application est reçu par le commutateur interne sur les interfaces de fond de panier, le commutateur lit l'étiquette VLAN d'interface de sortie et l'étiquette VN, identifie l'application et l'interface de sortie, supprime l'étiquette VLAN de port et l'étiquette VN, et transfère le paquet au réseau.

Pare-feu sécurisé 3100

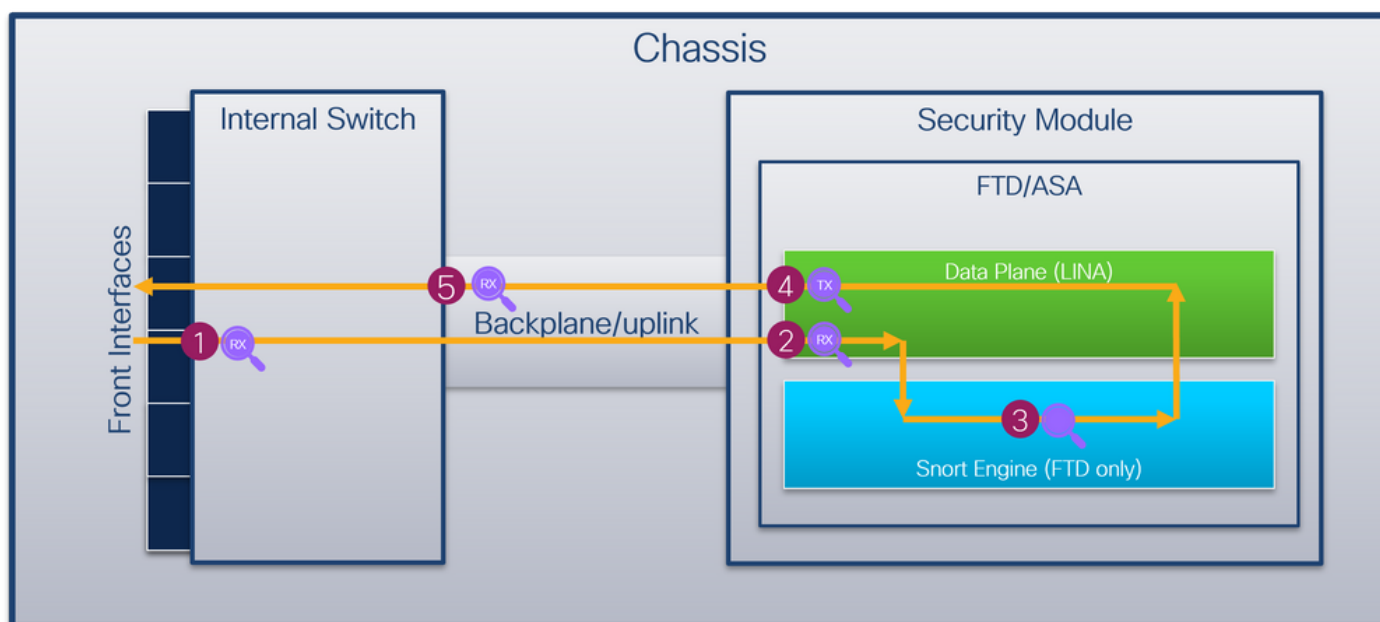
Comme dans Firepower 4100/9300, l'étiquette VLAN du port est utilisée par le commutateur interne pour identifier une interface.

L'étiquette VLAN du port est partagée avec l'application. L'application insère les balises VLAN d'interface de sortie respectives dans chaque paquet. Lorsqu'un paquet provenant de l'application est reçu par le commutateur interne sur l'interface de liaison ascendante, le commutateur lit l'étiquette VLAN de l'interface de sortie, identifie l'interface de sortie, supprime l'étiquette VLAN du port et transfère le paquet au réseau.

Flux de paquets et points de capture

Les pare-feu Firepower 4100/9300 et Secure Firewall 3100 prennent en charge les captures de paquets sur les interfaces du commutateur interne.

Cette figure montre les points de capture de paquets le long du chemin des paquets dans le châssis et l'application :



Les points de capture sont les suivants :

1. Point de capture d'entrée de l'interface avant du commutateur interne. Une interface avant est une interface connectée aux périphériques homologues, tels que les commutateurs.
2. Point de capture d'entrée interface du plan de données

3. Point de capture Snort
4. Point de capture de sortie interface du plan de données
5. Fond de panier interne du commutateur ou point de capture d'entrée de liaison ascendante.
Une interface de fond de panier ou de liaison ascendante connecte le commutateur interne à l'application.

Le commutateur interne prend uniquement en charge les captures d'interface d'entrée. Cela signifie que seuls les paquets reçus du réseau ou de l'application ASA/FTD peuvent être capturés. **Les captures de paquets en sortie ne sont pas prises en charge.**

Configuration et vérification sur Firepower 4100/9300

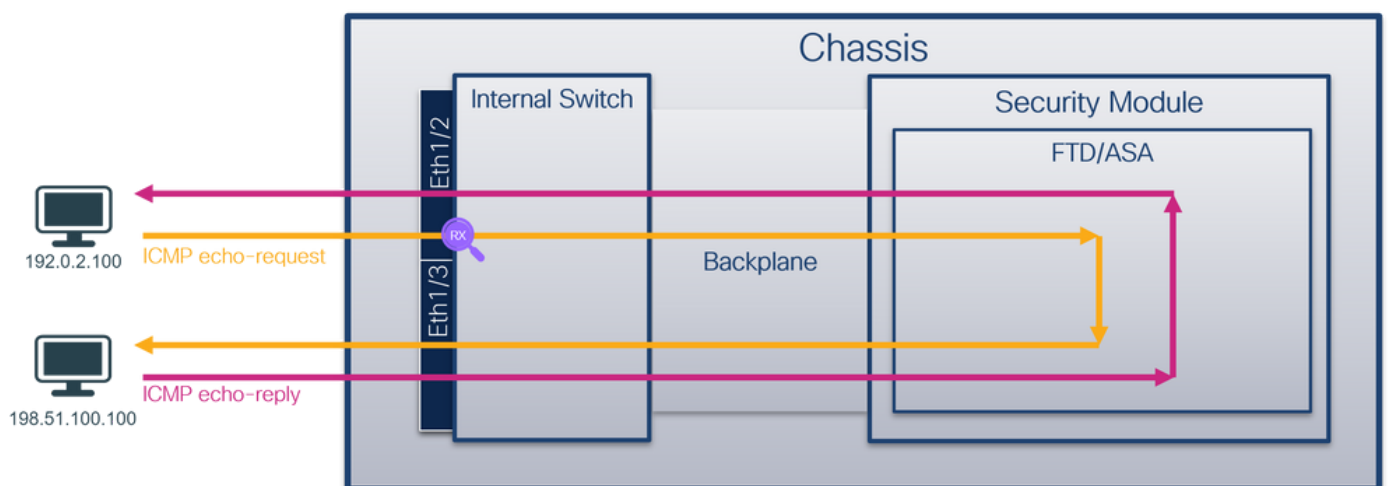
Les captures du commutateur interne Firepower 4100/9300 peuvent être configurées dans **Outils > Capture de paquets** sur FCM ou dans **capture de paquets de portée** dans l'interface de ligne de commande de FXOS. **Pour la description des options de capture de paquets, référez-vous au Guide de configuration de Cisco Firepower 4100/9300 FXOS Chassis Manager ou au Guide de configuration de l'interface de ligne de commande de Cisco Firepower 4100/9300 FXOS, chapitre Troubleshooting, section Packet Capture.**

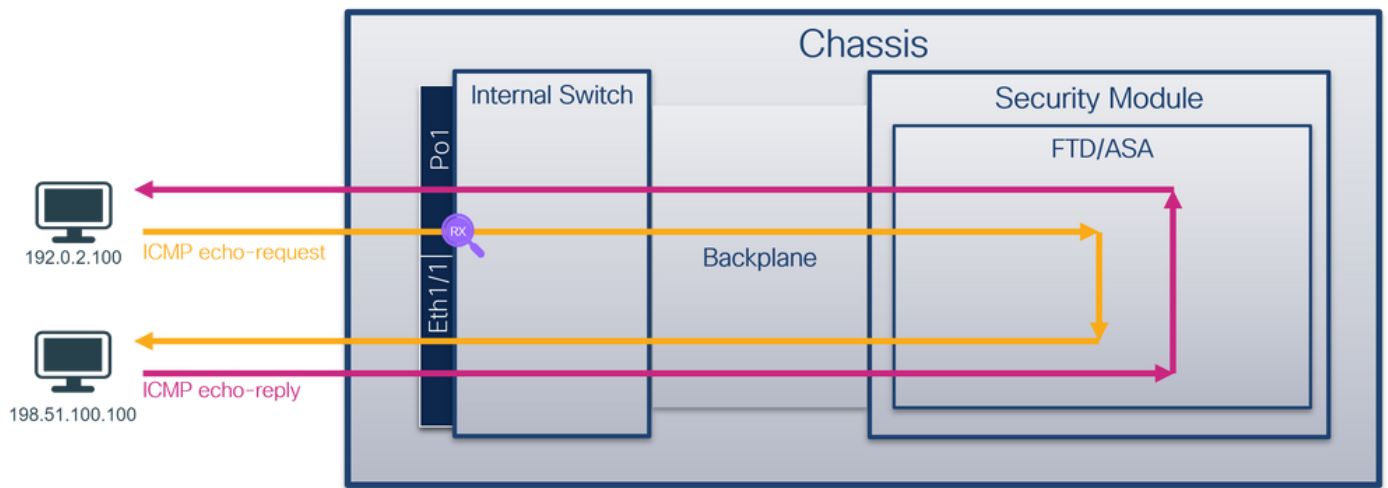
Ces scénarios couvrent les cas d'utilisation courants des captures de commutateur interne Firepower 4100/9300.

Capture de paquets sur une interface physique ou Port Channel

Utilisez FCM et CLI pour configurer et vérifier une capture de paquets sur l'interface Ethernet1/2 ou l'interface Portchannel1. Dans le cas d'une interface port-channel, veillez à sélectionner toutes les interfaces membres physiques.

Topologie, flux de paquets et points de capture



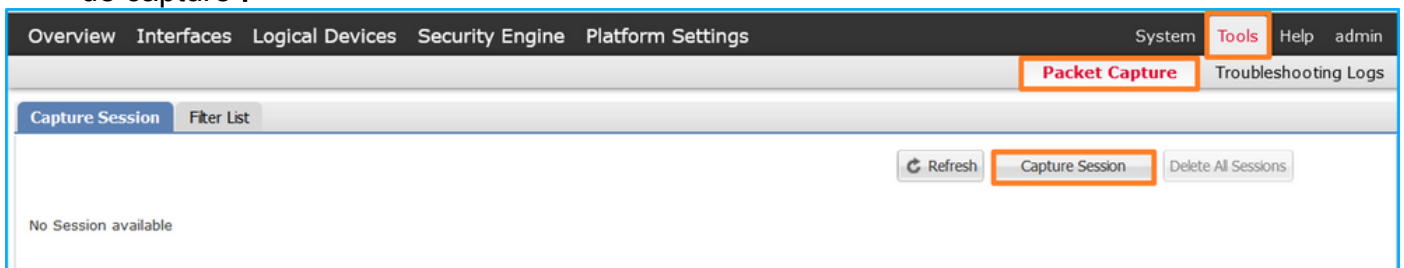


Configuration

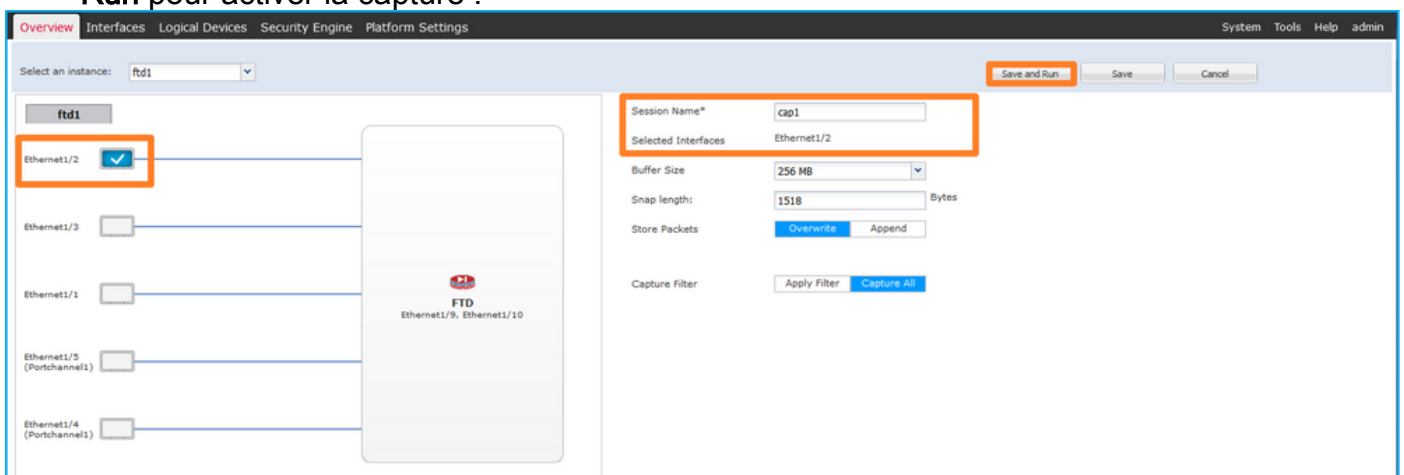
FCM

Procédez comme suit sur FCM pour configurer une capture de paquets sur les interfaces Ethernet1/2 ou Portchannel1 :

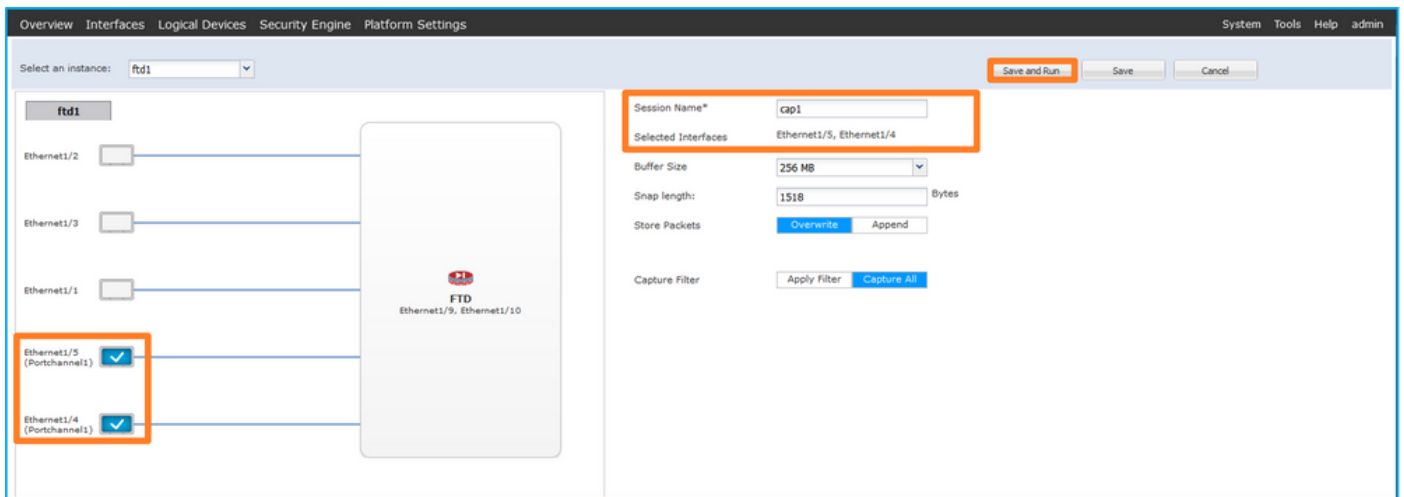
1. Utilisez **Outils > Capture de paquets > Session de capture** pour créer une nouvelle session de capture :



2. Sélectionnez l'interface **Ethernet1/2**, fournissez le nom de la session et cliquez sur **Save and Run** pour activer la capture :



3. Dans le cas d'une interface port-channel, sélectionnez toutes les interfaces membres physiques, fournissez le nom de session et cliquez sur **Save and Run** pour activer la capture :



CLI FXOS

Procédez comme suit sur l'interface de ligne de commande FXOS pour configurer une capture de paquets sur les interfaces Ethernet1/2 ou Portchannel1 :

1. Identifiez le type et l'identificateur de l'application :

```
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           ftd1           1           Enabled   Online           7.2.0.82      7.2.0.82
Native        No              Not Applicable None
```

2. Dans le cas d'une interface port-channel, identifiez ses interfaces membres :

```
firepower# connect fxos
<output skipped>
firepower(fxos) # show port-channel summary
Flags: D - Down          P - Up in port-channel (members)
       I - Individual    H - Hot-standby (LACP only)
       s - Suspended     r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met

-----
Group Port-      Type      Protocol  Member Ports
Channel
-----
1      Po1(SU)    Eth       LACP      Eth1/4(P)  Eth1/5(P)
```

3. Créez une session de capture :

```
firepower# scope packet-capture
firepower /packet-capture # create session cap1
firepower /packet-capture/session* # create phy-port Eth1/2
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # set app-identifier ftd1
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # enable
firepower /packet-capture/session* # commit
firepower /packet-capture/session #
```

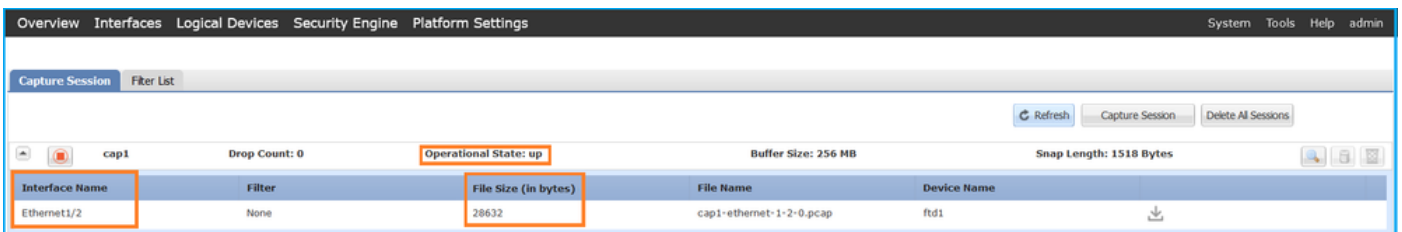
Pour les interfaces port-channel, une capture distincte est configurée pour chaque interface membre :

```
firepower# scope packet-capture
firepower /packet-capture # create session cap1
firepower /packet-capture/session* # create phy-port Eth1/4
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # set app-identifler ftd1
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # create phy-port Eth1/5
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # set app-identifler ftd1
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # enable
firepower /packet-capture/session* # commit
firepower /packet-capture/session #
```

Vérification

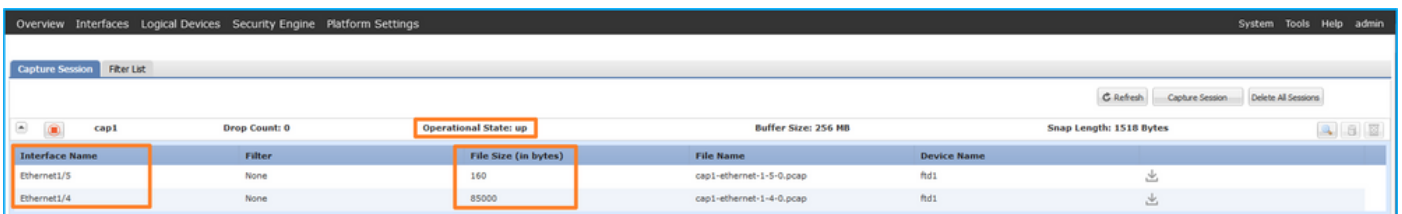
FCM

Vérifiez le nom de l'interface, assurez-vous que l'état opérationnel est up et que la taille du fichier (en octets) augmente :



Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/2	None	28632	cap1-ethernet-1-2-0.pcap	ftd1

Portchannel1 avec interfaces membres Ethernet1/4 et Ethernet1/5 :



Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/5	None	160	cap1-ethernet-1-5-0.pcap	ftd1
Ethernet1/4	None	85000	cap1-ethernet-1-4-0.pcap	ftd1

CLI FXOS

Vérifiez les détails de capture dans la portée 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

Port-channel 1 avec interfaces membres Ethernet1/4 et 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

Collecter les fichiers de capture

Suivez les étapes de la section **Collecter les fichiers de capture internes du commutateur Firepower 4100/9300**.

Capturer l'analyse des fichiers

Utilisez une application de lecture de fichier de capture de paquets pour ouvrir le fichier de capture pour Ethernet1/2. Sélectionnez le premier paquet et vérifiez les points clés :

1. Seuls les paquets de requête d'écho ICMP sont capturés. Chaque paquet est capturé et affiché 2 fois.
2. L'en-tête de paquet d'origine est sans étiquette VLAN.
3. Le commutateur interne insère une étiquette VLAN de port supplémentaire 102 qui identifie l'interface d'entrée Ethernet1/2.
4. Le commutateur interne insère une étiquette VN supplémentaire.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-07-13 06:23:58.285080930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found)
2	2022-07-13 06:23:58.285082858	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found)
3	2022-07-13 06:23:59.309848886	192.0.2.100	198.51.100.100	ICMP	108	0x9e00 (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found)
4	2022-07-13 06:23:59.309193731	192.0.2.100	198.51.100.100	ICMP	108	0x9e00 (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found)
5	2022-07-13 06:24:00.333054190	192.0.2.100	198.51.100.100	ICMP	108	0x9f20 (40736)	64	Echo (ping) request id=0x001a, seq=9/2304, ttl=64 (no response found)
6	2022-07-13 06:24:00.333056014	192.0.2.100	198.51.100.100	ICMP	108	0x9f20 (40736)	64	Echo (ping) request id=0x001a, seq=9/2304, ttl=64 (no response found)
7	2022-07-13 06:24:01.357173530	192.0.2.100	198.51.100.100	ICMP	108	0x9f2d (40749)	64	Echo (ping) request id=0x001a, seq=10/2560, ttl=64 (no response found)
8	2022-07-13 06:24:01.357174708	192.0.2.100	198.51.100.100	ICMP	108	0x9f2d (40749)	64	Echo (ping) request id=0x001a, seq=10/2560, ttl=64 (no response found)
9	2022-07-13 06:24:02.381073741	192.0.2.100	198.51.100.100	ICMP	108	0x9f88 (40840)	64	Echo (ping) request id=0x001a, seq=11/2816, ttl=64 (no response found)
10	2022-07-13 06:24:02.381074999	192.0.2.100	198.51.100.100	ICMP	108	0x9f88 (40840)	64	Echo (ping) request id=0x001a, seq=11/2816, ttl=64 (no response found)
11	2022-07-13 06:24:03.405199041	192.0.2.100	198.51.100.100	ICMP	108	0xa077 (41079)	64	Echo (ping) request id=0x001a, seq=12/3072, ttl=64 (no response found)
12	2022-07-13 06:24:03.405200261	192.0.2.100	198.51.100.100	ICMP	108	0xa077 (41079)	64	Echo (ping) request id=0x001a, seq=12/3072, ttl=64 (no response found)
13	2022-07-13 06:24:04.429155683	192.0.2.100	198.51.100.100	ICMP	108	0xa10f (41231)	64	Echo (ping) request id=0x001a, seq=13/3328, ttl=64 (no response found)
14	2022-07-13 06:24:04.429156831	192.0.2.100	198.51.100.100	ICMP	108	0xa10f (41231)	64	Echo (ping) request id=0x001a, seq=13/3328, ttl=64 (no response found)
15	2022-07-13 06:24:05.453156612	192.0.2.100	198.51.100.100	ICMP	108	0xa16a (41322)	64	Echo (ping) request id=0x001a, seq=14/3584, ttl=64 (no response found)
16	2022-07-13 06:24:05.453158052	192.0.2.100	198.51.100.100	ICMP	108	0xa16a (41322)	64	Echo (ping) request id=0x001a, seq=14/3584, ttl=64 (no response found)
17	2022-07-13 06:24:06.477127687	192.0.2.100	198.51.100.100	ICMP	108	0xa1e9 (41449)	64	Echo (ping) request id=0x001a, seq=15/3840, ttl=64 (no response found)
18	2022-07-13 06:24:06.477129899	192.0.2.100	198.51.100.100	ICMP	108	0xa1e9 (41449)	64	Echo (ping) request id=0x001a, seq=15/3840, ttl=64 (no response found)
19	2022-07-13 06:24:07.501291314	192.0.2.100	198.51.100.100	ICMP	108	0xa1f6 (41462)	64	Echo (ping) request id=0x001a, seq=16/4096, ttl=64 (no response found)
20	2022-07-13 06:24:07.501293041	192.0.2.100	198.51.100.100	ICMP	108	0xa1f6 (41462)	64	Echo (ping) request id=0x001a, seq=16/4096, ttl=64 (no response found)
21	2022-07-13 06:24:08.525089956	192.0.2.100	198.51.100.100	ICMP	108	0xa257 (41559)	64	Echo (ping) request id=0x001a, seq=17/4352, ttl=64 (no response found)
22	2022-07-13 06:24:08.525092088	192.0.2.100	198.51.100.100	ICMP	108	0xa257 (41559)	64	Echo (ping) request id=0x001a, seq=17/4352, ttl=64 (no response found)
23	2022-07-13 06:24:09.549236500	192.0.2.100	198.51.100.100	ICMP	108	0xa2a9 (41641)	64	Echo (ping) request id=0x001a, seq=18/4608, ttl=64 (no response found)
24	2022-07-13 06:24:09.549238564	192.0.2.100	198.51.100.100	ICMP	108	0xa2a9 (41641)	64	Echo (ping) request id=0x001a, seq=18/4608, ttl=64 (no response found)
25	2022-07-13 06:24:10.573110146	192.0.2.100	198.51.100.100	ICMP	108	0xa345 (41797)	64	Echo (ping) request id=0x001a, seq=19/4864, ttl=64 (no response found)
26	2022-07-13 06:24:10.573112504	192.0.2.100	198.51.100.100	ICMP	108	0xa345 (41797)	64	Echo (ping) request id=0x001a, seq=19/4864, ttl=64 (no response found)
27	2022-07-13 06:24:11.597086071	192.0.2.100	198.51.100.100	ICMP	108	0xa349 (41801)	64	Echo (ping) request id=0x001a, seq=20/5120, ttl=64 (no response found)
28	2022-07-13 06:24:11.597088170	192.0.2.100	198.51.100.100	ICMP	108	0xa349 (41801)	64	Echo (ping) request id=0x001a, seq=20/5120, ttl=64 (no response found)
29	2022-07-13 06:24:12.621061022	192.0.2.100	198.51.100.100	ICMP	108	0xa3dc (41948)	64	Echo (ping) request id=0x001a, seq=21/5376, ttl=64 (no response found)

Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_1, id 0
 Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)

VN-Tag

1. = Direction: From Bridge
 .0. = Pointer: vif_id
 ..00 0000 0000 1010 = Destination: 10
 = Looped: No
 = Reserved: 0
 = Version: 0
 0000 0000 0000 = Source: 0
 Type: 802.1Q Virtual LAN (0x8100)

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
 000. = Priority: Best Effort (default) (0)
 ...0 = DEI: Ineligible
 ... 0000 0110 0110 = ID: 102
 Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
 Internet Control Message Protocol

Sélectionnez le deuxième paquet et vérifiez les points clés :

1. Seuls les paquets de requête d'écho ICMP sont capturés. Chaque paquet est capturé et affiché 2 fois.
2. L'en-tête de paquet d'origine est sans étiquette VLAN.
3. Le commutateur interne insère une étiquette VLAN de port supplémentaire 102 qui identifie l'interface d'entrée Ethernet1/2.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-07-13 06:23:58.28508930	192.0.2.100	198.51.100.100	ICMP	108	0x90dc (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found)
2	2022-07-13 06:23:58.285088258	192.0.2.100	198.51.100.100	ICMP	102	0x90dc (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found)
3	2022-07-13 06:23:59.309048886	192.0.2.100	198.51.100.100	ICMP	108	0x9e0d (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found)
4	2022-07-13 06:23:59.309193731	192.0.2.100	198.51.100.100	ICMP	102	0x9e0d (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found)
5	2022-07-13 06:24:00.333054190	192.0.2.100	198.51.100.100	ICMP	108	0xf920 (40736)	64	Echo (ping) request id=0x001a, seq=9/2304, ttl=64 (no response found)
6	2022-07-13 06:24:00.333056014	192.0.2.100	198.51.100.100	ICMP	102	0xf920 (40736)	64	Echo (ping) request id=0x001a, seq=9/2304, ttl=64 (no response found)
7	2022-07-13 06:24:01.357173530	192.0.2.100	198.51.100.100	ICMP	108	0xf92d (40749)	64	Echo (ping) request id=0x001a, seq=10/2560, ttl=64 (no response found)
8	2022-07-13 06:24:01.357174708	192.0.2.100	198.51.100.100	ICMP	102	0xf92d (40749)	64	Echo (ping) request id=0x001a, seq=10/2560, ttl=64 (no response found)
9	2022-07-13 06:24:02.381073741	192.0.2.100	198.51.100.100	ICMP	108	0xf988 (40840)	64	Echo (ping) request id=0x001a, seq=11/2816, ttl=64 (no response found)
10	2022-07-13 06:24:02.381074999	192.0.2.100	198.51.100.100	ICMP	102	0xf988 (40840)	64	Echo (ping) request id=0x001a, seq=11/2816, ttl=64 (no response found)
11	2022-07-13 06:24:03.405199041	192.0.2.100	198.51.100.100	ICMP	108	0xa077 (41079)	64	Echo (ping) request id=0x001a, seq=12/3072, ttl=64 (no response found)
12	2022-07-13 06:24:03.405200261	192.0.2.100	198.51.100.100	ICMP	102	0xa077 (41079)	64	Echo (ping) request id=0x001a, seq=12/3072, ttl=64 (no response found)
13	2022-07-13 06:24:04.429155683	192.0.2.100	198.51.100.100	ICMP	108	0xa10f (41231)	64	Echo (ping) request id=0x001a, seq=13/3328, ttl=64 (no response found)
14	2022-07-13 06:24:04.429156831	192.0.2.100	198.51.100.100	ICMP	102	0xa10f (41231)	64	Echo (ping) request id=0x001a, seq=13/3328, ttl=64 (no response found)
15	2022-07-13 06:24:05.453158612	192.0.2.100	198.51.100.100	ICMP	108	0xa16a (41322)	64	Echo (ping) request id=0x001a, seq=14/3584, ttl=64 (no response found)
16	2022-07-13 06:24:05.453158052	192.0.2.100	198.51.100.100	ICMP	102	0xa16a (41322)	64	Echo (ping) request id=0x001a, seq=14/3584, ttl=64 (no response found)
17	2022-07-13 06:24:06.477127687	192.0.2.100	198.51.100.100	ICMP	108	0xa1e9 (41449)	64	Echo (ping) request id=0x001a, seq=15/3840, ttl=64 (no response found)
18	2022-07-13 06:24:06.477129899	192.0.2.100	198.51.100.100	ICMP	102	0xa1e9 (41449)	64	Echo (ping) request id=0x001a, seq=15/3840, ttl=64 (no response found)
19	2022-07-13 06:24:07.501291314	192.0.2.100	198.51.100.100	ICMP	108	0xa1f6 (41462)	64	Echo (ping) request id=0x001a, seq=16/4096, ttl=64 (no response found)
20	2022-07-13 06:24:07.501293041	192.0.2.100	198.51.100.100	ICMP	102	0xa1f6 (41462)	64	Echo (ping) request id=0x001a, seq=16/4096, ttl=64 (no response found)
21	2022-07-13 06:24:08.525098956	192.0.2.100	198.51.100.100	ICMP	108	0xa257 (41599)	64	Echo (ping) request id=0x001a, seq=17/4352, ttl=64 (no response found)
22	2022-07-13 06:24:08.525092888	192.0.2.100	198.51.100.100	ICMP	102	0xa257 (41599)	64	Echo (ping) request id=0x001a, seq=17/4352, ttl=64 (no response found)
23	2022-07-13 06:24:09.549236500	192.0.2.100	198.51.100.100	ICMP	108	0xa2a9 (41641)	64	Echo (ping) request id=0x001a, seq=18/4608, ttl=64 (no response found)
24	2022-07-13 06:24:09.549238554	192.0.2.100	198.51.100.100	ICMP	102	0xa2a9 (41641)	64	Echo (ping) request id=0x001a, seq=18/4608, ttl=64 (no response found)
25	2022-07-13 06:24:10.573110146	192.0.2.100	198.51.100.100	ICMP	108	0xa345 (41797)	64	Echo (ping) request id=0x001a, seq=19/4864, ttl=64 (no response found)
26	2022-07-13 06:24:10.573112504	192.0.2.100	198.51.100.100	ICMP	102	0xa345 (41797)	64	Echo (ping) request id=0x001a, seq=19/4864, ttl=64 (no response found)
27	2022-07-13 06:24:11.597086627	192.0.2.100	198.51.100.100	ICMP	108	0xa349 (41801)	64	Echo (ping) request id=0x001a, seq=20/5120, ttl=64 (no response found)
28	2022-07-13 06:24:11.597088170	192.0.2.100	198.51.100.100	ICMP	102	0xa349 (41801)	64	Echo (ping) request id=0x001a, seq=20/5120, ttl=64 (no response found)
29	2022-07-13 06:24:12.621061022	192.0.2.100	198.51.100.100	ICMP	108	0xa3dc (41948)	64	Echo (ping) request id=0x001a, seq=21/5376, ttl=64 (no response found)

Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture_u0_1, id 0
 Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)

802.1Q ID (0x0800)

000. = Priority: Best Effort (default) (0)
 ...0 = DEI: Ineligible
 ... 0000 0110 0110 = ID: 102
 Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100

Internet Control Message Protocol

```

0000 58 97 bd b9 77 0e 00 50 56 9d e8 be 81 00 00 66 X...w:P V.....f
0010 08 00 45 00 00 54 9d ec 40 00 40 01 af c0 c0 00 ..E..T..@.....d
0020 02 64 c6 33 64 64 08 00 4e a2 00 1a 00 07 f4 64 -d-3dd..N.....d
0030 ce 62 00 00 00 20 a2 07 00 00 00 00 10 11 1b .....:.....
0040 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 .....:.....I
0050 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 "#$%&'()*+,-./01
0060 32 33 34 35 36 37 234567
  
```

Ouvrez les fichiers de capture pour les interfaces membres Portchannel1. Sélectionnez le premier paquet et vérifiez les points clés :

1. Seuls les paquets de requête d'écho ICMP sont capturés. Chaque paquet est capturé et affiché 2 fois.
2. L'en-tête de paquet d'origine est sans étiquette VLAN.
3. Le commutateur interne insère une étiquette VLAN de port supplémentaire 1001 qui identifie l'interface d'entrée Portchannel1.
4. Le LAN interne insère une étiquette VN supplémentaire.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-05 23:07:31.865872877	192.0.2.100	198.51.100.100	ICMP	108	0x322e (12846)	64	Echo (ping) request id=0x002d, seq=245/62720, ttl=64 (no response found)
2	2022-08-05 23:07:31.865875131	192.0.2.100	198.51.100.100	ICMP	102	0x322e (12846)	64	Echo (ping) request id=0x002d, seq=245/62720, ttl=64 (no response found)
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 (no response found)
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 (no response found)
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 (no response found)
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 (no response found)
7	2022-08-05 23:07:34.883049425	192.0.2.100	198.51.100.100	ICMP	108	0x3373 (13171)	64	Echo (ping) request id=0x002d, seq=248/63488, ttl=64 (no response found)
8	2022-08-05 23:07:34.883051449	192.0.2.100	198.51.100.100	ICMP	102	0x3373 (13171)	64	Echo (ping) request id=0x002d, seq=248/63488, ttl=64 (no response found)
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 (no response found)
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 (no response found)
11	2022-08-05 23:07:36.889741625	192.0.2.100	198.51.100.100	ICMP	108	0x344e (13534)	64	Echo (ping) request id=0x002d, seq=250/64000, ttl=64 (no response found)
12	2022-08-05 23:07:36.889742853	192.0.2.100	198.51.100.100	ICMP	102	0x344e (13534)	64	Echo (ping) request id=0x002d, seq=250/64000, ttl=64 (no response found)
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 (no response found)
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 (no response found)
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 (no response found)
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 (no response found)
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 (no response found)
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 (no response found)
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 (no response found)

Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_3, id 0
 Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: a2:76:f2:00:00:25 (a2:76:f2:00:00:25)

VN-Tag

1. = Direction: From Bridge
 .0. = Pointer: vif_id
 ..00 0000 0101 0100 = Destination: 84
 = Looped: No
 = Reserved: 0
 = Version: 0
 0000 0000 0000 = Source: 0
 Type: 802.1Q Virtual LAN (0x8100)

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1001

000. = Priority: Best Effort (default) (0)
 ...0 = DEI: Ineligible
 ... 0011 1110 1001 = ID: 1001
 Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100

Internet Control Message Protocol

```

0000 a2 76 f2 00 00 25 00 50 56 9d e8 be 89 26 80 54 v...%P V.....&T
0010 00 00 81 00 03 e9 08 00 45 00 00 54 32 2e 40 00 .....E..T2.@
0020 40 01 1b 7f c0 00 02 64 c6 33 64 64 08 00 1e d6 @.....d-3dd...
0030 00 2d 00 f5 a6 a2 ed 62 00 00 00 00 7a 2f 0b 00 .....b....z/..
0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b .....:.....
0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ....!#" $%&'()*+
0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,--./0123 4567
  
```

Sélectionnez le deuxième paquet et vérifiez les points clés :

1. Seuls les paquets de requête d'écho ICMP sont capturés. Chaque paquet est capturé et affiché 2 fois.
2. L'en-tête de paquet d'origine est sans étiquette VLAN.

3. Le commutateur interne insère une étiquette VLAN de port supplémentaire 1001 qui identifie l'interface d'entrée Portchannel1.

The screenshot shows a packet capture in Wireshark. The top pane displays a list of 19 ICMP Echo (ping) requests. The IP ID is consistently 0x322e (12846) and the IP TTL is 64. The bottom pane shows the details of packet 2, which is an ICMP Echo request. The Ethernet II layer is highlighted, showing a Priority of Best Effort (default) (0) and a VLAN ID of 1001. The Internet Protocol Version 4 layer shows the source as 192.0.2.100 and the destination as 198.51.100.100. The Internet Control Message Protocol layer is also highlighted.

Explication

Lorsqu'une capture de paquets sur une interface avant est configurée, le commutateur capture simultanément chaque paquet deux fois :

- Après l'insertion de l'étiquette VLAN du port.
- Après l'insertion de la balise VN.

Dans l'ordre des opérations, l'étiquette VLAN est insérée à un stade ultérieur à celui de l'insertion de l'étiquette VLAN du port. Cependant, dans le fichier de capture, le paquet avec l'étiquette VLAN est affiché plus tôt que le paquet avec l'étiquette VLAN de port.

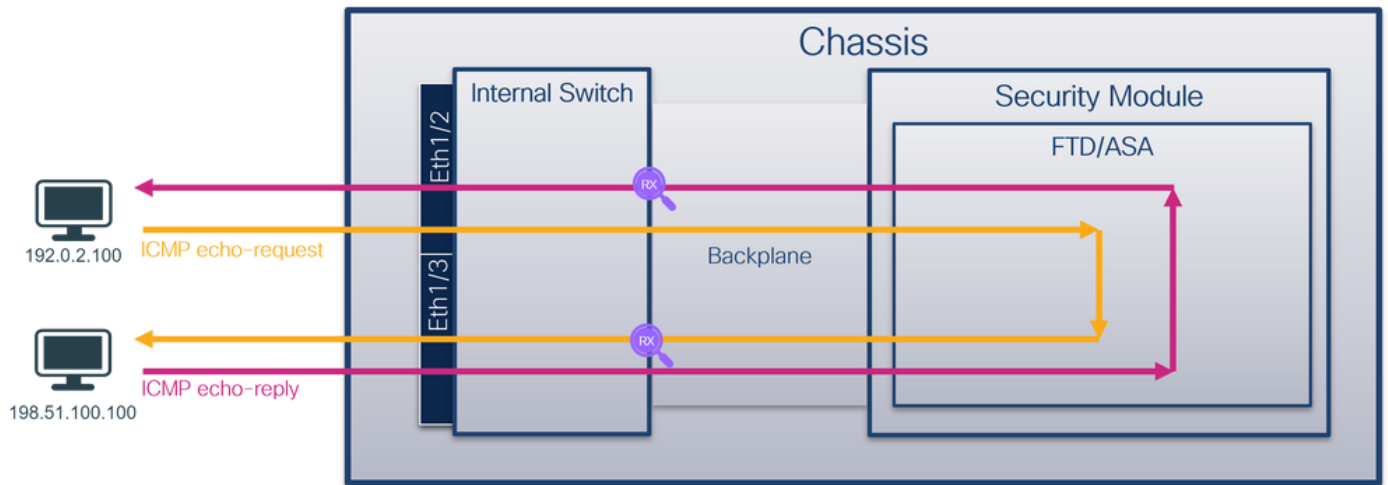
Ce tableau récapitule la tâche :

Tâche	Point de capture	VLAN de port interne dans les paquets capturés	Direction	Trafic capturé
Configurer et vérifier une capture de paquets sur l'interface Ethernet1/2	Ethernet1/2	102	Entrée uniquement	Requêtes d'écho ICMP de l'hôte 192.0.2.100 vers l'hôte 198.51.100.100
Configurez et vérifiez une capture de paquets sur l'interface Portchannel1 avec les interfaces membres Ethernet1/4 et Ethernet1/5	Ethernet1/4 Ethernet1/5	1001	Entrée uniquement	Requêtes d'écho ICMP de l'hôte 192.0.2.100 vers l'hôte 198.51.100.100

Captures de paquets sur les interfaces de fond de panier

Utilisez FCM et CLI pour configurer et vérifier une capture de paquets sur les interfaces de fond de panier.

Topologie, flux de paquets et points de capture

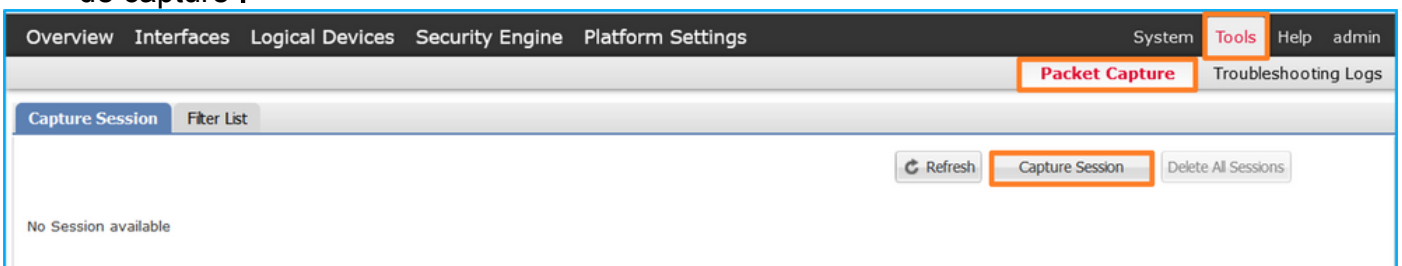


Configuration

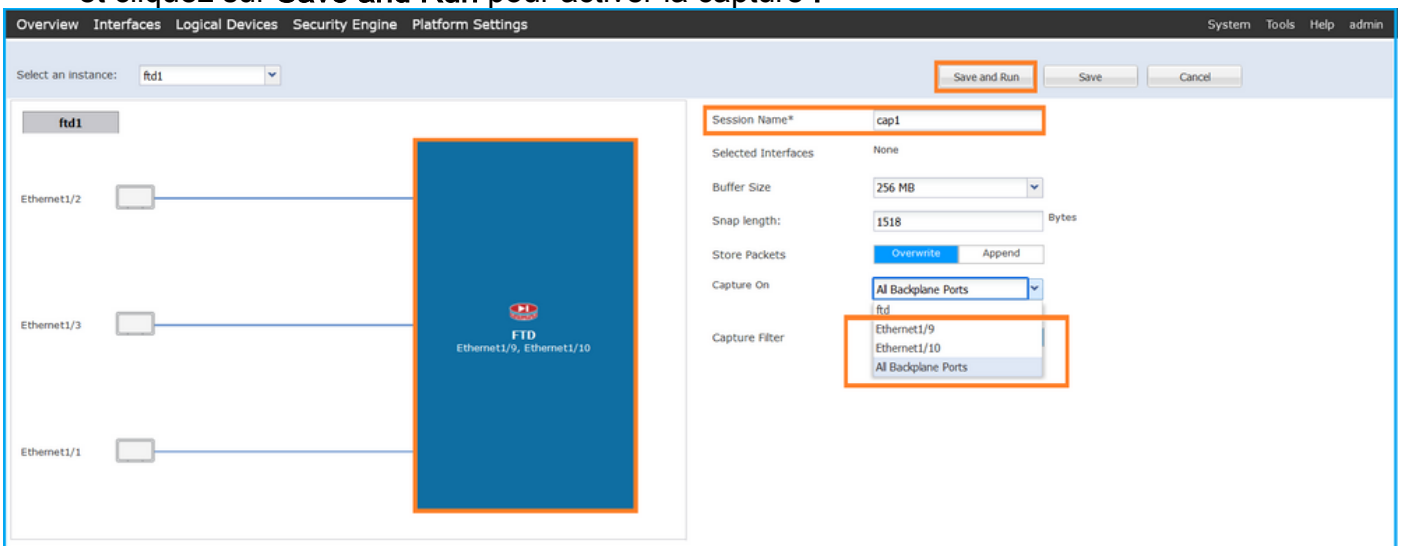
FCM

Procédez comme suit sur FCM pour configurer les captures de paquets sur les interfaces de fond de panier :

1. Utilisez **Outils > Capture de paquets > Session de capture** pour créer une nouvelle session de capture :



2. Pour capturer des paquets sur toutes les interfaces de fond de panier, sélectionnez l'application, puis **All Backplane Ports** dans la liste déroulante **Capture On**. Vous pouvez également choisir l'interface de fond de panier spécifique. Dans ce cas, les interfaces de fond de panier Ethernet1/9 et Ethernet1/10 sont disponibles. Fournissez le **nom de session** et cliquez sur **Save and Run** pour activer la capture :



CLI FXOS

Procédez comme suit sur l'interface de ligne de commande FXOS pour configurer les captures de paquets sur les interfaces de fond de panier :

1. Identifiez le type et l'identificateur de l'application :

```
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          ftd1          1          Enabled      Online          7.2.0.82      7.2.0.82
Native      No            Not Applicable None
```

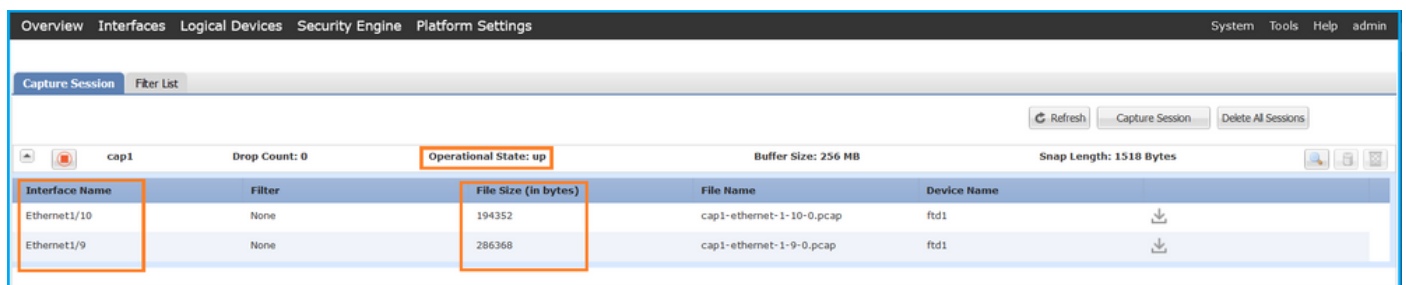
2. Créez une session de capture :

```
firepower# scope packet-capture
firepower /packet-capture # create session cap1
firepower /packet-capture/session* # create phy-port Eth1/9
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # set app-identifiant ftd1
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # create phy-port Eth1/10
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # set app-identifiant ftd1
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # enable
firepower /packet-capture/session* # commit
firepower /packet-capture/session #
```

Vérification

FCM

Vérifiez le nom de l'interface, assurez-vous que l'état opérationnel est up et que la taille du fichier (en octets) augmente :



CLI FXOS

Vérifiez les détails de capture dans la portée 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

Application Name: ftd

Collecter les fichiers de capture

Suivez les étapes de la section **Collecter les fichiers de capture internes du commutateur Firepower 4100/9300**.

Capturer l'analyse des fichiers

Utilisez une application de lecture de fichiers de capture de paquets pour ouvrir les fichiers de capture. Dans le cas de plusieurs interfaces de fond de panier, assurez-vous d'ouvrir tous les fichiers de capture pour chaque interface de fond de panier. Dans ce cas, les paquets sont capturés sur l'interface de fond de panier Ethernet1/9.

Sélectionnez le premier et le deuxième paquet, puis vérifiez les points clés :

1. Chaque paquet de requête d'écho ICMP est capturé et affiché 2 fois.
2. L'en-tête de paquet d'origine est sans étiquette VLAN.
3. Le commutateur interne insère une étiquette VLAN de port supplémentaire **103** qui identifie l'interface de sortie Ethernet1/3.
4. Le commutateur interne insère une étiquette VN supplémentaire.

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	198.51.100.100	192.0.2.100	ICMP	108	0xc2c2 (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 2)
4	2022-07-14 20:20:36.514119312	198.51.100.100	192.0.2.100	ICMP	108	0xc2c2 (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	192.0.2.100	ICMP	108	0xc9b9 (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 6)
8	2022-07-14 20:20:37.538048311	198.51.100.100	192.0.2.100	ICMP	108	0xc9b9 (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64
9	2022-07-14 20:20:38.561776064	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (no response found!)
10	2022-07-14 20:20:38.561778310	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (reply in 11)
11	2022-07-14 20:20:38.562048288	198.51.100.100	192.0.2.100	ICMP	108	0xc4c4 (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 10)
12	2022-07-14 20:20:38.562050333	198.51.100.100	192.0.2.100	ICMP	108	0xc4c4 (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	192.0.2.100	ICMP	108	0xcdbd (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	192.0.2.100	ICMP	108	0xcdbd (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	0x5b7e (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	0x5b7e (23419)	64	Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (reply in 19)
19	2022-07-14 20:20:40.610179685	198.51.100.100	192.0.2.100	ICMP	108	0xcdf8 (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64 (request in 18)
20	2022-07-14 20:20:40.610181944	198.51.100.100	192.0.2.100	ICMP	108	0xcdf8 (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, ttl=64 (no response found!)
22	2022-07-14 20:20:41.633806997	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (reply in 23)
23	2022-07-14 20:20:41.634084102	198.51.100.100	192.0.2.100	ICMP	108	0xc3e6 (52790)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64 (request in 22)
24	2022-07-14 20:20:41.634085368	198.51.100.100	192.0.2.100	ICMP	108	0xc3e6 (52790)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64
25	2022-07-14 20:20:42.657709988	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (no response found!)
26	2022-07-14 20:20:42.657711660	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (reply in 27)
27	2022-07-14 20:20:42.657980675	198.51.100.100	192.0.2.100	ICMP	108	0xc649 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64 (request in 26)
28	2022-07-14 20:20:42.657981971	198.51.100.100	192.0.2.100	ICMP	108	0xc649 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64
29	2022-07-14 20:20:43.681736697	192.0.2.100	198.51.100.100	ICMP	108	0x5c52 (23634)	64	Echo (ping) request id=0x0001, seq=22/5632, ttl=64 (no response found!)

> Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
 > Ethernet II, Src: Cisco b9:77:2d (58:97:bd:b9:77:2d), Dst: VMware 9d:e7:50 (00:50:56:9d:e7:50)

```

  0000 00 50 56 9d e7 50 58 97 bd b9 77 2d 89 26 00 00  -PV-PX- -w-&-
  0010 00 0a 81 00 00 67 08 00 45 00 00 54 59 90 40 00  -...g- E-TY@
  0020 40 01 f4 1c c0 00 02 64 c6 33 64 64 08 00 22 68  @-----d 3dd-~h
  0030 00 01 00 0f 89 7a d0 62 00 00 00 00 b3 d7 09 00  -...z-b -.....
  0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b  -.....
  0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b  !"# $%&'()*+
  0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37  -.../0123 4567
  
```

0 = Direction: To Bridge
 .0. = Pointer: vif_id
 ..00 0000 0000 0000 = Destination: 0
0 = Looped: No
0 = Reserved: 0
00 = Version: 0
0000 0000 1010 = Source: 10
 Type: 802.1Q Virtual LAN (0x8100)
 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 103
 000. = Priority: Best Effort (default) (0)
 ...0 = DEI: Ineligible
0000 0110 0111 = ID: 103
 Type: IPv4 (0x0800)
 > Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
 > Internet Control Message Protocol

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	198.51.100.100	192.0.2.100	ICMP	108	0xc2c2 (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 2)
4	2022-07-14 20:20:36.514119312	198.51.100.100	192.0.2.100	ICMP	108	0xc2c2 (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	192.0.2.100	ICMP	108	0xc9b9 (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 6)
8	2022-07-14 20:20:37.538048311	198.51.100.100	192.0.2.100	ICMP	108	0xc9b9 (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64
9	2022-07-14 20:20:38.561776064	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (no response found!)
10	2022-07-14 20:20:38.561778310	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (reply in 11)
11	2022-07-14 20:20:38.562048288	198.51.100.100	192.0.2.100	ICMP	108	0xc4c4 (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 10)
12	2022-07-14 20:20:38.562050333	198.51.100.100	192.0.2.100	ICMP	108	0xc4c4 (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	192.0.2.100	ICMP	108	0xcdbd (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	192.0.2.100	ICMP	108	0xcdbd (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	0x5b7e (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	0x5b7e (23419)	64	Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (reply in 19)
19	2022-07-14 20:20:40.610179685	198.51.100.100	192.0.2.100	ICMP	108	0xcdf8 (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64 (request in 18)
20	2022-07-14 20:20:40.610181944	198.51.100.100	192.0.2.100	ICMP	108	0xcdf8 (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, ttl=64 (no response found!)
22	2022-07-14 20:20:41.633806997	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (reply in 23)
23	2022-07-14 20:20:41.634084102	198.51.100.100	192.0.2.100	ICMP	108	0xc3e6 (52790)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64 (request in 22)
24	2022-07-14 20:20:41.634085368	198.51.100.100	192.0.2.100	ICMP	108	0xc3e6 (52790)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64
25	2022-07-14 20:20:42.657709988	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (no response found!)
26	2022-07-14 20:20:42.657711660	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (reply in 27)
27	2022-07-14 20:20:42.657980675	198.51.100.100	192.0.2.100	ICMP	108	0xc649 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64 (request in 26)
28	2022-07-14 20:20:42.657981971	198.51.100.100	192.0.2.100	ICMP	108	0xc649 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64
29	2022-07-14 20:20:43.681736697	192.0.2.100	198.51.100.100	ICMP	108	0x5c52 (23634)	64	Echo (ping) request id=0x0001, seq=22/5632, ttl=64 (no response found!)

> Frame 2: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
 > Ethernet II, Src: Cisco b9:77:2d (58:97:bd:b9:77:2d), Dst: VMware 9d:e7:50 (00:50:56:9d:e7:50)

```

  0000 00 50 56 9d e7 50 58 97 bd b9 77 2d 89 26 00 00  -PV-PX- -w-&-
  0010 00 0a 81 00 00 67 08 00 45 00 00 54 59 90 40 00  -...g- E-TY@
  0020 40 01 f4 1c c0 00 02 64 c6 33 64 64 08 00 22 68  @-----d 3dd-~h
  0030 00 01 00 0f 89 7a d0 62 00 00 00 00 b3 d7 09 00  -...z-b -.....
  0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b  -.....
  0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b  !"# $%&'()*+
  0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37  -.../0123 4567
  
```

0 = Direction: To Bridge
 .0. = Pointer: vif_id
 ..00 0000 0000 0000 = Destination: 0
0 = Looped: No
0 = Reserved: 0
00 = Version: 0
0000 0110 0111 = ID: 103
 Type: 802.1Q Virtual LAN (0x8100)
 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 103
 000. = Priority: Best Effort (default) (0)
 ...0 = DEI: Ineligible
0000 0110 0111 = ID: 103
 Type: IPv4 (0x0800)
 > Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
 > Internet Control Message Protocol

Sélectionnez le troisième et le quatrième paquet, puis vérifiez les points clés :

1. Chaque réponse d'écho ICMP est capturée et affichée 2 fois.
2. L'en-tête de paquet d'origine est sans étiquette VLAN.
3. Le commutateur interne insère une étiquette VLAN de port supplémentaire 102 qui identifie l'interface de sortie Ethernet1/2.
4. Le commutateur interne insère une étiquette VN supplémentaire.

The screenshot displays a network traffic capture in Wireshark. The top pane shows a list of ICMP Echo (ping) requests and replies. The middle pane shows the details of a selected frame (Frame 3), highlighting the Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol layers. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Explication

Lorsqu'une capture de paquet sur une interface de fond de panier est configurée, le commutateur capture simultanément chaque paquet deux fois. Dans ce cas, le commutateur interne reçoit des paquets qui sont déjà étiquetés par l'application sur le module de sécurité avec l'étiquette VLAN de port et l'étiquette VLAN. L'étiquette VLAN identifie l'interface de sortie que le châssis interne utilise pour transférer les paquets au réseau. L'étiquette VLAN 103 dans les paquets de requête d'écho ICMP identifie Ethernet1/3 comme interface de sortie, tandis que l'étiquette VLAN 102 dans les paquets de réponse d'écho ICMP identifie Ethernet1/2 comme interface de sortie. Le commutateur interne supprime l'étiquette VLAN et l'étiquette VLAN d'interface interne avant que les paquets ne soient transférés au réseau.

Ce tableau récapitule la tâche :

Tâche	Point de capture	VLAN de port interne dans les paquets capturés	Direction	Trafic capturé
Configurer et vérifier les captures de paquets sur les interfaces de fond de panier	Interfaces du fond de panier	102 103	Entrée unique	Requêtes d'écho ICMP de l'hôte 192.0.2.100 vers l'hôte 198.51.100.100 Réponses d'écho ICMP de l'hôte 198.51.100.100 à l'hôte 192.0.2.100

Captures de paquets sur les ports des applications et des applications

Les captures de paquets de port d'application ou d'application sont toujours configurées sur les interfaces de fond de panier et également sur les interfaces avant si l'utilisateur spécifie la direction de capture d'application.

Il existe principalement 2 cas d'utilisation :

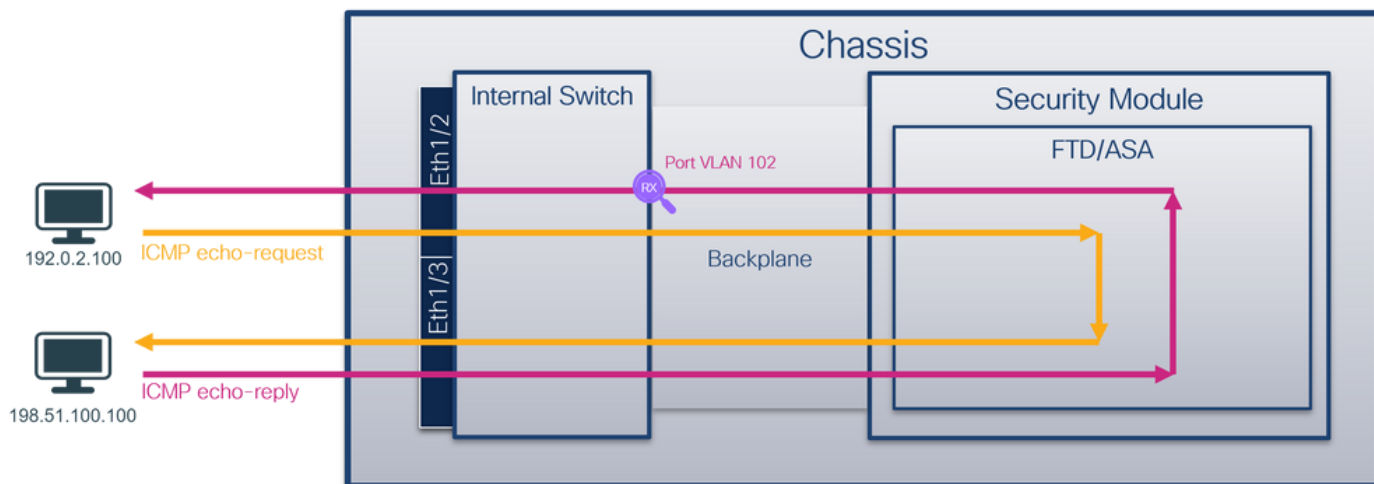
- Configurez les captures de paquets sur les interfaces de fond de panier pour les paquets qui quittent une interface avant spécifique. Par exemple, configurez les captures de paquets sur l'interface de fond de panier Ethernet1/9 pour les paquets qui quittent l'interface Ethernet1/2.
- Configurez des captures de paquets simultanées sur une interface avant spécifique et sur les interfaces de fond de panier. Par exemple, configurez des captures de paquets simultanées sur l'interface Ethernet1/2 et sur l'interface de fond de panier Ethernet1/9 pour les paquets qui quittent l'interface Ethernet1/2.

Cette section couvre les deux cas d'utilisation.

Tâche 1

Utilisez le FCM et la CLI pour configurer et vérifier une capture de paquets sur l'interface de fond de panier. Les paquets pour lesquels le port d'application Ethernet1/2 est identifié comme interface de sortie sont capturés. Dans ce cas, les réponses ICMP sont capturées.

Topologie, flux de paquets et points de capture

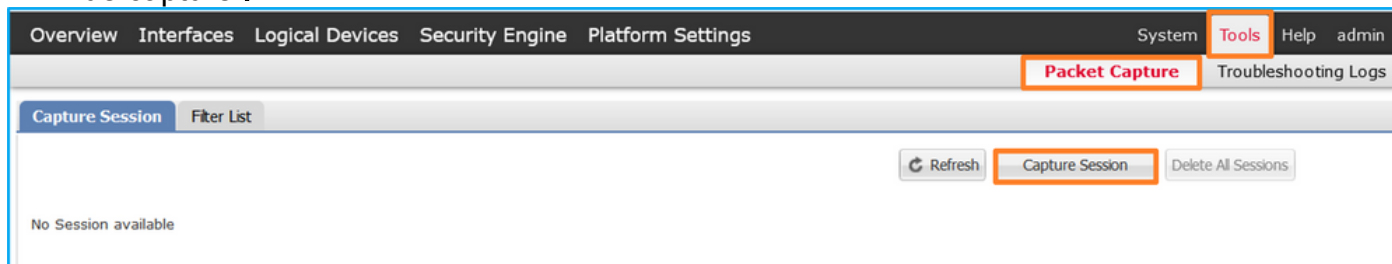


Configuration

FCM

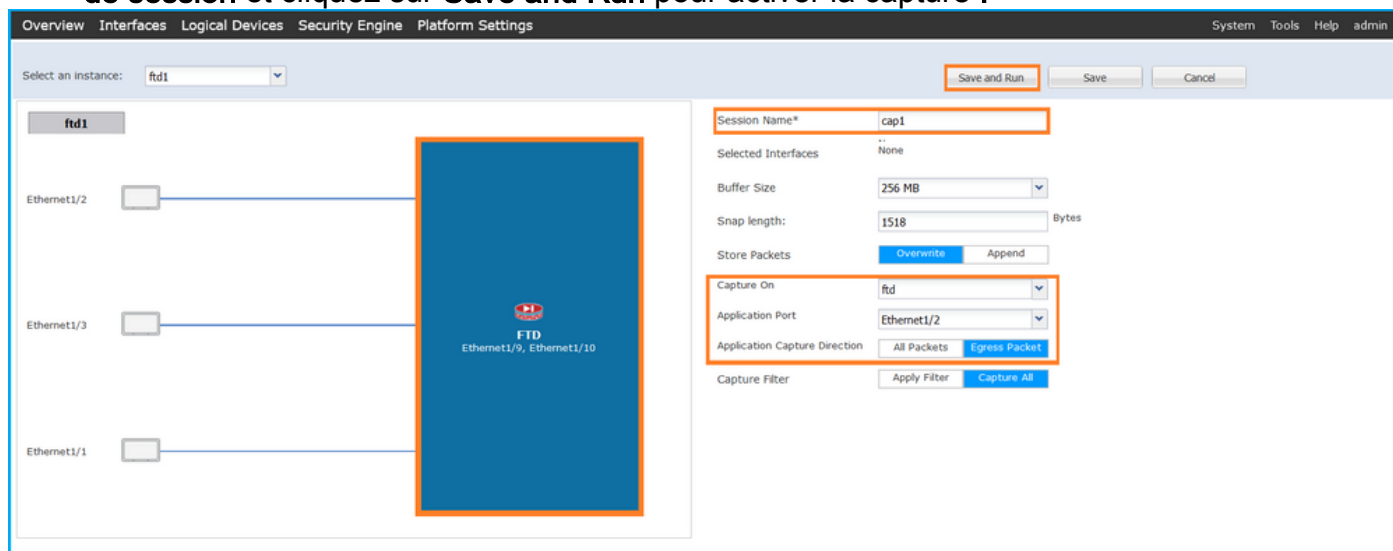
Procédez comme suit sur FCM pour configurer une capture de paquets sur l'application FTD et le port d'application Ethernet1/2 :

1. Utilisez **Outils > Capture de paquets > Session de capture** pour créer une nouvelle session de capture :



2. Sélectionnez l'application **Ethernet1/2** dans la liste déroulante **Port d'application** et

sélectionnez **Paquet de sortie** dans la direction de **capture d'application**. Fournissez le **nom de session** et cliquez sur **Save and Run** pour activer la capture :



CLI FXOS

Procédez comme suit sur l'interface de ligne de commande FXOS pour configurer les captures de paquets sur les interfaces de fond de panier :

1. Identifiez le type et l'identificateur de l'application :

```
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      ftd1      1          Enabled  Online      7.2.0.82      7.2.0.82
Native   No                Not Applicable  None
```

2. Créez une session de capture :

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

Vérification

FCM

Vérifiez le **nom de l'interface**, assurez-vous que l'**état opérationnel** est up et que la **taille du fichier (en octets)** augmente :

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/2 - Ethernet1/10	None	576	cap1-vethernet-1175.pcap	ftd1
Ethernet1/2 - Ethernet1/9	None	4360	cap1-vethernet-1036.pcap	ftd1

CLI FXOS

Vérifiez les détails de capture dans la portée 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:
```

Collecter les fichiers de capture

Suivez les étapes de la section **Collecter les fichiers de capture internes du commutateur Firepower 4100/9300**.

Capturer l'analyse des fichiers

Utilisez une application de lecture de fichiers de capture de paquets pour ouvrir les fichiers de capture. Dans le cas de plusieurs interfaces de fond de panier, assurez-vous d'ouvrir tous les fichiers de capture pour chaque interface de fond de panier. Dans ce cas, les paquets sont capturés sur l'interface de fond de panier Ethernet1/9.

Sélectionnez le premier et le deuxième paquet, puis vérifiez les points clés :

1. Chaque réponse d'écho ICMP est capturée et affichée 2 fois.
2. L'en-tête de paquet d'origine est sans étiquette VLAN.
3. Le commutateur interne insère une étiquette VLAN de port supplémentaire 102 qui identifie l'interface de sortie Ethernet1/2.
4. Le commutateur interne insère une étiquette VN supplémentaire.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 10:03:22.231237959	198.51.100.100	192.0.2.100	ICMP	108	0x42f8 (17144)	64	Echo (ping) reply id=0x0012, seq=1/256, ttl=64
2	2022-08-01 10:03:22.231239747	198.51.100.100	192.0.2.100	ICMP	108	0x42f8 (17144)	64	Echo (ping) reply id=0x0012, seq=1/256, ttl=64
3	2022-08-01 10:03:23.232244769	198.51.100.100	192.0.2.100	ICMP	108	0x4305 (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	0x4303 (17331)	64	Echo (ping) reply id=0x0012, seq=2/512, ttl=64
5	2022-08-01 10:03:24.234793981	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 10:03:24.234796751	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 10:03:29.354796706	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply id=0x0012, seq=8/2048, ttl=64
17	2022-08-01 10:03:30.378795204	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64	Echo (ping) reply id=0x0012, seq=9/2304, ttl=64
18	2022-08-01 10:03:30.378798172	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64	Echo (ping) reply id=0x0012, seq=9/2304, ttl=64
19	2022-08-01 10:03:31.402772217	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64	Echo (ping) reply id=0x0012, seq=10/2560, ttl=64
20	2022-08-01 10:03:31.402774775	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64	Echo (ping) reply id=0x0012, seq=10/2560, ttl=64
21	2022-08-01 10:03:32.426693254	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64	Echo (ping) reply id=0x0012, seq=11/2816, ttl=64
22	2022-08-01 10:03:32.426695691	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64	Echo (ping) reply id=0x0012, seq=11/2816, ttl=64


```

> Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
> Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VMware 9d:e8:be (00:50:56:9d:e8:be)
  0000  00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00  |PV...X...w-&..
  0010  00 0a 81 00 00 06 08 00 45 00 00 54 42 f8 00 00  |...f...E...TB...
  0020  40 01 4a b5 c6 33 64 64 c0 00 02 64 00 00 90 04  |@...3dd...d...
  0030  00 12 00 01 dd a4 e7 62 00 00 00 00 e3 0d 09 00  |.....b.....
  0040  00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b  |.....
  0050  1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b  |....!%$%()*+
  0060  2c 2d 2e 2f 30 31 32 33 34 35 36 37             |...-/0123 4567
  
```

```

VN-Tag
0... .. = Direction: To Bridge
.0... .. = Pointer: vif_id
..00 0000 0000 0000 .. = Destination: 0
... .. = Looped: No
... .. = Reserved: 0
... .. = Version: 0
... .. 0000 0000 1010 = Source: 10
Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
000... .. = Priority: Best Effort (default) (0)
... .. = DEI: Ineligible
... 0000 0110 0110 = ID: 102
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100
Internet Control Message Protocol
  
```

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 10:03:22.231237959	198.51.100.100	192.0.2.100	ICMP	108	0x42f8 (17144)	64	Echo (ping) reply
2	2022-08-01 10:03:22.231239747	198.51.100.100	192.0.2.100	ICMP	108	0x42f8 (17144)	64	Echo (ping) reply
3	2022-08-01 10:03:23.232244769	198.51.100.100	192.0.2.100	ICMP	108	0x4303 (17331)	64	Echo (ping) reply
4	2022-08-01 10:03:23.232247753	198.51.100.100	192.0.2.100	ICMP	108	0x43b3 (17331)	64	Echo (ping) reply
5	2022-08-01 10:03:24.234703981	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64	Echo (ping) reply
6	2022-08-01 10:03:24.234706751	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64	Echo (ping) reply
7	2022-08-01 10:03:25.258672449	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64	Echo (ping) reply
8	2022-08-01 10:03:25.258674861	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64	Echo (ping) reply
9	2022-08-01 10:03:26.282663169	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64	Echo (ping) reply
10	2022-08-01 10:03:26.282666183	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64	Echo (ping) reply
11	2022-08-01 10:03:27.306671694	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64	Echo (ping) reply
12	2022-08-01 10:03:27.306674378	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64	Echo (ping) reply
13	2022-08-01 10:03:28.330664677	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64	Echo (ping) reply
14	2022-08-01 10:03:28.330667153	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64	Echo (ping) reply
15	2022-08-01 10:03:29.354795931	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply
16	2022-08-01 10:03:29.354796786	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply
17	2022-08-01 10:03:30.378795204	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64	Echo (ping) reply
18	2022-08-01 10:03:30.378798172	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64	Echo (ping) reply
19	2022-08-01 10:03:31.402772217	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64	Echo (ping) reply
20	2022-08-01 10:03:31.402774775	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64	Echo (ping) reply
21	2022-08-01 10:03:32.426693254	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64	Echo (ping) reply
22	2022-08-01 10:03:32.426695691	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64	Echo (ping) reply


```

> Frame 2: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
> Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VMware 9d:e8:be (00:50:56:9d:e8:be)
  > VLAN-Tag
    0... .. = Direction: To Bridge
    .0... .. = Pointer: vif_id
    ..00 0000 0000 0000 .. = Destination: 0
    .. .. = Looped: No
    ..0... .. = Reserved: 0
    .. ..00 .. = Version: 0
    .. ..0000 0000 1010 = Source: 10
    Type: 802.1Q Virtual LAN (0x8100)
  > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
    000... .. = Priority: Best Effort (default) (0)
    ...0 .. = DEI: Ineligible
    ...0000 0110 0110 = ID: 102
    Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100
  > Internet Control Message Protocol
  
```

Explication

Dans ce cas, Ethernet1/2 avec l'étiquette VLAN de port 102 est l'interface de sortie pour les paquets de réponse d'écho ICMP.

Lorsque la direction de capture d'application est définie sur **Egress** dans les options de capture, les paquets avec l'étiquette VLAN de port 102 dans l'en-tête Ethernet sont capturés sur les interfaces de fond de panier dans la direction d'entrée.

Ce tableau récapitule la tâche :

Tâche	Point de capture	VLAN de port interne dans les paquets capturés	Direction	Trafic capturé
Configuration et vérification des captures sur l'application et le port d'application Ethernet1/2	Interfaces du fond de panier	102	Entrée unique	Réponses d'écho ICMP de l'hôte 198.51.100.100 à l'interface 192.0.2.100

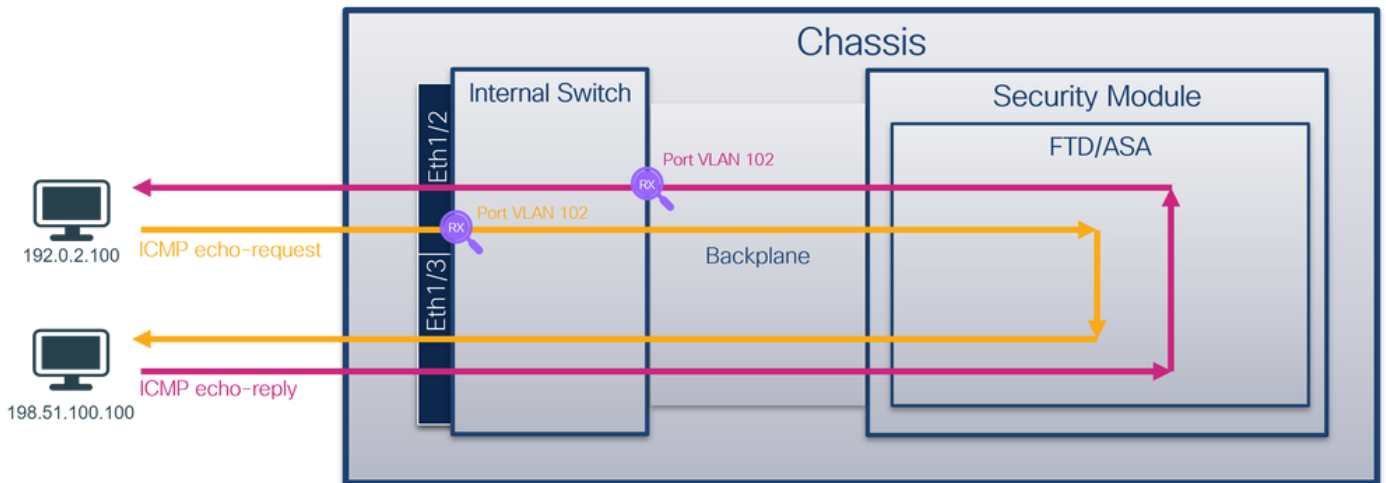
Tâche 2

Utilisez le FCM et l'interface de ligne de commande pour configurer et vérifier une capture de paquets sur l'interface de fond de panier et l'interface avant Ethernet1/2.

Les captures de paquets simultanées sont configurées sur :

- Interface avant : les paquets avec le port VLAN 102 sur l'interface Ethernet1/2 sont capturés. Les paquets capturés sont des requêtes d'écho ICMP.
- Interfaces de fond de panier : les paquets pour lesquels Ethernet1/2 est identifié comme interface de sortie, ou les paquets avec le port VLAN 102, sont capturés. Les paquets capturés sont des réponses d'écho ICMP.

Topologie, flux de paquets et points de capture

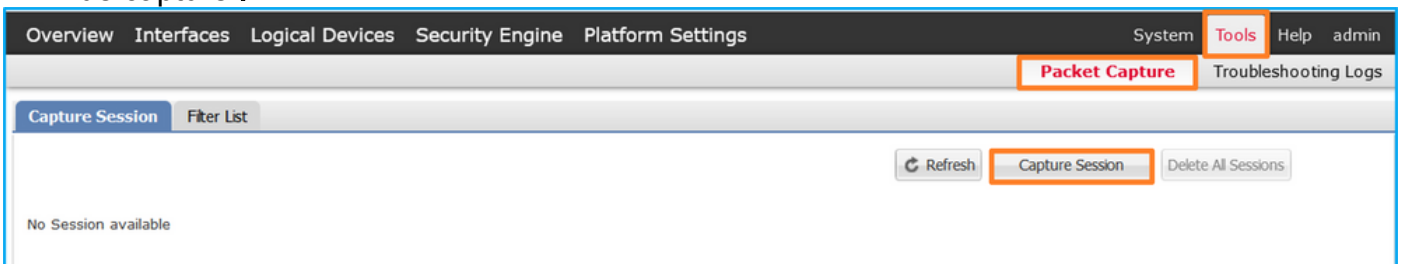


Configuration

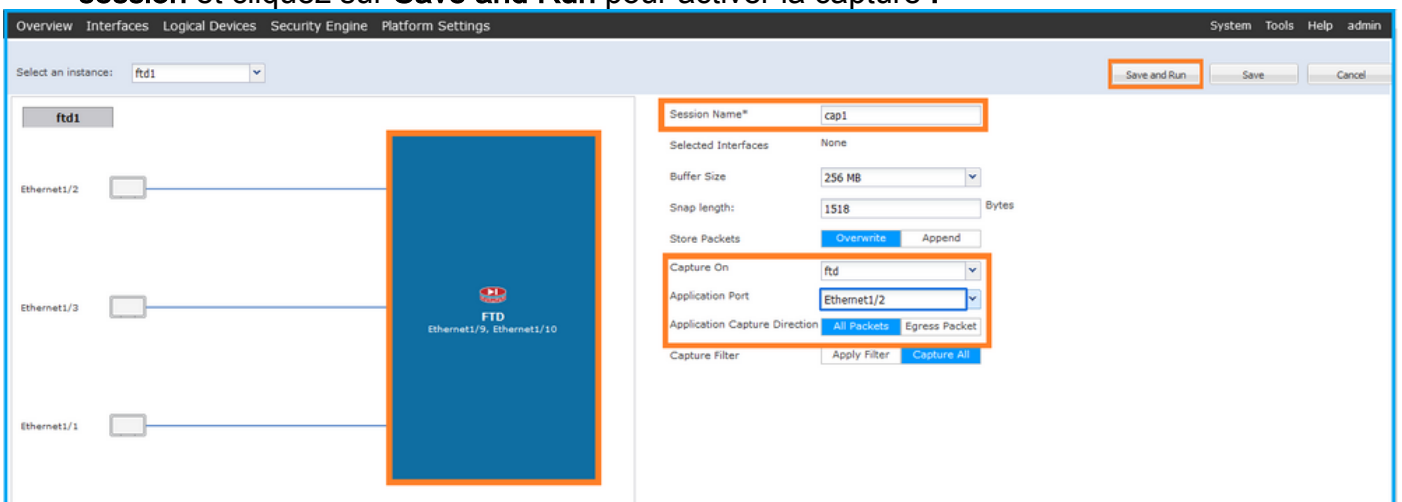
FCM

Procédez comme suit sur FCM pour configurer une capture de paquets sur l'application FTD et le port d'application Ethernet1/2 :

1. Utilisez **Outils > Capture de paquets > Session de capture** pour créer une nouvelle session de capture :



2. Sélectionnez l'application FTD, **Ethernet1/2** dans la liste déroulante **Application Port** et sélectionnez **All Packets** dans la direction de **capture d'application**. Fournissez le nom de **session** et cliquez sur **Save and Run** pour activer la capture :



CLI FXOS

Procédez comme suit sur l'interface de ligne de commande FXOS pour configurer les captures de

paquets sur les interfaces de fond de panier :

1. Identifiez le type et l'identificateur de l'application :

```
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           ftd1         1             Enabled      Online          7.2.0.82       7.2.0.82
Native        No                               Not Applicable None
```

2. Créez une session de capture :

```
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-identifiant 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-identifiant ftd1
firepower /packet-capture/session* # enable
firepower /packet-capture/session* # commit
firepower /packet-capture/session # commit
```

Vérification

FCM

Vérifiez le nom de l'interface, assurez-vous que l'état opérationnel est up et que la taille du fichier (en octets) augmente :

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	11040	cap1-vethernet-1036.pcap	ftd1

CLI FXOS

Vérifiez les détails de capture dans la portée 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
Vlan: 102

Filter:

Collecter les fichiers de capture

Suivez les étapes de la section **Collecter les fichiers de capture internes du commutateur Firepower 4100/9300**.

Capturer l'analyse des fichiers

Utilisez une application de lecture de fichiers de capture de paquets pour ouvrir les fichiers de capture. Dans le cas de plusieurs interfaces de fond de panier, assurez-vous d'ouvrir tous les fichiers de capture pour chaque interface de fond de panier. Dans ce cas, les paquets sont capturés sur l'interface de fond de panier Ethernet1/9.

Ouvrez le fichier de capture pour l'interface Ethernet1/2, sélectionnez le premier paquet et vérifiez les points clés :

1. Seuls les paquets de requête d'écho ICMP sont capturés. Chaque paquet est capturé et affiché 2 fois.
2. L'en-tête de paquet d'origine est sans étiquette VLAN.
3. Le commutateur interne insère une étiquette VLAN de port supplémentaire **102** qui identifie l'interface d'entrée Ethernet1/2.

4. Le commutateur interne insère une étiquette VN supplémentaire.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 11:33:19.070693081	192.0.2.100	198.51.100.100	ICMP	108	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
2	2022-08-01 11:33:19.070695347	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
3	2022-08-01 11:33:19.071217121	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
4	2022-08-01 11:33:19.071218458	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
5	2022-08-01 11:33:20.072036625	192.0.2.100	198.51.100.100	ICMP	108	0xc0ae (49326)	64	Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found)
6	2022-08-01 11:33:20.072038399	192.0.2.100	198.51.100.100	ICMP	102	0xc0ae (49326)	64	Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found)
7	2022-08-01 11:33:21.073266630	192.0.2.100	198.51.100.100	ICMP	102	0xc167 (49511)	64	Echo (ping) request 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) request id=0x0013, seq=3/768, ttl=64 (no response found)
9	2022-08-01 11:33:22.074576640	192.0.2.100	198.51.100.100	ICMP	108	0xc175 (49525)	64	Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found)
10	2022-08-01 11:33:22.074578010	192.0.2.100	198.51.100.100	ICMP	102	0xc175 (49525)	64	Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found)
11	2022-08-01 11:33:23.075779809	192.0.2.100	198.51.100.100	ICMP	108	0xc208 (49672)	64	Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found)
12	2022-08-01 11:33:23.075781513	192.0.2.100	198.51.100.100	ICMP	102	0xc208 (49672)	64	Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found)
13	2022-08-01 11:33:24.081839490	192.0.2.100	198.51.100.100	ICMP	108	0xc211 (49681)	64	Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found)
14	2022-08-01 11:33:24.081841386	192.0.2.100	198.51.100.100	ICMP	102	0xc211 (49681)	64	Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found)
15	2022-08-01 11:33:25.105806249	192.0.2.100	198.51.100.100	ICMP	108	0xc2e2 (49890)	64	Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found)
16	2022-08-01 11:33:25.105807895	192.0.2.100	198.51.100.100	ICMP	102	0xc2e2 (49890)	64	Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found)
17	2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	ICMP	108	0xc3b4 (50100)	64	Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found)
18	2022-08-01 11:33:26.129838114	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100)	64	Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found)
19	2022-08-01 11:33:27.153828653	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found)
20	2022-08-01 11:33:27.153830201	192.0.2.100	198.51.100.100	ICMP	102	0xc476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found)
21	2022-08-01 11:33:28.177847175	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found)
22	2022-08-01 11:33:28.177849075	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found)
23	2022-08-01 11:33:29.201804760	192.0.2.100	198.51.100.100	ICMP	108	0xc578 (50552)	64	Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found)
24	2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	102	0xc578 (50552)	64	Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found)
25	2022-08-01 11:33:30.225834765	192.0.2.100	198.51.100.100	ICMP	108	0xc585 (50565)	64	Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found)
26	2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (50565)	64	Echo (ping) request id=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) request id=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) request id=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) request id=0x0013, seq=14/3584, ttl=64 (no response found)


```

Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_1, id 0
Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)
VNI-Tag
1. .... = Direction: From Bridge
.0. .... = Pointer: vif_id
..00 0000 0000 1010 .... = Destination: 10
..... = Looped: No
..... = Reserved: 0
..... = Version: 0
..... = Source: 0
Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
000. .... = Priority: Best Effort (default) (0)
...0 .... = DEI: Ineligible
... 0000 0110 0110 = ID: 102
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
Internet Control Message Protocol
    
```

Sélectionnez le deuxième paquet et vérifiez les points clés :

1. Seuls les paquets de requête d'écho ICMP sont capturés. Chaque paquet est capturé et affiché 2 fois.
2. L'en-tête de paquet d'origine est sans étiquette VLAN.
3. Le commutateur interne insère une étiquette VLAN de port supplémentaire 102 qui identifie l'interface d'entrée Ethernet1/2.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 11:33:19.070693081	192.0.2.100	198.51.100.100	ICMP	108	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
2	2022-08-01 11:33:19.070695347	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
3	2022-08-01 11:33:19.071217121	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
4	2022-08-01 11:33:19.071218458	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
5	2022-08-01 11:33:20.072036625	192.0.2.100	198.51.100.100	ICMP	108	0xc0ae (49326)	64	Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found)
6	2022-08-01 11:33:20.072038399	192.0.2.100	198.51.100.100	ICMP	102	0xc0ae (49326)	64	Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found)
7	2022-08-01 11:33:21.073266630	192.0.2.100	198.51.100.100	ICMP	102	0xc167 (49511)	64	Echo (ping) request 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) request id=0x0013, seq=3/768, ttl=64 (no response found)
9	2022-08-01 11:33:22.074576640	192.0.2.100	198.51.100.100	ICMP	108	0xc175 (49525)	64	Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found)
10	2022-08-01 11:33:22.074578010	192.0.2.100	198.51.100.100	ICMP	102	0xc175 (49525)	64	Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found)
11	2022-08-01 11:33:23.075779809	192.0.2.100	198.51.100.100	ICMP	108	0xc208 (49672)	64	Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found)
12	2022-08-01 11:33:23.075781513	192.0.2.100	198.51.100.100	ICMP	102	0xc208 (49672)	64	Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found)
13	2022-08-01 11:33:24.081839490	192.0.2.100	198.51.100.100	ICMP	108	0xc211 (49681)	64	Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found)
14	2022-08-01 11:33:24.081841386	192.0.2.100	198.51.100.100	ICMP	102	0xc211 (49681)	64	Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found)
15	2022-08-01 11:33:25.105806249	192.0.2.100	198.51.100.100	ICMP	108	0xc2e2 (49890)	64	Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found)
16	2022-08-01 11:33:25.105807895	192.0.2.100	198.51.100.100	ICMP	102	0xc2e2 (49890)	64	Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found)
17	2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	ICMP	108	0xc3b4 (50100)	64	Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found)
18	2022-08-01 11:33:26.129838114	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100)	64	Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found)
19	2022-08-01 11:33:27.153828653	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found)
20	2022-08-01 11:33:27.153830201	192.0.2.100	198.51.100.100	ICMP	102	0xc476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found)
21	2022-08-01 11:33:28.177847175	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found)
22	2022-08-01 11:33:28.177849075	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found)
23	2022-08-01 11:33:29.201804760	192.0.2.100	198.51.100.100	ICMP	108	0xc578 (50552)	64	Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found)
24	2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	102	0xc578 (50552)	64	Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found)
25	2022-08-01 11:33:30.225834765	192.0.2.100	198.51.100.100	ICMP	108	0xc585 (50565)	64	Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found)
26	2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (50565)	64	Echo (ping) request id=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) request id=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) request id=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) request id=0x0013, seq=14/3584, ttl=64 (no response found)


```

Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture_u0_1, id 0
Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
000. .... = Priority: Best Effort (default) (0)
...0 .... = DEI: Ineligible
... 0000 0110 0110 = ID: 102
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
Internet Control Message Protocol
    
```

Ouvrez le fichier de capture pour l'interface Ethernet1/9, sélectionnez le premier et le deuxième paquet, puis vérifiez les points clés :

1. Chaque réponse d'écho ICMP est capturée et affichée 2 fois.
2. L'en-tête de paquet d'origine est sans étiquette VLAN.

3. Le commutateur interne insère une étiquette VLAN de port supplémentaire 102 qui identifie l'interface de sortie Ethernet1/2.

4. Le commutateur interne insère une étiquette VN supplémentaire.

No.	Time	Source	Destination	Protocol	Length	ID	PTTL	Info
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	0x4f70 (20875)	64	Echo (ping) reply 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 11:33:22.075247152	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 11:33:22.075249303	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 11:33:23.076449786	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 11:33:23.076449786	198.51.100.100	192.0.2.100	ICMP	108	0x528e (21134)	64	Echo (ping) reply id=0x0013, seq=6/1536, ttl=64
13	2022-08-01 11:33:25.106382424	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64	Echo (ping) reply id=0x0013, seq=7/1792, ttl=64
14	2022-08-01 11:33:25.106384549	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64	Echo (ping) reply id=0x0013, seq=7/1792, ttl=64
15	2022-08-01 11:33:26.130437851	198.51.100.100	192.0.2.100	ICMP	108	0x53a6 (21414)	64	Echo (ping) reply id=0x0013, seq=8/2048, ttl=64
16	2022-08-01 11:33:26.130440320	198.51.100.100	192.0.2.100	ICMP	108	0x53a6 (21414)	64	Echo (ping) reply id=0x0013, seq=8/2048, ttl=64
17	2022-08-01 11:33:27.154398212	198.51.100.100	192.0.2.100	ICMP	108	0x5446 (21574)	64	Echo (ping) reply id=0x0013, seq=9/2304, ttl=64
18	2022-08-01 11:33:27.154400198	198.51.100.100	192.0.2.100	ICMP	108	0x5446 (21574)	64	Echo (ping) reply id=0x0013, seq=9/2304, ttl=64
19	2022-08-01 11:33:28.178469866	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64	Echo (ping) reply id=0x0013, seq=10/2560, ttl=64
20	2022-08-01 11:33:28.178471810	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64	Echo (ping) reply id=0x0013, seq=10/2560, ttl=64
21	2022-08-01 11:33:29.202395869	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21748)	64	Echo (ping) reply 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) reply 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) reply 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) reply 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) reply 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) reply 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) reply 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) reply id=0x0013, seq=14/3584, ttl=64
29	2022-08-01 11:33:33.298397657	198.51.100.100	192.0.2.100	ICMP	108	0x56e7 (22247)	64	Echo (ping) reply id=0x0013, seq=15/3840, ttl=64

```

Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VMware 9d:e8:be (00:50:56:9d:e8:be)

  0000  00 50 56 9d e8 be 58 97  bd b9 77 0e 89 26 00 00  -PV...X:..w.&..
  0010  00 0a 81 00 00 66 08 00  45 00 00 54 4f 27 00 00  -...f..E..T0...
  0020  40 01 3e 86 c6 33 64 64  c0 00 02 64 00 00 95 7c  -@>...3dd...d...|
  0030  00 13 00 01 f2 b9 e7 62  00 00 00 00 cb 7f 06 00  -...b...
  0040  00 00 00 00 10 11 12 13  14 15 16 17 18 19 1a 1b  -...
  0050  1c 1d 1e 1f 20 21 22 23  24 25 26 27 28 29 2a 2b  -...l"e $%&'()*+
  0060  2c 2d 2e 2f 30 31 32 33  34 35 36 37  -.../0123 4567

  0... .. = Direction: To Bridge
  .0... .. = Pointer: vif_id
  ..00 0000 0000 0000 .. = Destination: 0
  ..0... .. = Looped: No
  ..0... .. = Reserved: 0
  ..0... .. = Version: 0
  ..0000 0000 1010 .. = Source: 10
  Type: 802.1Q Virtual LAN (0x8100)

  802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
  000... .. = Priority: Best Effort (default) (0)
  ..0... .. = DEI: Ineligible
  .... 0000 0110 0110 = ID: 102
  Type: IPv4 (0x0800)

  Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100
  Internet Control Message Protocol
  
```

No.	Time	Source	Destination	Protocol	Length	ID	PTTL	Info
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	0x4f70 (20875)	64	Echo (ping) reply 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 11:33:22.075247152	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 11:33:22.075249303	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 11:33:23.076449786	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 11:33:23.076449786	198.51.100.100	192.0.2.100	ICMP	108	0x528e (21134)	64	Echo (ping) reply id=0x0013, seq=6/1536, ttl=64
13	2022-08-01 11:33:25.106382424	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64	Echo (ping) reply id=0x0013, seq=7/1792, ttl=64
14	2022-08-01 11:33:25.106384549	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64	Echo (ping) reply id=0x0013, seq=7/1792, ttl=64
15	2022-08-01 11:33:26.130437851	198.51.100.100	192.0.2.100	ICMP	108	0x53a6 (21414)	64	Echo (ping) reply id=0x0013, seq=8/2048, ttl=64
16	2022-08-01 11:33:26.130440320	198.51.100.100	192.0.2.100	ICMP	108	0x53a6 (21414)	64	Echo (ping) reply id=0x0013, seq=8/2048, ttl=64
17	2022-08-01 11:33:27.154398212	198.51.100.100	192.0.2.100	ICMP	108	0x5446 (21574)	64	Echo (ping) reply id=0x0013, seq=9/2304, ttl=64
18	2022-08-01 11:33:27.154400198	198.51.100.100	192.0.2.100	ICMP	108	0x5446 (21574)	64	Echo (ping) reply id=0x0013, seq=9/2304, ttl=64
19	2022-08-01 11:33:28.178469866	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64	Echo (ping) reply id=0x0013, seq=10/2560, ttl=64
20	2022-08-01 11:33:28.178471810	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64	Echo (ping) reply id=0x0013, seq=10/2560, ttl=64
21	2022-08-01 11:33:29.202395869	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21748)	64	Echo (ping) reply 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) reply 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) reply 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) reply 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) reply 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) reply 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) reply 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) reply id=0x0013, seq=14/3584, ttl=64
29	2022-08-01 11:33:33.298397657	198.51.100.100	192.0.2.100	ICMP	108	0x56e7 (22247)	64	Echo (ping) reply id=0x0013, seq=15/3840, ttl=64

```

Frame 2: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VMware 9d:e8:be (00:50:56:9d:e8:be)

  0000  00 50 56 9d e8 be 58 97  bd b9 77 0e 89 26 00 00  -PV...X:..w.&..
  0010  00 0a 81 00 00 66 08 00  45 00 00 54 4f 27 00 00  -...f..E..T0...
  0020  40 01 3e 86 c6 33 64 64  c0 00 02 64 00 00 95 7c  -@>...3dd...d...|
  0030  00 13 00 01 f2 b9 e7 62  00 00 00 00 cb 7f 06 00  -...b...
  0040  00 00 00 00 10 11 12 13  14 15 16 17 18 19 1a 1b  -...
  0050  1c 1d 1e 1f 20 21 22 23  24 25 26 27 28 29 2a 2b  -...l"e $%&'()*+
  0060  2c 2d 2e 2f 30 31 32 33  34 35 36 37  -.../0123 4567

  0... .. = Direction: To Bridge
  .0... .. = Pointer: vif_id
  ..00 0000 0000 0000 .. = Destination: 0
  ..0... .. = Looped: No
  ..0... .. = Reserved: 0
  ..0... .. = Version: 0
  ..0000 0000 1010 .. = Source: 10
  Type: 802.1Q Virtual LAN (0x8100)

  802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
  000... .. = Priority: Best Effort (default) (0)
  ..0... .. = DEI: Ineligible
  .... 0000 0110 0110 = ID: 102
  Type: IPv4 (0x0800)

  Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100
  Internet Control Message Protocol
  
```

Explication

Si l'option **All Packets in the Application Capture Direction** est sélectionnée, 2 captures de paquets simultanées liées au port d'application Ethernet1/2 sélectionné sont configurées : une capture sur l'interface avant Ethernet1/2 et une capture sur les interfaces de fond de panier sélectionnées.

Lorsqu'une capture de paquets sur une interface avant est configurée, le commutateur capture simultanément chaque paquet deux fois :

- Après l'insertion de l'étiquette VLAN du port.
- Après l'insertion de la balise VN.

Dans l'ordre des opérations, l'étiquette VLAN est insérée à un stade ultérieur à celui de l'insertion de l'étiquette VLAN du port. Mais dans le fichier de capture, le paquet avec l'étiquette VLAN est affiché plus tôt que le paquet avec l'étiquette VLAN de port. Dans cet exemple, l'étiquette VLAN 102 dans les paquets de requête d'écho ICMP identifie Ethernet1/2 comme interface d'entrée.

Lorsqu'une capture de paquet sur une interface de fond de panier est configurée, le commutateur capture simultanément chaque paquet deux fois. Le commutateur interne reçoit des paquets qui sont déjà étiquetés par l'application sur le module de sécurité avec l'étiquette VLAN de port et l'étiquette VLAN. L'étiquette VLAN de port identifie l'interface de sortie que le châssis interne utilise pour transférer les paquets au réseau. Dans cet exemple, l'étiquette VLAN 102 dans les paquets de réponse d'écho ICMP identifie Ethernet1/2 comme interface de sortie.

Le commutateur interne supprime l'étiquette VLAN et l'étiquette VLAN d'interface interne avant que les paquets ne soient transférés au réseau.

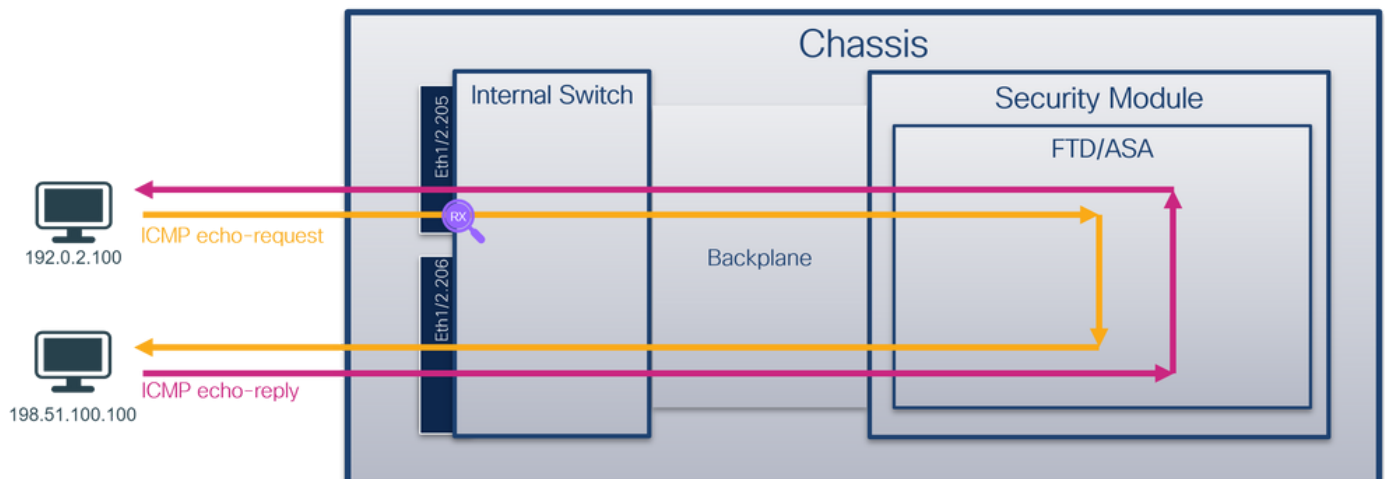
Ce tableau récapitule la tâche :

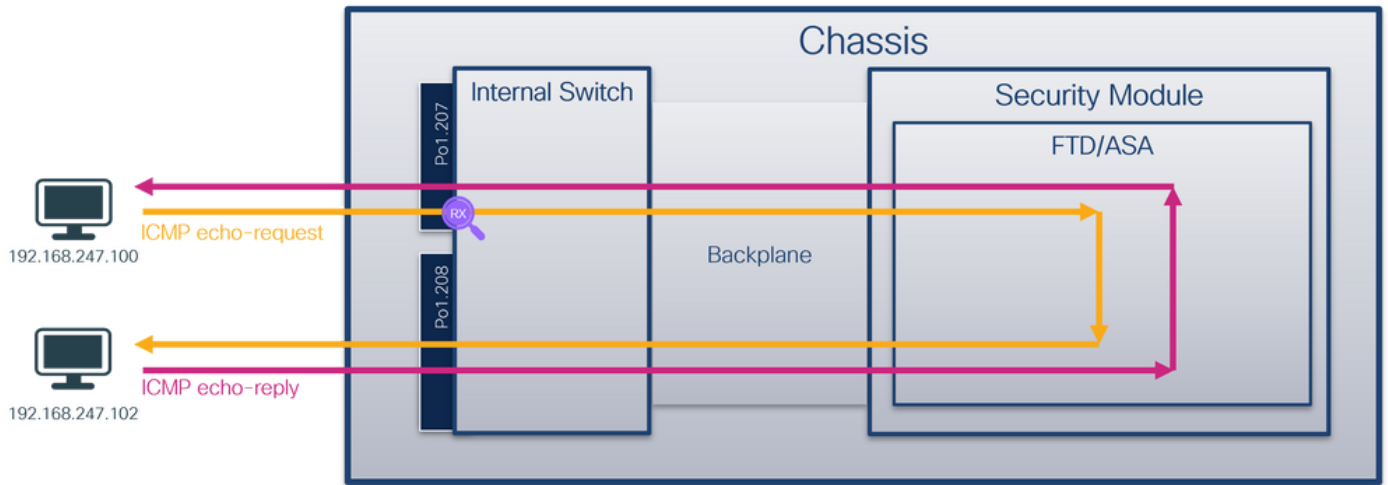
Tâche	Point de capture	VLAN de port interne dans les paquets capturés	Direction	Trafic capturé
Configuration et vérification des captures sur l'application et le port d'application Ethernet1/2	Interfaces du fond de panier	102	Entrée uniquement	Réponses d'écho ICMP de l'hôte 198.51.100.100 à l'hôte 192.0.2.100
	Interface Ethernet1/2	102	Entrée uniquement	Requêtes d'écho ICMP de l'hôte 192.0.2.100 vers l'hôte 198.51.100.100

Capture de paquets sur une sous-interface d'une interface physique ou Port Channel

Utilisez FCM et CLI pour configurer et vérifier une capture de paquets sur la sous-interface Ethernet1/2.205 ou la sous-interface Port Channel1.207. Les sous-interfaces et les captures sur les sous-interfaces sont prises en charge uniquement pour l'application FTD en mode conteneur. Dans ce cas, une capture de paquets sur Ethernet1/2.205 et Portchannel1.207 est configurée.

Topologie, flux de paquets et points de capture



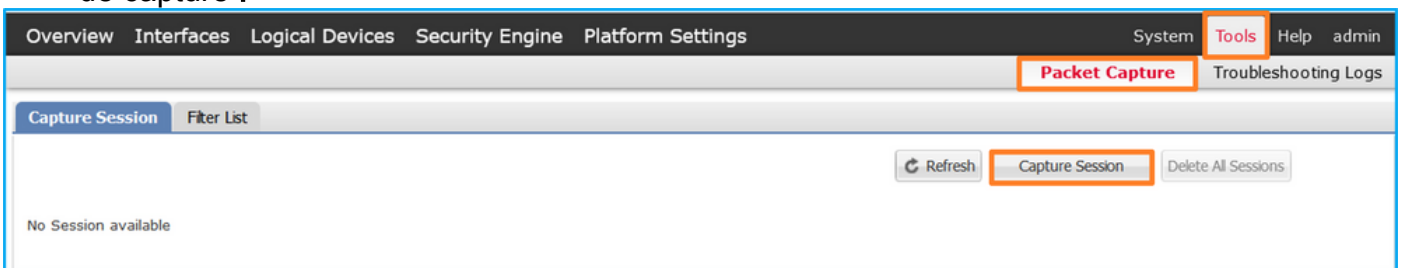


Configuration

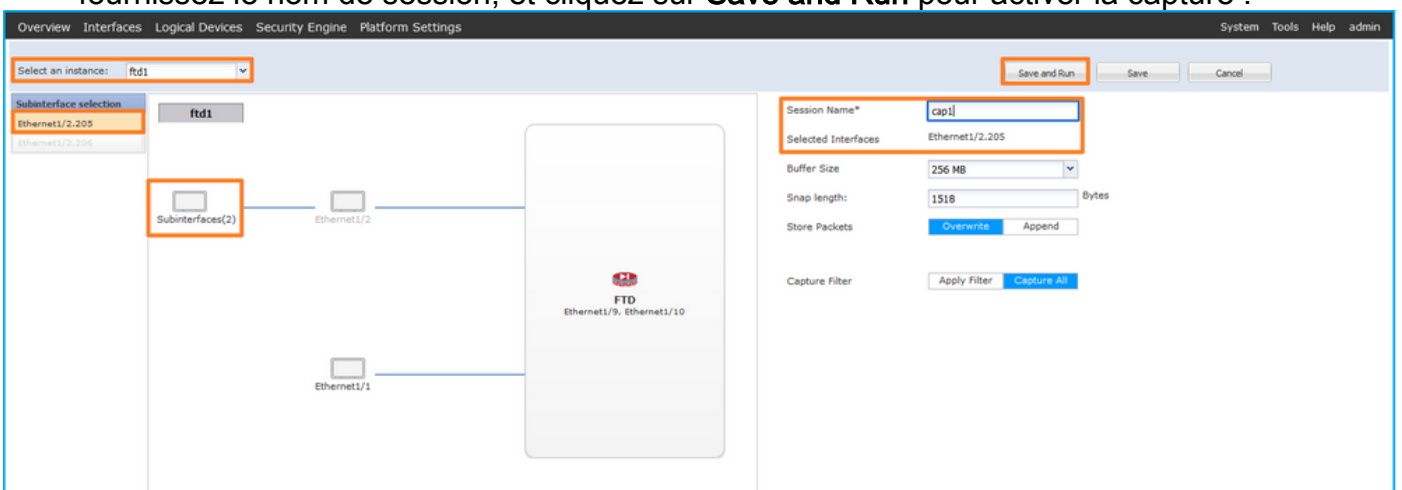
FCM

Procédez comme suit sur FCM pour configurer une capture de paquets sur l'application FTD et le port d'application Ethernet1/2 :

1. Utilisez **Outils > Capture de paquets > Session de capture** pour créer une nouvelle session de capture :



2. Sélectionnez l'instance d'application spécifique ftd1, la sous-interface Ethernet1/2.205, fournissez le nom de session, et cliquez sur **Save and Run** pour activer la capture :



3. Dans le cas d'une sous-interface port-channel, en raison de l'ID de bogue Cisco [CSCvq3119](https://tools.cisco.com/bugcenter/bug/?bugid=CSCvq3119), les sous-interfaces ne sont pas visibles dans le FCM. Utilisez l'interface de ligne de commande FXOS pour configurer les captures sur les sous-interfaces port-channel.

CLI FXOS

Procédez comme suit sur l'interface de ligne de commande FXOS pour configurer une capture de paquets sur les sous-interfaces Ethernet1/2.205 et Portchannel1.207 :

1. Identifiez le type et l'identificateur de l'application :

```
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       ftd1       1           Enabled  Online           7.2.0.82      7.2.0.82
Container No      RP20        Not Applicable None
ftd       ftd2       1           Enabled  Online           7.2.0.82      7.2.0.82
Container No      RP20        Not Applicable None
```

2. Dans le cas d'une interface port-channel, identifiez ses interfaces membres :

```
firepower# connect fxos
<output skipped>
firepower(fxos)# show port-channel summary
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        S - Switched     R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
-----
Group Port-      Type      Protocol  Member Ports
Channel
-----
1      Po1(SU)     Eth       LACP      Eth1/3(P)  Eth1/3(P)
```

3. Créez une session de capture :

```
firepower# scope packet-capture
firepower /packet-capture # create session cap1
firepower /packet-capture/session* # create phy-port Eth1/2
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # set app-identifier ftd1
firepower /packet-capture/session/phy-port* # set subinterface 205
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # enable
firepower /packet-capture/session* # commit
firepower /packet-capture/session #
```

Pour les sous-interfaces port-channel, créez une capture de paquets pour chaque interface membre port-channel :

```
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 #

```

Vérification

FCM

Vérifiez le nom de l'interface, assurez-vous que l'état opérationnel est up et que la taille du fichier (en octets) augmente :

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/2.205	None	233992	cap1-ethernet-1-2-0.pcap	rd1

Les captures de sous-interface de canal de port configurées sur l'interface de ligne de commande FXOS sont également visibles sur FCM ; toutefois, ils ne peuvent pas être modifiés :

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

Vérifiez les détails de capture dans la portée 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
```

Port-channel 1 avec interfaces membres Ethernet1/3 et Ethernet1/4 :

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

Traffic Monitoring Session:

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

Physical ports involved in Packet Capture:

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

Collecter les fichiers de capture

Suivez les étapes de la section **Collecter les fichiers de capture internes du commutateur Firepower 4100/9300**.

Capturer l'analyse des fichiers

Utilisez une application de lecture de fichier de capture de paquets pour ouvrir le fichier de capture. Sélectionnez le premier paquet et vérifiez les points clés :

1. Seuls les paquets de requête d'écho ICMP sont capturés. Chaque paquet est capturé et affiché 2 fois.
2. L'en-tête de paquet d'origine a l'étiquette VLAN 205.
3. Le commutateur interne insère une étiquette VLAN de port supplémentaire 102 qui identifie l'interface d'entrée Ethernet1/2.
4. Le commutateur interne insère une étiquette VN supplémentaire.

No.	Time	Source	Destination	Protocol	Length	IP ID	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) request id=0x0022, seq=1/256, ttl=64 (no response found)
2	2022-08-04 07:21:56.993303597	192.0.2.100	198.51.100.100	ICMP	102	0x9574 (38260)	64	Echo (ping) request id=0x0022, seq=1/256, ttl=64 (no response found)
3	2022-08-04 07:22:06.214264777	192.0.2.100	198.51.100.100	ICMP	112	0x9a81 (39553)	64	Echo (ping) request id=0x0022, seq=10/2560, ttl=64 (no response found)
4	2022-08-04 07:22:06.214267373	192.0.2.100	198.51.100.100	ICMP	102	0x9a81 (39553)	64	Echo (ping) request id=0x0022, seq=10/2560, ttl=64 (no response found)
5	2022-08-04 07:22:07.215113393	192.0.2.100	198.51.100.100	ICMP	112	0x9ac3 (39619)	64	Echo (ping) request id=0x0022, seq=11/2816, ttl=64 (no response found)
6	2022-08-04 07:22:07.215115445	192.0.2.100	198.51.100.100	ICMP	102	0x9ac3 (39619)	64	Echo (ping) request id=0x0022, seq=11/2816, ttl=64 (no response found)
7	2022-08-04 07:22:08.229938577	192.0.2.100	198.51.100.100	ICMP	112	0x9b33 (39731)	64	Echo (ping) request id=0x0022, seq=12/3072, ttl=64 (no response found)
8	2022-08-04 07:22:08.229940829	192.0.2.100	198.51.100.100	ICMP	102	0x9b33 (39731)	64	Echo (ping) request id=0x0022, seq=12/3072, ttl=64 (no response found)
9	2022-08-04 07:22:09.253946601	192.0.2.100	198.51.100.100	ICMP	112	0x9c0e (39950)	64	Echo (ping) request id=0x0022, seq=13/3328, ttl=64 (no response found)
10	2022-08-04 07:22:09.253946899	192.0.2.100	198.51.100.100	ICMP	102	0x9c0e (39950)	64	Echo (ping) request id=0x0022, seq=13/3328, ttl=64 (no response found)
11	2022-08-04 07:22:10.277953070	192.0.2.100	198.51.100.100	ICMP	112	0x9ccb (40139)	64	Echo (ping) request id=0x0022, seq=14/3584, ttl=64 (no response found)
12	2022-08-04 07:22:10.277954736	192.0.2.100	198.51.100.100	ICMP	102	0x9ccb (40139)	64	Echo (ping) request id=0x0022, seq=14/3584, ttl=64 (no response found)
13	2022-08-04 07:22:11.301931282	192.0.2.100	198.51.100.100	ICMP	112	0x9d84 (40324)	64	Echo (ping) request id=0x0022, seq=15/3840, ttl=64 (no response found)
14	2022-08-04 07:22:11.301933600	192.0.2.100	198.51.100.100	ICMP	102	0x9d84 (40324)	64	Echo (ping) request id=0x0022, seq=15/3840, ttl=64 (no response found)
15	2022-08-04 07:22:12.325936521	192.0.2.100	198.51.100.100	ICMP	112	0x9da2 (40354)	64	Echo (ping) request id=0x0022, seq=16/4096, ttl=64 (no response found)
16	2022-08-04 07:22:12.325937895	192.0.2.100	198.51.100.100	ICMP	102	0x9da2 (40354)	64	Echo (ping) request id=0x0022, seq=16/4096, ttl=64 (no response found)
17	2022-08-04 07:22:13.326988040	192.0.2.100	198.51.100.100	ICMP	112	0x9e07 (40455)	64	Echo (ping) request id=0x0022, seq=17/4352, ttl=64 (no response found)
18	2022-08-04 07:22:13.326990258	192.0.2.100	198.51.100.100	ICMP	102	0x9e07 (40455)	64	Echo (ping) request id=0x0022, seq=17/4352, ttl=64 (no response found)
19	2022-08-04 07:22:14.341944773	192.0.2.100	198.51.100.100	ICMP	112	0x9e6a (40554)	64	Echo (ping) request id=0x0022, seq=18/4608, ttl=64 (no response found)
20	2022-08-04 07:22:14.341946249	192.0.2.100	198.51.100.100	ICMP	102	0x9e6a (40554)	64	Echo (ping) request id=0x0022, seq=18/4608, ttl=64 (no response found)
21	2022-08-04 07:22:15.365941588	192.0.2.100	198.51.100.100	ICMP	112	0x9efb (40699)	64	Echo (ping) request id=0x0022, seq=19/4864, ttl=64 (no response found)
22	2022-08-04 07:22:15.365942566	192.0.2.100	198.51.100.100	ICMP	102	0x9efb (40699)	64	Echo (ping) request id=0x0022, seq=19/4864, ttl=64 (no response found)
23	2022-08-04 07:22:16.389973843	192.0.2.100	198.51.100.100	ICMP	112	0x9f08 (40936)	64	Echo (ping) request id=0x0022, seq=20/5120, ttl=64 (no response found)
24	2022-08-04 07:22:16.389975129	192.0.2.100	198.51.100.100	ICMP	102	0x9f08 (40936)	64	Echo (ping) request id=0x0022, seq=20/5120, ttl=64 (no response found)
25	2022-08-04 07:22:17.413936452	192.0.2.100	198.51.100.100	ICMP	112	0xa079 (41081)	64	Echo (ping) request id=0x0022, seq=21/5376, ttl=64 (no response found)
26	2022-08-04 07:22:17.413938090	192.0.2.100	198.51.100.100	ICMP	102	0xa079 (41081)	64	Echo (ping) request id=0x0022, seq=21/5376, ttl=64 (no response found)
27	2022-08-04 07:22:18.437954335	192.0.2.100	198.51.100.100	ICMP	112	0xa11e (41246)	64	Echo (ping) request id=0x0022, seq=22/5632, ttl=64 (no response found)

```

> Frame 1: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface capture_u0_1, id 0
> Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: a2:76:f2:00:00:1b (a2:76:f2:00:00:1b)

VLAN-Tag
1. .... = Direction: From Bridge
..0. .... = Pointer: vif_id
..00 0000 0101 0100 .... = Destination: 84
..... = Looped: No
..... = Reserved: 0
..... = Version: 0
..... = Source: 0
Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
000. .... = Priority: Best Effort (default) (0)
..0. .... = DEI: Ineligible
... 0000 0110 0110 = ID: 102
Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 205
000. .... = Priority: Best Effort (default) (0)
..0. .... = DEI: Ineligible
... 0000 1100 1101 = ID: 205
Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
> Internet Control Message Protocol
  
```

Sélectionnez le deuxième paquet et vérifiez les points clés :

1. Seuls les paquets de requête d'écho ICMP sont capturés. Chaque paquet est capturé et affiché 2 fois.
2. L'en-tête de paquet d'origine a l'étiquette VLAN 205.

No.	Time	Source	Destination	Protocol	Length	IP ID	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) request id=0x0022, seq=1/256, ttl=64 (no response found)
2	2022-08-04 07:21:56.993303597	192.0.2.100	198.51.100.100	ICMP	102	0x9574 (38260)	64	Echo (ping) request id=0x0022, seq=1/256, ttl=64 (no response found)
3	2022-08-04 07:22:06.214264777	192.0.2.100	198.51.100.100	ICMP	112	0x9a81 (39553)	64	Echo (ping) request id=0x0022, seq=10/2560, ttl=64 (no response found)
4	2022-08-04 07:22:06.214267373	192.0.2.100	198.51.100.100	ICMP	102	0x9a81 (39553)	64	Echo (ping) request id=0x0022, seq=10/2560, ttl=64 (no response found)
5	2022-08-04 07:22:07.215113393	192.0.2.100	198.51.100.100	ICMP	112	0x9ac3 (39619)	64	Echo (ping) request id=0x0022, seq=11/2816, ttl=64 (no response found)
6	2022-08-04 07:22:07.215115445	192.0.2.100	198.51.100.100	ICMP	102	0x9ac3 (39619)	64	Echo (ping) request id=0x0022, seq=11/2816, ttl=64 (no response found)
7	2022-08-04 07:22:08.229938577	192.0.2.100	198.51.100.100	ICMP	112	0x9b33 (39731)	64	Echo (ping) request id=0x0022, seq=12/3072, ttl=64 (no response found)
8	2022-08-04 07:22:08.229940829	192.0.2.100	198.51.100.100	ICMP	102	0x9b33 (39731)	64	Echo (ping) request id=0x0022, seq=12/3072, ttl=64 (no response found)
9	2022-08-04 07:22:09.253946601	192.0.2.100	198.51.100.100	ICMP	112	0x9c0e (39950)	64	Echo (ping) request id=0x0022, seq=13/3328, ttl=64 (no response found)
10	2022-08-04 07:22:09.253946899	192.0.2.100	198.51.100.100	ICMP	102	0x9c0e (39950)	64	Echo (ping) request id=0x0022, seq=13/3328, ttl=64 (no response found)
11	2022-08-04 07:22:10.277953070	192.0.2.100	198.51.100.100	ICMP	112	0x9ccb (40139)	64	Echo (ping) request id=0x0022, seq=14/3584, ttl=64 (no response found)
12	2022-08-04 07:22:10.277954736	192.0.2.100	198.51.100.100	ICMP	102	0x9ccb (40139)	64	Echo (ping) request id=0x0022, seq=14/3584, ttl=64 (no response found)
13	2022-08-04 07:22:11.301931282	192.0.2.100	198.51.100.100	ICMP	112	0x9d84 (40324)	64	Echo (ping) request id=0x0022, seq=15/3840, ttl=64 (no response found)
14	2022-08-04 07:22:11.301933600	192.0.2.100	198.51.100.100	ICMP	102	0x9d84 (40324)	64	Echo (ping) request id=0x0022, seq=15/3840, ttl=64 (no response found)
15	2022-08-04 07:22:12.325936521	192.0.2.100	198.51.100.100	ICMP	112	0x9da2 (40354)	64	Echo (ping) request id=0x0022, seq=16/4096, ttl=64 (no response found)
16	2022-08-04 07:22:12.325937895	192.0.2.100	198.51.100.100	ICMP	102	0x9da2 (40354)	64	Echo (ping) request id=0x0022, seq=16/4096, ttl=64 (no response found)
17	2022-08-04 07:22:13.326988040	192.0.2.100	198.51.100.100	ICMP	112	0x9e07 (40455)	64	Echo (ping) request id=0x0022, seq=17/4352, ttl=64 (no response found)
18	2022-08-04 07:22:13.326990258	192.0.2.100	198.51.100.100	ICMP	102	0x9e07 (40455)	64	Echo (ping) request id=0x0022, seq=17/4352, ttl=64 (no response found)
19	2022-08-04 07:22:14.341944773	192.0.2.100	198.51.100.100	ICMP	112	0x9e6a (40554)	64	Echo (ping) request id=0x0022, seq=18/4608, ttl=64 (no response found)
20	2022-08-04 07:22:14.341946249	192.0.2.100	198.51.100.100	ICMP	102	0x9e6a (40554)	64	Echo (ping) request id=0x0022, seq=18/4608, ttl=64 (no response found)
21	2022-08-04 07:22:15.365941588	192.0.2.100	198.51.100.100	ICMP	112	0x9efb (40699)	64	Echo (ping) request id=0x0022, seq=19/4864, ttl=64 (no response found)
22	2022-08-04 07:22:15.365942566	192.0.2.100	198.51.100.100	ICMP	102	0x9efb (40699)	64	Echo (ping) request id=0x0022, seq=19/4864, ttl=64 (no response found)
23	2022-08-04 07:22:16.389973843	192.0.2.100	198.51.100.100	ICMP	112	0x9f08 (40936)	64	Echo (ping) request id=0x0022, seq=20/5120, ttl=64 (no response found)
24	2022-08-04 07:22:16.389975129	192.0.2.100	198.51.100.100	ICMP	102	0x9f08 (40936)	64	Echo (ping) request id=0x0022, seq=20/5120, ttl=64 (no response found)
25	2022-08-04 07:22:17.413936452	192.0.2.100	198.51.100.100	ICMP	112	0xa079 (41081)	64	Echo (ping) request id=0x0022, seq=21/5376, ttl=64 (no response found)
26	2022-08-04 07:22:17.413938090	192.0.2.100	198.51.100.100	ICMP	102	0xa079 (41081)	64	Echo (ping) request id=0x0022, seq=21/5376, ttl=64 (no response found)
27	2022-08-04 07:22:18.437954335	192.0.2.100	198.51.100.100	ICMP	112	0xa11e (41246)	64	Echo (ping) request id=0x0022, seq=22/5632, ttl=64 (no response found)

```

> Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture_u0_1, id 0
> Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: a2:76:f2:00:00:1b (a2:76:f2:00:00:1b)

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 205
000. .... = Priority: Best Effort (default) (0)
..0. .... = DEI: Ineligible
... 0000 1100 1101 = ID: 205
Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
> Internet Control Message Protocol
  
```

Ouvrez à présent les fichiers de capture pour Portchannel1.207. Sélectionnez le premier paquet et vérifiez les points clés

1. Seuls les paquets de requête d'écho ICMP sont capturés. Chaque paquet est capturé et affiché 2 fois.
2. L'en-tête de paquet d'origine a l'étiquette VLAN 207.
3. Le commutateur interne insère une étiquette VLAN de port supplémentaire 1001 qui identifie

l'interface d'entrée Portchannel1.

4. Le commutateur interne insère une étiquette VN supplémentaire.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-04 08:18:24.572548869	192.168.247.100	192.168.247.102	ICMP	128	0x609e (24734)	255	Echo (ping) request
2	2022-08-04 08:18:24.572550073	192.168.247.100	192.168.247.102	ICMP	118	0x609e (24734)	255	Echo (ping) request
3	2022-08-04 08:18:24.573286630	192.168.247.100	192.168.247.102	ICMP	128	0x609f (24735)	255	Echo (ping) request
4	2022-08-04 08:18:24.573287640	192.168.247.100	192.168.247.102	ICMP	118	0x609f (24735)	255	Echo (ping) request
5	2022-08-04 08:18:24.573794751	192.168.247.100	192.168.247.102	ICMP	128	0x60a0 (24736)	255	Echo (ping) request
6	2022-08-04 08:18:24.573795748	192.168.247.100	192.168.247.102	ICMP	118	0x60a0 (24736)	255	Echo (ping) request
7	2022-08-04 08:18:24.574368638	192.168.247.100	192.168.247.102	ICMP	128	0x60a1 (24737)	255	Echo (ping) request
8	2022-08-04 08:18:24.574369574	192.168.247.100	192.168.247.102	ICMP	118	0x60a1 (24737)	255	Echo (ping) request
9	2022-08-04 08:18:24.574914512	192.168.247.100	192.168.247.102	ICMP	128	0x60a2 (24738)	255	Echo (ping) request
10	2022-08-04 08:18:24.574915415	192.168.247.100	192.168.247.102	ICMP	118	0x60a2 (24738)	255	Echo (ping) request
11	2022-08-04 08:18:24.575442569	192.168.247.100	192.168.247.102	ICMP	128	0x60a3 (24739)	255	Echo (ping) request
12	2022-08-04 08:18:24.575443691	192.168.247.100	192.168.247.102	ICMP	118	0x60a3 (24739)	255	Echo (ping) request
13	2022-08-04 08:18:24.575918119	192.168.247.100	192.168.247.102	ICMP	128	0x60a4 (24740)	255	Echo (ping) request
14	2022-08-04 08:18:24.575919057	192.168.247.100	192.168.247.102	ICMP	118	0x60a4 (24740)	255	Echo (ping) request
15	2022-08-04 08:18:24.576406771	192.168.247.100	192.168.247.102	ICMP	128	0x60a5 (24741)	255	Echo (ping) request
16	2022-08-04 08:18:24.576408585	192.168.247.100	192.168.247.102	ICMP	118	0x60a5 (24741)	255	Echo (ping) request
17	2022-08-04 08:18:24.576885643	192.168.247.100	192.168.247.102	ICMP	128	0x60a6 (24742)	255	Echo (ping) request
18	2022-08-04 08:18:24.576886561	192.168.247.100	192.168.247.102	ICMP	118	0x60a6 (24742)	255	Echo (ping) request
19	2022-08-04 08:18:24.577394328	192.168.247.100	192.168.247.102	ICMP	128	0x60a7 (24743)	255	Echo (ping) request
20	2022-08-04 08:18:24.577395234	192.168.247.100	192.168.247.102	ICMP	118	0x60a7 (24743)	255	Echo (ping) request
21	2022-08-04 08:18:24.577987632	192.168.247.100	192.168.247.102	ICMP	128	0x60a8 (24744)	255	Echo (ping) request
22	2022-08-04 08:18:24.577989290	192.168.247.100	192.168.247.102	ICMP	118	0x60a8 (24744)	255	Echo (ping) request
23	2022-08-04 08:18:24.578448781	192.168.247.100	192.168.247.102	ICMP	128	0x60a9 (24745)	255	Echo (ping) request
24	2022-08-04 08:18:24.578449909	192.168.247.100	192.168.247.102	ICMP	118	0x60a9 (24745)	255	Echo (ping) request
25	2022-08-04 08:18:24.578900043	192.168.247.100	192.168.247.102	ICMP	128	0x60aa (24746)	255	Echo (ping) request
26	2022-08-04 08:18:24.578900897	192.168.247.100	192.168.247.102	ICMP	118	0x60aa (24746)	255	Echo (ping) request
27	2022-08-04 08:18:24.579426962	192.168.247.100	192.168.247.102	ICMP	128	0x60ab (24747)	255	Echo (ping) request


```

Frame 1: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface capture_u0_3, id 0
Ethernet II, Src: Cisco d6ec:00 (00:17:df:d6:ec:00), Dst: a2:76:f2:00:00:1c (a2:76:f2:00:00:1c)
VN-Tag
  1. .... = Direction: From Bridge
  .0. .... = Pointer: vif_id
  ..00 0000 0011 1101 .... = Destination: 61
  .... = Looped: No
  .... = Reserved: 0
  .... = Version: 0
  .... 0000 0000 0000 = Source: 0
Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1001
  000. .... = Priority: Best Effort (default) (0)
  ...0 .... = DEI: Ineligible
  .... 0011 1110 1001 = ID: 1001
Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 207
  000. .... = Priority: Best Effort (default) (0)
  ...0 .... = DEI: Ineligible
  .... 0000 1100 1111 = ID: 207
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.247.100, Dst: 192.168.247.102
Internet Control Message Protocol
  
```

Sélectionnez le deuxième paquet et vérifiez les points clés :

1. Seuls les paquets de requête d'écho ICMP sont capturés. Chaque paquet est capturé et affiché 2 fois.
2. L'en-tête de paquet d'origine a l'étiquette VLAN 207.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-04 08:18:24.572548869	192.168.247.100	192.168.247.102	ICMP	128	0x609e (24734)	255	Echo (ping) request
2	2022-08-04 08:18:24.572550073	192.168.247.100	192.168.247.102	ICMP	118	0x609e (24734)	255	Echo (ping) request
3	2022-08-04 08:18:24.573286630	192.168.247.100	192.168.247.102	ICMP	128	0x609f (24735)	255	Echo (ping) request
4	2022-08-04 08:18:24.573287640	192.168.247.100	192.168.247.102	ICMP	118	0x609f (24735)	255	Echo (ping) request
5	2022-08-04 08:18:24.573794751	192.168.247.100	192.168.247.102	ICMP	128	0x60a0 (24736)	255	Echo (ping) request
6	2022-08-04 08:18:24.573795748	192.168.247.100	192.168.247.102	ICMP	118	0x60a0 (24736)	255	Echo (ping) request
7	2022-08-04 08:18:24.574368638	192.168.247.100	192.168.247.102	ICMP	128	0x60a1 (24737)	255	Echo (ping) request
8	2022-08-04 08:18:24.574369574	192.168.247.100	192.168.247.102	ICMP	118	0x60a1 (24737)	255	Echo (ping) request
9	2022-08-04 08:18:24.574914512	192.168.247.100	192.168.247.102	ICMP	128	0x60a2 (24738)	255	Echo (ping) request
10	2022-08-04 08:18:24.574915415	192.168.247.100	192.168.247.102	ICMP	118	0x60a2 (24738)	255	Echo (ping) request
11	2022-08-04 08:18:24.575442569	192.168.247.100	192.168.247.102	ICMP	128	0x60a3 (24739)	255	Echo (ping) request
12	2022-08-04 08:18:24.575443691	192.168.247.100	192.168.247.102	ICMP	118	0x60a3 (24739)	255	Echo (ping) request
13	2022-08-04 08:18:24.575918119	192.168.247.100	192.168.247.102	ICMP	128	0x60a4 (24740)	255	Echo (ping) request
14	2022-08-04 08:18:24.575919057	192.168.247.100	192.168.247.102	ICMP	118	0x60a4 (24740)	255	Echo (ping) request
15	2022-08-04 08:18:24.576406771	192.168.247.100	192.168.247.102	ICMP	128	0x60a5 (24741)	255	Echo (ping) request
16	2022-08-04 08:18:24.576408585	192.168.247.100	192.168.247.102	ICMP	118	0x60a5 (24741)	255	Echo (ping) request
17	2022-08-04 08:18:24.576885643	192.168.247.100	192.168.247.102	ICMP	128	0x60a6 (24742)	255	Echo (ping) request
18	2022-08-04 08:18:24.576886561	192.168.247.100	192.168.247.102	ICMP	118	0x60a6 (24742)	255	Echo (ping) request
19	2022-08-04 08:18:24.577394328	192.168.247.100	192.168.247.102	ICMP	128	0x60a7 (24743)	255	Echo (ping) request
20	2022-08-04 08:18:24.577395234	192.168.247.100	192.168.247.102	ICMP	118	0x60a7 (24743)	255	Echo (ping) request
21	2022-08-04 08:18:24.577987632	192.168.247.100	192.168.247.102	ICMP	128	0x60a8 (24744)	255	Echo (ping) request
22	2022-08-04 08:18:24.577989290	192.168.247.100	192.168.247.102	ICMP	118	0x60a8 (24744)	255	Echo (ping) request
23	2022-08-04 08:18:24.578448781	192.168.247.100	192.168.247.102	ICMP	128	0x60a9 (24745)	255	Echo (ping) request
24	2022-08-04 08:18:24.578449909	192.168.247.100	192.168.247.102	ICMP	118	0x60a9 (24745)	255	Echo (ping) request
25	2022-08-04 08:18:24.578900043	192.168.247.100	192.168.247.102	ICMP	128	0x60aa (24746)	255	Echo (ping) request
26	2022-08-04 08:18:24.578900897	192.168.247.100	192.168.247.102	ICMP	118	0x60aa (24746)	255	Echo (ping) request
27	2022-08-04 08:18:24.579426962	192.168.247.100	192.168.247.102	ICMP	128	0x60ab (24747)	255	Echo (ping) request


```

Frame 2: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface capture_u0_3, id 0
Ethernet II, Src: Cisco d6ec:00 (00:17:df:d6:ec:00), Dst: a2:76:f2:00:00:1c (a2:76:f2:00:00:1c)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 207
  000. .... = Priority: Best Effort (default) (0)
  ...0 .... = DEI: Ineligible
  .... 0000 1100 1111 = ID: 207
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.247.100, Dst: 192.168.247.102
Internet Control Message Protocol
  
```

Explication

Lorsqu'une capture de paquets sur une interface avant est configurée, le commutateur capture simultanément chaque paquet deux fois :

- Après l'insertion de l'étiquette VLAN du port.
- Après l'insertion de la balise VN.

Dans l'ordre des opérations, l'étiquette VLAN est insérée à un stade ultérieur à celui de l'insertion de l'étiquette VLAN du port. Mais dans le fichier de capture, le paquet avec l'étiquette VLAN est affiché plus tôt que le paquet avec l'étiquette VLAN de port. En outre, dans le cas des sous-interfaces, dans les fichiers de capture, un paquet sur deux ne contient pas l'étiquette VLAN de port.

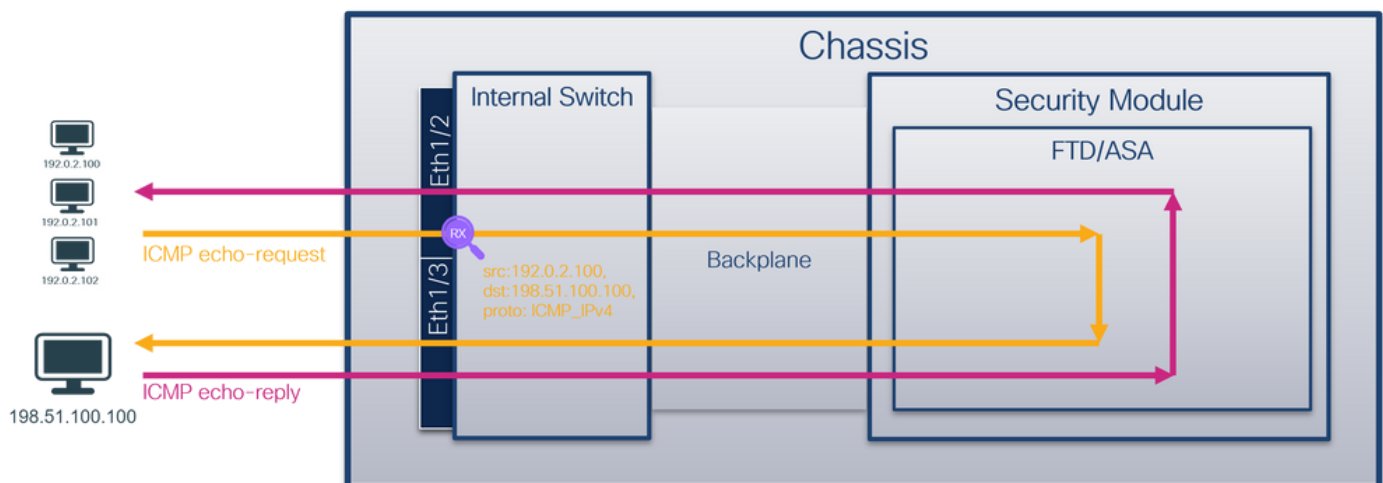
Ce tableau récapitule la tâche :

Tâche	Point de capture	VLAN de port interne dans les paquets capturés	Direction	Trafic capturé
Configurer et vérifier une capture de paquets sur la sous-interface Ethernet1/2.205	Ethernet1/2.205	102	Entrée unique	Requêtes d'écho ICMP de l'hôte 192.0.2.100 vers l'hôte 198.51.100.100
Configurez et vérifiez une capture de paquets sur la sous-interface Portchannel1 avec les interfaces membres Ethernet1/3 et Ethernet1/4	Ethernet1/3 Ethernet1/4	1001	Entrée unique	Requêtes d'écho ICMP de 192.168.207.100 vers l'hôte 192.168.207.102

Filtres de capture de paquets

Utilisez FCM et CLI pour configurer et vérifier une capture de paquets sur l'interface Ethernet1/2 avec un filtre.

Topologie, flux de paquets et points de capture

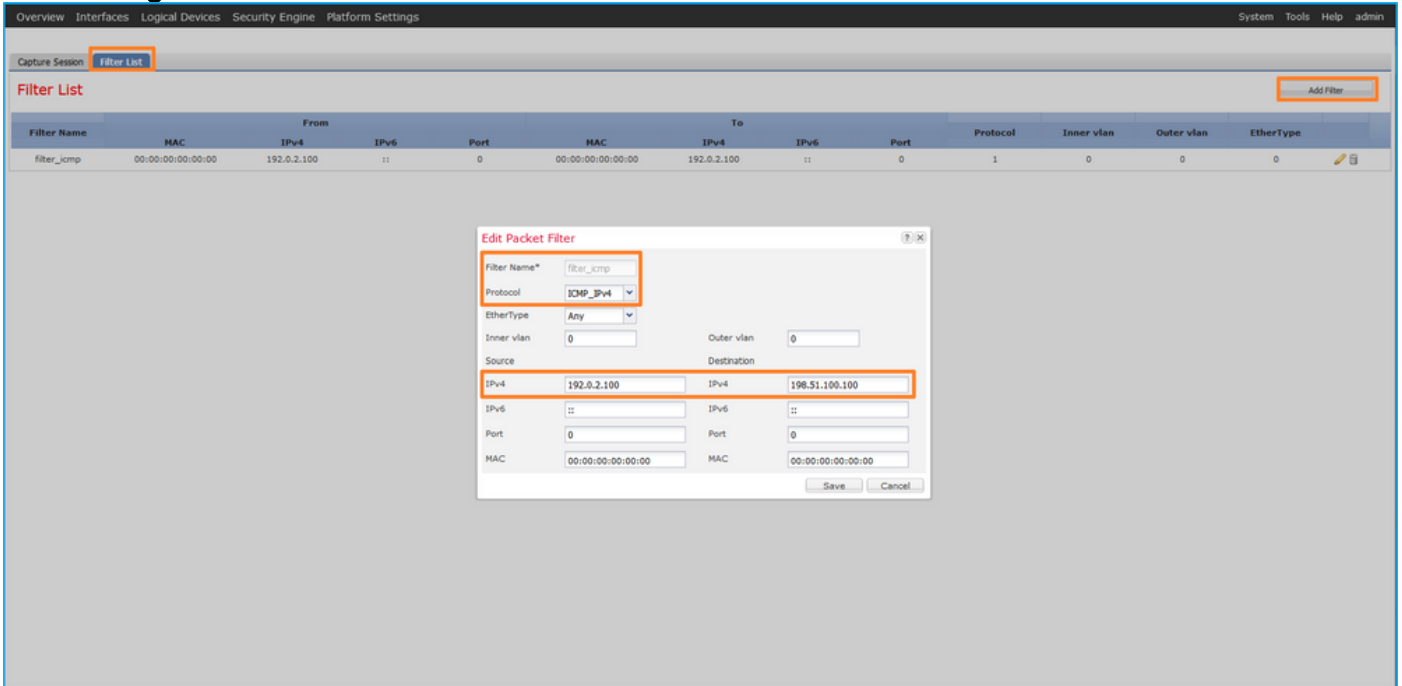


Configuration

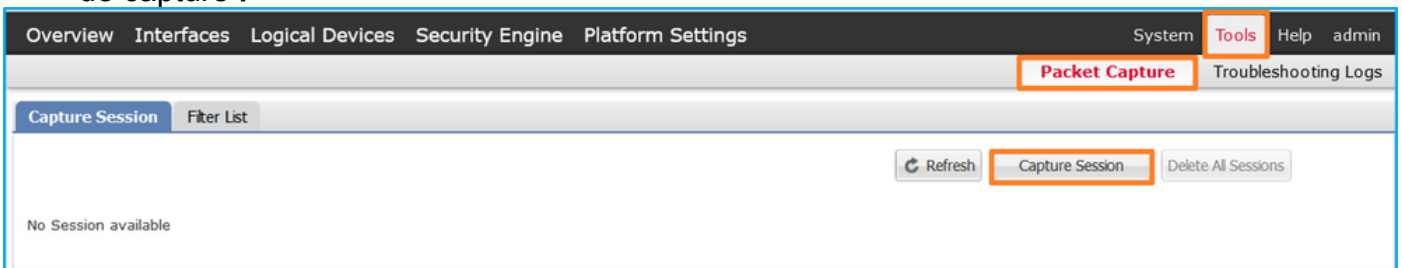
FCM

Suivez ces étapes sur FCM pour configurer un filtre de capture pour les paquets de requête d'écho ICMP de l'hôte 192.0.2.100 à l'hôte 198.51.100.100 et l'appliquer à la capture de paquets sur l'interface Ethernet1/2 :

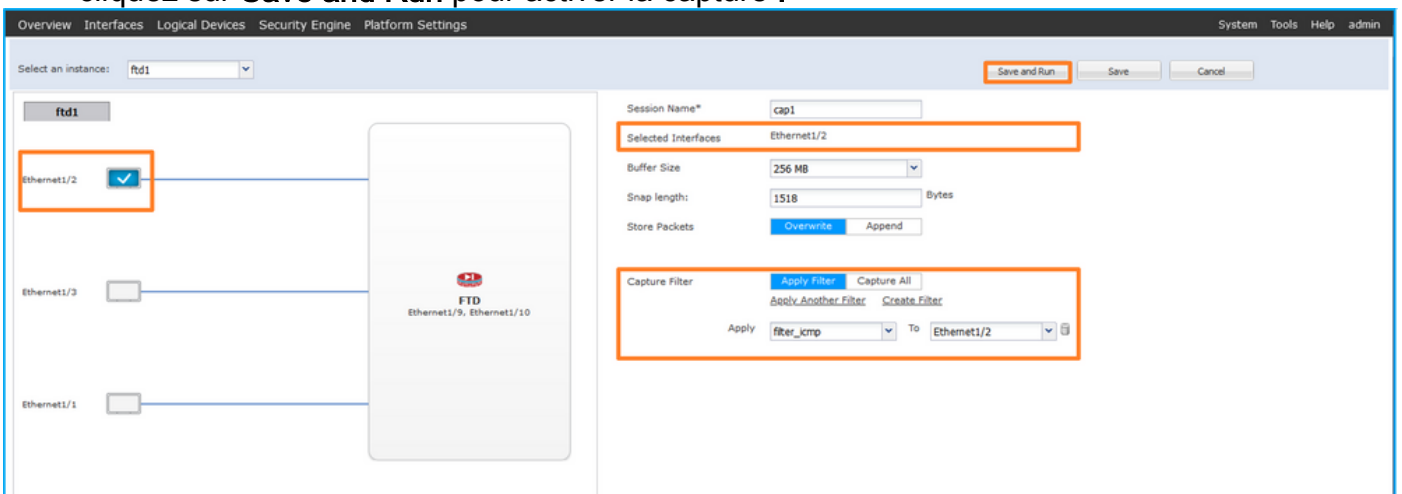
1. Utilisez **Outils > Capture de paquets > Liste de filtres > Ajouter un filtre** pour créer un filtre de capture.
2. Spécifiez le **nom du filtre**, le **protocole**, l'**IPv4 source**, l'**IPv4 de destination** et cliquez sur **Enregistrer** :



3. Utilisez **Outils > Capture de paquets > Session de capture** pour créer une nouvelle session de capture :



4. Sélectionnez **Ethernet1/2**, indiquez le **nom de session**, appliquez le filtre de capture et cliquez sur **Save and Run** pour activer la capture :



CLI FXOS

Procédez comme suit sur l'interface de ligne de commande FXOS pour configurer les captures de

paquets sur les interfaces de fond de panier :

1. Identifiez le type et l'identificateur de l'application :

```
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          ftd1         1             Enabled      Online          7.2.0.82      7.2.0.82
Native       No           Not Applicable  None
```

2. Identifiez le numéro de protocole IP dans <https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>. Dans ce cas, le numéro de protocole ICMP est 1.

3. Créez une session de capture :

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-identifieur 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 #
```

Vérification

FCM

Vérifiez le nom de l'interface, assurez-vous que l'état opérationnel est up et que la taille du fichier (en octets) augmente :

Filter Name	MAC	From IPv4	From IPv6	Port	MAC	To IPv4	To IPv6	Port	Protocol	Inner vlan	Outer vlan	EtherType
filter_icmp	00:00:00:00:00:00	192.0.2.100	::	0	00:00:00:00:00:00	198.51.100.100	::	0	1	0	0	0

Vérifiez le nom de l'interface, le filtre, assurez-vous que l'état opérationnel est activé et que la taille du fichier (en octets) augmente dans Outils > Capture de paquets > Session de capture :

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

Vérifiez les détails de capture dans la portée 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
```

Collecter les fichiers de capture

Suivez les étapes de la section **Collecter les fichiers de capture internes du commutateur Firepower 4100/9300**.

Capturer l'analyse des fichiers

Utilisez une application de lecture de fichier de capture de paquets pour ouvrir le fichier de capture. Sélectionnez le premier paquet et vérifiez les points clés

1. Seuls les paquets de requête d'écho ICMP sont capturés. Chaque paquet est capturé et affiché 2 fois.
2. L'en-tête de paquet d'origine est sans étiquette VLAN.
3. Le commutateur interne insère une étiquette VLAN de port supplémentaire **102** qui identifie

l'interface d'entrée Ethernet1/2.

4. Le commutateur interne insère une étiquette VN supplémentaire.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-02 15:46:55.603277760	192.0.2.100	198.51.100.100	ICMP	108	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 15:47:01.747163204	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 bits), 108 bytes captured (864 bits) on interface capture_u0_1, i
> Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)

VN-Tag

- 1... .. = Direction: From Bridge
- .0.. .. = Pointer: vif_id
- ..00 0000 1010 .. = Destination: 10
-0..... = Looped: No
-0.. = Reserved: 0
-000 = Version: 0
-0000 0000 0000 = Source: 0
- Type: 802.1Q Virtual LAN (0x8100)

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102

- 000. = Priority: Best Effort (default) (0)
- ...0 .. = DEI: Ineligible
- ... 0000 0110 0110 = ID: 102
- Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100

Internet Control Message Protocol

Sélectionnez le deuxième paquet et vérifiez les points clés :

1. Seuls les paquets de requête d'écho ICMP sont capturés. Chaque paquet est capturé et affiché 2 fois.
2. L'en-tête de paquet d'origine est sans étiquette VLAN.
3. Le commutateur interne insère une étiquette VLAN de port supplémentaire 102 qui identifie l'interface d'entrée Ethernet1/2.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-02 15:46:55.603277760	192.0.2.100	198.51.100.100	ICMP	108	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 15:47:01.747163204	192.0.2.100	198.51.100.100	ICMP	108	0x026e (622)	64	Echo (ping) request id=0x0018, seq=355/25345, ttl=64 (no r
14	2022-08-02 15:47:01.747163783	192.0.2.100	198.51.100.100	ICMP	102	0x026e (622)	64	Echo (ping) request id=0x0018, seq=355/25345, ttl=64 (no r
15	2022-08-02 15:47:02.771209952	192.0.2.100	198.51.100.100	ICMP	108	0x02bc (700)	64	Echo (ping) request id=0x0018, seq=356/25601, ttl=64 (no r
16	2022-08-02 15:47:02.771211062	192.0.2.100	198.51.100.100	ICMP	102	0x02bc (700)	64	Echo (ping) request id=0x0018, seq=356/25601, ttl=64 (no r
17	2022-08-02 15:47:03.772258550	192.0.2.100	198.51.100.100	ICMP	108	0x032f (815)	64	Echo (ping) request id=0x0018, seq=357/25857, ttl=64 (no r
18	2022-08-02 15:47:03.772259724	192.0.2.100	198.51.100.100	ICMP	102	0x032f (815)	64	Echo (ping) request id=0x0018, seq=357/25857, ttl=64 (no r
19	2022-08-02 15:47:04.791118519	192.0.2.100	198.51.100.100	ICMP	108	0x040f (1039)	64	Echo (ping) request id=0x0018, seq=358/26113, ttl=64 (no r
20	2022-08-02 15:47:04.791119721	192.0.2.100	198.51.100.100	ICMP	102	0x040f (1039)	64	Echo (ping) request id=0x0018, seq=358/26113, ttl=64 (no r

Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture_u0_1, i
> Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102

- 000. = Priority: Best Effort (default) (0)
- ...0 .. = DEI: Ineligible
- ... 0000 0110 0110 = ID: 102
- Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100

Internet Control Message Protocol

Explication

Lorsqu'une capture de paquets sur une interface avant est configurée, le commutateur capture simultanément chaque paquet deux fois :

- Après l'insertion de l'étiquette VLAN du port.
- Après l'insertion de la balise VN.

Dans l'ordre des opérations, l'étiquette VLAN est insérée à un stade ultérieur à celui de l'insertion de l'étiquette VLAN du port. Mais dans le fichier de capture, le paquet avec l'étiquette VLAN est affiché plus tôt que le paquet avec l'étiquette VLAN de port.

Lorsqu'un filtre de capture est appliqué, seuls les paquets qui correspondent au filtre dans la direction d'entrée sont capturés.

Ce tableau récapitule la tâche :

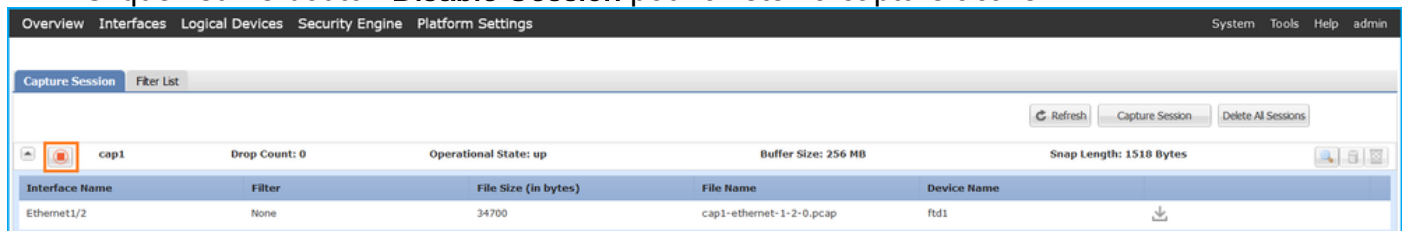
Tâche	Point de capture	VLAN de port interne dans les paquets capturés	Direction	Filtre utilisateur	Trafic capturé
Configurer et vérifier une capture de paquets avec un filtre sur l'interface avant Ethernet1/2	Ethernet1/2	102	Entrée unique	Protocole : ICMP Source : 192.0.2.100 Destination : 198.51.100.100	Requêtes d'écho ICMP de l'hôte 192.0.2.100 vers l'hôte 198.51.100.100

Collecter les fichiers de capture du commutateur interne Firepower 4100/9300

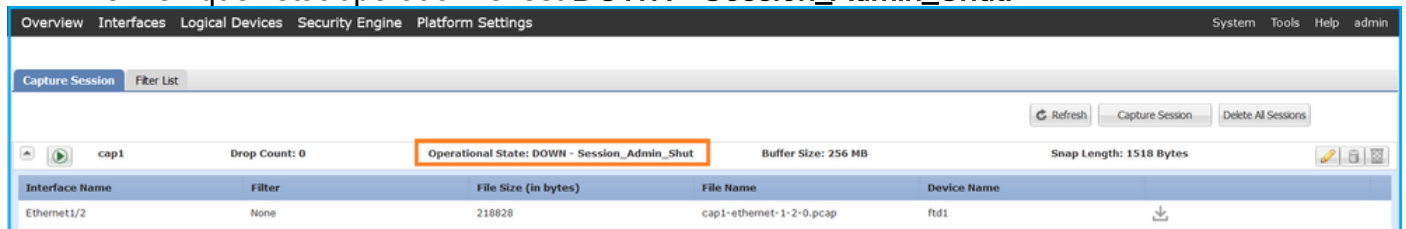
FCM

Procédez comme suit sur FCM pour collecter les fichiers de capture internes du commutateur :

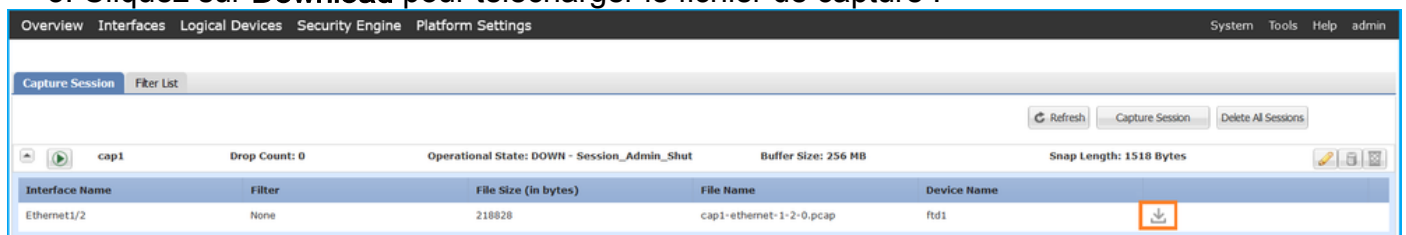
1. Cliquez sur le bouton **Disable Session** pour arrêter la capture active :



2. Vérifiez que l'état opérationnel est **DOWN - Session_Admin_Shut**:



3. Cliquez sur **Download** pour télécharger le fichier de capture :



Dans le cas des interfaces port-channel, répétez cette étape pour chaque interface membre.

CLI FXOS

Procédez comme suit sur l'interface de ligne de commande FXOS pour collecter les fichiers de capture :

1. Arrêtez la capture active :

```
firepower# scope packet-capture
firepower /packet-capture # scope session cap1
firepower /packet-capture/session # disable
firepower /packet-capture/session* # commit
firepower /packet-capture/session # up
firepower /packet-capture # show session cap1 detail
```

Traffic Monitoring Session:

```
Packet Capture Session Name: cap1
Session: 1
Admin State: Disabled
Oper State: Down
Oper State Reason: Admin Disable
Config Success: Yes
Config Fail Reason:
Append Flag: Overwrite
Session Mem Usage: 256 MB
Session Pcap Snap Len: 1518 Bytes
Error Code: 0
Drop Count: 0
```

Physical ports involved in Packet Capture:

```
Slot Id: 1
Port Id: 2
Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap
Pcapsize: 115744 bytes
Filter:
Sub Interface: 0
Application Instance Identifier: ftd1
Application Name: ftd
```

2. Téléchargez le fichier de capture à partir de la portée de la commande local-mgmt :

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

```
firepower(local-mgmt)# copy /packet-capture/session-1/cap1-ethernet-1-2-0.pcap
```

```
ftp://ftpuser@10.10.10.1/cap1-ethernet-1-2-0.pcap
```

Password:

Dans le cas des interfaces port-channel, copiez le fichier de capture pour chaque interface membre.

Recommandations, limites et meilleures pratiques pour Commutateur interne

Capture de paquets

Pour connaître les consignes et les restrictions relatives à la capture interne du commutateur Firepower 4100/9300, reportez-vous au *Guide de configuration du gestionnaire de châssis FXOS Cisco Firepower 4100/9300* ou au *Guide de configuration de l'interface de ligne de commande FXOS Cisco Firepower 4100/9300*, chapitre **Troubleshooting**, section **Packet Capture**.

Voici la liste des meilleures pratiques basées sur l'utilisation de la capture de paquets dans les cas TAC :

- Soyez conscient des directives et des limites.
- Capturez les paquets sur toutes les interfaces membres port-channel et analysez tous les fichiers de capture.
- Utiliser des filtres de capture.
- Tenez compte de l'impact de la fonction NAT sur les adresses IP des paquets lorsqu'un filtre de capture est configuré.
- Augmentez ou diminuez la **lentille d'accrochage** qui spécifie la taille de trame au cas où elle serait différente de la valeur par défaut de 1 518 octets. Une taille plus courte entraîne une augmentation du nombre de paquets capturés et vice versa.
- Réglez la **taille** de la **mémoire tampon** si nécessaire.
- Soyez conscient du nombre de **pertes** sur FCM ou FXOS CLI. Une fois la taille limite de la mémoire tampon atteinte, le compteur d'abandon augmente.
- Utilisez le filtre **!vntag** sur Wireshark pour afficher uniquement les paquets sans la balise VN. Ceci est utile pour masquer les paquets étiquetés VN dans les fichiers de capture de paquets de l'interface avant.
- Utilisez le filtre **frame.number&1** sur Wireshark pour afficher uniquement les trames impaires. Ceci est utile pour masquer les paquets en double dans les fichiers de capture de paquets de l'interface de fond de panier.
- Dans le cas de protocoles tels que TCP, Wireshark applique par défaut des règles de coloration qui affichent les paquets avec des conditions spécifiques dans différentes couleurs. Dans le cas de captures internes du commutateur dues à des paquets dupliqués dans des fichiers de capture, le paquet peut être coloré et marqué d'une manière faussement positive. Si vous analysez les fichiers de capture de paquets et appliquez un filtre, exportez les paquets affichés dans un nouveau fichier et ouvrez le nouveau fichier à la place.

Configuration et vérification sur Pare-feu sécurisé 3100

À la différence de Firepower 4100/9300, les captures de commutateur interne sur le pare-feu sécurisé 3100 sont configurées sur l'interface de ligne de commande d'application via la commande **capture <name>switch**, où l'option **switch** spécifie que les captures sont configurées sur le commutateur interne.

Voici la commande **capture** avec l'option **switch** :

```
> capture cap_sw switch ?
buffer          Configure size of capture buffer, default is 256MB
ethernet-type   Capture Ethernet packets of a particular type, default is IP
interface       Capture packets on a specific interface
ivlan          Inner Vlan
```

```

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

```

Les étapes générales de configuration de la capture de paquets sont les suivantes :

1. Spécifiez une interface d'entrée :

La configuration de capture du commutateur accepte le **nom d'interface d'entrée if**. L'utilisateur peut spécifier les noms des interfaces de données, la liaison ascendante interne ou les interfaces de gestion :

```
> 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. Spécifiez l'EtherType de trame Ethernet. L'EtherType par défaut est IP. Les valeurs de l'option **ethernet-type** spécifient l'EtherType :

```
> capture capsw switch interface inside ethernet-type ?
```

```

802.1Q
<0-65535>  Ethernet type
arp
ip
ip6
pppoed
pppoes
rarp
sgt
vlan

```

3. Spécifiez les conditions de correspondance. L'option de **correspondance** de capture spécifie les critères de correspondance :

```
> capture capsw switch interface inside match ?
```

```

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

```

```
nos
ospf
pcp
pim
pptp
sctp
snp
spi          SPI value
tcp
udp
<cr>
```

4. Spécifiez d'autres paramètres facultatifs tels que la taille de la mémoire tampon, la longueur du paquet, etc.
5. Activez la capture. La commande **no capture <name> switch stop** active la capture :

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

6. Vérifiez les détails de la capture :

- L'état administratif est **activé** et l'état opérationnel est **activé** et actif.
- Taille du fichier de capture de paquets **Pcapsize** augmente.
- Le nombre de paquets capturés dans le résultat de la commande **show capture <cap_name>** est différent de zéro.
- Chemin de capture **Pcapfile**. Les paquets capturés sont automatiquement enregistrés dans le dossier **/mnt/disk0/packet-capture/**.
- Capturer les conditions. Le logiciel crée automatiquement des filtres de capture en fonction des conditions de capture.

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

```
>show capture capsw detail
```

Packet Capture info

```
Name:          capsw
Session:         1
Admin State:  enabled
Oper State:   up
Oper State Reason: Active
Config Success:  yes
Config Fail Reason:
Append Flag:     overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code:      0
Drop Count:      0
```

Total Physical ports involved in Packet Capture: 1

Physical port:

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

Packet Capture Filter Info

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

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

7. Arrêtez les captures si nécessaire :

```
> capture caps switch stop
```

```
>show capture caps detail
```

Packet Capture info

Name: caps
Session: 1
Admin State: disabled
Oper State: down
Oper State Reason: Session_Admin_Shut
Config Success: yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1
Port Id: 1
Pcapfile: /mnt/disk0/packet-capture/sess-1-caps-ethernet-1-1-0.pcap
Pcapsize: 24
Filter: caps-1-1

Packet Capture Filter Info

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

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

8. Collectez les fichiers de capture. Suivez les étapes de la section **Collecter les fichiers de capture internes du commutateur Secure Firewall 3100**.

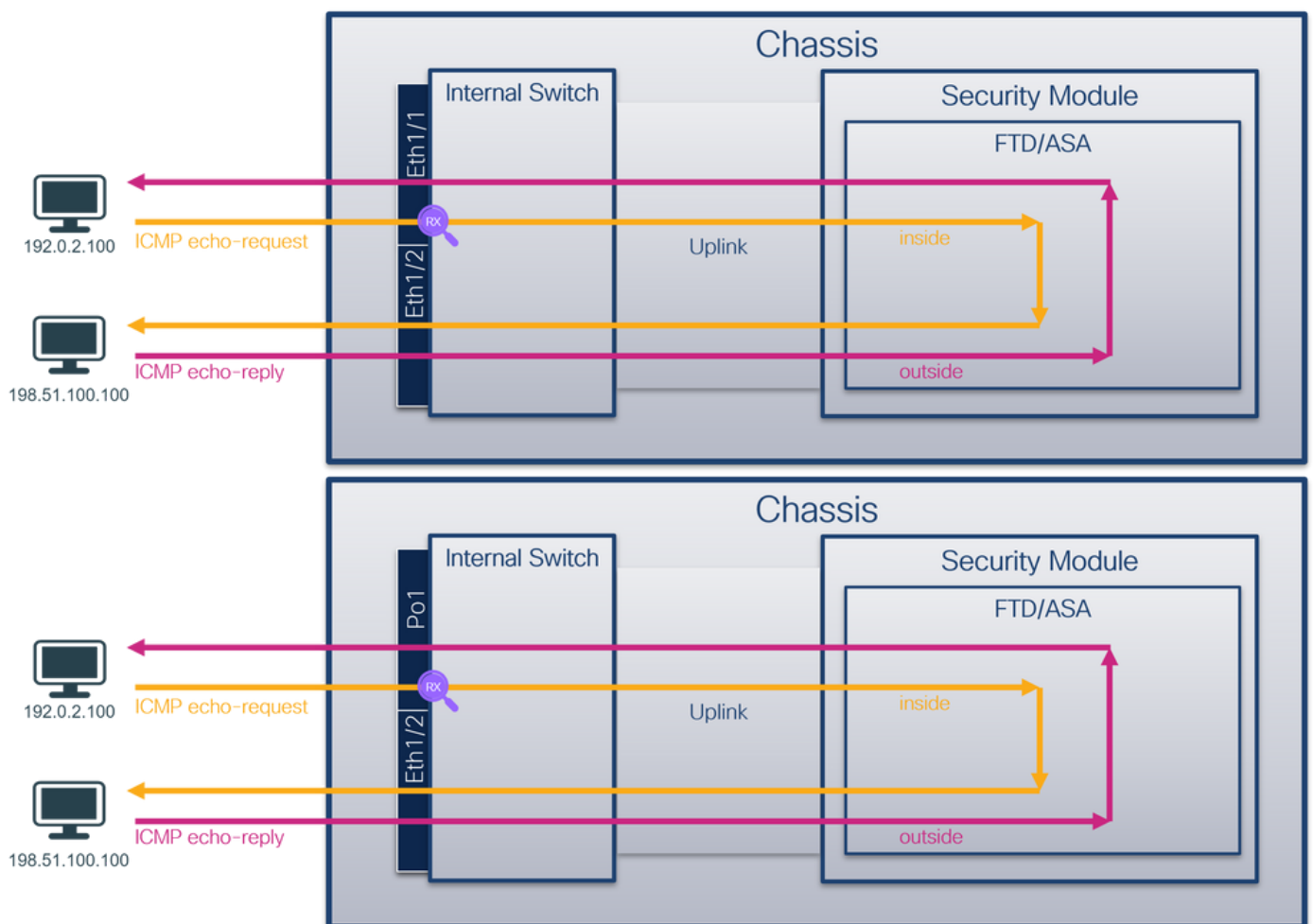
Dans la version 7.2, la configuration de capture interne du commutateur n'est pas prise en charge sur FMC ou FDM. Dans le cas du logiciel ASA version 9.18(1) et ultérieure, les captures de commutateurs internes peuvent être configurées dans ASDM versions 7.18.1.x et ultérieures.

Ces scénarios couvrent les cas d'utilisation courants des captures internes du commutateur Secure Firewall 3100.

Capture de paquets sur une interface physique ou Port Channel

Utilisez l'interface de ligne de commande FTD ou ASA pour configurer et vérifier une capture de paquets sur l'interface Ethernet1/1 ou l'interface Portchannel1. Les deux interfaces portent le nom if **inside**.

Topologie, flux de paquets et points de capture



Configuration

Procédez comme suit sur l'interface de ligne de commande ASA ou FTD pour configurer une capture de paquets sur l'interface Ethernet1/1 ou Port-channel1 :

1. Vérifiez le nom si :

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

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

2. Créez une session de capture :

```
> capture capsw switch interface inside
```

3. Activez la session de capture :

```
> no capture capsw switch stop
```

Vérification

Vérifiez le nom de la session de capture, l'état administratif et opérationnel, le logement d'interface et l'identificateur. Assurez-vous que la valeur **Pcapsize** en octets augmente et que le nombre de paquets capturés est différent de zéro :

```
> show capture capsw detail
```

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

```
Total Physical ports involved in Packet Capture: 1
```

```
Physical port:
```

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

```
Packet Capture Filter Info
```

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

Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

79 packets captured on disk using switch capture

Reading of capture file from disk is not supported

Dans le cas de Port-channel1, la capture est configurée sur toutes les interfaces membres :

> **show capture capsw detail**

Packet Capture info

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

Total Physical ports involved in Packet Capture: 2

Physical port:

Slot Id: 1
Port Id: 4
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-4-0.pcap
Pcapsize: 28824
Filter: capsw-1-4

Packet Capture Filter Info

Name: capsw-1-4
Protocol: 0
Ivlan: 0
Ovlan: 0
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Physical port:

Slot Id: 1
Port Id: 3
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-3-0.pcap
Pcapsize: 18399
Filter: capsw-1-3

Packet Capture Filter Info

Name: capsw-1-3
Protocol: 0
Ivlan: 0

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

Total Physical breakout ports involved in Packet Capture: 0

56 packet captured on disk using switch capture

Reading of capture file from disk is not supported

Les interfaces membres port-channel peuvent être vérifiées dans l'interpréteur de commandes FXOS **local-mgmt** via la commande **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
-----
1      Po1(U)      Eth      LACP      Eth1/3(P)  Eth1/4(P)
```

LACP KeepAlive Timer:

```
-----
Channel  PeerKeepAliveTimerFast
-----
1      Po1(U)      False
```

Cluster LACP Status:

```
-----
Channel  ClusterSpanned  ClusterDetach  ClusterUnitID  ClusterSysID
-----
1      Po1(U)      False          False          0              clust
```

Pour accéder à FXOS sur ASA, exécutez la commande **connect fxos admin**. Dans le cas d'un contexte multiple, exécutez la commande dans le contexte admin.

Collecter les fichiers de capture

Suivez les étapes de la section **Collecter les fichiers de capture internes du commutateur Secure Firewall 3100**.

Capturer l'analyse des fichiers

Utilisez une application de lecture de fichiers de capture de paquets pour ouvrir les fichiers de capture pour Ethernet1/1. Sélectionnez le premier paquet et vérifiez les points clés :

1. Seuls les paquets de requête d'écho ICMP sont capturés.
2. L'en-tête de paquet d'origine est sans étiquette VLAN.

Ouvrez les fichiers de capture pour les interfaces membres Portchannel1. Sélectionnez le premier paquet et vérifiez les points clés :

1. Seuls les paquets de requête d'écho ICMP sont capturés.
2. L'en-tête de paquet d'origine est sans étiquette VLAN.

Explication

Les captures du commutateur sont configurées sur les interfaces Ethernet1/1 ou Portchannel1.

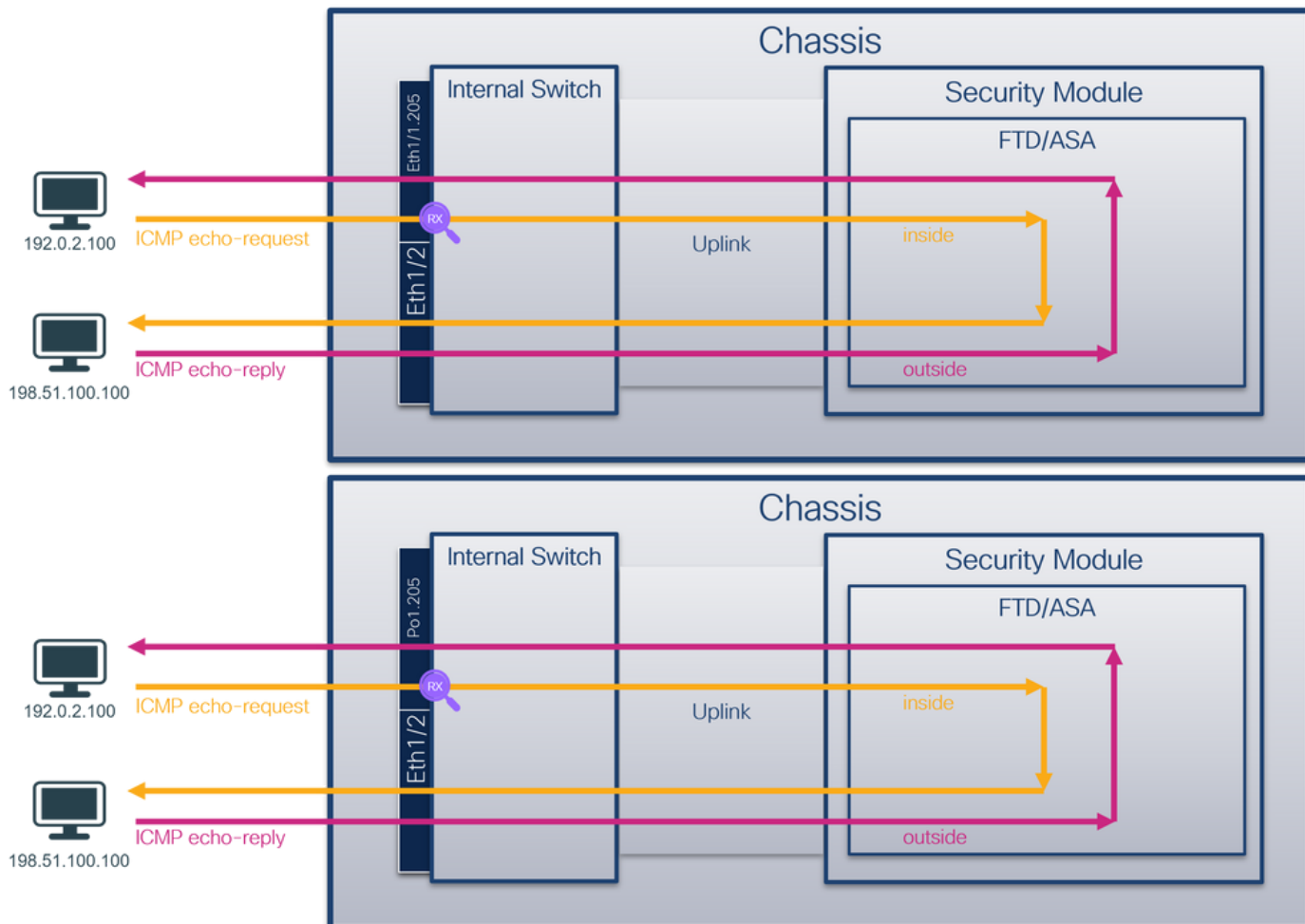
Ce tableau récapitule la tâche :

Tâche	Point de capture	Filtre interne	Direction	Trafic capturé
Configurer et vérifier une capture de paquets sur l'interface Ethernet1/1	Ethernet1/1	Aucune	Entrée uniquement	Requêtes d'écho ICMP de l'hôte 192.0.2.100 vers l'hôte 198.51.100.100
Configurez et vérifiez une capture de paquets sur l'interface Portchannel1 avec les interfaces membres Ethernet1/3 et Ethernet1/4	Ethernet1/3 Ethernet1/4	Aucune	Entrée uniquement	Requêtes d'écho ICMP de l'hôte 192.0.2.100 vers l'hôte 198.51.100.100

Capture de paquets sur une sous-interface d'une interface physique ou Port Channel

Utilisez la CLI FTD ou ASA pour configurer et vérifier une capture de paquets sur les sous-interfaces Ethernet1/1.205 ou Portchannel1.205. Les deux sous-interfaces portent le nom if **inside**.

Topologie, flux de paquets et points de capture



Configuration

Procédez comme suit sur l'interface de ligne de commande ASA ou FTD pour configurer une capture de paquets sur l'interface Ethernet1/1 ou Port-channel1 :

1. Vérifiez le nom si :

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

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

2. Créez une session de capture :

```
> capture capsw switch interface inside
```

3. Activez la session de capture :

```
> no capture capsw switch stop
```

Vérification

Vérifiez le nom de la session de capture, l'état administratif et opérationnel, le logement d'interface et l'identificateur. Assurez-vous que la valeur **Pcapsize** en octets augmente et que le nombre de paquets capturés est différent de zéro :

```
> show capture capsw detail
```

Packet Capture info

```
Name: capsw
Session: 1
Admin State: enabled
Oper State: up
Oper State Reason: Active
Config Success: yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0
```

Total Physical ports involved in Packet Capture: 1

Physical port:

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

Packet Capture Filter Info

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

Total Physical breakout ports involved in Packet Capture: 0

46 packets captured on disk using switch capture

Reading of capture file from disk is not supported

Dans ce cas, un filtre avec le VLAN externe **Ovlan=205** est créé et appliqué à l'interface.

Dans le cas de Port-channel1, la capture avec un filtre **Ovlan=205** est configurée sur toutes les

interfaces membres :

> **show capture capsw detail**

Packet Capture info

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

Total Physical ports involved in Packet Capture: 2

Physical port:

Slot Id: 1
Port Id: 4
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-4-0.pcap
Pcapsize: 23442
Filter: capsw-1-4

Packet Capture Filter Info

Name: capsw-1-4
Protocol: 0
Ivlan: 0
Ovlan: 205
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Physical port:

Slot Id: 1
Port Id: 3
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-3-0.pcap
Pcapsize: 5600
Filter: capsw-1-3

Packet Capture Filter Info

Name: capsw-1-3
Protocol: 0
Ivlan: 0
Ovlan: 205
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

49 packet captured on disk using switch capture

Reading of capture file from disk is not supported

Les interfaces membres port-channel peuvent être vérifiées dans l'interpréteur de commandes FXOS **local-mgmt** via la commande **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  
-----  
1    Po1(U)      Eth       LACP      Eth1/3(P)  Eth1/4(P)
```

```
LACP KeepAlive Timer:
```

```
-----  
Channel PeerKeepAliveTimerFast  
-----
```

```
1    Po1(U)      False
```

```
Cluster LACP Status:
```

```
-----  
Channel ClusterSpanned ClusterDetach ClusterUnitID ClusterSysID  
-----
```

```
1    Po1(U)      False      False      0          clust
```

Pour accéder à FXOS sur ASA, exécutez la commande **connect fxos admin**. Dans le cas du multi-contexte, exécutez cette commande dans le contexte admin.

Collecter les fichiers de capture

Suivez les étapes de la section **Collecter les fichiers de capture internes du commutateur Secure Firewall 3100**.

Capturer l'analyse des fichiers

Utilisez une application de lecture de fichiers de capture de paquets pour ouvrir les fichiers de capture pour Ethernet1/1.205. Sélectionnez le premier paquet et vérifiez les points clés :

1. Seuls les paquets de requête d'écho ICMP sont capturés.
2. L'en-tête de paquet d'origine a la balise VLAN 205.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-07 21:21:01.607187	192.0.2.100	198.51.100.100	ICMP	106	0x411f (16671)	64	Echo (ping) request id=0x0037, seq=1/256, ttl=64 (no res
2	2022-08-07 21:21:02.609418	192.0.2.100	198.51.100.100	ICMP	106	0x413a (16698)	64	Echo (ping) request id=0x0037, seq=2/512, ttl=64 (no res
3	2022-08-07 21:21:03.610671	192.0.2.100	198.51.100.100	ICMP	106	0x421a (16922)	64	Echo (ping) request id=0x0037, seq=3/768, ttl=64 (no res
4	2022-08-07 21:21:04.609160	192.0.2.100	198.51.100.100	ICMP	106	0x426c (17004)	64	Echo (ping) request id=0x0037, seq=4/1024, ttl=64 (no res
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 res
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 res
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 res
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 res
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 res
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 res
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 res
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 res
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 res
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 res
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 res
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 res
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 res
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 res

Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco_34:9a:14 (bc:e7:12:34:9a:14) 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 205 000. = Priority: Best Effort (default) (0) ...0 = DEI: Ineligible ... 0000 1100 1101 = ID: 205 Type: IPv4 (0x0800) Trailer: 55555555 Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100 Internet Control Message Protocol		0000 bc e7 12 34 9a 14 00 50 56 9d e8 be 81 00 00 cd ...4...P V..... 0010 08 00 45 00 00 54 41 1f 40 00 40 01 0c 8e c0 00 ...E:TA: @ @..... 0020 02 64 c6 33 64 64 08 00 06 67 00 37 00 01 b0 2c ...d:3dd...g:7... 0030 f0 62 00 00 00 00 8e fe 03 00 00 00 00 10 11 ...b..... 0040 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 ...!..... 0050 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 ..."%'()*+,-./01 0060 32 33 34 35 36 37 55 55 55 55 234567UU UU
---	--	--

Ouvrez les fichiers de capture pour les interfaces membres Portchannel1. Sélectionnez le premier paquet et vérifiez les points clés :

1. Seuls les paquets de requête d'écho ICMP sont capturés.
2. L'en-tête de paquet d'origine a la balise VLAN 205.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-07 21:21:01.607187	192.0.2.100	198.51.100.100	ICMP	106	0x411f (16671)	64	Echo (ping) request id=0x0037, seq=1/256, ttl=64 (no res
2	2022-08-07 21:21:02.609418	192.0.2.100	198.51.100.100	ICMP	106	0x413a (16698)	64	Echo (ping) request id=0x0037, seq=2/512, ttl=64 (no res
3	2022-08-07 21:21:03.610671	192.0.2.100	198.51.100.100	ICMP	106	0x421a (16922)	64	Echo (ping) request id=0x0037, seq=3/768, ttl=64 (no res
4	2022-08-07 21:21:04.609160	192.0.2.100	198.51.100.100	ICMP	106	0x426c (17004)	64	Echo (ping) request id=0x0037, seq=4/1024, ttl=64 (no res
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 res
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 res
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 res
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 res
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 res
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 res
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 res
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 res
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 res
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 res
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 res
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 res
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 res
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 res

Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco_34:9a:14 (bc:e7:12:34:9a:14) 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 205 000. = Priority: Best Effort (default) (0) ...0 = DEI: Ineligible ... 0000 1100 1101 = ID: 205 Type: IPv4 (0x0800) Trailer: 55555555 Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100 Internet Control Message Protocol		0000 bc e7 12 34 9a 14 00 50 56 9d e8 be 81 00 00 cd ...4...P V..... 0010 08 00 45 00 00 54 41 1f 40 00 40 01 0c 8e c0 00 ...E:TA: @ @..... 0020 02 64 c6 33 64 64 08 00 06 67 00 37 00 01 b0 2c ...d:3dd...g:7... 0030 f0 62 00 00 00 00 8e fe 03 00 00 00 00 10 11 ...b..... 0040 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 ...!..... 0050 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 ..."%'()*+,-./01 0060 32 33 34 35 36 37 55 55 55 55 234567UU UU
---	--	--

Explication

Les captures de commutateur sont configurées sur les sous-interfaces Ethernet1/1.205 ou Portchannel1.205 avec un filtre qui correspond au VLAN externe 205.

Ce tableau récapitule la tâche :

Tâche	Point de capture	Filtre interne	Direction	Trafic capturé
Configurer et vérifier une capture de paquets sur la sous-interface Ethernet1/1.205	Ethernet 1/1	VLAN externe 205	Entrée unique	Requêtes d'écho ICMP de l'hôte 192.0.2.100 vers l'hôte 198.51.100.100
Configurez et vérifiez une capture de paquets sur la sous-interface Portchannel1.205 avec les interfaces membres Ethernet1/3 et Ethernet1/4	Ethernet 1/3 Ethernet 1/4	VLAN externe 205	Entrée unique	Requêtes d'écho ICMP de l'hôte 192.0.2.100 vers l'hôte 198.51.100.100

Capture de paquets sur des interfaces internes

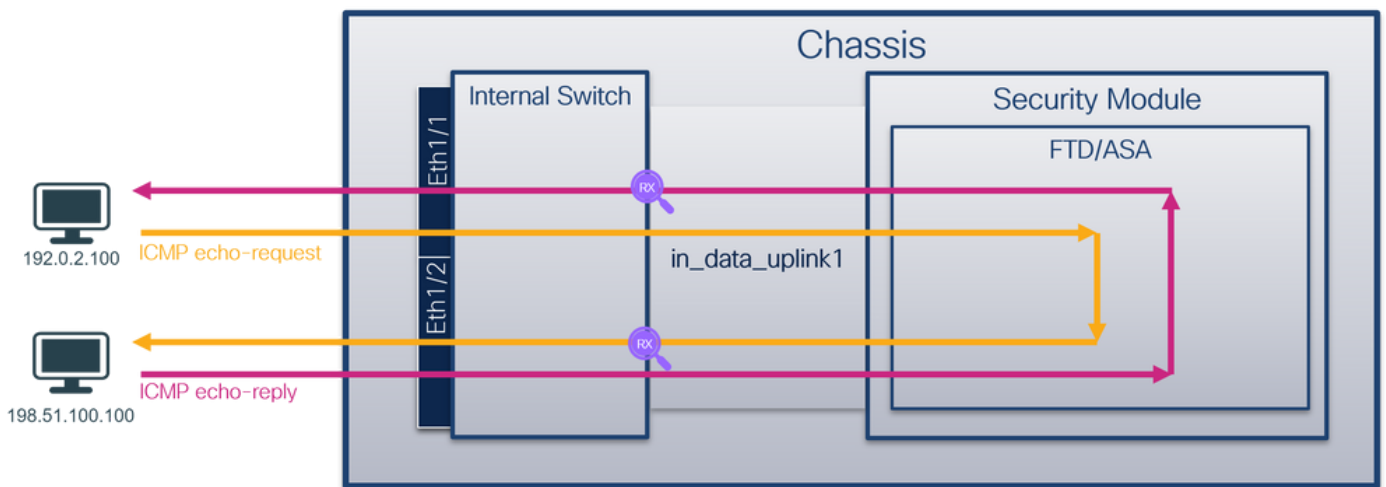
Le pare-feu sécurisé dispose de 2 interfaces internes :

- **in_data_uplink1** - connecte l'application au commutateur interne.
- **in_mgmt_uplink1** - fournit un chemin de paquets dédié pour les connexions de gestion, telles que SSH à l'interface de gestion, ou la connexion de gestion, également appelée sftunnel, entre le FMC et le FTD.

Tâche 1

Utilisez la CLI FTD ou ASA pour configurer et vérifier une capture de paquets sur l'interface de liaison ascendante **in_data_uplink1**.

Topologie, flux de paquets et points de capture



Configuration

Procédez comme suit sur l'interface de ligne de commande ASA ou FTD pour configurer une capture de paquets sur l'interface **in_data_uplink1** :

1. Créez une session de capture :

```
> capture capsw switch interface in_data_uplink1
```

2. Activez la session de capture :

```
> no capture capsw switch stop
```

Vérification

Vérifiez le nom de la session de capture, l'état administratif et opérationnel, le logement d'interface et l'identificateur. Assurez-vous que la valeur **Pcapsize** en octets augmente et que le nombre de paquets capturés est différent de zéro :

```
> show capture capsw detail
```

Packet Capture info

```
Name:          capsw
Session:       1
```

```

Admin State:      enabled
Oper State:      up
Oper State Reason: Active
Config Success:     yes
Config Fail Reason:
Append Flag:        overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code:         0
Drop Count:         0

```

Total Physical ports involved in Packet Capture: 1

Physical port:

```

Slot Id:        1
Port Id:        18
Pcapfile:           /mnt/disk0/packet-capture/sess-1-capsw-data-uplink1.pcap
Pcapsize:       7704
Filter:             capsw-1-18

```

Packet Capture Filter Info

```

Name:               capsw-1-18
Protocol:           0
Ivlan:              0
Ovlan:              0
Src Ip:             0.0.0.0
Dest Ip:            0.0.0.0
Src Ipv6:           ::
Dest Ipv6:          ::
Src MAC:            00:00:00:00:00:00
Dest MAC:           00:00:00:00:00:00
Src Port:           0
Dest Port:          0
Ethertype:          0

```

Total Physical breakout ports involved in Packet Capture: 0

66 packets captured on disk using switch capture

Reading of capture file from disk is not supported

Dans ce cas, une capture est créée sur l'interface avec un ID interne **18** qui est l'interface `in_data_uplink1` sur le pare-feu sécurisé 3130. La commande **show portmanager switch status** dans l'interpréteur de commandes FXOS `local-mgmt` affiche les ID d'interface :

```
> connect fxos
```

```

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

```

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

Pour accéder à FXOS sur ASA, exécutez la commande `connect fxos admin`. Dans le cas du multi-contexte, exécutez cette commande dans le contexte admin.

Collecter les fichiers de capture

Suivez les étapes de la section **Collecter les fichiers de capture internes du commutateur Secure Firewall 3100**.

Capter l'analyse des fichiers

Utilisez une application de lecture de fichiers de capture de paquets pour ouvrir les fichiers de capture pour l'interface `in_data_uplink1`. Vérifiez le point clé : dans ce cas, les paquets de requête et de réponse d'écho ICMP sont capturés. Il s'agit des paquets envoyés par l'application au commutateur interne.

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) request id=0x003a, seq=33/8448, ttl=64 (req)
2	2022-08-07 22:40:06.685615	198.51.100.100	192.0.2.100	ICMP	102	0x6cdc (27868)	64	Echo (ping) reply id=0x003a, seq=33/8448, ttl=64 (repl)
3	2022-08-07 22:40:07.684219	192.0.2.100	198.51.100.100	ICMP	102	0x4d08 (19944)	64	Echo (ping) request id=0x003a, seq=34/8704, ttl=64 (req)
4	2022-08-07 22:40:07.689300	198.51.100.100	192.0.2.100	ICMP	102	0x6db2 (28082)	64	Echo (ping) reply id=0x003a, seq=34/8704, ttl=64 (repl)
5	2022-08-07 22:40:08.685736	192.0.2.100	198.51.100.100	ICMP	102	0x4edc (20188)	64	Echo (ping) request id=0x003a, seq=35/8960, ttl=64 (req)
6	2022-08-07 22:40:08.690806	198.51.100.100	192.0.2.100	ICMP	102	0x6dbf (28095)	64	Echo (ping) reply id=0x003a, seq=35/8960, ttl=64 (repl)
7	2022-08-07 22:40:09.690737	192.0.2.100	198.51.100.100	ICMP	102	0x4f2d (20269)	64	Echo (ping) request id=0x003a, seq=36/9216, ttl=64 (req)
8	2022-08-07 22:40:09.690744	198.51.100.100	192.0.2.100	ICMP	102	0x6e80 (28288)	64	Echo (ping) reply id=0x003a, seq=36/9216, ttl=64 (repl)
9	2022-08-07 22:40:10.692266	192.0.2.100	198.51.100.100	ICMP	102	0x4fb1 (20401)	64	Echo (ping) request id=0x003a, seq=37/9472, ttl=64 (req)
10	2022-08-07 22:40:10.692272	198.51.100.100	192.0.2.100	ICMP	102	0x6ed5 (28373)	64	Echo (ping) reply id=0x003a, seq=37/9472, ttl=64 (repl)
11	2022-08-07 22:40:11.691159	192.0.2.100	198.51.100.100	ICMP	102	0x5008 (20488)	64	Echo (ping) request id=0x003a, seq=38/9728, ttl=64 (req)
12	2022-08-07 22:40:11.691166	198.51.100.100	192.0.2.100	ICMP	102	0x6f3b (28475)	64	Echo (ping) reply id=0x003a, seq=38/9728, ttl=64 (repl)
13	2022-08-07 22:40:12.692135	192.0.2.100	198.51.100.100	ICMP	102	0x50b8 (20664)	64	Echo (ping) request id=0x003a, seq=39/9984, ttl=64 (req)
14	2022-08-07 22:40:12.697209	198.51.100.100	192.0.2.100	ICMP	102	0x6fd7 (28631)	64	Echo (ping) reply id=0x003a, seq=39/9984, ttl=64 (repl)
15	2022-08-07 22:40:13.697320	192.0.2.100	198.51.100.100	ICMP	102	0x5184 (20868)	64	Echo (ping) request id=0x003a, seq=40/10240, ttl=64 (req)
16	2022-08-07 22:40:13.697327	198.51.100.100	192.0.2.100	ICMP	102	0x703e (28734)	64	Echo (ping) reply id=0x003a, seq=40/10240, ttl=64 (repl)
17	2022-08-07 22:40:14.698512	192.0.2.100	198.51.100.100	ICMP	102	0x51d8 (20952)	64	Echo (ping) request id=0x003a, seq=41/10496, ttl=64 (req)
18	2022-08-07 22:40:14.698518	198.51.100.100	192.0.2.100	ICMP	102	0x70dd (28893)	64	Echo (ping) reply id=0x003a, seq=41/10496, ttl=64 (repl)

```

> Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on 0
> Ethernet II, Src: Cisco_34:9a:15 (bc:e7:12:34:9a:15), Dst: VMware_9d:e7:50 (00:50:56:9d:e7:50)
> Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
> Internet Control Message Protocol
0000 00 50 56 9d e7 50 bc e7 12 34 9a 15 08 00 45 00  .PV.P..4...E.
0010 00 54 4d 93 40 00 40 01 00 1a c0 00 02 64 c6 33  .TM@.@....d3
0020 64 64 08 00 7f 15 00 00 00 21 3f f0 62 00 00 00  dd... .197.b...
0030 00 00 8b 1a 05 00 00 00 00 00 10 11 12 13 14 15  .
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  .
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
0060 36 37 55 55 55 55  .67UUUU

```

Explication

Lorsqu'une capture de commutateur sur l'interface de liaison ascendante est configurée, seuls les

paquets envoyés de l'application au commutateur interne sont capturés. Les paquets envoyés à l'application ne sont pas capturés.

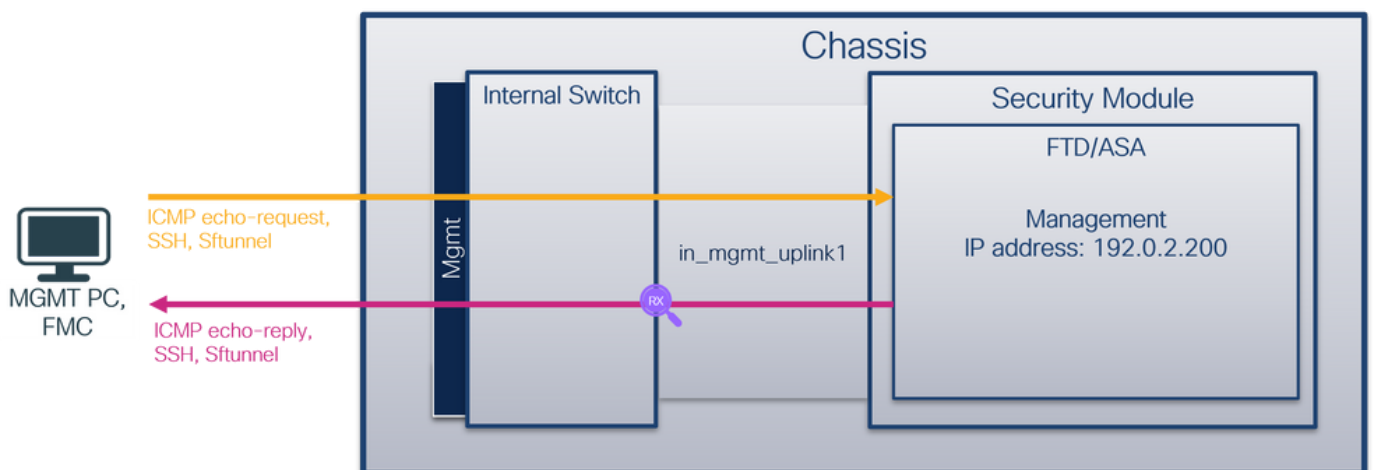
Ce tableau récapitule la tâche :

Tâche	Point de capture	Filtre interne	Direction	Trafic capturé
Configurez et vérifiez une capture de paquets sur l'interface de liaison ascendante in_data_uplink1	in_data_uplink1	Aucune	Entrée uniquement	Requêtes d'écho ICMP de l'hôte 192.0.2.100 vers l'hôte 198.51.100.100 Réponses d'écho ICMP de l'hôte 198.51.100.100 à l'hôte 192.0.2.100

Tâche 2

Utilisez l'interface de ligne de commande FTD ou ASA pour configurer et vérifier une capture de paquets sur l'interface de liaison ascendante in_mgmt_uplink1. Seuls les paquets des connexions du plan de gestion sont capturés.

Topologie, flux de paquets et points de capture



Configuration

Procédez comme suit sur l'interface de ligne de commande ASA ou FTD pour configurer une capture de paquets sur l'interface in_mgmt_uplink1 :

1. Créez une session de capture :

```
> capture capsw switch interface in_mgmt_uplink1
```

2. Activez la session de capture :

```
> no capture capsw switch stop
```

Vérification

Vérifiez le nom de la session de capture, l'état administratif et opérationnel, le logement d'interface et l'identificateur. Assurez-vous que la valeur **Pcapsize** en octets augmente et que le nombre de paquets capturés est différent de zéro :

> show capture capsw detail

Packet Capture info

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

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1
Port Id: 19
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-mgmt-uplink1.pcap
Pcapsize: 137248
Filter: capsw-1-19

Packet Capture Filter Info

Name: capsw-1-19
Protocol: 0
Ivlan: 0
Ovlan: 0
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

281 packets captured on disk using switch capture

Reading of capture file from disk is not supported

Dans ce cas, une capture est créée sur l'interface avec un ID interne 19 qui est l'interface **in_mgmt_uplink1** sur le pare-feu sécurisé 3130. La commande **show portmanager switch status** dans l'interpréteur de commandes FXOS **local-mgmt** affiche les ID d'interface :

> connect fxos

...

KSEC-FPR3100-1 connect local-mgmt

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

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

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

Pour accéder à FXOS sur ASA, exécutez la commande **connect fxos admin**. Dans le cas du multi-contexte, exécutez cette commande dans le contexte admin.

Collecter les fichiers de capture

Suivez les étapes de la section **Collecter les fichiers de capture internes du commutateur Secure Firewall 3100**.

Capturer l'analyse des fichiers

Utilisez une application de lecture de fichiers de capture de paquets pour ouvrir les fichiers de capture pour l'interface **in_mgmt_uplink1**. Vérifiez le point clé : dans ce cas, seuls les paquets de l'adresse IP de gestion 192.0.2.200 sont affichés. Exemples : paquets de réponse d'écho SSH, Sftunnel ou ICMP. Il s'agit des paquets envoyés de l'interface de gestion des applications au réseau via le commutateur interne.

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	0xbd9e (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	0xbd9f (48543)	64	Echo (ping) reply id=0x0001, seq=4541/48146, 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	0xbe48 (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	0xbe4e (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	0xbec1 (48833)	64	Echo (ping) reply id=0x0001, seq=4544/49169, ttl=64
217	2022-08-07 23:21:51.142842	192.0.2.200	192.0.2.101	TCP	70	0xbfd7 (47063)	64	39181 → 8305 [ACK] Seq=69004 Ack=967 Win=1384 Len=0 TSval
218	2022-08-07 23:21:52.030118	192.0.2.200	192.0.2.100	ICMP	78	0xbf02 (48898)	64	Echo (ping) reply id=0x0001, seq=4545/49425, ttl=64
219	2022-08-07 23:21:53.042744	192.0.2.200	192.0.2.100	ICMP	78	0xbf59 (48985)	64	Echo (ping) reply id=0x0001, seq=4546/49681, ttl=64
220	2022-08-07 23:21:53.073144	192.0.2.200	192.0.2.100	SSH	170	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	0xad35 (44341)	64	22 → 53249 [ACK] Seq=1025 Ack=881 Win=946 Len=0
222	2022-08-07 23:21:53.905480	192.0.2.200	192.0.2.101	TLSv1.2	747	0x4a9f (19103)	64	Application Data
223	2022-08-07 23:21:54.102899	192.0.2.200	192.0.2.100	ICMP	78	0xbf63 (48995)	64	Echo (ping) reply id=0x0001, seq=4547/49937, ttl=64
224	2022-08-07 23:21:54.903675	192.0.2.200	192.0.2.101	TCP	70	0x4aa0 (19104)	64	8305 → 58885 [ACK] Seq=23407 Ack=26424 Win=4116 Len=0 TSv

Explication

Lorsqu'une capture de commutateur sur l'interface de gestion de liaison ascendante est configurée, seuls les paquets entrants envoyés depuis l'interface de gestion d'application sont capturés. Les paquets destinés à l'interface de gestion des applications ne sont pas capturés.

Ce tableau récapitule la tâche :

Tâche	Point de capture	Filtre interne	Direction	Trafic capturé
Configurer et vérifier une capture de paquets sur l'interface de gestion de liaison ascendante	in_mgmt_uplink1	Aucune	Entrée uniquement (de l'interface de gestion au réseau en passant par le commutateur interne)	Réponses d'écho ICMP de l'adresse IP de gestion FTD 192.0.2.200 à l'hôte 192.0.2.100 Sftunnel de l'adresse IP de gestion FTD 192.0.2.200 à l'adresse IP FMC 192.0.2.100 SSH de l'adresse IP de gestion FTD 192.0.2.200 vers l'hôte 192.0.2.100

Filtres de capture de paquets

Les filtres de capture de paquets du commutateur interne sont configurés de la même manière que les captures du plan de données. Utilisez les options **ethernet-type** et **match** pour configurer les filtres.

Configuration

Suivez ces étapes sur l'interface de ligne de commande ASA ou FTD pour configurer une capture de paquets avec un filtre qui correspond aux trames ARP ou aux paquets ICMP de l'hôte 198.51.100.100 sur l'interface Ethernet1/1 :

1. Vérifiez le nom si :

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

2. Créez une session de capture pour ARP ou ICMP :

```
> capture capsw switch interface inside ethernet-type arp
> capture capsw switch interface inside match icmp 198.51.100.100
```

Vérification

Vérifiez le nom de la session de capture et le filtre. La valeur Ethertype est **2054** en décimal et **0x0806** en hexadécimal :

```
> show capture capsw detail
```

Packet Capture info

```
Name:          capsw
Session:         1
Admin State:     disabled
Oper State:      down
Oper State Reason: Session_Admin_Shut
Config Success:  yes
Config Fail Reason:
Append Flag:     overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code:      0
Drop Count:      0
```

Total Physical ports involved in Packet Capture: 1

Physical port:

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

Packet Capture Filter Info

```
Name:          capsw-1-1
Protocol:        0
Ivlan:          0
Ovlan:          0
Src Ip:          0.0.0.0
Dest Ip:         0.0.0.0
Src Ipv6:        ::
Dest Ipv6:       ::
Src MAC:         00:00:00:00:00:00
Dest MAC:        00:00:00:00:00:00
Src Port:        0
Dest Port:       0
Ethertype:    2054
```

Total Physical breakout ports involved in Packet Capture: 0

0 packet captured on disk using switch capture

Reading of capture file from disk is not supported

Il s'agit de la vérification du filtre pour ICMP. Le protocole IP 1 est ICMP :

> **show capture capsw detail**

Packet Capture info

Name: capsw
Session: 1
Admin State: disabled
Oper State: down
Oper State Reason: Session_Admin_Shut
Config Success: yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0

Total Physical ports involved in Packet Capture: 1

Physical port:

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

Packet Capture Filter Info

Name: capsw-1-1
Protocol: 1
Ivlan: 0
Ovlan: 0
Src Ip: 198.51.100.100
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

0 packets captured on disk using switch capture

Reading of capture file from disk is not supported

Collecter les fichiers de capture internes du commutateur Secure Firewall 3100

Utilisez l'interface CLI ASA ou FTD pour collecter les fichiers de capture internes du commutateur. Sur FTD, le fichier de capture peut également être exporté via la commande CLI **copy** vers des destinations accessibles via les interfaces de données ou de diagnostic.

Vous pouvez également copier le fichier dans **/ngfw/var/common** en mode expert et le télécharger depuis FMC via l'option **File Download**.

Dans le cas des interfaces port-channel, assurez-vous de collecter les fichiers de capture de

paquets à partir de toutes les interfaces membres.

ASA

Procédez comme suit pour collecter les fichiers de capture de commutateur interne sur l'interface de ligne de commande ASA :

1. Arrêtez la capture :

```
asa# capture capsw switch stop
```

2. Vérifiez que la session de capture est arrêtée et notez le nom du fichier de capture.

```
asa# show capture capsw detail
```

Packet Capture info

```
Name:                capsw  
Session:                1  
Admin State:        disabled  
Oper State:         down  
Oper State Reason: Session_Admin_Shut  
Config Success:        yes  
Config Fail Reason:  
Append Flag:           overwrite  
Session Mem Usage:     256  
Session Pcap Snap Len: 1518  
Error Code:            0  
Drop Count:           0
```

Total Physical ports involved in Packet Capture: 1

Physical port:

```
Slot Id:                1  
Port Id:                1  
Pcapfile:           /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap  
Pcapsize:              139826  
Filter:                 capsw-1-1
```

Packet Capture Filter Info

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

Total Physical breakout ports involved in Packet Capture: 0

886 packets captured on disk using switch capture

Reading of capture file from disk is not supported

3. Utilisez la commande CLI **copy** pour exporter le fichier vers des destinations distantes :


```
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

Procédez comme suit pour collecter les fichiers de capture de commutateur interne sur l'interface de ligne de commande FTD et les copier sur des serveurs accessibles via des interfaces de données ou de diagnostic :

1. Accédez à la CLI de diagnostic :

```
> 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. Arrêtez la capture :

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

3. Vérifiez que la session de capture est arrêtée et notez le nom du fichier de capture :

```
firepower# show capture capsw detail
Packet Capture info
Name:          capsw
Session:         1
Admin State:  disabled
Oper State:   down
Oper State Reason: Session_Admin_Shut
Config Success:  yes
Config Fail Reason:
Append Flag:     overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code:      0
Drop Count:      0

Total Physical ports involved in Packet Capture: 1
Physical port:
Slot Id:         1
Port Id:         1
Pcapfile:     /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
```

```
Pcapsize:      139826
Filter:        capsw-1-1
```

Packet Capture Filter Info

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

Total Physical breakout ports involved in Packet Capture: 0

886 packets captured on disk using switch capture

Reading of capture file from disk is not supported

4. Utilisez la commande CLI **copy** pour exporter le fichier vers des destinations distantes.

```
firepower# copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap ?
```

```
cluster:      Copy to cluster: file system
disk0:        Copy to disk0: file system
disk1:        Copy to disk1: file system
flash:        Copy to flash: file system
ftp:          Copy to ftp: file system
running-config Update (merge with) current system configuration
scp:          Copy to scp: file system
smb:          Copy to smb: file system
startup-config Copy to startup configuration
system:       Copy to system: file system
tftp:         Copy to tftp: file system
```

```
firepower# copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap tftp://198.51.100.10/
```

```
Source filename [/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap]?
```

```
Destination filename [sess-1-capsw-ethernet-1-1-0.pcap]?
```

```
Copy in progress...C
```

```
139826 bytes copied in 0.532 secs
```

Procédez comme suit pour collecter des fichiers de capture à partir de FMC via l'option

Téléchargement de fichier :

1. Arrêtez la capture :

```
> capture capsw switch stop
```

2. Vérifiez que la session de capture est arrêtée et notez le nom de fichier et le chemin d'accès complet du fichier de capture :

```
> show capture capsw detail
```

```
Packet Capture info
```

```
Name:          capsw
Session:      1
Admin State:  disabled
Oper State:   down
```

Oper State Reason: Session_Admin_Shut

Config Success: yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1
Port Id: 1

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

Pcapsize: 139826

Filter: capsw-1-1

Packet Capture Filter Info

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

Total Physical breakout ports involved in Packet Capture: 0

886 packets captured on disk using switch capture

Reading of capture file from disk is not supported

3. Passez en mode expert et passez en mode racine :

> **expert**

admin@firepower:~\$ **sudo su**

root@firepower:/home/admin

4. Copiez le fichier de capture dans /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 -l /ngfw/var/common/sess***

-rwxr-xr-x 1 root admin 139826 Aug 7 20:14 **/ngfw/var/common/sess-1-capsw-ethernet-1-1-0.pcap**

-rwxr-xr-x 1 root admin 24 Aug 6 21:58 /ngfw/var/common/sess-1-capsw-ethernet-1-3-0.pcap

5. Sur FMC, choisissez Devices > File Download :

The screenshot shows the Firewall Management Center (FMC) interface. The 'Devices' menu is open, and the 'File Download' option is highlighted. The dashboard displays several widgets, including a line chart for 'Unique Applications over Time' and a bar chart for 'Traffic by Application Risk'. The 'File Download' option is highlighted in the 'Troubleshoot' sub-menu.

6. Choisissez le FTD, indiquez le nom du fichier de capture, puis cliquez sur **Download**:

The screenshot shows the 'File Download' page in the FMC. The 'Device' dropdown is set to 'FPR3100-1' and the 'File' field contains 'sess-1-capsw-ethernet-1-1-0.pcap'. The 'Download' button is highlighted.

Recommandations, limites et meilleures pratiques pour la capture de paquets de commutateur interne

Directives et limites :

- Plusieurs sessions de configuration de capture de commutateur sont prises en charge, mais une seule session de capture de commutateur peut être active à la fois. Une tentative d'activation de 2 sessions de capture ou plus génère l'erreur « **ERROR: Échec de l'activation de la session, car la limite maximale de 1 session active de capture de paquets a été atteinte** ».
- Impossible de supprimer une capture de commutateur active.
- Impossible de lire les captures de commutateur sur l'application. L'utilisateur doit exporter les fichiers.
- Certaines options de capture de plan de données, telles que **dump**, **decode**, **packet-number**, **trace** et autres, ne sont pas prises en charge pour les captures de commutateur.
- Dans le cas de l'ASA multicontexte, les captures du commutateur sur les interfaces de données sont configurées dans des contextes utilisateur. Les captures du commutateur sur les interfaces `in_data_uplink1` et `in_mgmt_uplink1` sont prises en charge uniquement dans le contexte admin.

Voici la liste des meilleures pratiques basées sur l'utilisation de la capture de paquets dans les cas TAC :

- Soyez conscient des directives et des limites.
- Utiliser des filtres de capture.
- Tenez compte de l'impact de la fonction NAT sur les adresses IP des paquets lorsqu'un filtre de capture est configuré.
- Augmentez ou diminuez la **longueur de paquet** qui spécifie la taille de trame, au cas où elle serait différente de la valeur par défaut de 1 518 octets. Une taille plus courte entraîne une augmentation du nombre de paquets capturés et vice versa.
- Ajustez la taille de la **mémoire tampon** selon vos besoins.
- Soyez conscient du nombre de **abandons** dans le résultat de la commande **show cap <cap_name>detail**. Une fois la taille limite de la mémoire tampon atteinte, le compteur d'abandon augmente.

Informations connexes

- [Guides de configuration du gestionnaire de châssis Firepower 4100/9300 et de l'interface de ligne de commande FXOS](#)
- [Guide de démarrage de Cisco Secure Firewall 3100](#)
- [Référence des commandes FXOS Cisco Firepower 4100/9300](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.