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

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
  - Présentation générale de l'architecture du 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 du pare-feu sécurisé 1200/3100/4200
  - 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
  - Capture de paquets sur les interfaces de port de commutation L2
  - Capture de paquets sur un châssis à instances multiples
  - Collecter les fichiers de capture internes du commutateur Secure Firewall
  - 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, et le pare-feu sécurisé capture le commutateur interne.

Conditions préalables

Exigences

Connaissances de base sur les produits, analyse de capture.

Composants utilisés

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.

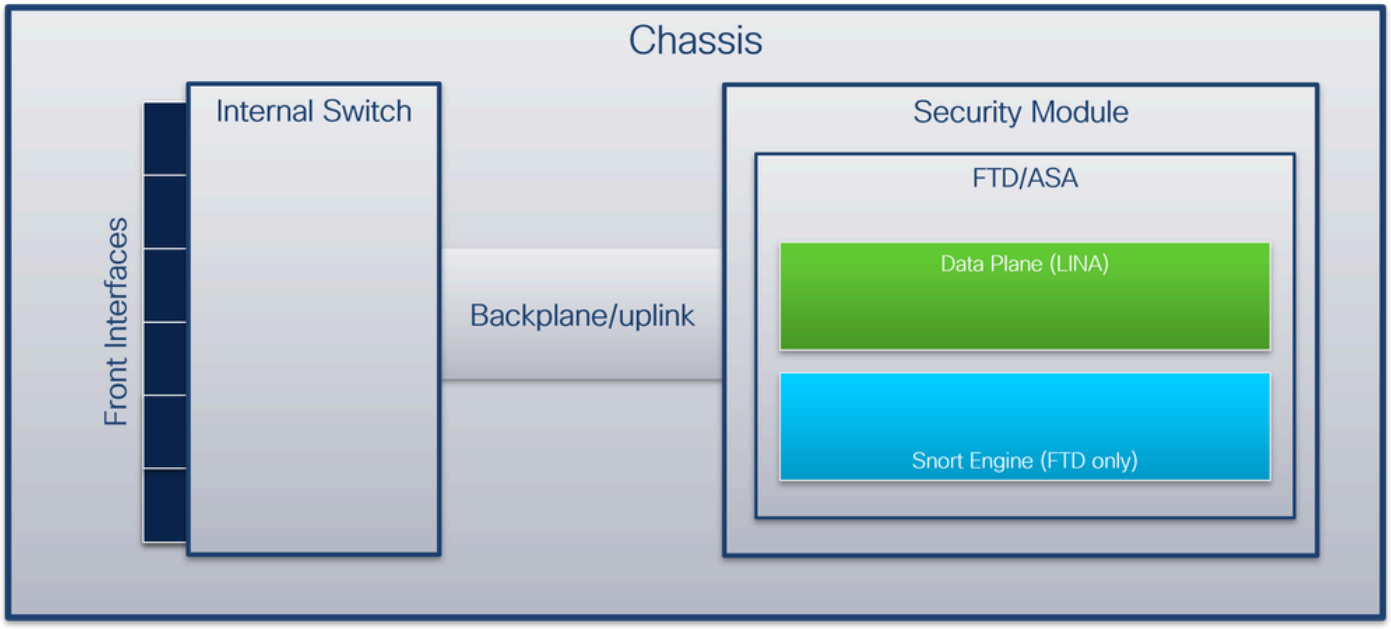
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Pare-feu sécurisé 1200, 3100, 4200
- Firepower 4100/9300
- Système d'exploitation extensible sécurisé Cisco (FXOS) 2.12.0.x, 2.17(0.x)
- Cisco Secure Firewall Threat Defense (FTD) 7.2.0.x, 7.4.1-172, 7.7.0.89
- Cisco Secure Firewall Management Center (FMC) 7.2.0.x, 7.4.1-172, 7.7.0.89
- Appareil de sécurité adaptatif (ASA) 9.18(1)x, 9.20(x)
- Wireshark 3.6.7 (https://www.wireshark.org/download.html)

Informations générales

Présentation générale de l'architecture du système

Du point de vue du flux de paquets, l'architecture des pare-feu Firepower 4100/9300 et Secure Firewall 1200/3100/4200 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.
- Liaison ascendante de gestion - interface interne exclusive à Secure Firewall 3100/4200 qui fournit le chemin du trafic de gestion entre le commutateur interne et l'application.
- Interface de gestion : interface physique du châssis.
- Interfaces de données : interfaces attribuées à l'application utilisée pour transférer le trafic.

Dans le cas du pare-feu sécurisé 3100/4200, les interfaces de données, de gestion et de liaison ascendante sont mappées à des ports de commutation internes spécifiques.

Remarque : Pour le pare-feu sécurisé 1200, les interfaces de données et de liaison ascendante sont mappées à des ports de commutation internes spécifiques. Cependant, le port de gestion est une interface hors bande et ne fait pas partie du commutateur interne.

Le mappage peut être vérifié dans le résultat de la commande shell de commande FXOS local-mgmt show portmanager switch status.

Dans cet exemple, le port 0/17 est l'interface de gestion du châssis, le port 0/18 est l'interface fond de panier/liaison ascendante et le port 0/19 est l'interface de gestion de liaison ascendante.

```
firepower-3140#
```

connect local-mgmt

```
Warning: network service is not available when entering 'connect local-mgmt'
firepower-3140(local-mgmt)#
```

show portmanager switch status

```
Dev/Port     Mode     Link   Speed  Duplex    Loopback      Autoneg      FEC         Link Scan   Port Mana
---------  --------  -----  -----  ------  -------------  ---------  ----------   -----------  --------
0/1          SGMII    Up     1G     Full        None        No         None          None       Link-Up
0/2          SGMII    Up     1G     Full        None        No         None          None       Link-Up
0/3          SGMII   Down    1G     Full         n/a        No         None          None      Force-Li
0/4          SGMII   Down    1G     Full         n/a        No         None          None      Force-Li
0/5          SGMII   Down    1G     Full         n/a        No         None          None      Force-Li
0/6          SGMII   Down    1G     Full         n/a        No         None          None      Force-Li
0/7          SGMII   Down    1G     Full         n/a        No         None          None      Force-Li
0/8          SGMII   Down    1G     Full         n/a        No         None          None      Force-Li
0/9          SR_LR   Down    25G    Full         n/a        No         None          None      Force-Li
0/10         SR_LR   Down    25G    Full         n/a        No         None          None      Force-Li
0/11       1000_BaseXDown     1G     Full         n/a        No         None          None      Force-Li
0/12       1000_BaseXDown     1G     Full         n/a        No         None          None      Force-Li
0/13       1000_BaseXDown     1G     Full         n/a        No         None          None      Force-Li
0/14       1000_BaseXDown     1G     Full         n/a        No         None          None      Force-Li
0/15       1000_BaseXDown     1G     Full         n/a        No         None          None      Force-Li
0/16       1000_BaseXDown     1G     Full         n/a        No         None          None      Force-Li
0/17       1000_BaseX Up      1G     Full        None        No         None          None       Link-Up
0/18          KR2     Up     50G
Full        None         No          None          None       Link-Up
0/19          KR      Up     25G
 Full        None         No          None          None       Link-Up
0/20          KR      Up     25G    Full        None        No         None          None       Link-Up
```

Ce tableau présente les interfaces de fond de panier sur Firepower 4100/9300 et les interfaces de liaison ascendante de données sur Secure Firewall 1200/3100/4200 :

Plateforme	Nombre de modules de sécurité pris en charge	Interface fond de panier/liaison ascendante	Port de commutation interne mappé pour fond de panier/liaison ascendante	Interface d'application mappée
Firepower 4100 (sauf Firepower 4110/4112)	1	SM1 : Ethernet1/9 Ethernet1/10	S/O	Internal-Data0/0 Données internes0/1

Firepower 4110/4112	1	Ethernet1/9	S/O	Internal-Data0/0 Données internes0/1
Firepower 9300	3	SM1 : Ethernet1/9 Ethernet1/10 SM2 : Ethernet1/11 Ethernet1/12 SM3 : Ethernet1/13 Ethernet1/14	S/O	Internal-Data0/0 Données internes0/1 Internal-Data0/0 Données internes0/1 Internal-Data0/0 Données internes0/1
Pare-feu sécurisé 1210	1	in_data_uplink1	Port 9	Données internes0/1
Pare-feu sécurisé 1220	1	in_data_uplink1 in_data_uplink2 in_data_uplink3	Port 11 Port 12 Port 13	Données internes0/1 Internal-Data0/2 Données internes0/3
Pare-feu sécurisé 1230 Pare-feu sécurisé 1240	1	in_data_uplink1 in_data_uplink2 in_data_uplink3	Port 13 Port 14 Port 15	Données internes0/1 Internal-Data0/2 Données internes0/3
Pare-feu sécurisé 1250	1	in_data_uplink1	Port 13	Données internes0/1
Pare-feu sécurisé 3100	1	in_data_uplink1	Port 18	Données internes0/1
Pare-feu	1	in_data_uplink1	Port 11	Données internes0/1

sécurisé 4200		in_data_uplink2 (seulement 4245)	Port 12 (4245 uniquement)	Internal-Data0/2 (seulement 4245)

Ce tableau présente les interfaces de gestion et les interfaces de gestion de liaison ascendante sur Secure Firewall 1200/3100/4200 :

Plateforme	Interface de gestion du châssis	Port de commutation interne mappé pour l'interface de gestion du châssis	Port de commutation interne mappé pour l'interface de gestion de liaison ascendante	Interface d'application mappée
Pare-feu sécurisé 1210	Gestion1	Non mappé à un port de commutateur interne	S/O	S/O
Pare-feu sécurisé 1200 (sauf 1210)	Gestion1	Non mappé à un port de commutateur interne	S/O	S/O
Pare-feu sécurisé 3100	Gestion1	Port 0/17	Port 0/19	in_mgmt_uplink1
Pare-feu sécurisé 4200	Gestion1 Gestion2	Port 0/9 Port 0/10	Port 0/13 Port 0/14	in_mgmt_uplink1 in_mgmt_uplink2

Dans le cas de Firepower 4100/9300 avec 2 interfaces de fond de panier par module ou de Secure Firewall 4245 avec 2 interfaces de liaison ascendante de données, 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 - noms des interfaces de fond de panier ou de liaison ascendante dans les applications, telles que FTD ou ASA.

En outre, le Secure Firewall 1200 intègre une nouvelle architecture avec trois interfaces de liaison ascendante de données. Le commutateur interne et l'application effectuent l'équilibrage de charge sur ces interfaces.

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

<#root>

>

show interface detail | grep Interface

```
Interface Internal-Control0/0 "ha_ctl_nlp_int_tap", is up, line protocol is up
  Control Point Interface States:
        Interface number is 6
        Interface config status is active
        Interface state is active
Interface Internal-Data0/0 "", is up, line protocol is up
  Control Point Interface States:
        Interface number is 2
        Interface config status is active
        Interface state is active
Interface Internal-Data0/1 "", is up, line protocol is up
  Control Point Interface States:
        Interface number is 3
        Interface config status is active
        Interface state is active
Interface Internal-Data0/2 "nlp_int_tap", is up, line protocol is up
  Control Point Interface States:
        Interface number is 4
        Interface config status is active
        Interface state is active
Interface Internal-Data0/3 "ccl_ha_nlp_int_tap", is up, line protocol is up
  Control Point Interface States:
        Interface number is 5
        Interface config status is active
        Interface state is active
Interface Internal-Data0/4 "cmi_mgmt_int_tap", is up, line protocol is up
  Control Point Interface States:
        Interface number is 7
        Interface config status is active
        Interface state is active
Interface Port-channel6.666 "", is up, line protocol is up
Interface Ethernet1/1 "diagnostic", is up, line protocol is up
  Control Point Interface States:
        Interface number is 8
        Interface config status is active
        Interface state is active
```

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 VN).

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 :

```
<#root>

firepower#

connect fxos


…
firepower(fxos)#

show run int e1/2


!Command: show running-config interface Ethernet1/2
!Time: Tue Jul 12 22:32:11 2022

version 5.0(3)N2(4.120)

interface Ethernet1/2
  description U: Uplink
  no lldp transmit
  no lldp receive
  no cdp enable
  switchport mode dot1q-tunnel


switchport trunk native vlan 102


  speed 1000
  duplex full
  udld disable
  no shutdown
```

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 1200/3100/4200

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

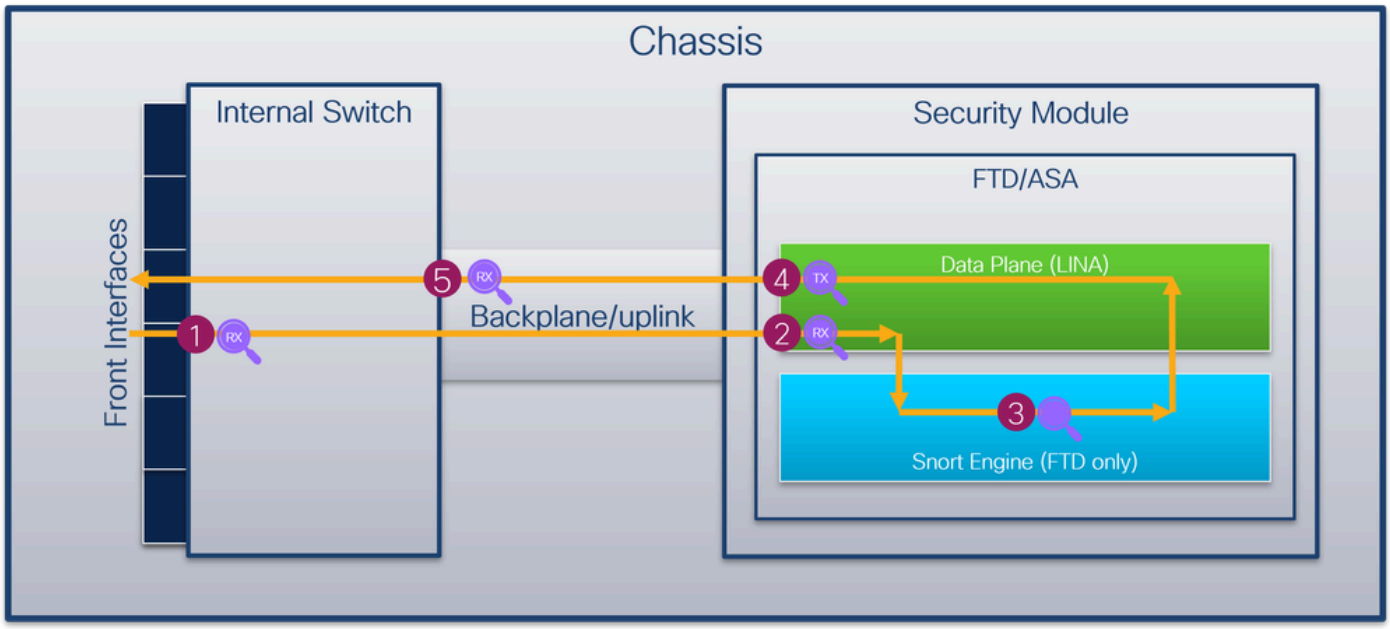
L'étiquette VLAN du port est partagée avec l'application. L'application insère les balises VLAN d'interface de sortie respectives dans chaque paquet. Lorsqu'un paquet provenant de l'application est reçu par le commutateur interne sur l'interface de liaison ascendante, le commutateur lit l'étiquette VLAN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

Firepower 4100/9300 et Secure Firewall 3100

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 au sein du châssis et de l'application :



Les points de capture sont les suivants :

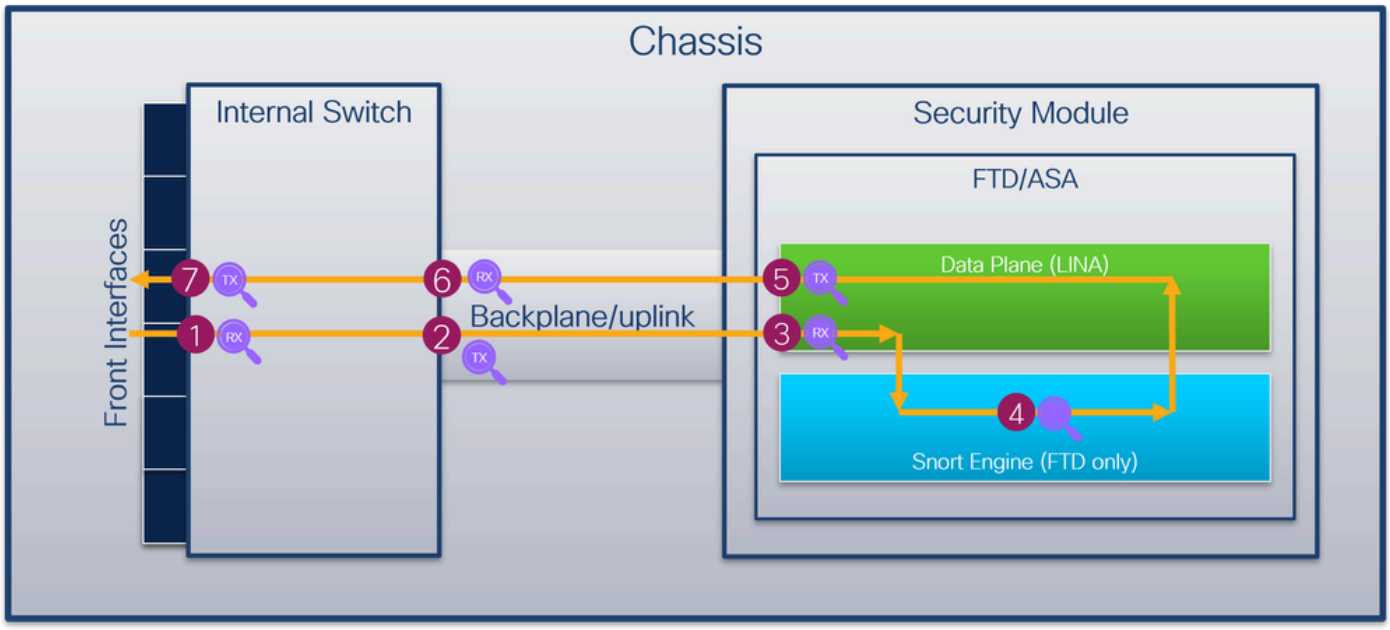
1. Point de capture d'entrée de l'interface avant du commutateur interne. Une interface avant est une interface connectée aux périphériques homologues, tels que les commutateurs.
2. Point de capture d'entrée interface du plan de données
3. Point de capture Snort
4. Point de capture de sortie d'interface 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. C'est-à-dire 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.

Pare-feu sécurisé 1200/4200

Les pare-feu Secure Firewall 1200/4200 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 au sein du châssis et de 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 de sortie d'interface de fond de panier du commutateur interne.
3. Point de capture d'entrée interface du plan de données
4. Point de capture Snort
5. Point de capture de sortie d'interface du plan de données
6. 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.
7. Point de capture de sortie de l'interface avant du commutateur interne.

Le commutateur interne prend éventuellement en charge les captures bidirectionnelles (entrées et sorties). Par défaut, le commutateur interne capture les paquets dans la direction d'entrée.

Remarque : L'interface de gestion du pare-feu Secure Firewall 1200 est une interface hors bande qui ne fait pas partie du commutateur interne. Pour cette raison, la capture du trafic de l'interface de gestion au niveau du commutateur n'est pas prise en charge sur le pare-feu sécurisé 1200.

Configuration et vérification sur Firepower 4100/9300

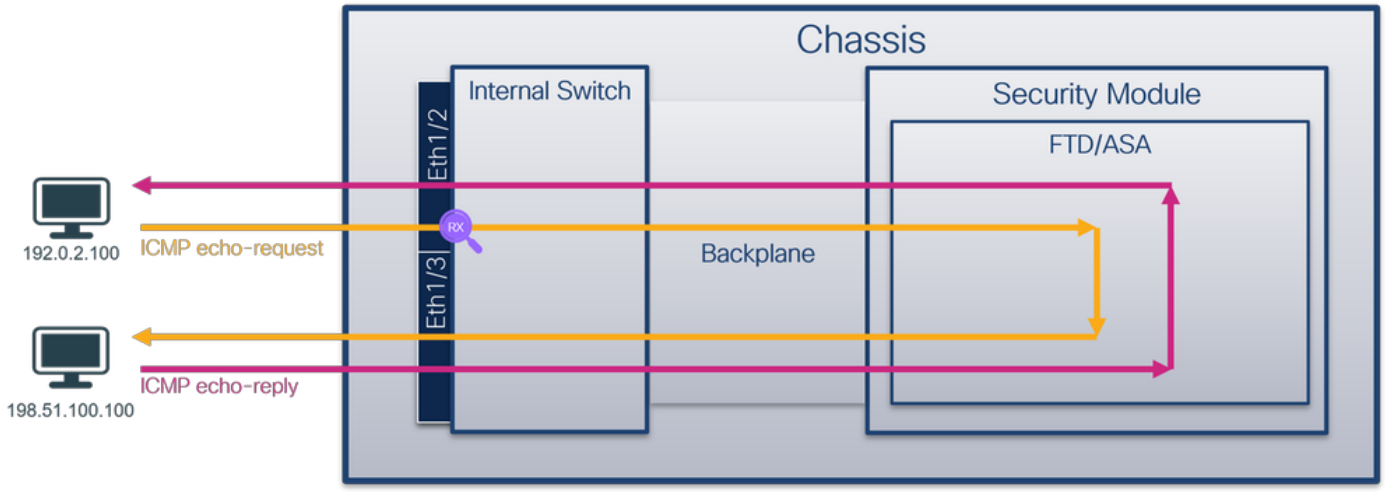
Les captures internes du commutateur Firepower 4100/9300 peuvent être configurées dans Outils > Capture de paquets sur FCM ou dans la capture de paquets de portée dans l'interface de ligne de commande FXOS. Pour la description des options de capture de paquets, référez-vous au Guide de configuration 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, assurez-vous de sélectionner toutes les interfaces membres physiques.

Topologie, flux de paquets et points de capture

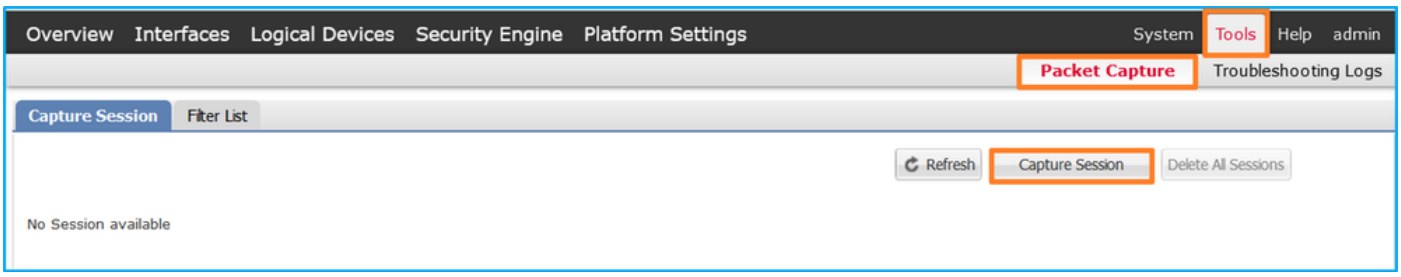


Configuration

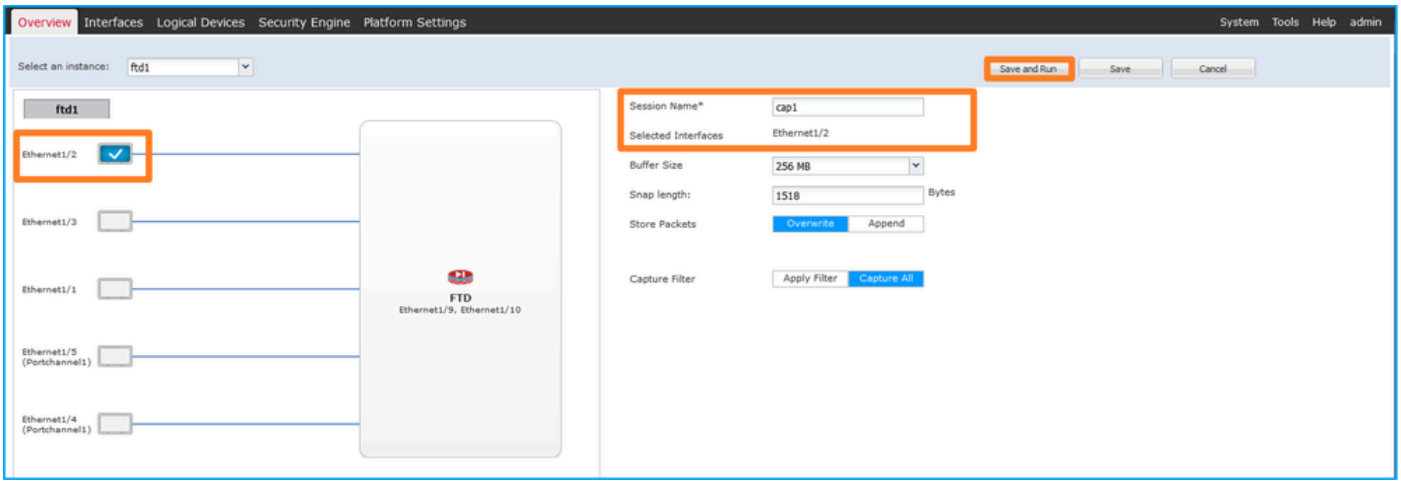
FCM

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

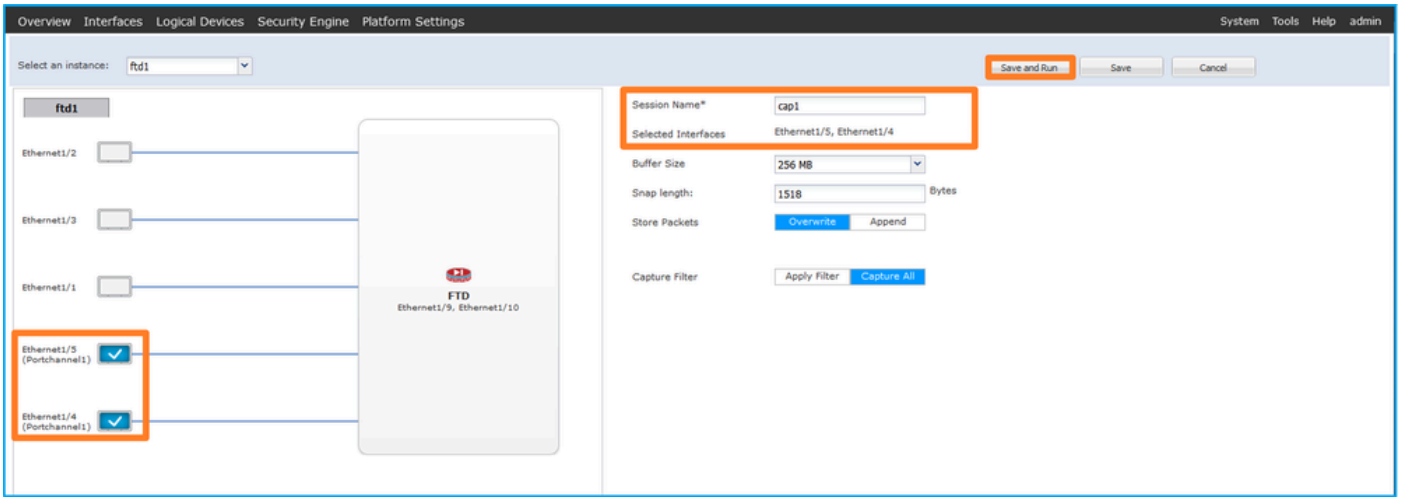
1. Utilisez Outils > Capture de paquets > Session de capture pour créer une nouvelle session de capture :



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 la 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 :

```
<#root>

firepower#

scope ssa


firepower /ssa #

show app-instance
```

```
App Name   Identifier Slot ID    Admin State Oper State       Running Version Startup Version Deploy Ty
---------- ---------- ---------- ----------- --------------- -------------- -------------- ---------

ftd        ftd1

       1          Enabled     Online          7.2.0.82        7.2.0.82        Native      No
```

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

```
<#root>

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 :

```
<#root>

firepower#

scope packet-capture


firepower /packet-capture #

create session cap1


firepower /packet-capture/session* #

create phy-port Eth1/2


firepower /packet-capture/session/phy-port* #

set app ftd
```

```
firepower /packet-capture/session/phy-port* #
set app-identifier ftd1

firepower /packet-capture/session/phy-port* #
up

firepower /packet-capture/session* #
enable

firepower /packet-capture/session* #
commit

firepower /packet-capture/session #
```

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

<#root>

```
firepower#
scope packet-capture

firepower /packet-capture #
create session cap1

firepower /packet-capture/session* #
create phy-port Eth1/4

firepower /packet-capture/session/phy-port* #
set app ftd

firepower /packet-capture/session/phy-port* #
set app-identifier ftd1

firepower /packet-capture/session/phy-port* #
up

firepower /packet-capture/session* #
create phy-port Eth1/5

firepower /packet-capture/session/phy-port* #
```

```
set app ftd

firepower /packet-capture/session/phy-port* #
set app-identifier ftd1

firepower /packet-capture/session/phy-port* #
up

firepower /packet-capture/session* #
enable

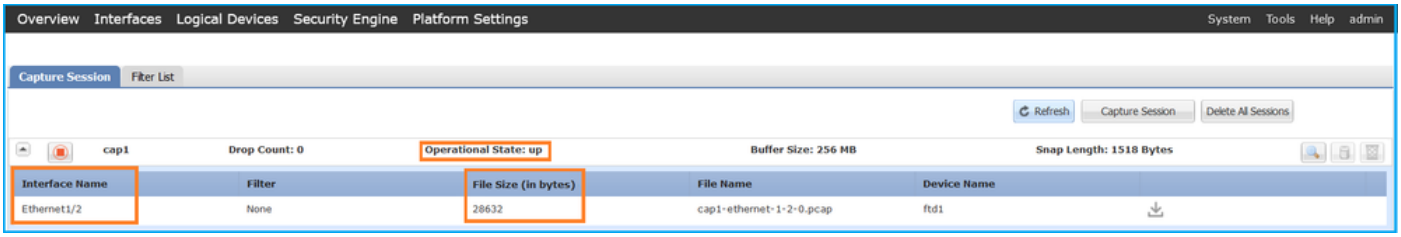
firepower /packet-capture/session* #
commit

firepower /packet-capture/session #
```

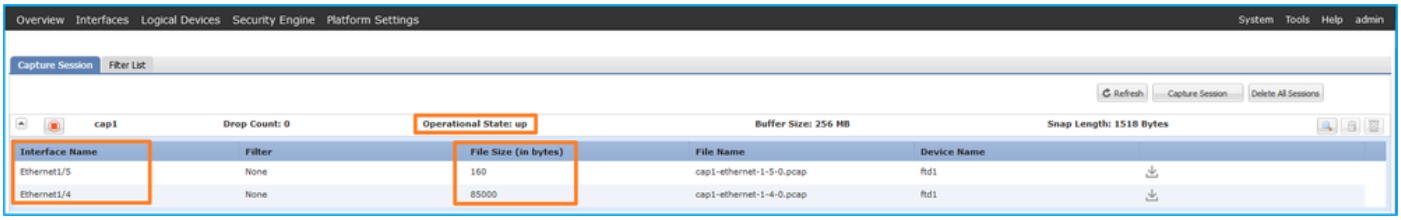
Vérification

FCM

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



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



CLI FXOS

Vérifiez les détails de capture dans la portée packet-capture :

```
<#root>

firepower#
scope packet-capture
```

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


Traffic Monitoring Session:
    Packet Capture Session Name: cap1

    Session: 1
    Admin State: Enabled

    Oper State: Up

    Oper State Reason: Active

    Config Success: Yes
    Config Fail Reason:
    Append Flag: Overwrite
    Session Mem Usage: 256  MB
    Session Pcap Snap Len: 1518  Bytes
    Error Code: 0
    Drop Count: 0

Physical ports involved in Packet Capture:
    Slot Id: 1

    Port Id: 2

    Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap

    Pcapsize: 75136  bytes

    Filter:
    Sub Interface: 0
    Application Instance Identifier: ftd1

    Application Name: ftd
```

Port-channel 1 avec interfaces membres Ethernet1/4 et Ethernet1/5 :

```
<#root>
firepower#
```

scope packet-capture

firepower /packet-capture #

show session cap1

Traffic Monitoring Session:

Packet Capture Session Name: cap1

Session: 1

Admin State: Enabled

Oper State: Up

Oper State Reason: Active

Config Success: Yes
Config Fail Reason:
Append Flag: Overwrite
Session Mem Usage: 256 MB
Session Pcap Snap Len: 1518 Bytes
Error Code: 0
Drop Count: 0

Physical ports involved in Packet Capture:

Slot Id: 1

Port Id: 4

Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-4-0.pcap

Pcapsize: 310276 bytes

Filter:
Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

Slot Id: 1

```
Port Id: 5


Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-5-0.pcap


Pcapsize: 160  bytes


Filter:
Sub Interface: 0
Application Instance Identifier: ftd1


Application Name: ftd
```

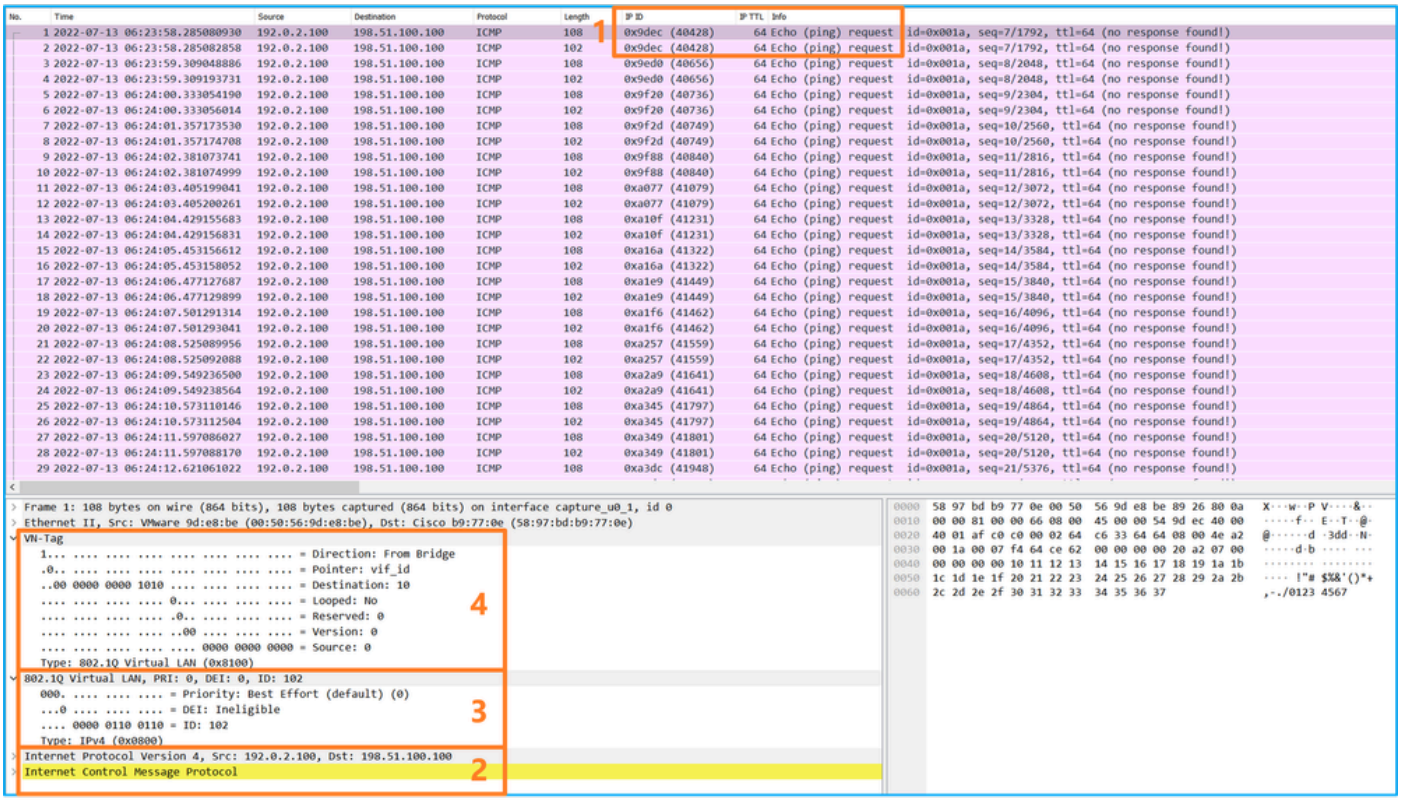
Collecter les fichiers de capture

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

Capturer l'analyse des fichiers

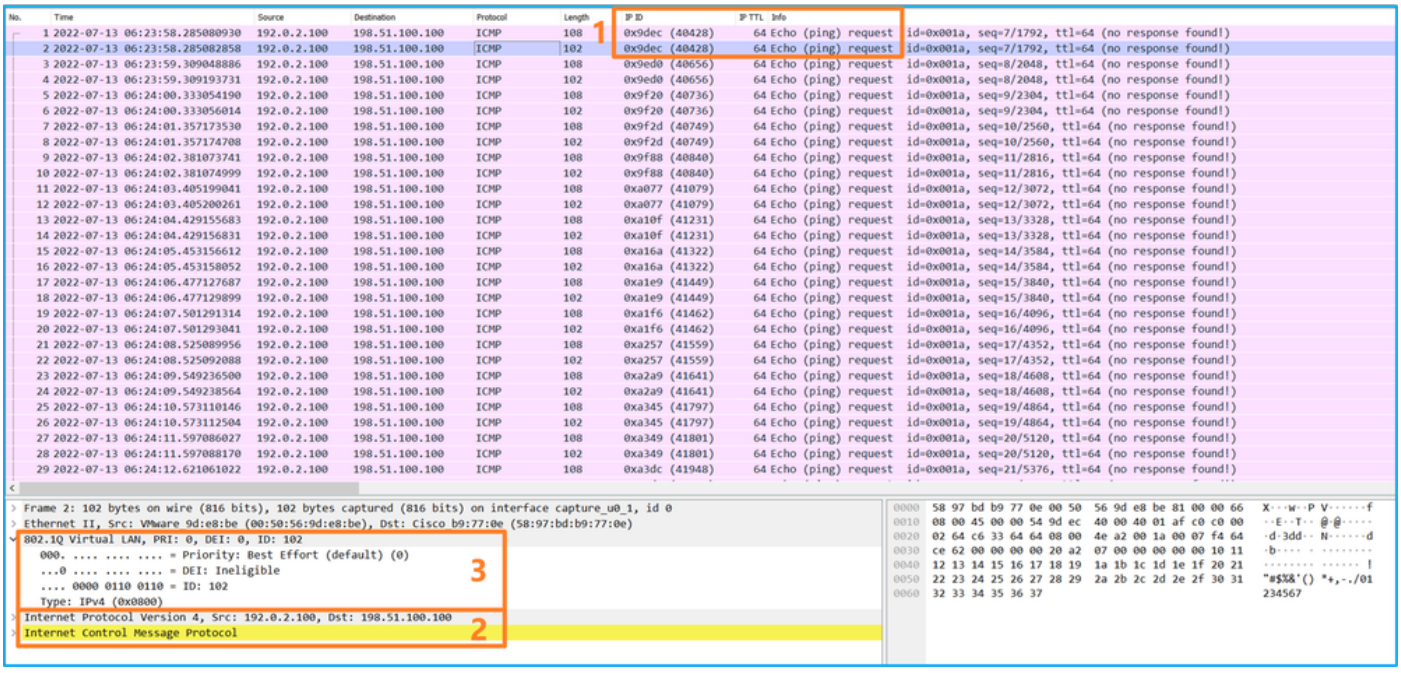
Utilisez une application de lecture de fichier de capture de paquets pour ouvrir le fichier de capture pour Ethernet1/2. Sélectionnez le premier paquet et vérifiez les points clés :

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.



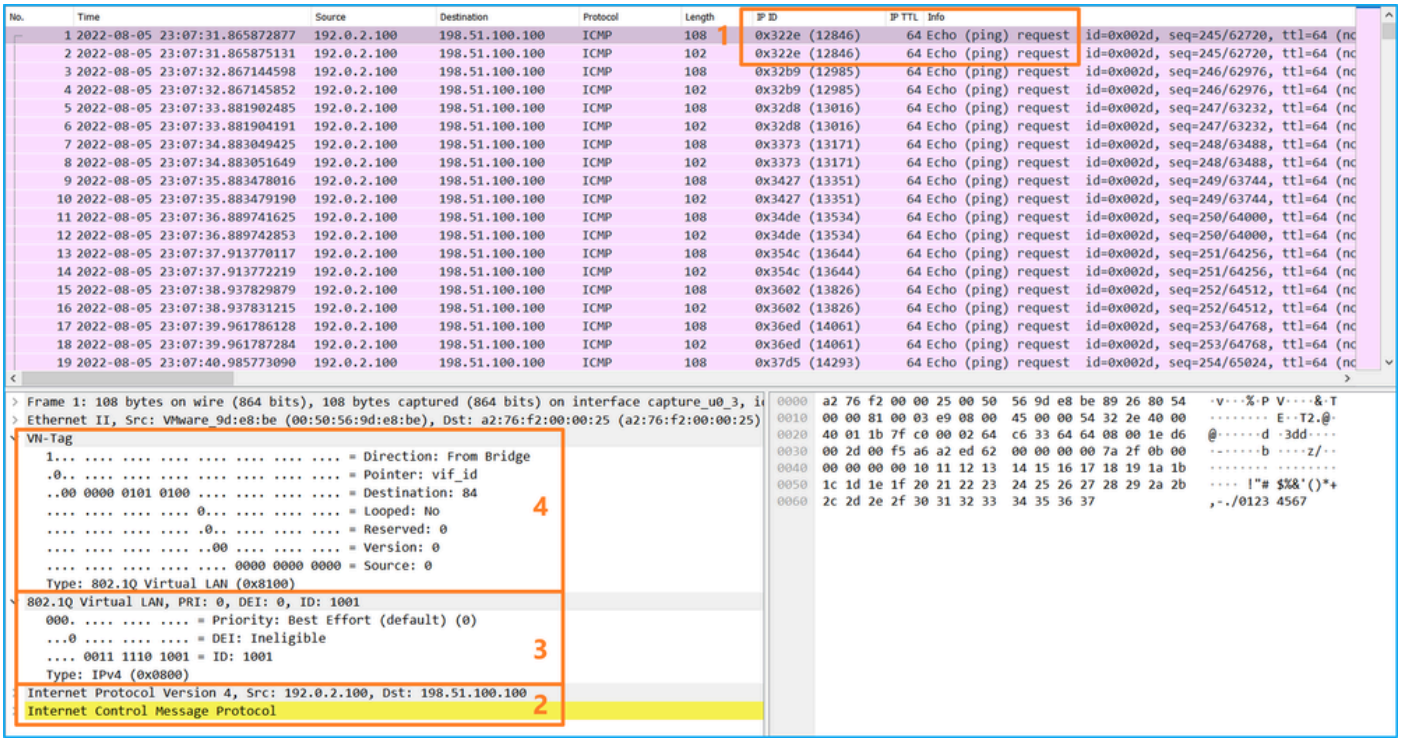
Sélectionnez le deuxième paquet et vérifiez les points clés :

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.



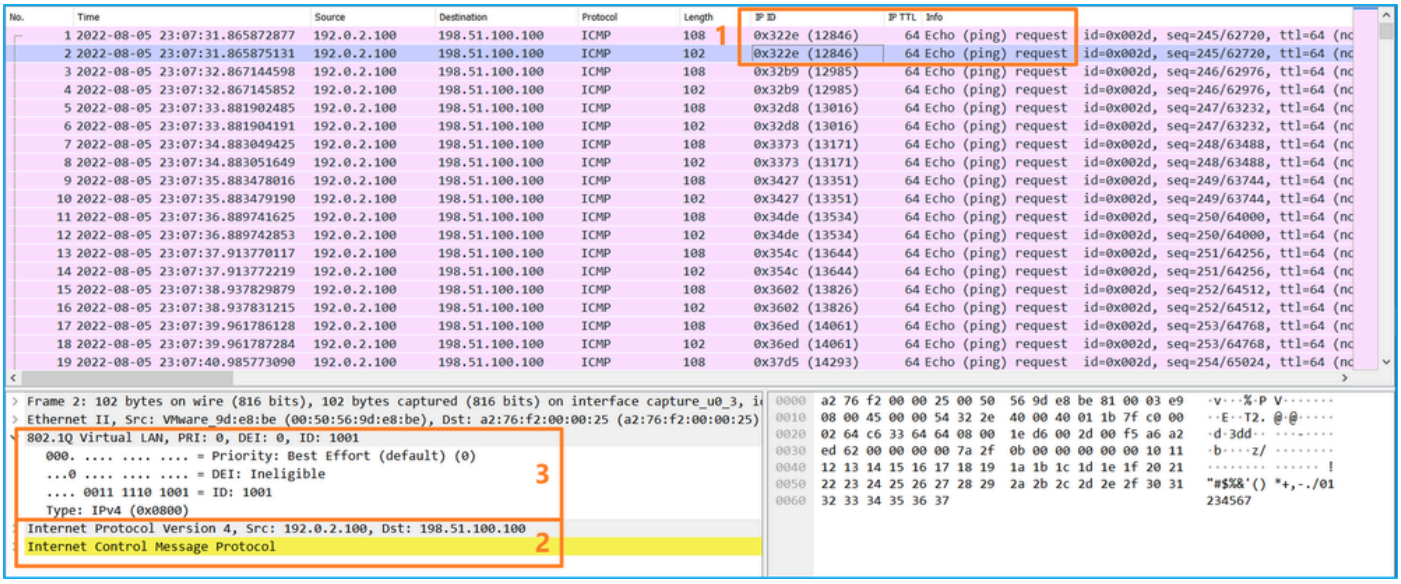
Ouvrez les fichiers de capture pour les interfaces membres Portchannel1. Sélectionnez le premier paquet et vérifiez les points clés :

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 commutateur interne insère une étiquette VN supplémentaire.



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.



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.

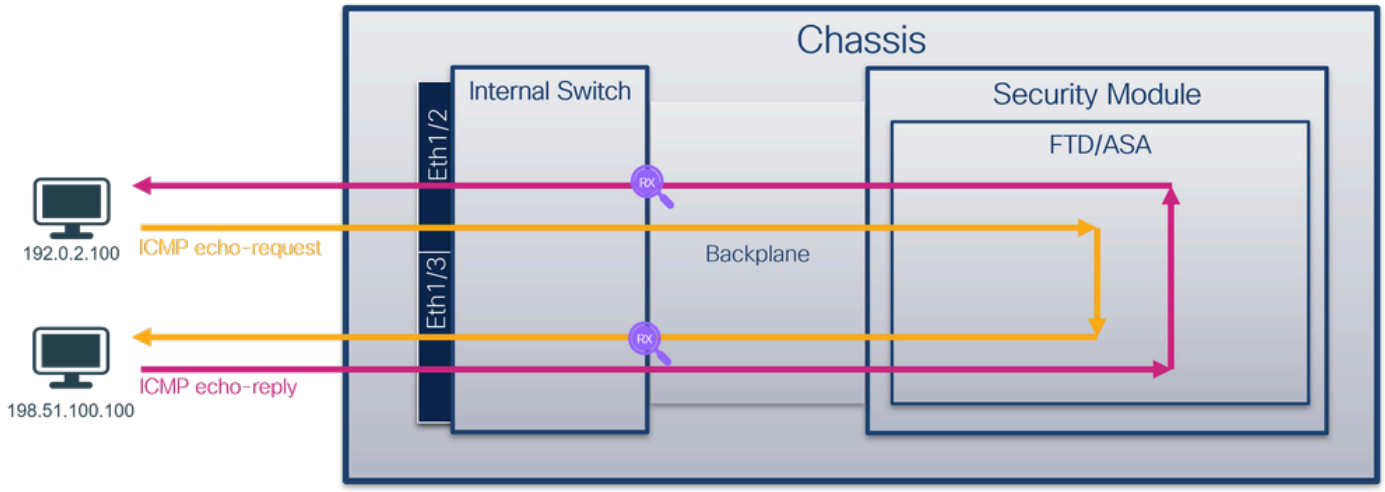
Ce tableau récapitule la tâche :

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

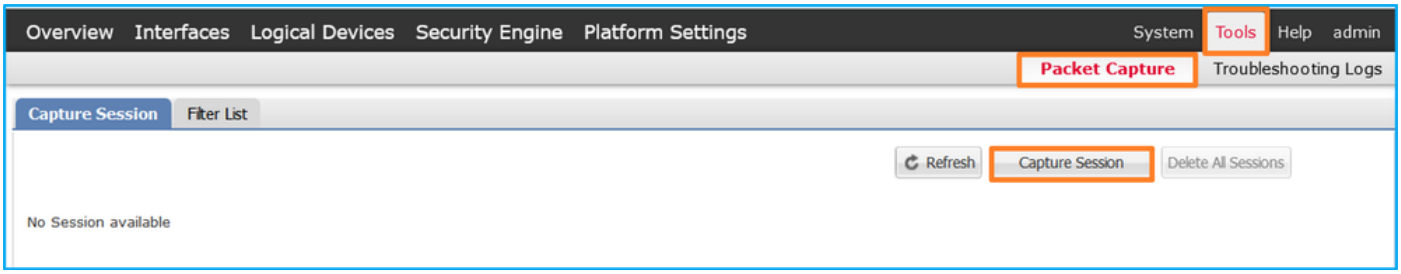


Configuration

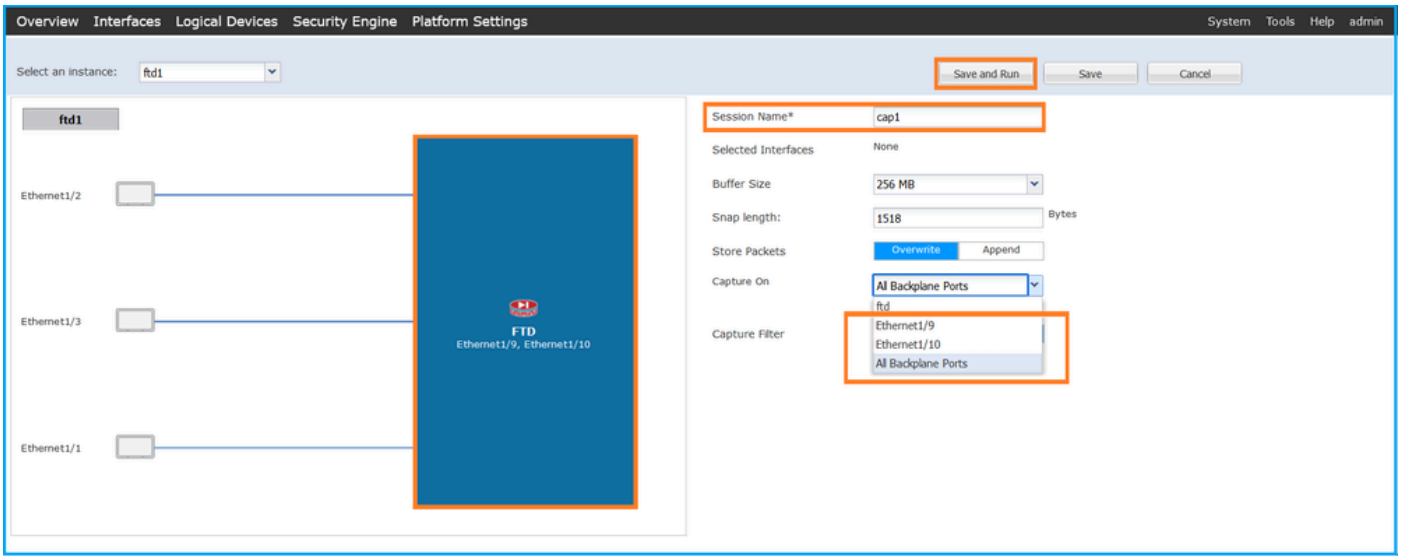
FCM

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 :

```
<#root>

firepower#

scope ssa

firepower /ssa#

show app-instance

App Name    Identifier Slot ID     Admin State Oper State       Running Version Startup Version Deploy Ty
---------- ---------- ---------- ----------- ---------------- --------------- --------------- ---------

ftd         ftd1

       1          Enabled     Online          7.2.0.82        7.2.0.82        Native      No
```

2. Créez une session de capture :

```
<#root>

firepower#

scope packet-capture

firepower /packet-capture #

create session cap1
```

```
firepower /packet-capture/session* #
create phy-port Eth1/9

firepower /packet-capture/session/phy-port* #
set app ftd

firepower /packet-capture/session/phy-port* #
set app-identifier ftd1

firepower /packet-capture/session/phy-port* #
up

firepower /packet-capture/session* #
create phy-port Eth1/10

firepower /packet-capture/session/phy-port* #
set app ftd

firepower /packet-capture/session/phy-port* #
set app-identifier ftd1

firepower /packet-capture/session/phy-port* #
up

firepower /packet-capture/session* #
enable

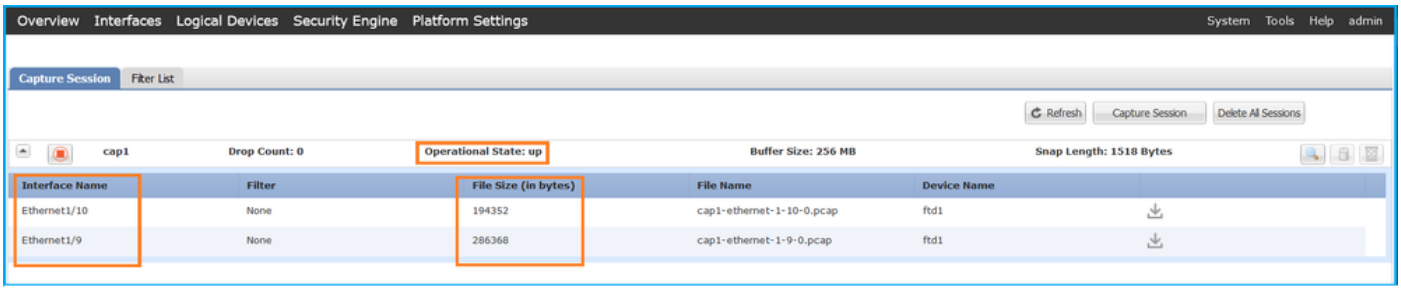
firepower /packet-capture/session* #
commit

firepower /packet-capture/session #
```

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 :

<#root>

firepower#

scope packet-capture

firepower /packet-capture #

show session cap1

Traffic Monitoring Session:

Packet Capture Session Name: cap1

Session: 1

Admin State: Enabled

Oper State: Up

Oper State Reason: Active

Config Success: Yes
Config Fail Reason:
Append Flag: Overwrite
Session Mem Usage: 256 MB
Session Pcap Snap Len: 1518 Bytes
Error Code: 0
Drop Count: 0

Physical ports involved in Packet Capture:

Slot Id: 1

Port Id: 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 interne du commutateur Firepower 4100/9300.

Capturer l'analyse des fichiers

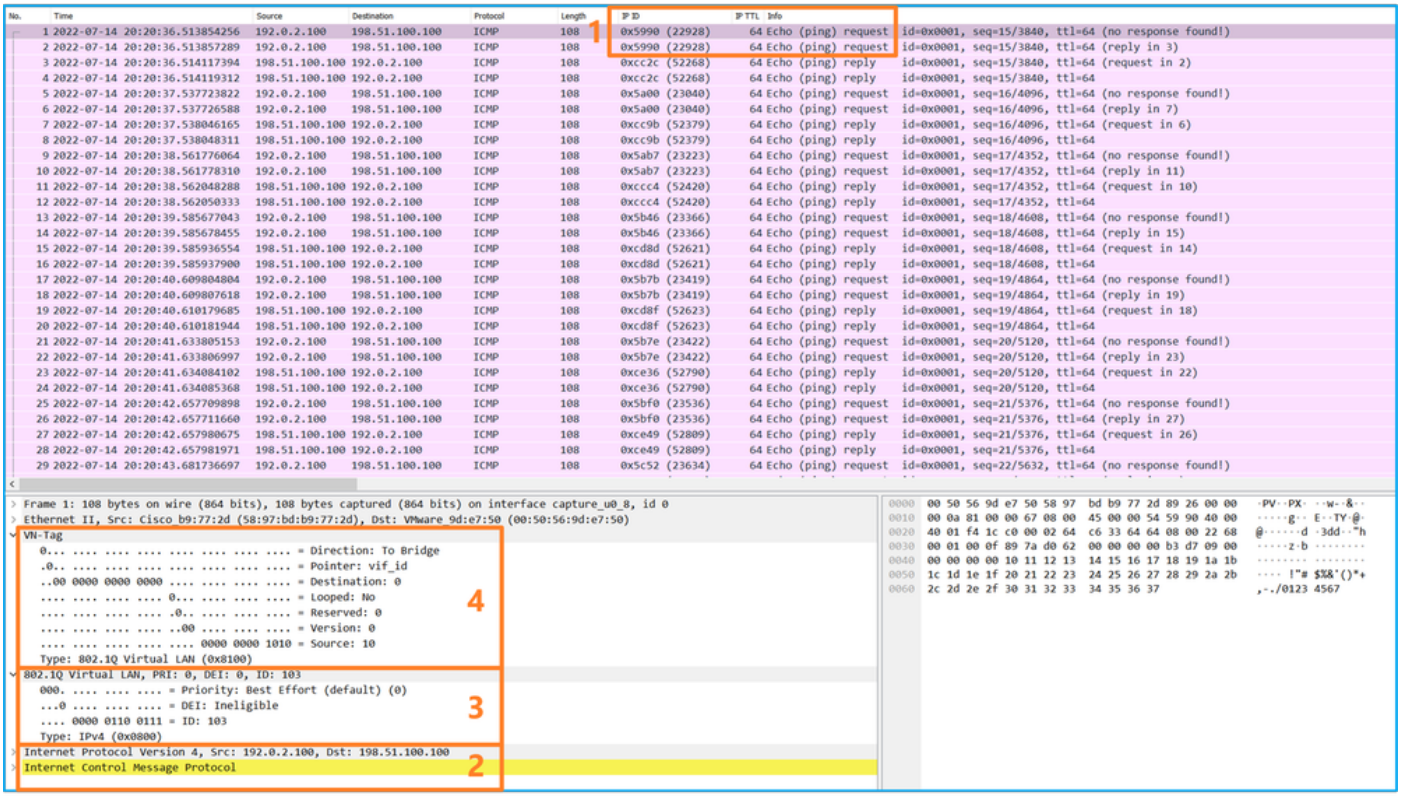
Utilisez une application de lecture de fichiers de capture de paquets pour ouvrir les fichiers de capture. Dans le cas de plusieurs interfaces de fond de panier, assurez-vous d'ouvrir tous les fichiers de capture pour chaque interface de fond de panier. Dans ce cas, les paquets sont capturés sur l'interface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

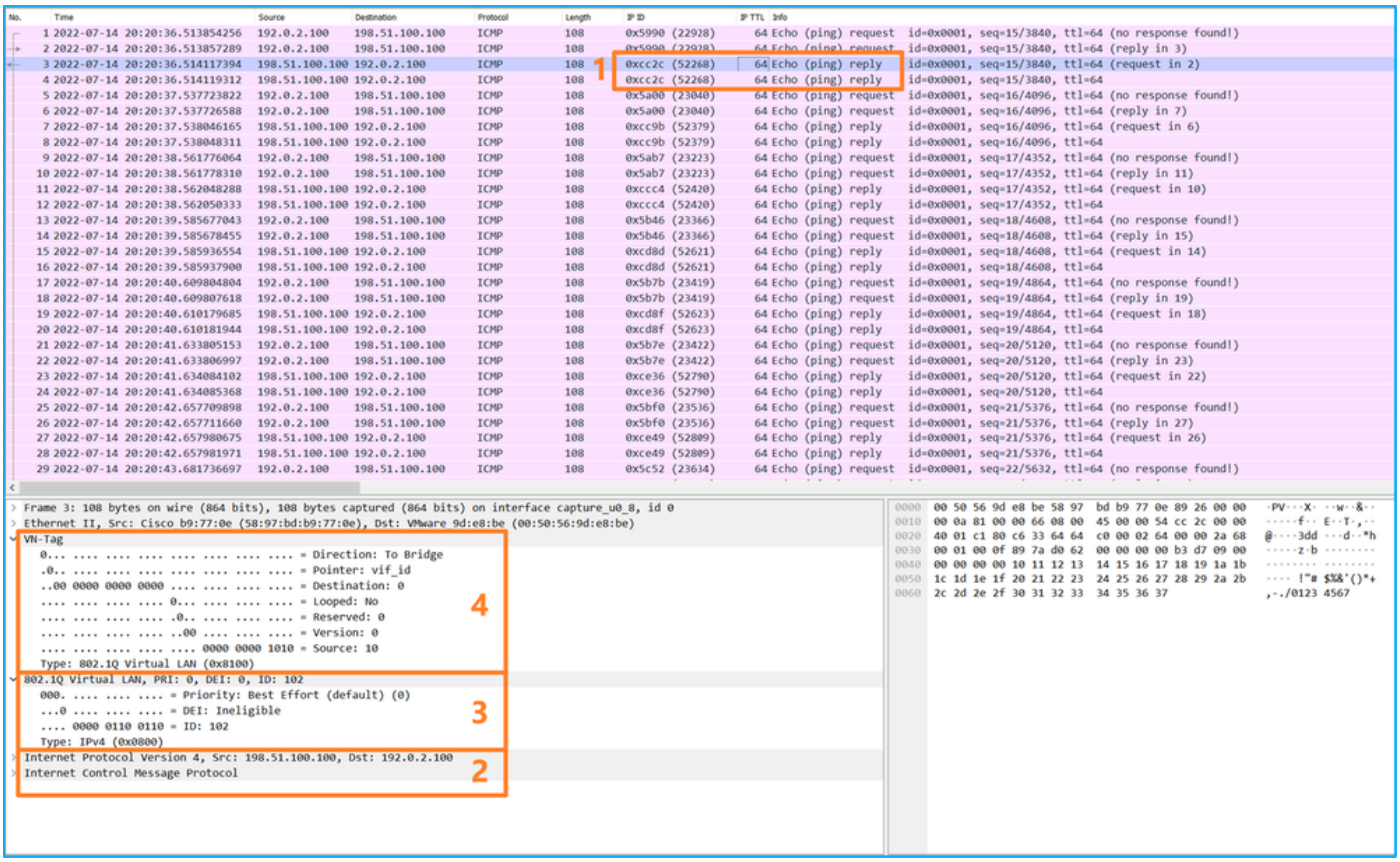
l'interface de sortie Ethernet1/3.

4. Le commutateur interne insère une étiquette VN supplémentaire.



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.



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 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

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 :

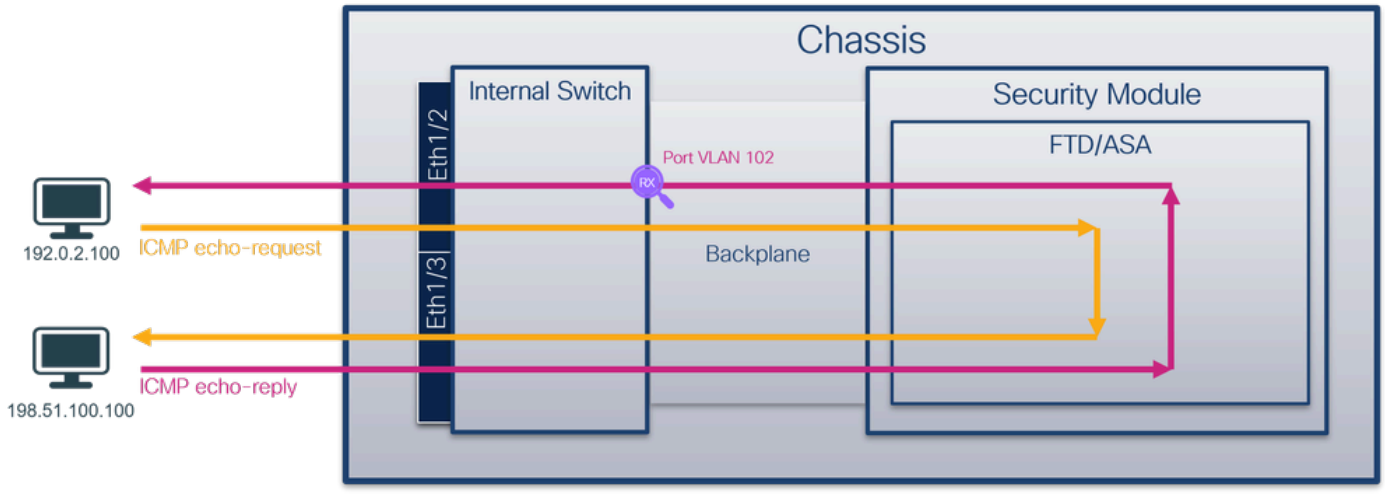
- Configurez les captures de paquets sur les interfaces de fond de panier pour les paquets qui quittent une interface avant spécifique. Par exemple, configurez les captures de paquets sur l'interface de fond de panier Ethernet1/9 pour les paquets qui quittent l'interface Ethernet1/2.
- Configurez des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

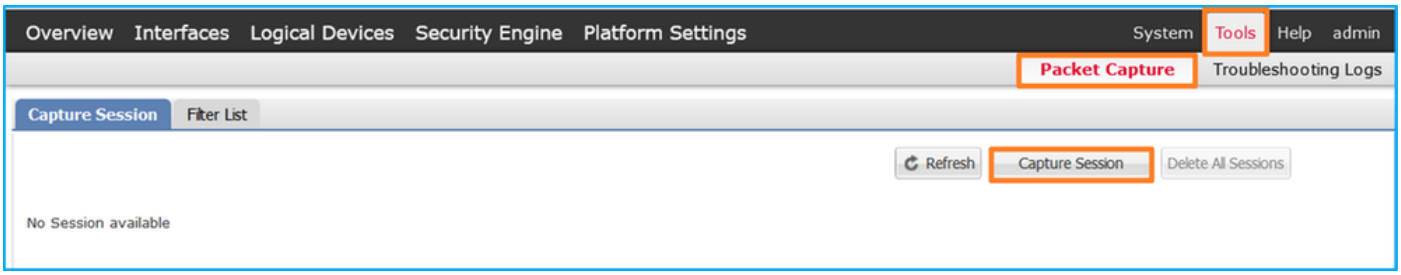


Configuration

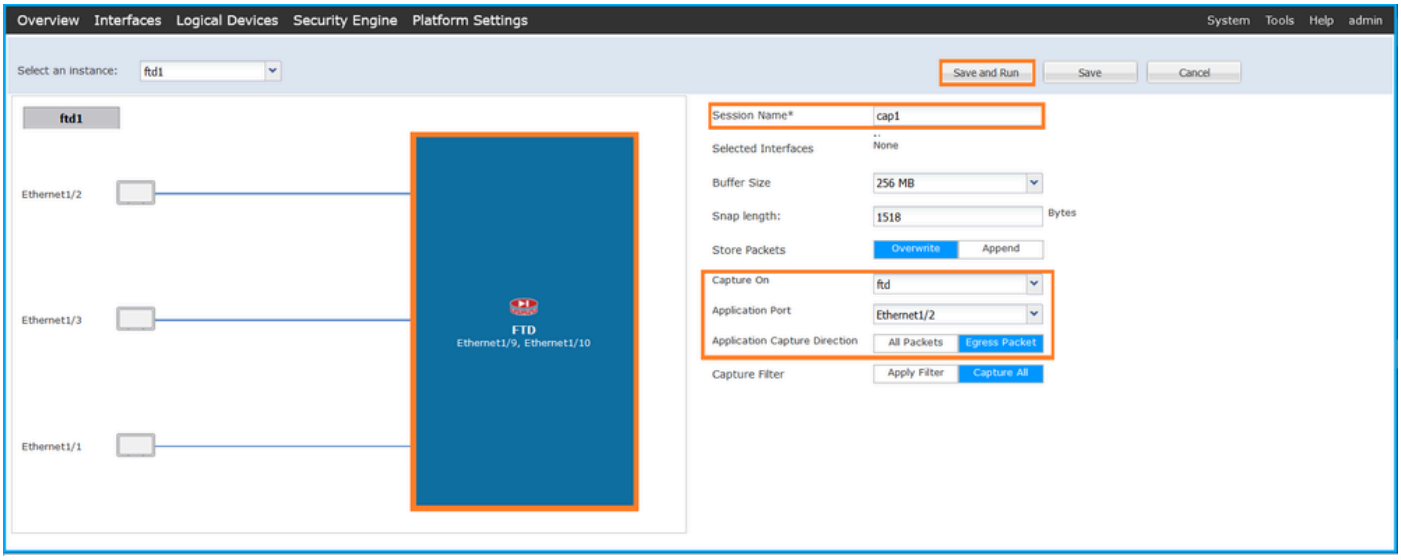
FCM

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 :

```
<#root>

firepower#

scope ssa

firepower /ssa#

show app-instance

App Name    Identifier Slot ID     Admin State Oper State       Running Version Startup Version Deploy Ty
----------  ---------- ----------  ----------- ---------------  --------------- --------------- ---------

ftd         ftd1
```

```
1          Enabled     Online          7.2.0.82        7.2.0.82        Native      No
```

2. Créez une session de capture :

```
<#root>
firepower#
scope packet-capture

firepower /packet-capture #
create session cap1

firepower /packet-capture/session* #
create app-port 1 l12 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

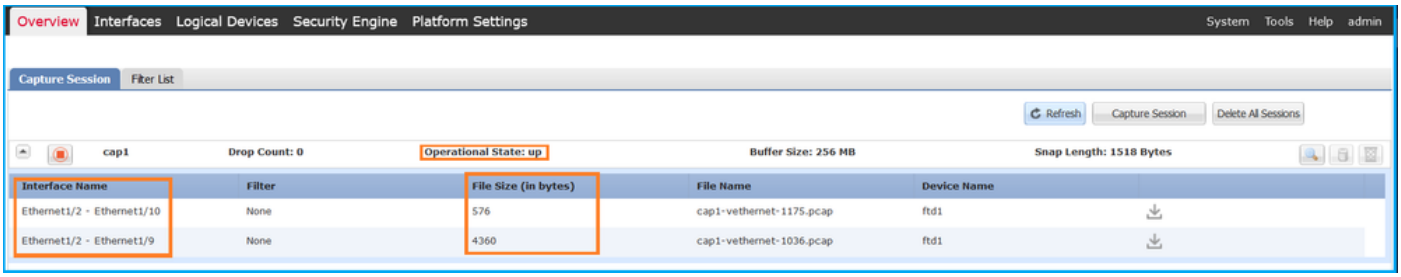
firepower /packet-capture/session/app-port* #
up

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 :



CLI FXOS

Vérifiez les détails de capture dans la portée packet-capture :

<#root>

```
firepower#
scope packet-capture

firepower /packet-capture #
show session cap1


Traffic Monitoring Session:
    Packet Capture Session Name: cap1

    Session: 1
    Admin State: Enabled


    Oper State: Up


    Oper State Reason: Active


    Config Success: Yes
    Config Fail Reason:
    Append Flag: Overwrite
    Session Mem Usage: 256  MB
    Session Pcap Snap Len: 1518  Bytes
    Error Code: 0
    Drop Count: 0

Application ports involved in Packet Capture:
    Slot Id: 1


    Link Name: l12


    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

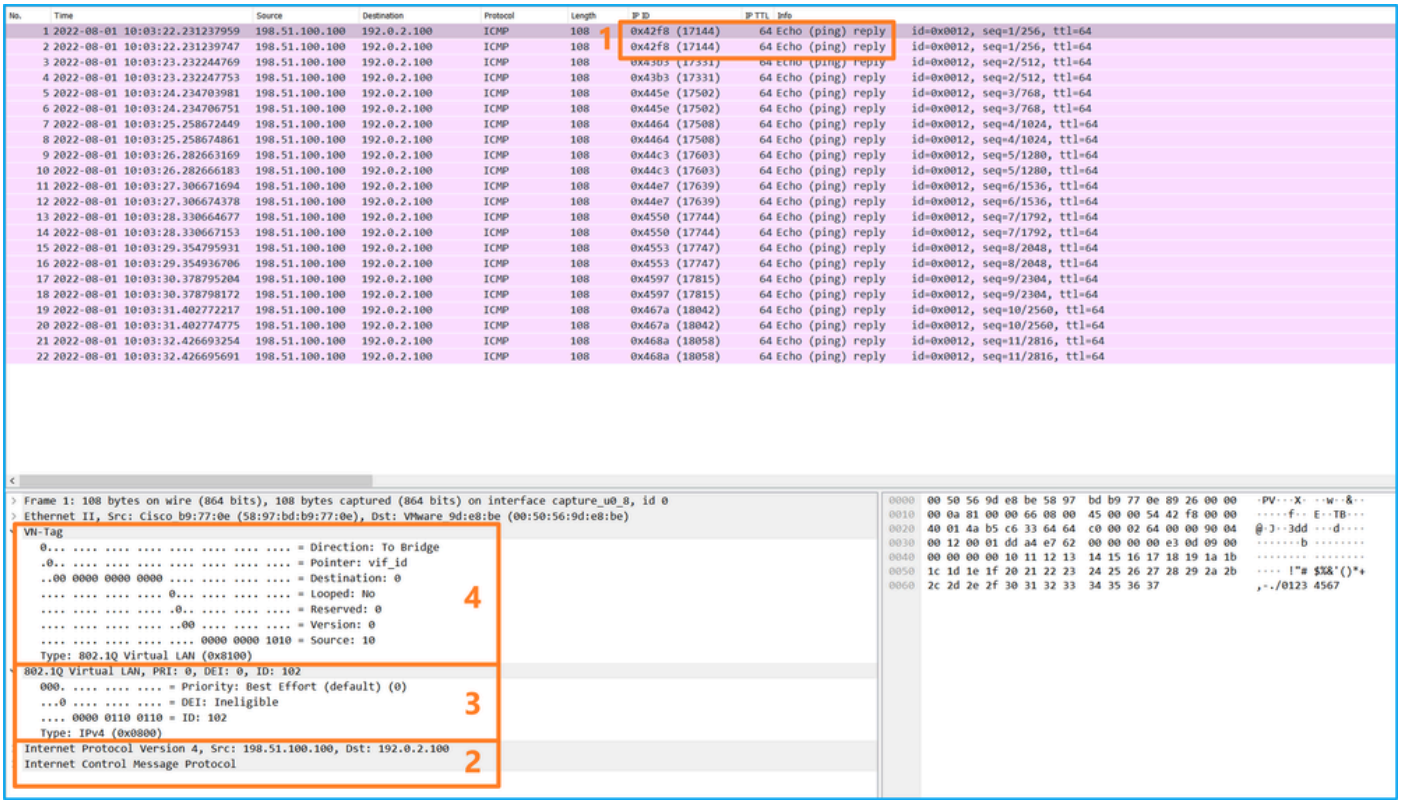
Suivez les étapes de la section Collecter les fichiers de capture interne du commutateur Firepower 4100/9300.

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.



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 uniquement	Réponses d'écho ICMP de l'hôte 198.51.100.100 à l'hôte 192.0.2.100

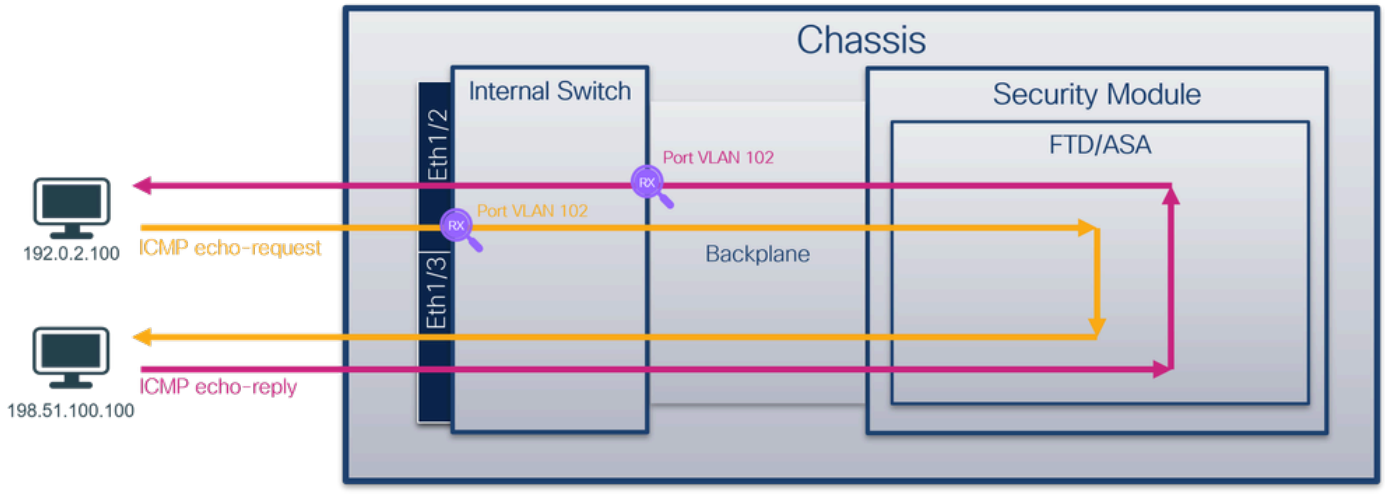
Tâche 2

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



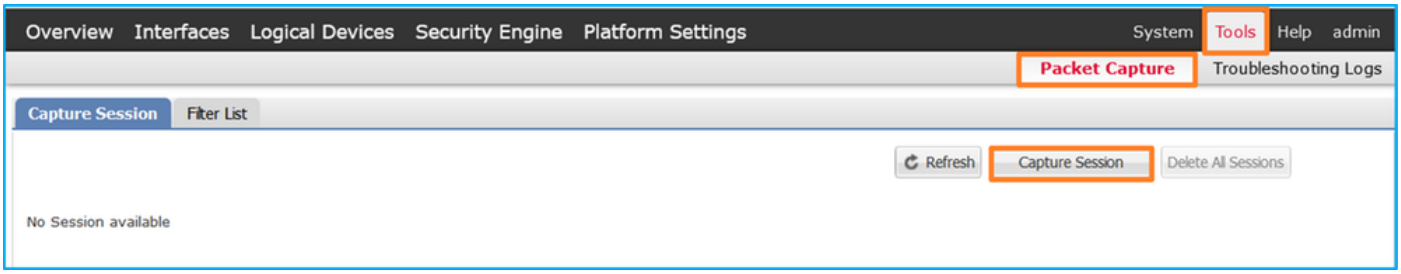
Configuration

FCM

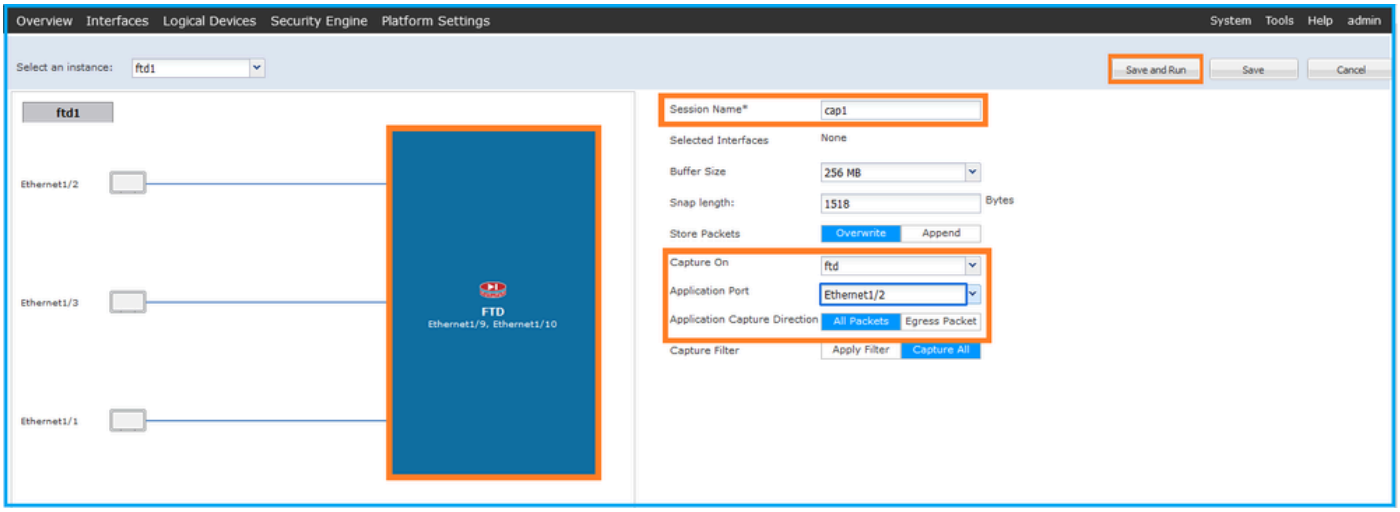
Procédez comme suit sur FCM pour configurer une capture de paquets sur l'application FTD et le port d'application Ethernet1/2 :

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 :

```
<#root>

firepower#

scope ssa


firepower /ssa#

show app-instance


App Name    Identifier Slot ID     Admin State Oper State       Running Version Startup Version Deploy Ty
----------- ---------- ---------- ----------- ---------------- --------------- --------------- ---------

ftd         ftd1

       1          Enabled     Online          7.2.0.82        7.2.0.82        Native      No
```

2. Créez une session de capture :

```
<#root>
firepower#
scope packet-capture

firepower /packet-capture #
create session cap1

firepower /packet-capture/session* #
create phy-port eth1/2

firepower /packet-capture/session/phy-port* #
set app-identifier ftd1

firepower /packet-capture/session/phy-port* #
exit

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

firepower /packet-capture/session/app-port* #
set app-identifier ftd1

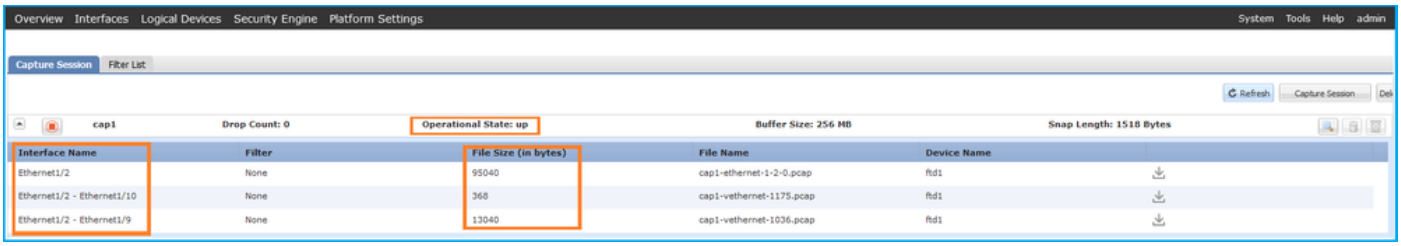
firepower /packet-capture/session* #
enable

firepower /packet-capture/session* #
commit
firepower /packet-capture/session # commit
```

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 :

<#root>

```
firepower#
scope packet-capture

firepower /packet-capture #
show session cap1


Traffic Monitoring Session:
    Packet Capture Session Name: cap1

    Session: 1
    Admin State: Enabled


    Oper State: Up


    Oper State Reason: Active


    Config Success: Yes
    Config Fail Reason:
    Append Flag: Overwrite
    Session Mem Usage: 256  MB
    Session Pcap Snap Len: 1518  Bytes
    Error Code: 0
    Drop Count: 0

Physical ports involved in Packet Capture:
    Slot Id: 1


    Port Id: 2


    Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap
```

Pcapsize: 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

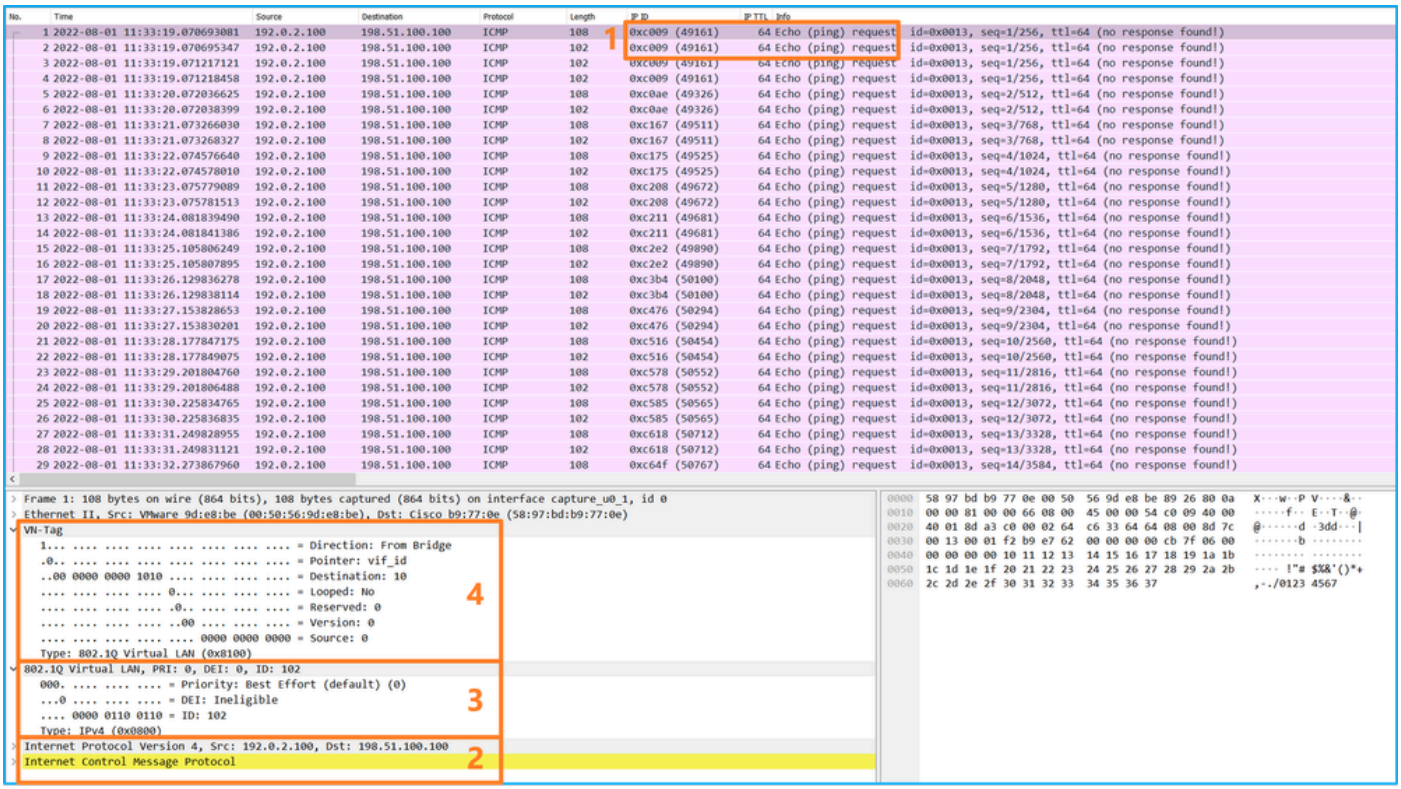
Suivez les étapes de la section Collecter les fichiers de capture interne du commutateur Firepower 4100/9300.

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.

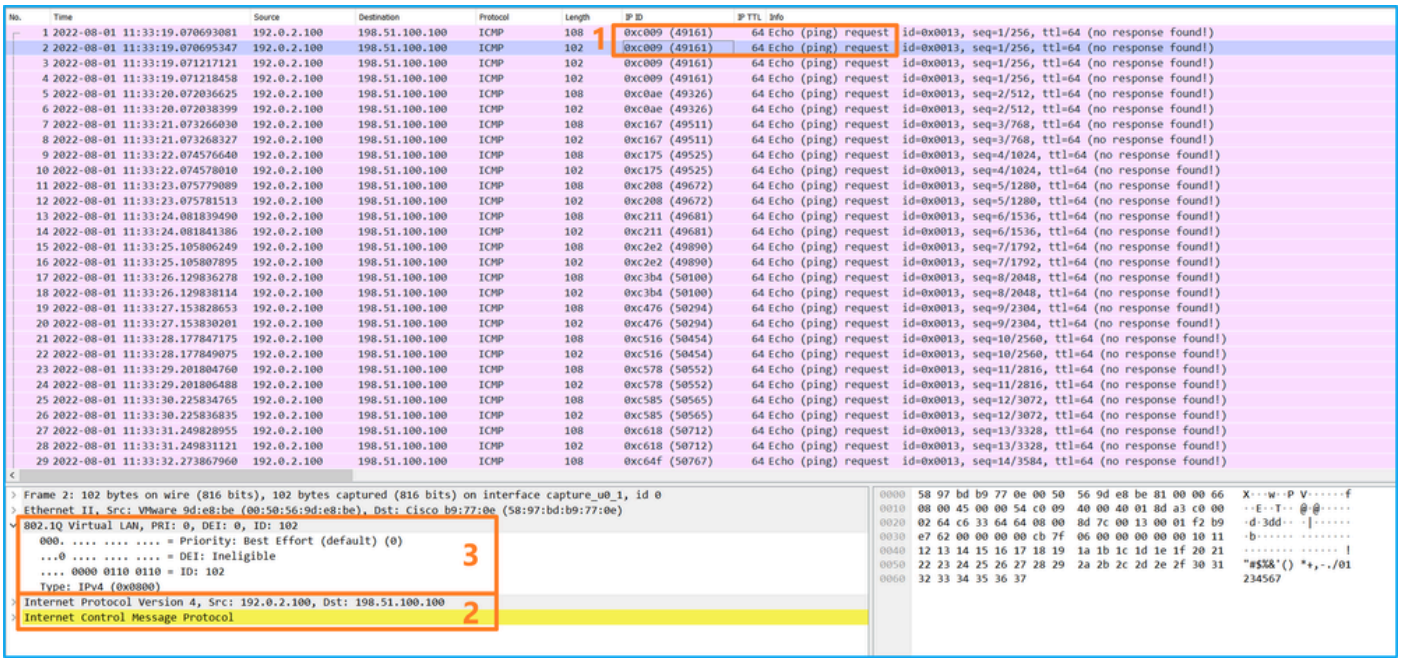
Ouvrez le fichier de capture pour l’interface Ethernet1/2, sélectionnez le premier paquet et vérifiez les points clés :

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.



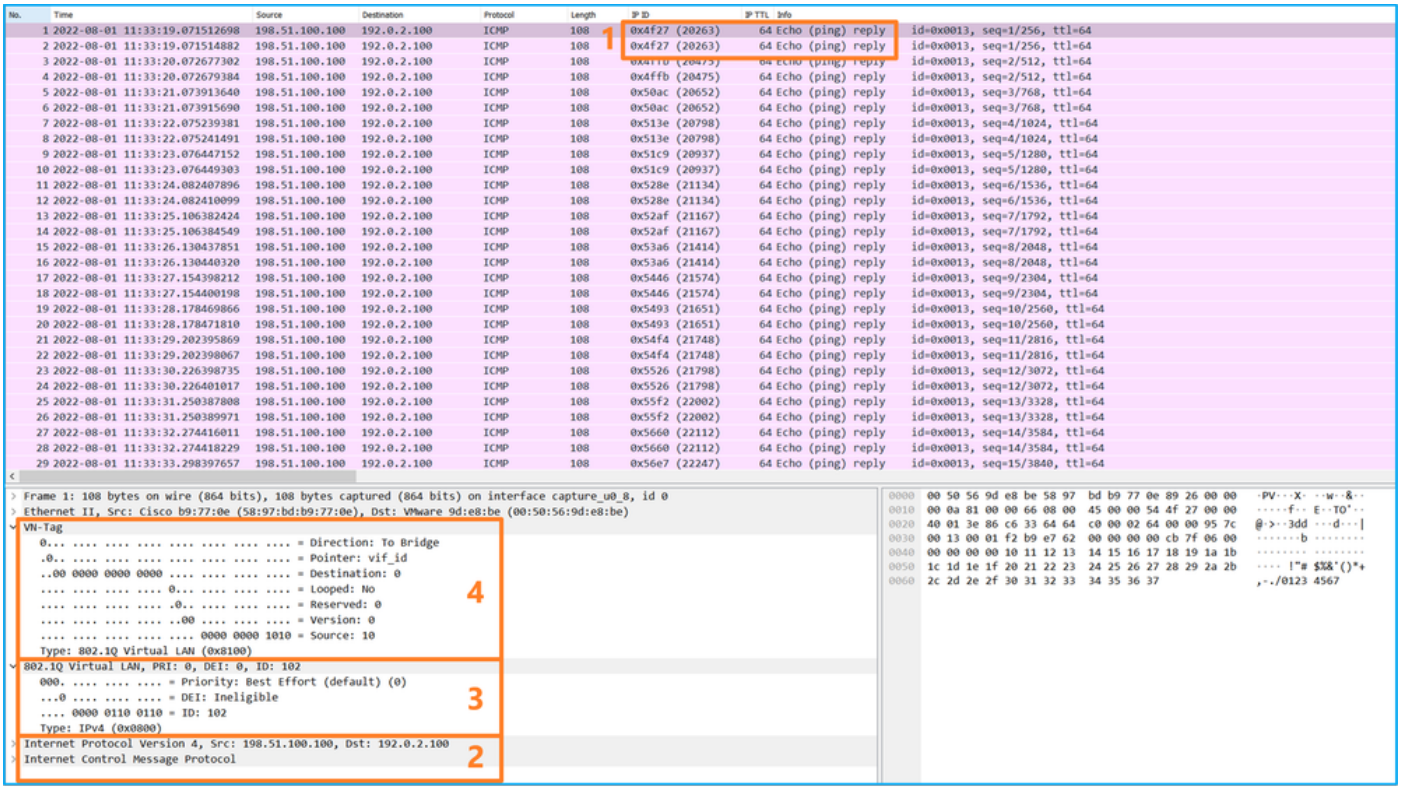
Sélectionnez le deuxième paquet et vérifiez les points clés :

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.



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.



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.

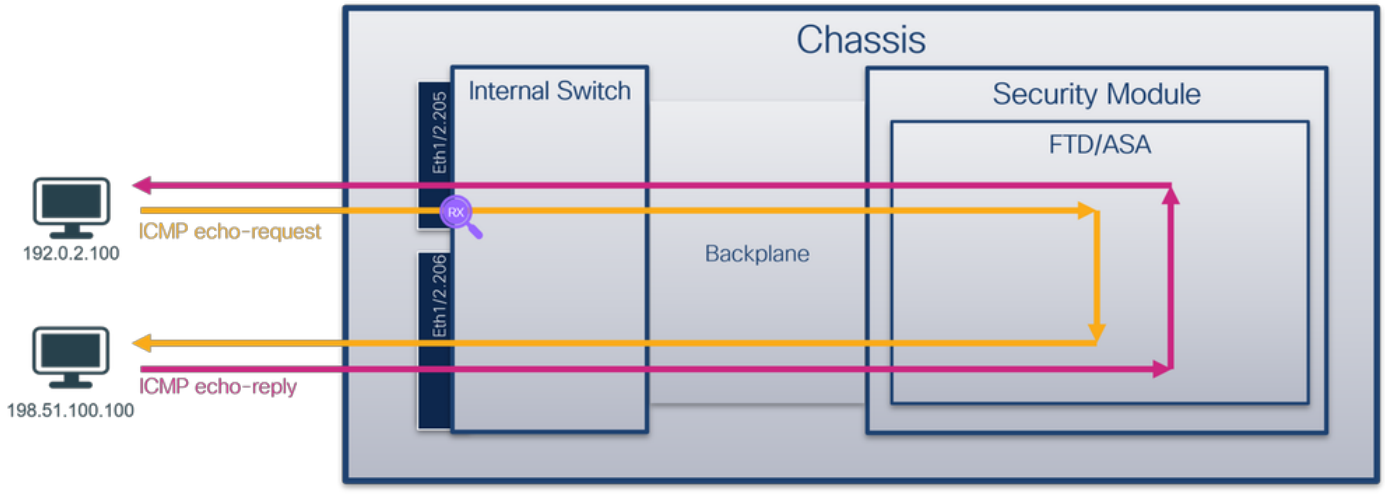
Ce tableau récapitule la tâche :

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

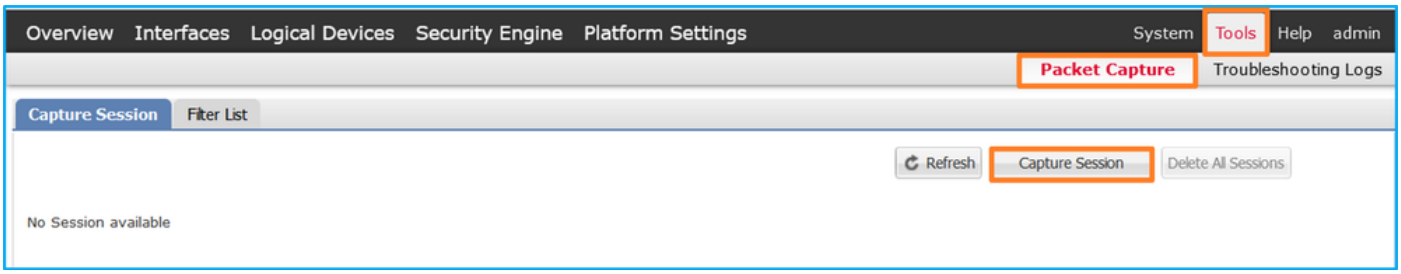


Configuration

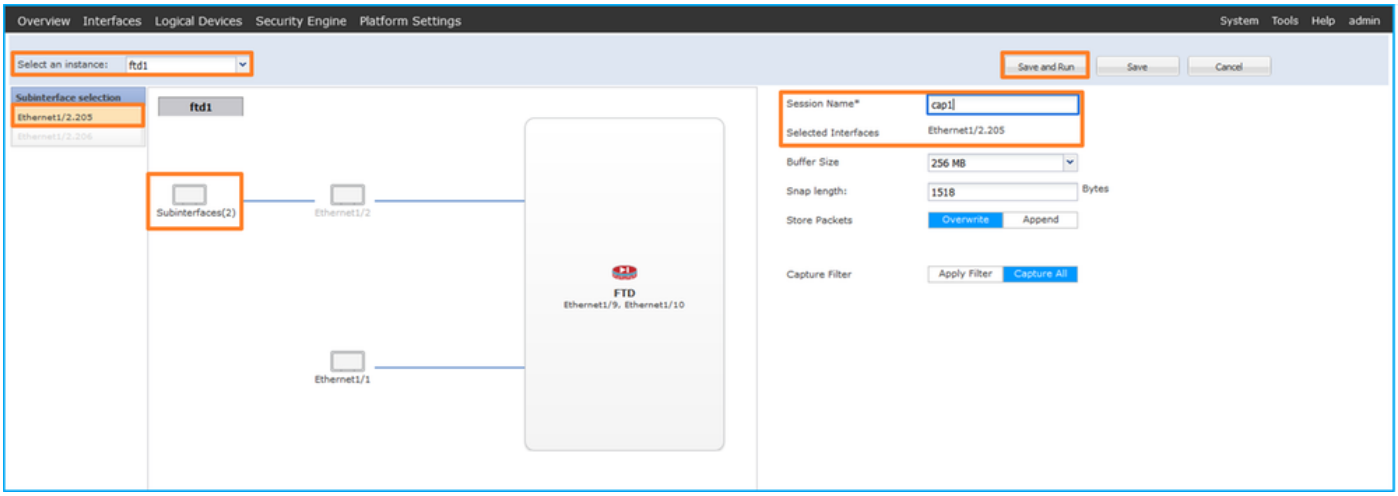
FCM

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, 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 :

<#root>

```
firepower#
```

scope ssa

```
firepower /ssa #
```

```
show app-instance

App Name   Identifier Slot ID    Admin State Oper State       Running Version Startup Version Deploy Ty
---------- ---------- ---------- ----------- --------------- --------------- --------------- ---------

ftd        ftd1

       1          Enabled     Online           7.2.0.82        7.2.0.82        Container   No         R
ftd        ftd2       1           Enabled     Online           7.2.0.82        7.2.0.82        Container
```

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

```
<#root>

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 :

```
<#root>

firepower#

scope packet-capture


firepower /packet-capture #

create session cap1


firepower /packet-capture/session* #

create phy-port Eth1/2
```

```
firepower /packet-capture/session/phy-port* #
set app ftd

firepower /packet-capture/session/phy-port* #
set app-identifier ftd1

firepower /packet-capture/session/phy-port* #
set subinterface 205

firepower /packet-capture/session/phy-port* #
up

firepower /packet-capture/session* #
enable

firepower /packet-capture/session* #
commit

firepower /packet-capture/session #
```

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

<#root>

```
firepower#
scope packet-capture

firepower /packet-capture #
create filter vlan207

firepower /packet-capture/filter* #
set ovlan 207

firepower /packet-capture/filter* #
up

firepower /packet-capture* #
create session cap1

firepower /packet-capture/session*
```

```
create phy-port Eth1/3

firepower /packet-capture/session/phy-port* #
set app ftd

firepower /packet-capture/session/phy-port* #
set app-identifier ftd1

firepower /packet-capture/session/phy-port* #
set subinterface 207

firepower /packet-capture/session/phy-port* #
up

firepower /packet-capture/session* #
create phy-port Eth1/4

firepower /packet-capture/session/phy-port* #
set app ftd

firepower /packet-capture/session/phy-port* #
set app-identifier ftd1

firepower /packet-capture/session/phy-port* #
set subinterface 207

firepower /packet-capture/session/phy-port* #
up

firepower /packet-capture/session* #
enable

firepower /packet-capture/session* #
commit

firepower /packet-capture/session #
```

Vérification

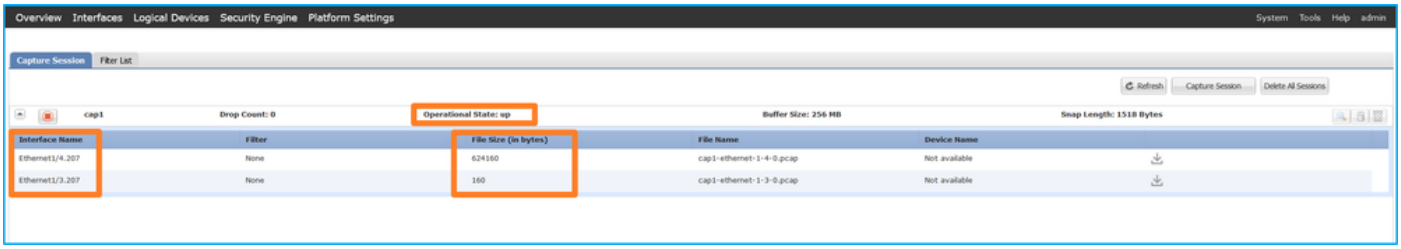
FCM

Vérifiez le nom de l'interface, assurez-vous que l'état opérationnel est up et que la taille du fichier

(en octets) augmente :



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 :



CLI FXOS

Vérifiez les détails de capture dans la portée packet-capture :

<#root>

```
firepower#
scope packet-capture

firepower /packet-capture #
show session cap1


Traffic Monitoring Session:
    Packet Capture Session Name: cap1

    Session: 1
    Admin State: Enabled


    Oper State: Up


    Oper State Reason: Active


    Config Success: Yes
    Config Fail Reason:
    Append Flag: Overwrite
    Session Mem Usage: 256  MB
    Session Pcap Snap Len: 1518  Bytes
    Error Code: 0
```

```
    Drop Count: 0
Physical ports involved in Packet Capture:
    Slot Id: 1

    Port Id: 2

    Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap

    Pcapsize: 9324  bytes

    Filter:
    Sub Interface: 205

    Application Instance Identifier: ftd1

    Application Name: ftd
```

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

```
<#root>
firepower#
scope packet-capture

firepower /packet-capture # show session cap1
Traffic Monitoring Session:
    Packet Capture Session Name: cap1

    Session: 1

Admin State: Enabled

    Oper State: Up

    Oper State Reason: Active

    Config Success: Yes
    Config Fail Reason:
    Append Flag: Overwrite
```

Session Mem Usage: 256 MB
Session Pcap Snap Len: 1518 Bytes
Error Code: 0
Drop Count: 0

Physical ports involved in Packet Capture:

Slot Id: 1

Port Id: 3

Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-3-0.pcap

Pcapsize: 160 bytes

Filter:

Sub Interface: 207

Application Instance Identifier: ftd1

Application Name: ftd

Slot Id: 1

Port Id: 4

Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-4-0.pcap

Pcapsize: 624160 bytes

Filter:

Sub Interface: 207

Application Instance Identifier: ftd1

Application Name: ftd

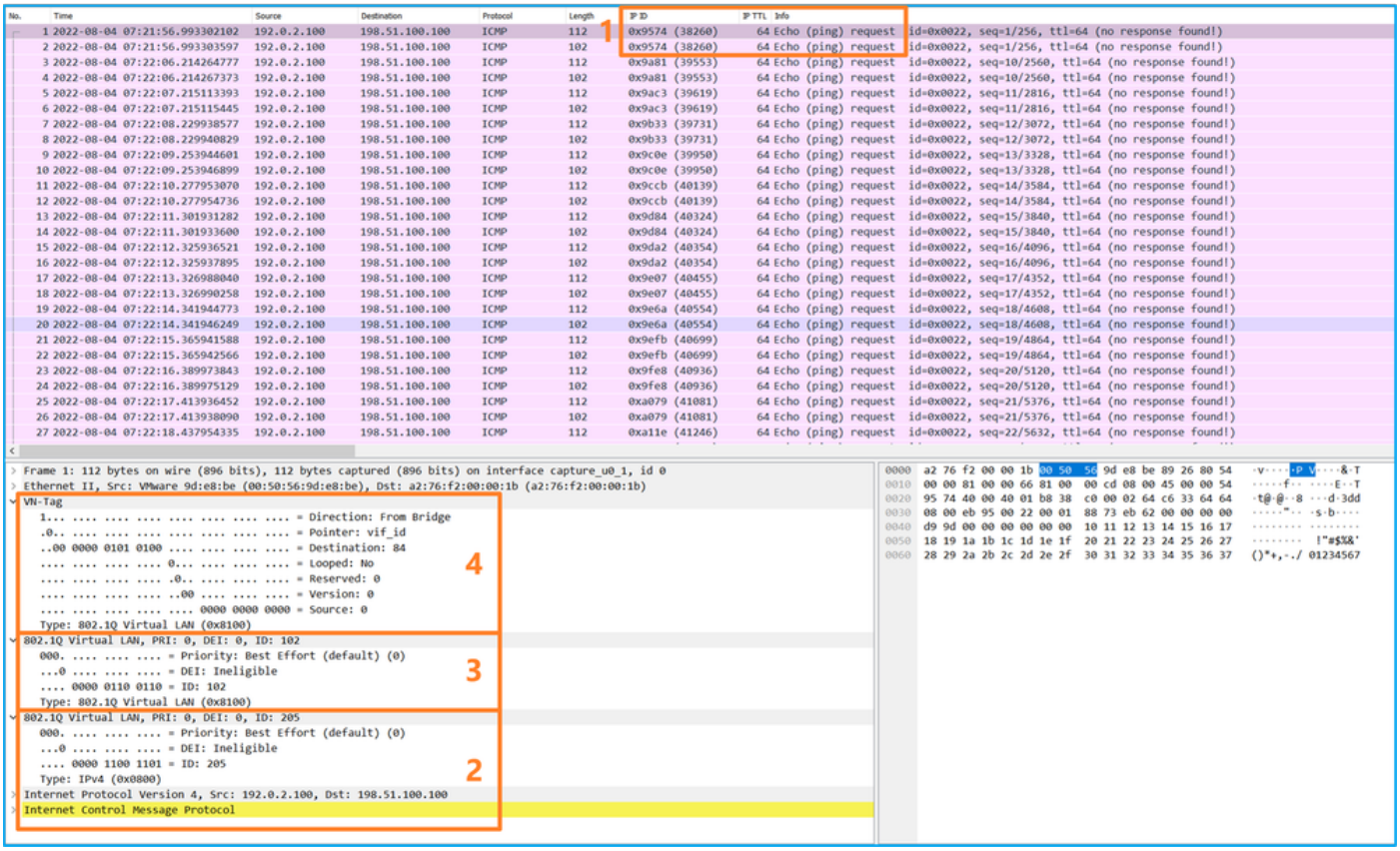
Collecter les fichiers de capture

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

Capturer l'analyse des fichiers

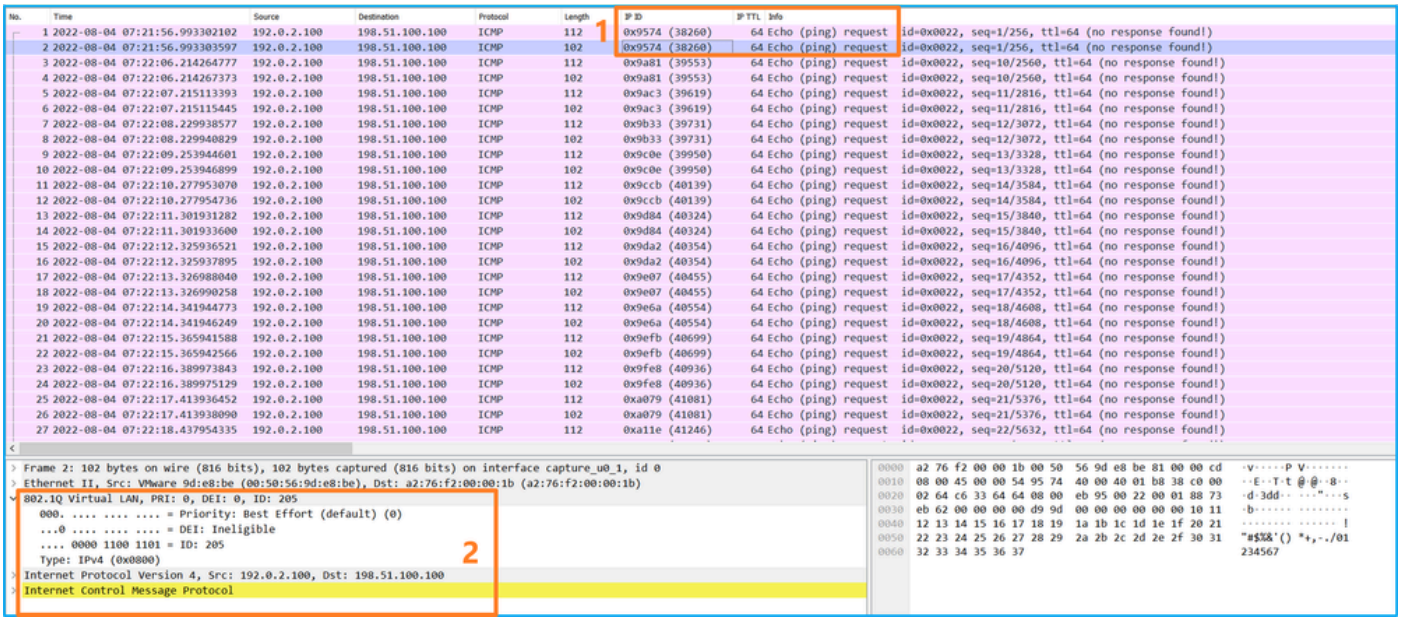
Utilisez une application de lecture de fichier de capture de paquets pour ouvrir le fichier de capture. Sélectionnez le premier paquet et vérifiez les points clés :

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.



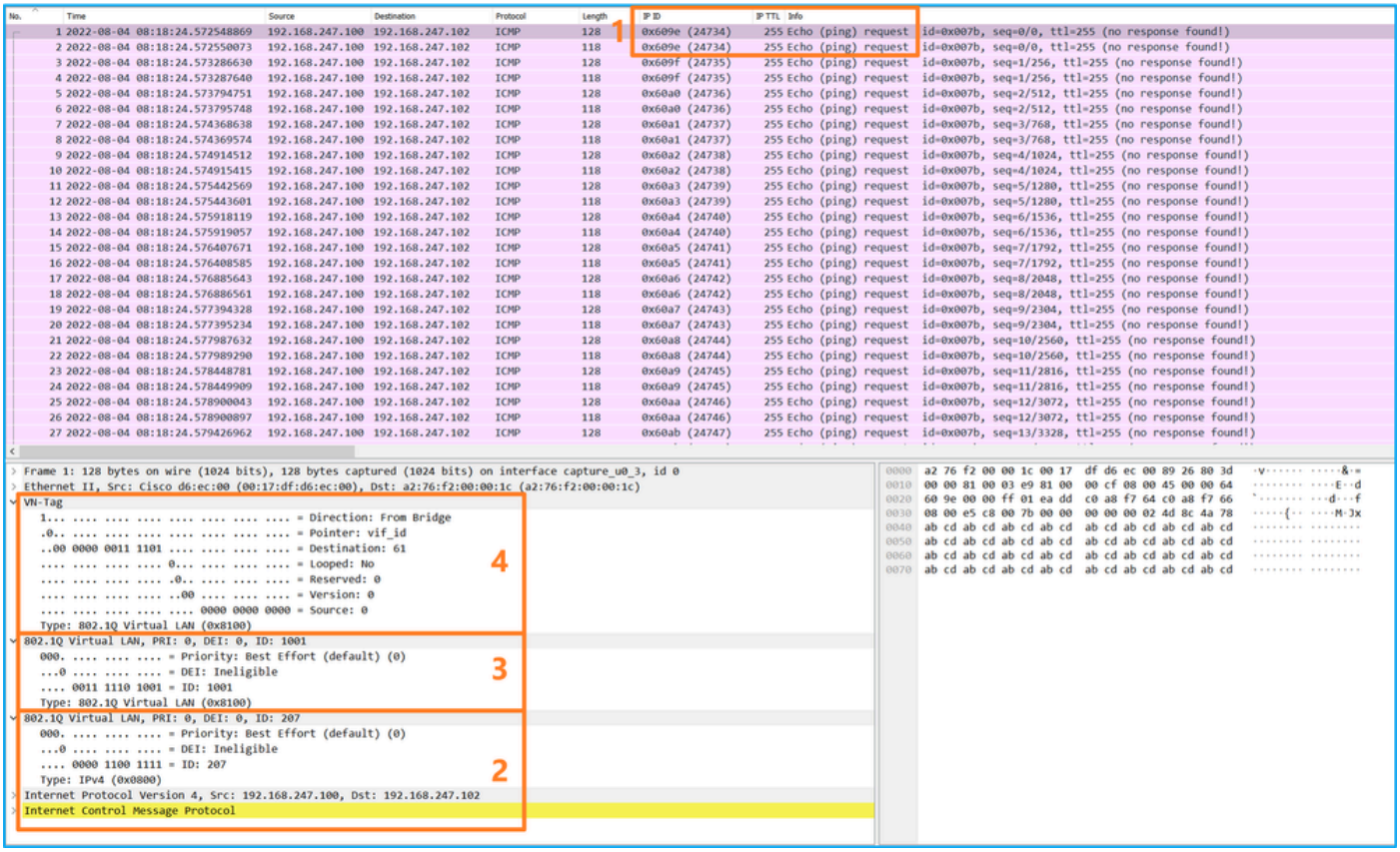
Sélectionnez le deuxième paquet et vérifiez les points clés :

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.



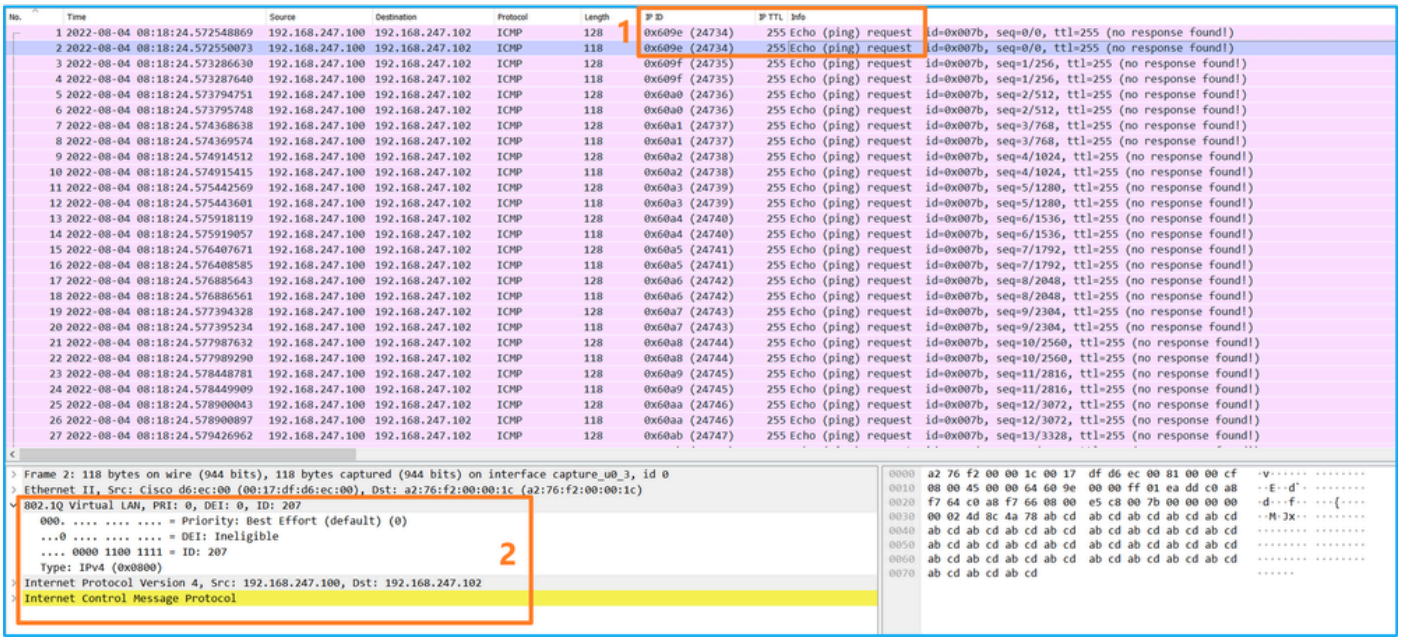
Ouvrez à présent les fichiers de capture pour Portchannel1.207. Sélectionnez le premier paquet et vérifiez les points clés

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.



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.



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 :

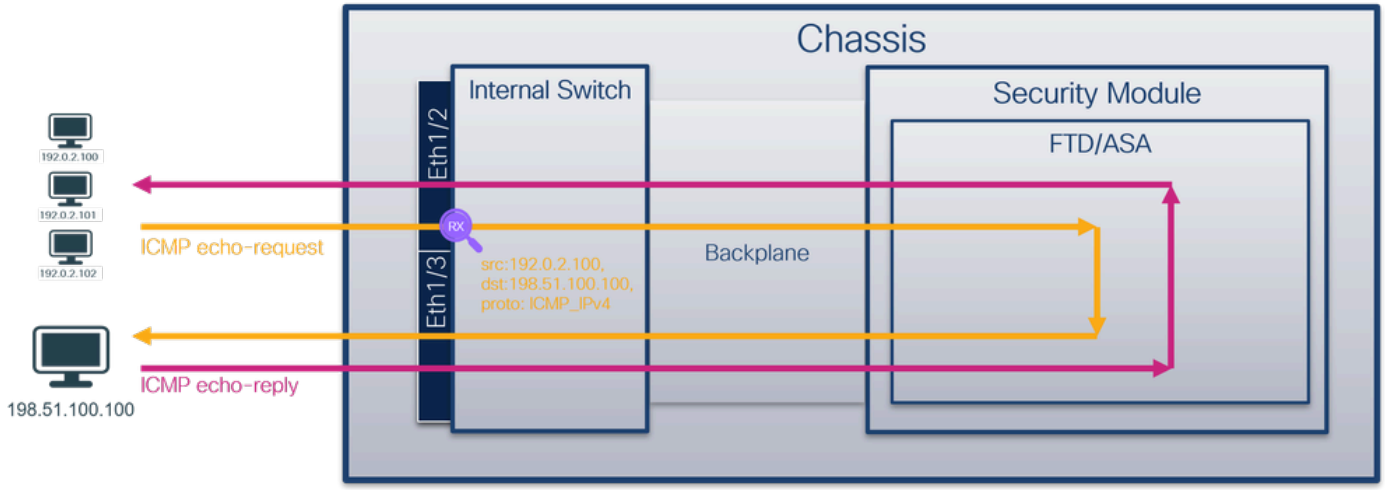
Tâche	Point de capture	VLAN de port interne dans les paquets capturés	Direction	Trafic capturé
Configurer et vérifier une capture de paquets sur la sous-interface Ethernet1/2.205	Ethernet1/2.205	102	Entrée uniquement	Requêtes d’écho ICMP de l’hôte 192.0.2.100 vers l’hôte 198.51.100.100

Configurez et vérifiez une capture de paquets sur la sous-interface Portchannel1 avec les interfaces membres Ethernet1/3 et Ethernet1/4	Ethernet1/3 Ethernet1/4	1001	Entrée uniquement	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



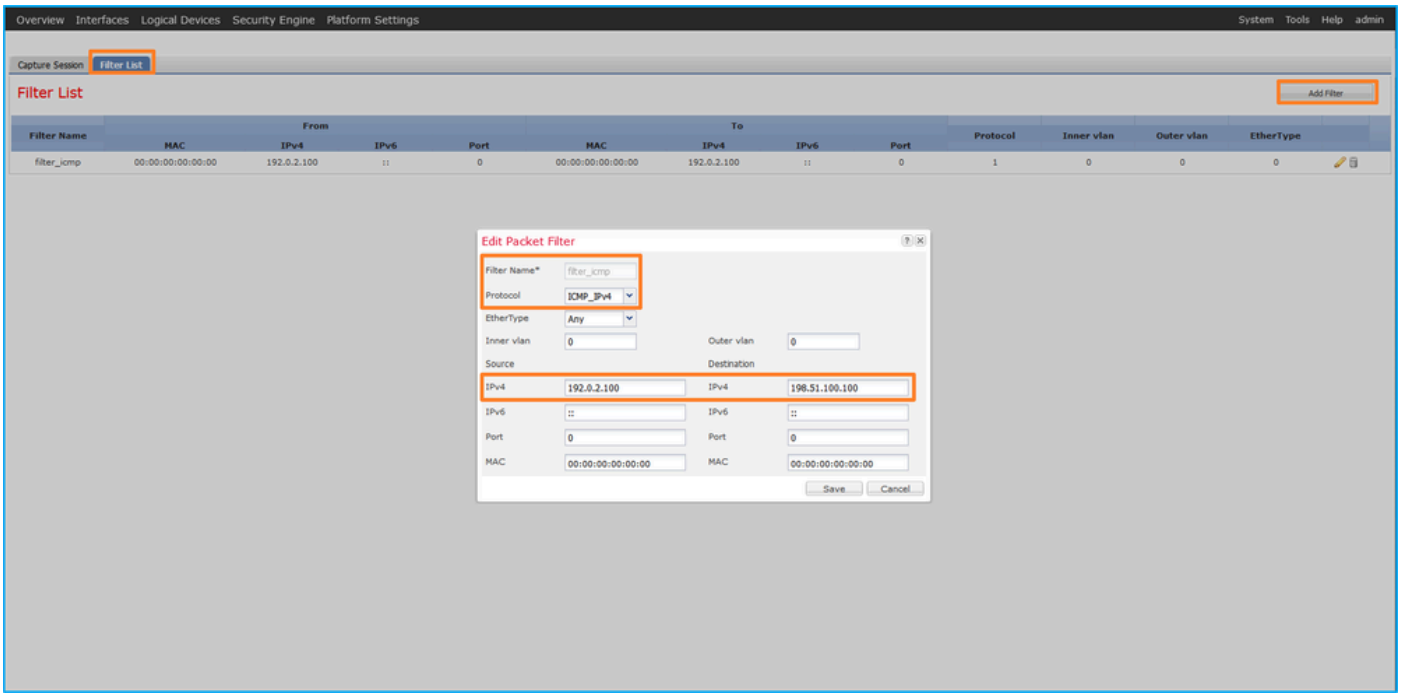
Configuration

FCM

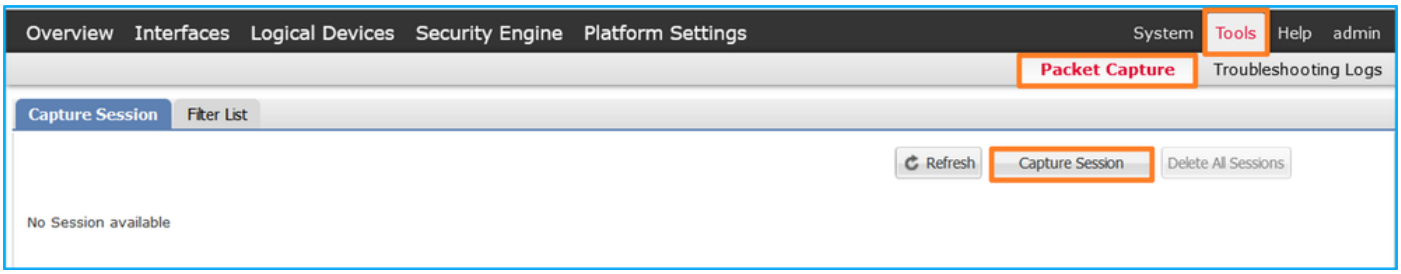
Exécutez ces étapes sur FCM pour configurer un filtre de capture pour les paquets de requête d'écho ICMP de l'hôte 192.0.2.100 à l'hôte 198.51.100.100 et l'appliquer à la capture de paquets sur l'interface Ethernet1/2 :

1. Utilisez Outils > Capture de paquets > Liste de filtres > Ajouter un filtre pour créer un filtre de capture.

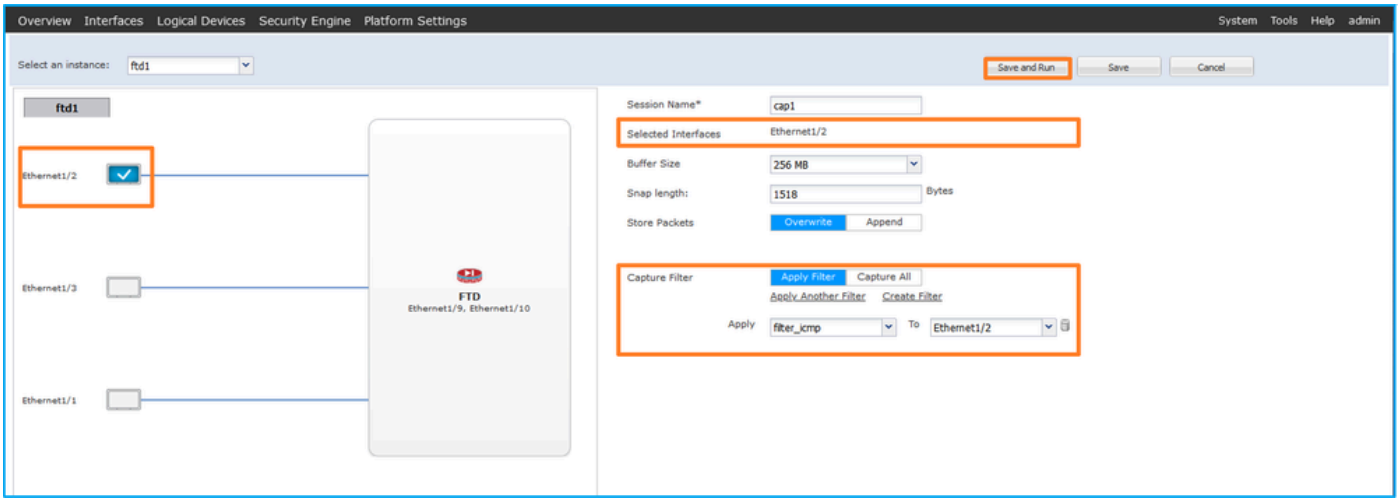
2. Spécifiez le nom du filtre, le protocole, l'IPv4 source, l'IPv4 de destination et cliquez sur Enregistrer :



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 :

```
<#root>

firepower#

scope ssa

firepower /ssa#

show app-instance

App Name   Identifier Slot ID    Admin State Oper State       Running Version Startup Version Deploy Ty
---------- ---------- ---------- ----------- ---------------- --------------- --------------- ---------

ftd        ftd1

       1          Enabled     Online           7.2.0.82        7.2.0.82        Native      No
```

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 :

```
<#root>

firepower#

scope packet-capture

firepower /packet-capture #

create filter filter_icmp

firepower /packet-capture/filter* #

set destip 198.51.100.100

firepower /packet-capture/filter* #

set protocol 1

firepower /packet-capture/filter* #

set srcip 192.0.2.100

firepower /packet-capture/filter* #

exit

firepower /packet-capture* #
```

```
create session cap1

firepower /packet-capture/session* #
create phy-port Ethernet1/2

firepower /packet-capture/session/phy-port* #
set app ftd

firepower /packet-capture/session/phy-port* #
set app-identifier ftd1

firepower /packet-capture/session/phy-port* #
set filter filter_icmp

firepower /packet-capture/session/phy-port* #
exit

firepower /packet-capture/session* #
enable

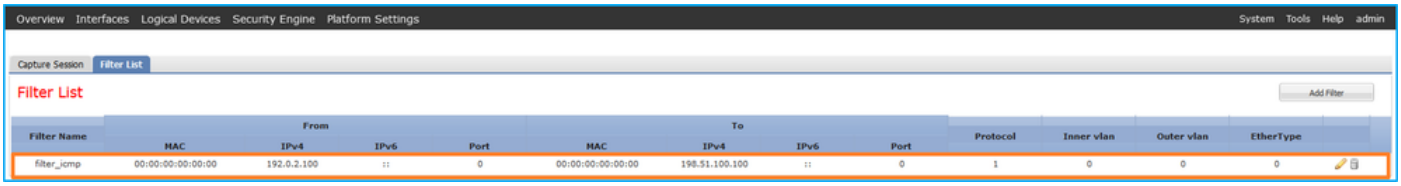
firepower /packet-capture/session* #
commit

firepower /packet-capture/session #
```

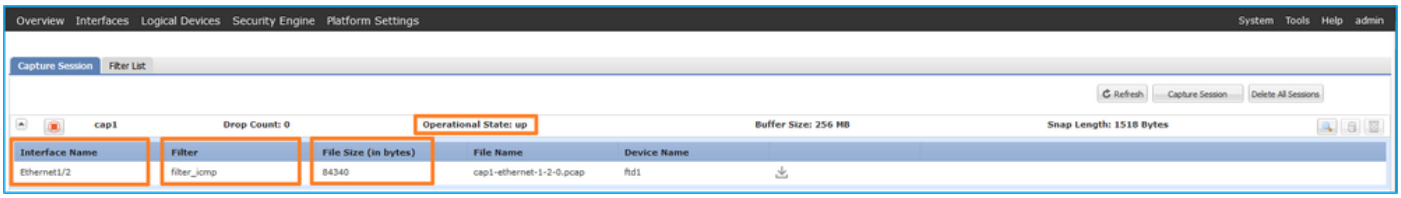
Vérification

FCM

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



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 :



CLI FXOS

Vérifiez les détails de capture dans la portée packet-capture :

<#root>

firepower#

scope packet-capture

firepower /packet-capture #

show filter detail

Configure a filter for packet capture:

Name: filter_icmp

    Protocol: 1

    Ivlan: 0
    Ovlan: 0

Src Ip: 192.0.2.100

    Dest Ip: 198.51.100.100

    Src MAC: 00:00:00:00:00:00
    Dest MAC: 00:00:00:00:00:00
    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 interne du commutateur Firepower 4100/9300.

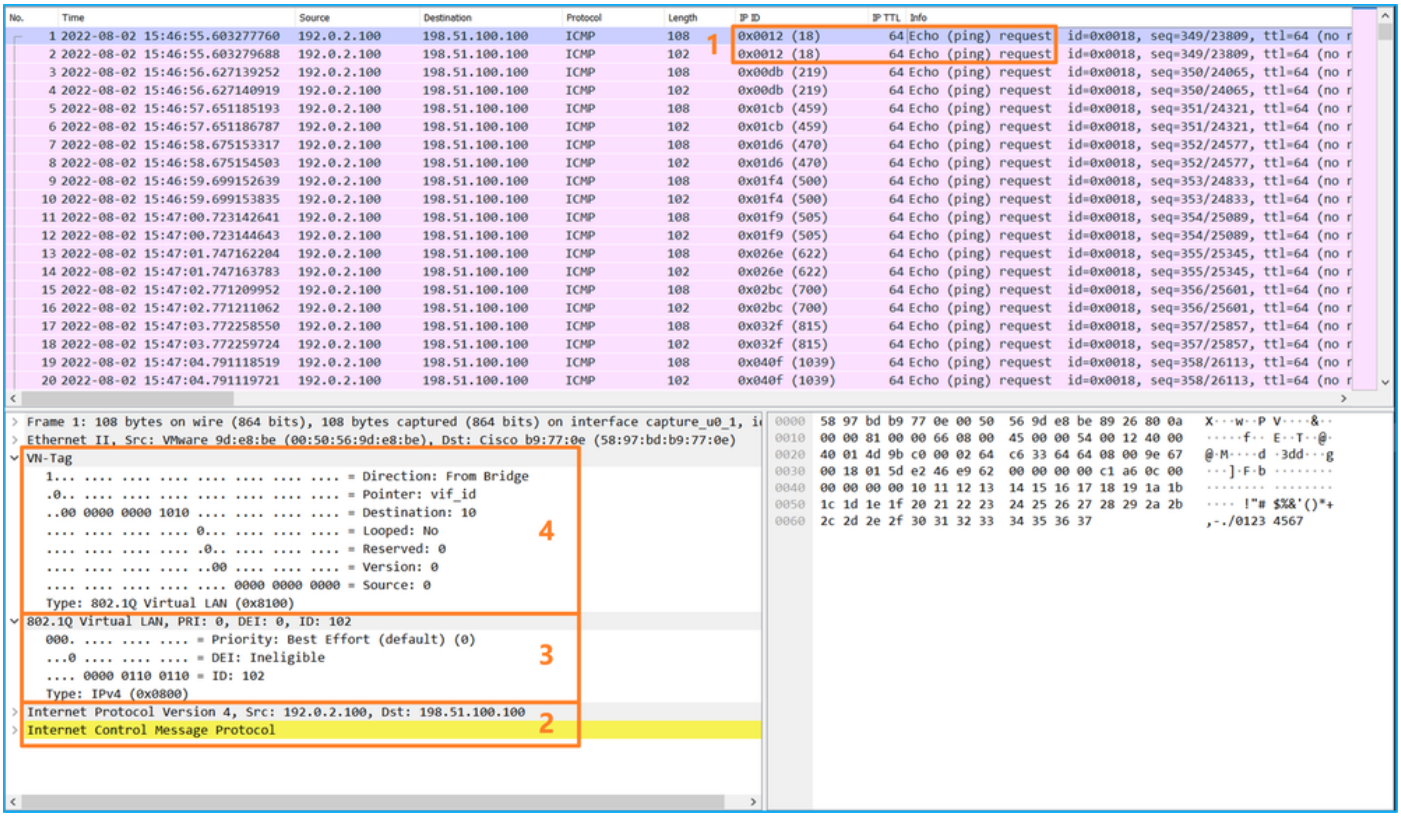
Capturer l'analyse des fichiers

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

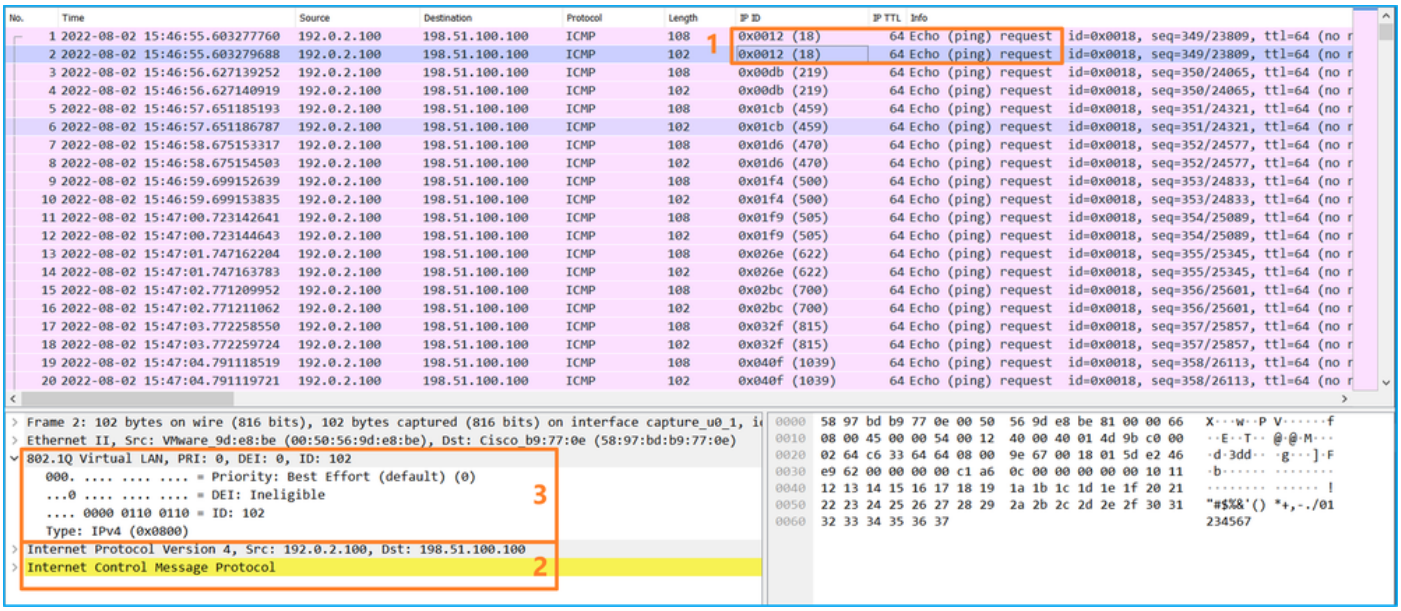
affiché 2 fois.

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.



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.



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 :

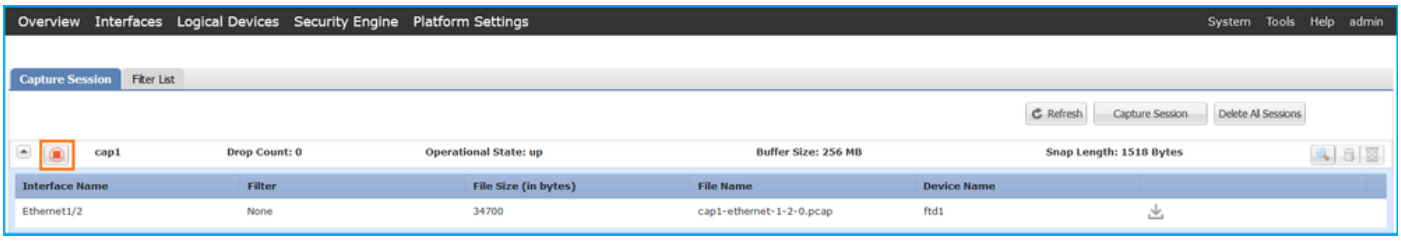
Tâche	Point de capture	VLAN de port interne dans les paquets capturés	Direction	Filtre utilisateur	Trafic capturé
Configurer et vérifier une capture de paquets avec un filtre sur l'interface avant Ethernet1/2	Ethernet1/2	102	Entrée uniquement	Protocole : ICMP Source : 192.0.2.100 Destination : 198.51.100.100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

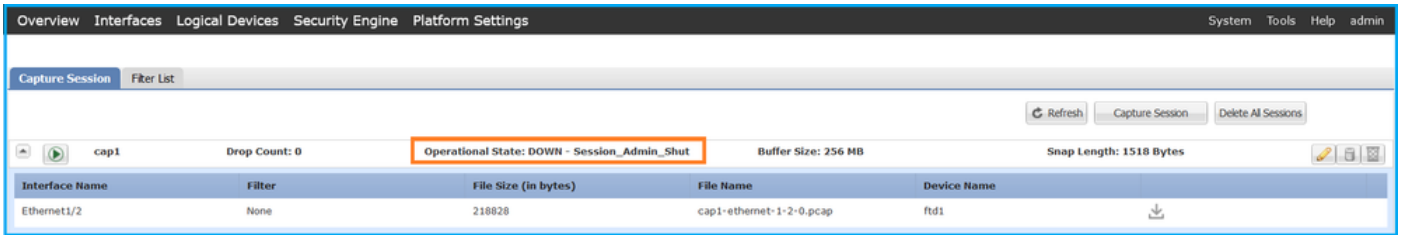
FCM

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

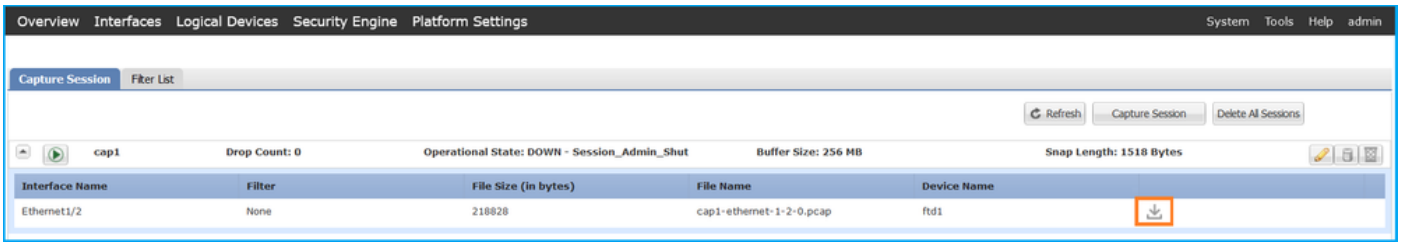
1. Cliquez sur le bouton Disable Session pour arrêter la capture active :



2. Assurez-vous 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 :

```
<#root>

firepower#

scope packet-capture

firepower /packet-capture #

scope session cap1
```

```
firepower /packet-capture/session #
disable

firepower /packet-capture/session* #
commit

firepower /packet-capture/session #
up

firepower /packet-capture #
show session cap1 detail


Traffic Monitoring Session:
    Packet Capture Session Name:
cap1

    Session: 1
    Admin State: Disabled

    Oper State: Down

    Oper State Reason: Admin Disable

    Config Success: Yes
    Config Fail Reason:
    Append Flag: Overwrite
    Session Mem Usage: 256  MB
    Session Pcap Snap Len: 1518  Bytes
    Error Code: 0
    Drop Count: 0

Physical ports involved in Packet Capture:
    Slot Id: 1
    Port Id: 2
    Pcapfile:
/workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap

    Pcapsize: 115744  bytes
    Filter:
    Sub Interface: 0
    Application Instance Identifier: ftd1
    Application Name: ftd
```

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

```
<#root>

firepower#

connect local-mgmt


firepower(local-mgmt)#

copy /packet-capture/session-1/cap1-ethernet-1-2-0.pcap ?


  ftp:        Dest File URI
  http:       Dest File URI
  https:      Dest File URI
  scp:        Dest File URI
  sftp:       Dest File URI
  tftp:       Dest File URI
  usbdrive:   Dest File URI
  volatile:   Dest File URI
  workspace:  Dest File URI

firepower(local-mgmt)#

copy /packet-capture/session-1/cap1-ethernet-1-2-0.pcap ftp://ftpuser@10.10.10.1/cap1-ethernet-1-2-0.pca


Password:
```

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

Recommandations, limites et meilleures pratiques pour la capture des paquets internes du commutateur

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 de nombre d'abandons augmente.
- Utilisez le filtre !vntag sur Wireshark pour afficher uniquement les paquets sans le VN-tag. 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 Secure Firewall 1200/3100/4200

À la différence de Firepower 4100/9300, les captures internes du pare-feu sécurisé 1200/3100/4200 sont configurées sur l'interface de ligne de commande de l'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 :

<#root>

```
> capture cap_sw switch

 ?
  buffer         Configure size of capture buffer, default is 256MB
  ethernet-type  Capture Ethernet packets of a particular type, default is IP
  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 :

<#root>

>

capture capsw switch interface ?

```
Available interfaces to listen:
  in_data_uplink1  Capture packets on internal data uplink1 interface
  in_mgmt_uplink1  Capture packets on internal mgmt uplink1 interface
  inside           Name of interface Ethernet1/1.205

  management       Name of interface Management1/1
```

Le pare-feu sécurisé 1200/4200 prend en charge les captures bidirectionnelles. La valeur par défaut est ingress, sauf indication contraire :

<#root>

>

capture capi switch interface inside direction

```
  both     To capture switch bi-directional traffic
  egress   To capture switch egressing traffic
  ingress  To capture switch ingressing traffic
```

En outre, le pare-feu sécurisé 4245 dispose de 2 interfaces de données internes et de 2 interfaces de gestion de liaison ascendante :

<#root>

>

capture capsw switch interface

```
  eventing         Name of interface Management1/2
  in_data_uplink1  Capture packets on internal data uplink1 interface
  in_data_uplink2  Capture packets on internal data uplink2 interface
  in_mgmt_uplink1  Capture packets on internal mgmt uplink1 interface
  in_mgmt_uplink2  Capture packets on internal mgmt uplink2 interface
  management       Name of 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 :

```
<#root>

>

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 :

```
<#root>

>

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 :

```
<#root>

>

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.

```
<#root>

>

show capture capsw


27 packet captured on disk using switch capture

Reading of capture file from disk is not supported

>

show capture capsw  detail

Packet Capture info
  Name:              capsw

  Session:           1
  Admin State:       enabled


  Oper State:        up
```

```
Oper State Reason: Active

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

Total Physical ports involved in Packet Capture: 1
Physical port:
  Slot Id:           1
  Port Id:           1

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

  Pcapsize:          18838

  Filter:            capsw-1-1

Packet Capture Filter Info

  Name:              capsw-1-1

  Protocol:          0
  Ivlan:             0

Ovlan:             205

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

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

7. Arrêtez les captures si nécessaire :

<#root>

>

capture capsw switch stop

>

show capture capsw detail

Packet Capture info

  Name: **capsw**

  Session: 1

  Admin State: **disabled**

  Oper State: **down**

  Oper State Reason: **Session_Admin_Shut**

  Config Success: yes
  Config Fail Reason:
  Append Flag: overwrite
  Session Mem Usage: 256
  Session Pcap Snap Len: 1518
  Error Code: 0
  Drop Count: 0
Total Physical ports involved in Packet Capture: 1

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

Packet Capture Filter Info
  Name: capsw-1-1
  Protocol: 0
  Ivlan: 0
  Ovlan: 205
  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 du pare-feu sécurisé.

Dans la version 7.7 du logiciel Secure Firewall, la configuration de capture interne du commutateur n'est pas prise en charge sur le FMC ou le 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.

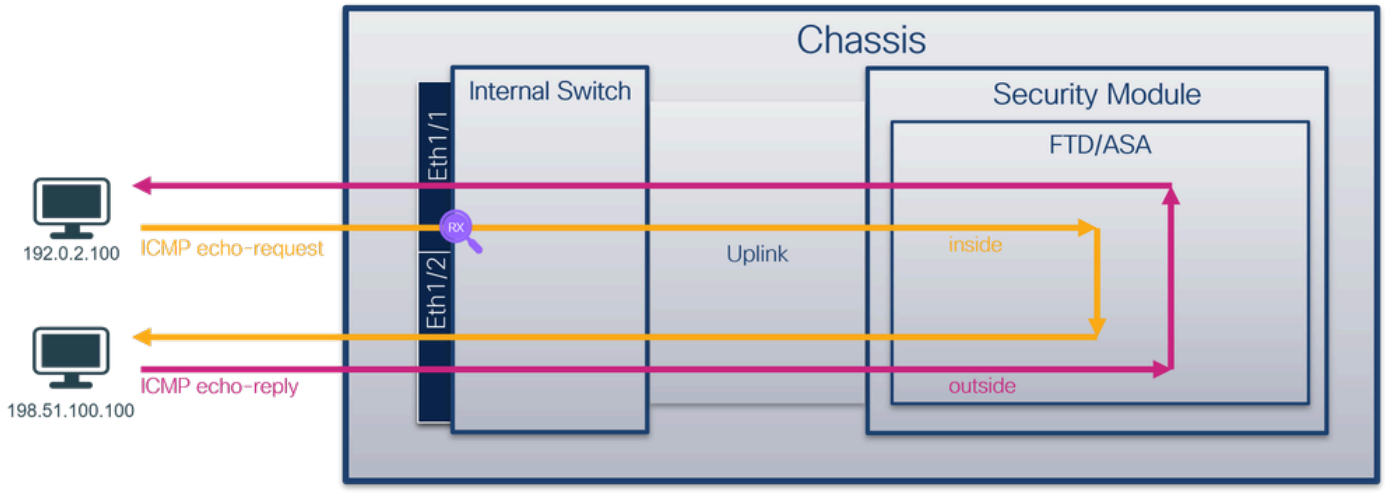
Ces scénarios couvrent les cas d'utilisation courants des captures internes du commutateur Secure Firewall 1200/3100/4200.

Capture de paquets sur une interface physique ou Port Channel

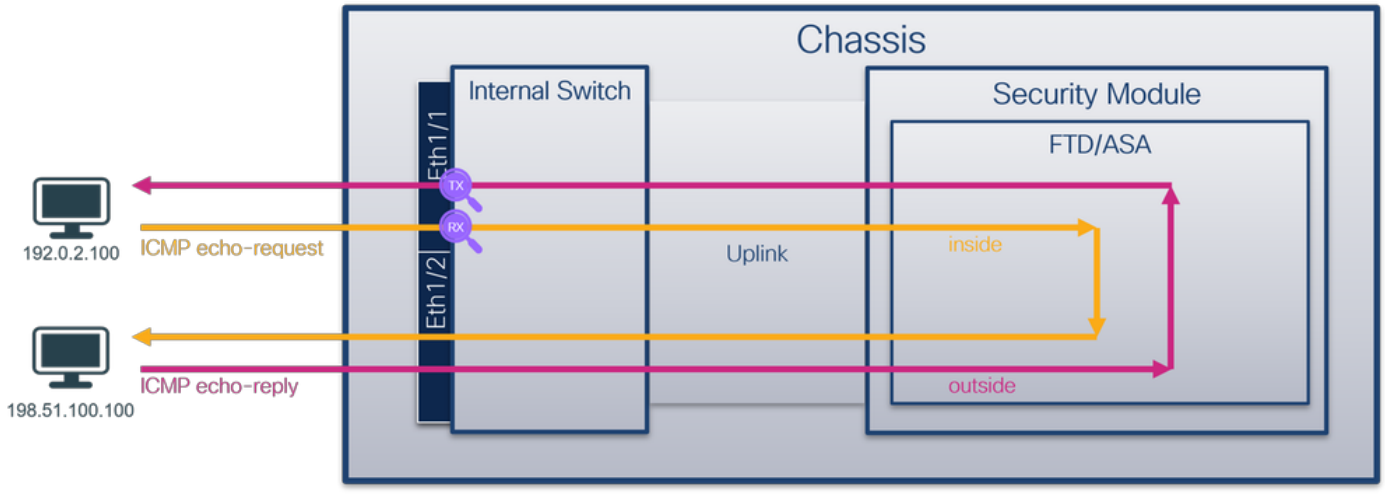
Utilisez l'interface de ligne de commande FTD ou ASA pour configurer et vérifier une capture de paquets sur l'interface Ethernet1/1 ou l'interface Portchannel1. Les deux interfaces portent le nom if inside.

Topologie, flux de paquets et points de capture

Secure Firewall 3100 :



Pare-feu sécurisé 1200/4200 :



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 :

```
<#root>

>

show nameif

Interface                  Name                       Security
Ethernet1/1                inside                     0

Ethernet1/2                outside                    0
Management1/1              diagnostic                 0
```

```
<#root>

>

show nameif

Interface                  Name                       Security
Port-channel1              inside                     0

Ethernet1/2                outside                    0
Management1/1              diagnostic                 0
```

2. Créer une session de capture

```
<#root>

>

capture capsw switch interface inside
```

Le pare-feu sécurisé 1200/4200 prend en charge la directionnalité de capture :

```
<#root>

> capture capsw switch interface inside direction ?
```

```
  both To capture switch bi-directional traffic
  egress To capture switch egressing traffic
  ingress To capture switch ingressing traffic
```

```
> capture capsw switch interface inside direction both
```

3. Activez la session de capture :

<#root>

```
> 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 :

<#root>

```
>
show capture capsw detail

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

```
  Port Id:           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
```

Pare-feu sécurisé 1200/4200 :

<#root>

>

 show cap 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:          0


Direction:         both


  Drop:              disable
  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

33 packet 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 :

```
<#root>

>

show capture capsw detail


Packet Capture info

  Name:              capsw
```

```
  Session:           1
  Admin State:       enabled


  Oper State:        up


  Oper State Reason: Active


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

Total Physical ports involved in Packet Capture: 2

Physical port:
  Slot Id:           1


  Port Id:           4


  Pcapfile:          /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-4-0.pcap
  Pcapsize:          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 de port-channel peuvent être vérifiées dans l'interpréteur de commandes FXOS local-mgmt via la commande show portchannel summary :

```
<#root>

>

connect fxos


…
firewall#

connect local-mgmt


firewall(local-mgmt)#

show portchannel summary


Flags:  D - Down        P - Up in port-channel (members)
I - Individual  H - Hot-standby (LACP only)
s - Suspended   r - Module-removed
S - Switched    R - Routed
U - Up (port-channel)
M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
```

```
------------------------------------------------------------------------------
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.

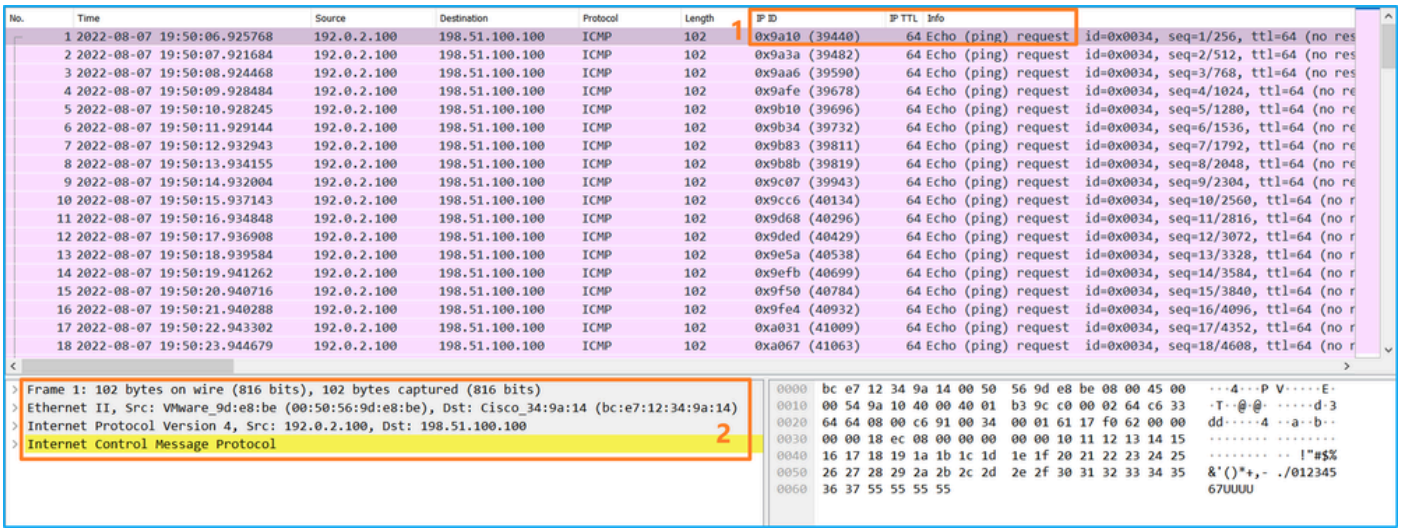
Collecter les fichiers de capture

Suivez les étapes de la section Collecter les fichiers de capture internes du commutateur du pare-feu sécurisé.

Capturer l'analyse des fichiers

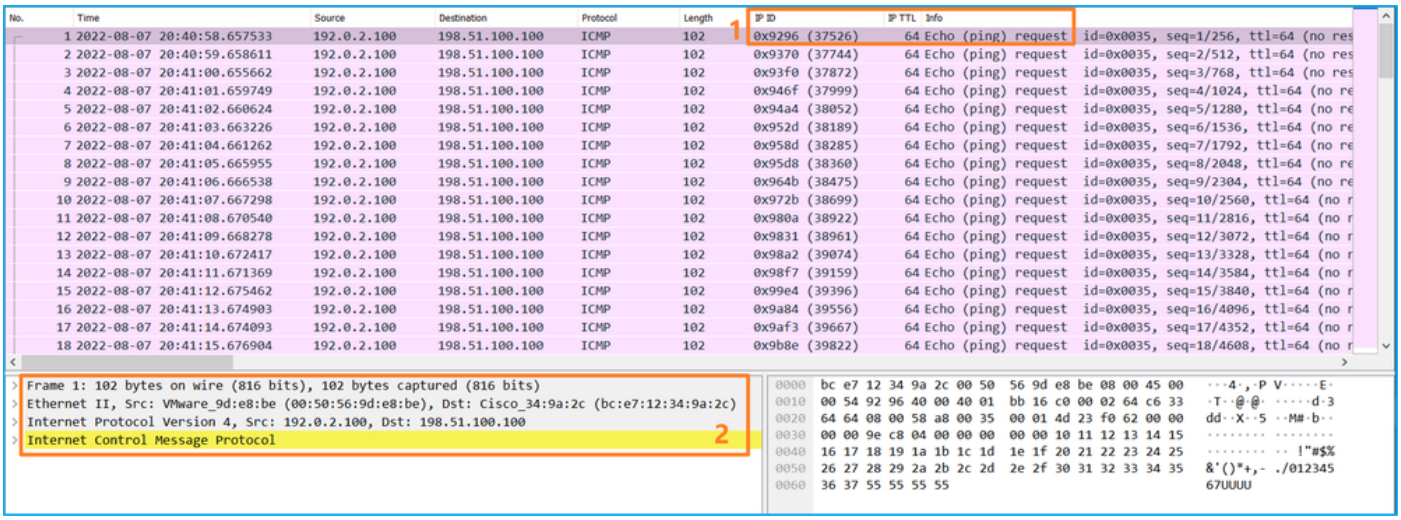
Utilisez une application de lecture de fichiers de capture de paquets pour ouvrir les fichiers de capture pour Ethernet1/1. Dans cet exemple, les paquets capturés sur le pare-feu sécurisé 3100 sont analysés. Sélectionnez le premier paquet et vérifiez les points clés :

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

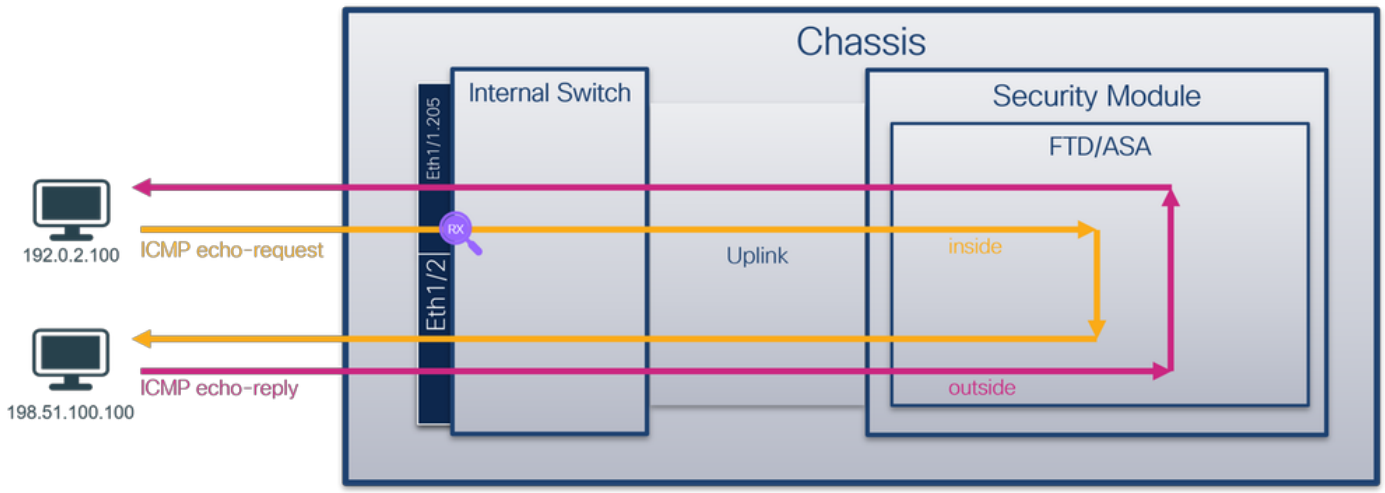
* Contrairement au modèle 3100, le pare-feu sécurisé 1200/4200 prend en charge les captures bidirectionnelles (entrée et sortie).

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

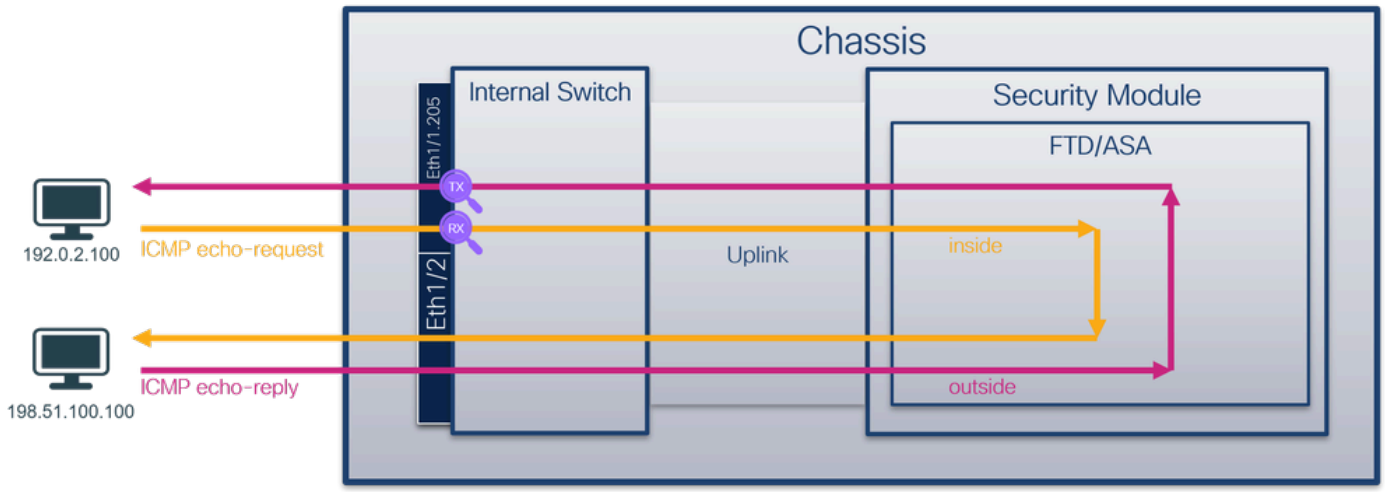
Utilisez la CLI FTD ou ASA pour configurer et vérifier une capture de paquets sur les sous-interfaces Ethernet1/1.205 ou Portchannel1.205. Les deux sous-interfaces portent le nom if inside.

Topologie, flux de paquets et points de capture

Secure Firewall 3100 :



Pare-feu sécurisé 1200/4200 :



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 :

```
<#root>

>

show nameif

Interface                  Name                       Security
Ethernet1/1.205            inside                     0

Ethernet1/2                outside                    0
Management1/1              diagnostic                 0
```

<#root>

>

show nameif

```
Interface                Name                    Security
Port-channel1.205        inside                    0

Ethernet1/2              outside                   0
Management1/1            diagnostic                0
```

2. Créez une session de capture :

<#root>

>

capture capsw switch interface inside

Le pare-feu sécurisé 1200/4200 prend en charge la directionnalité de capture :

<#root>

> capture capsw switch interface inside direction ?

```
  both To capture switch bi-directional traffic
  egress To capture switch egressing traffic
  ingress To capture switch ingressing traffic
```

> capture capsw switch interface inside direction both

3. Activez la session de capture :

<#root>

> 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 :

<#root>

>

show capture capsw detail

Packet Capture info

Name: **capsw**

Session: 1

Admin State: **enabled**

Oper State: **up**

Oper State Reason: **Active**

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

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: **1**

Port Id: **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 :

```
<#root>

>

show capture capsw detail


Packet Capture info

  Name:              capsw

  Session:           1

  Admin State:       enabled


  Oper State:        up


  Oper State Reason: Active


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

Total Physical ports involved in Packet Capture: 2

Physical port:

  Slot Id:           1


  Port Id:           4
```

```
  Pcapfile:          /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-4-0.pcap
  Pcapsize:          23442

  Filter:            capsw-1-4

Packet Capture 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 de port-channel peuvent être vérifiées dans l'interpréteur de commandes FXOS local-mgmt via la commande show portchannel summary :

```
<#root>

>

connect fxos


…
firewall#

connect local-mgmt


firewall(local-mgmt)#

show portchannel summary


Flags:  D - Down        P - Up in port-channel (members)
I - Individual  H - Hot-standby (LACP only)
s - Suspended   r - Module-removed
S - Switched    R - Routed
U - Up (port-channel)
M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------

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.

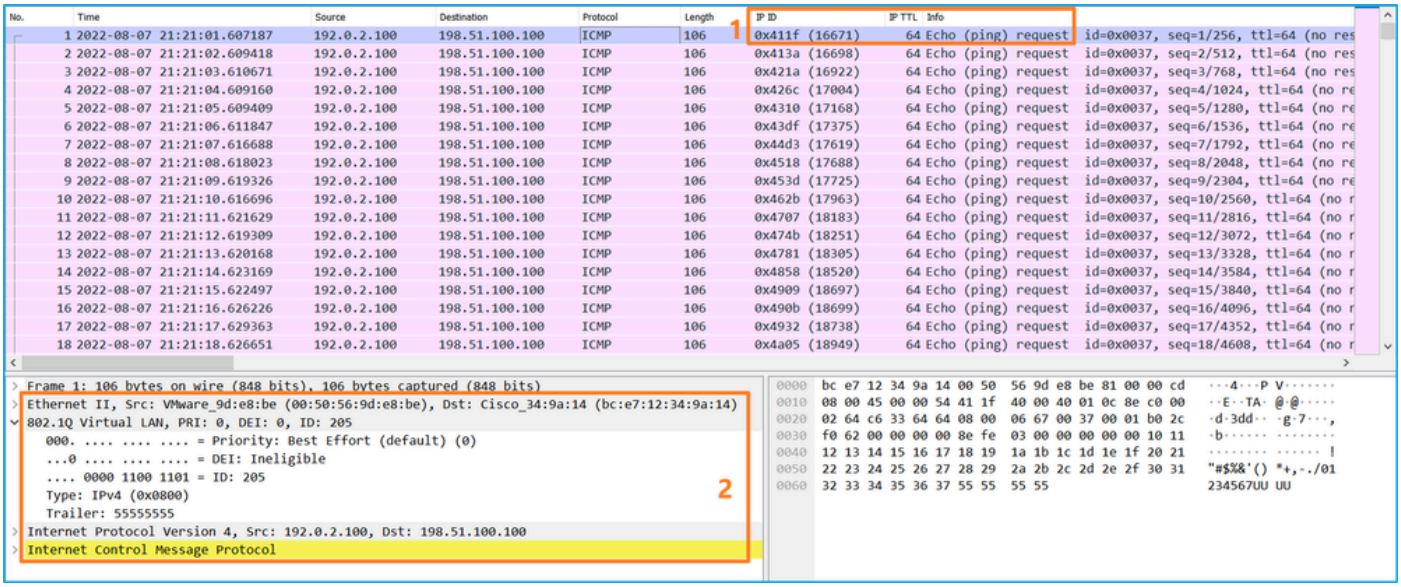
Collecter les fichiers de capture

Suivez les étapes de la section Collecter les fichiers de capture internes du commutateur du pare-feu sécurisé.

Capturer l'analyse des fichiers

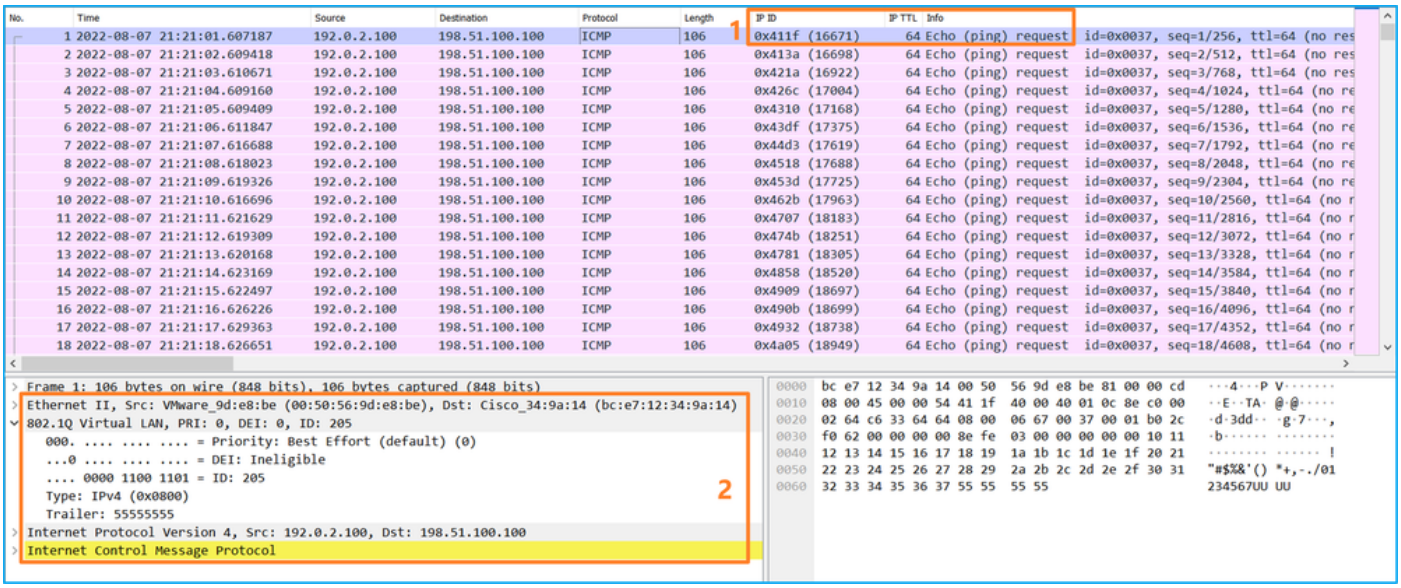
Utilisez une application de lecture de fichiers de capture de paquets pour ouvrir les fichiers de capture pour Ethernet1/1.205. Dans cet exemple, les paquets capturés sur le pare-feu sécurisé 3100 sont analysés. Sélectionnez le premier paquet et vérifiez les points clés :

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



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.



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	Ethernet1/1	VLAN externe 205	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 la sous-interface Portchannel1.205 avec les interfaces membres Ethernet1/3 et Ethernet1/4	Ethernet1/3 Ethernet1/4	VLAN externe 205	Entrée uniquement*	Requêtes d'écho ICMP de l'hôte 192.0.2.100 vers l'hôte 198.51.100.100

* Contrairement au modèle 3100, le pare-feu sécurisé 1200/4200 prend en charge les captures bidirectionnelles (entrée et sortie).

Capture de paquets sur des interfaces internes

Le pare-feu sécurisé 3100 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.

Le pare-feu sécurisé 1200 comporte jusqu'à 3 interfaces internes :

- in_data_uplink1 - spécifiques à 1210 et 1250, ces interfaces connectent l'application au commutateur interne.
- in_data_uplink1, in_data_uplink2, in_data_uplink3 et in_mgmt_uplink2 - spécifiques à 1220, 1230 et 1240, ces interfaces connectent l'application au commutateur interne.

Remarque : Comme l'interface de gestion du pare-feu Secure Firewall 1200 est hors bande, il n'existe aucune interface in_mgmt_uplink disponible sur ce modèle.

Le pare-feu sécurisé 4200 comporte jusqu'à 4 interfaces internes :

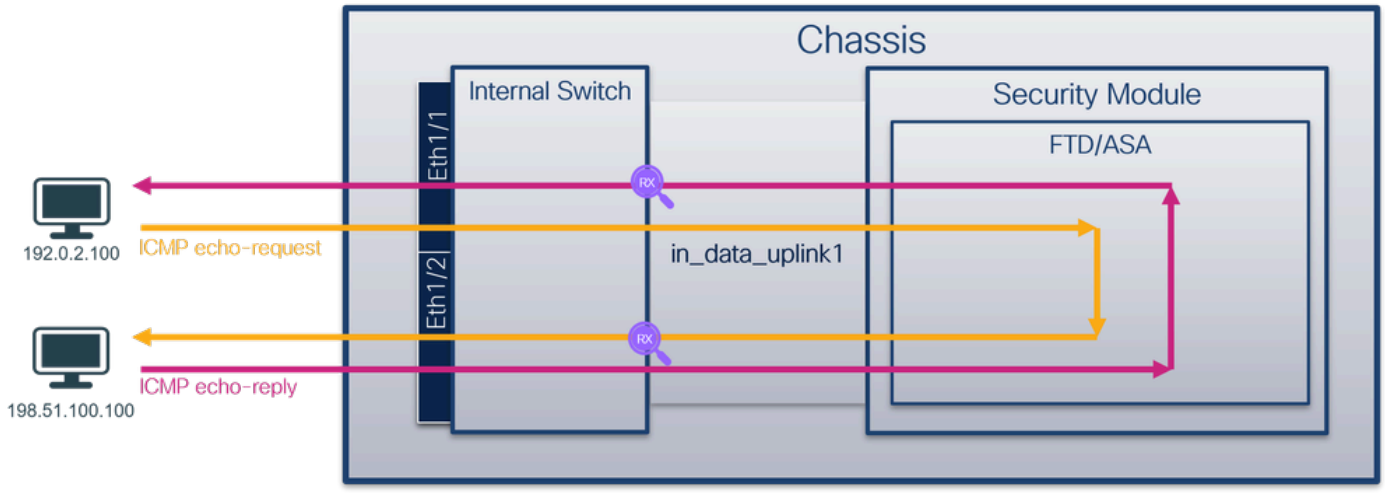
- in_data_uplink1 et in_data_uplink2 (4245 uniquement) : ces interfaces connectent l'application au commutateur interne. Dans le cas de la norme 4245, les paquets sont équilibrés en charge sur les deux interfaces de liaison ascendante.
- in_mgmt_uplink1 et in_mgmt_uplink2 - ces interfaces fournissent un chemin de paquets dédié pour les connexions de gestion, telles que SSH vers l'interface de gestion, ou la connexion de gestion, également appelée sftunnel, entre le FMC et le FTD. Le pare-feu sécurisé 4200 prend en charge 2 interfaces de gestion.

Tâche 1

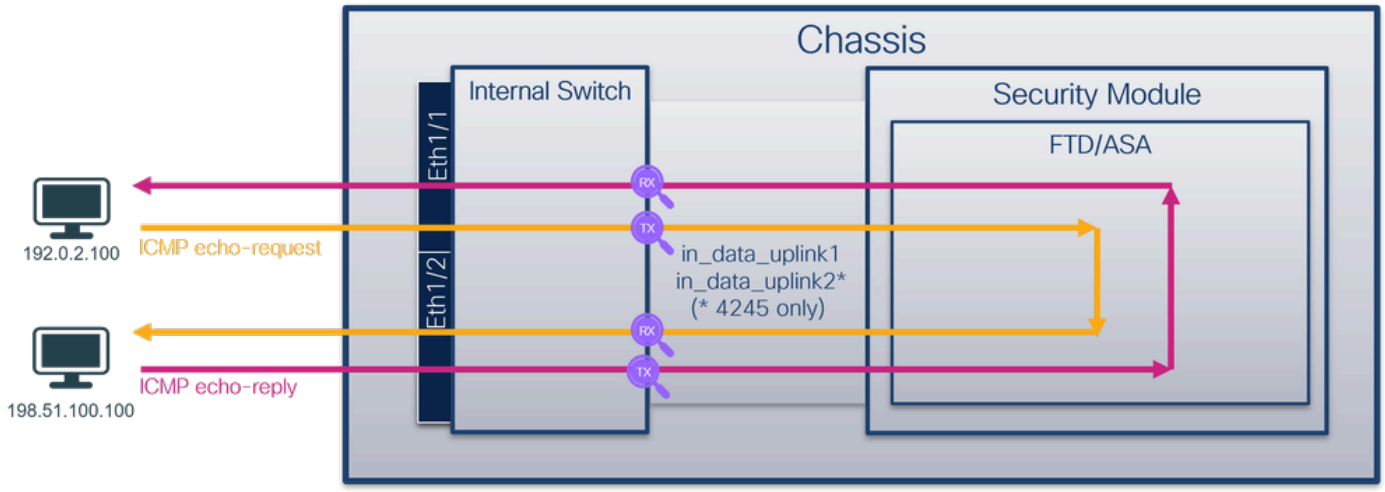
Utilisez l'interface de ligne de commande FTD ou ASA pour configurer et vérifier une capture de paquets sur des interfaces de liaison ascendante de données.

Topologie, flux de paquets et points de capture

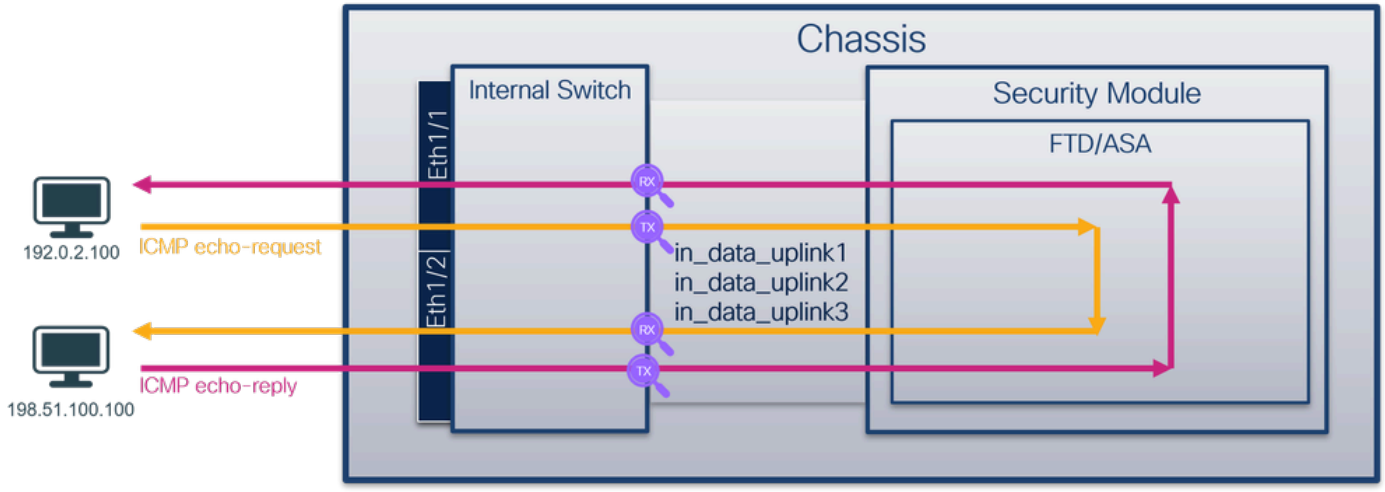
Secure Firewall 3100 :



Secure Firewall 4200 :



Pare-feu sécurisé 1200 :



Configuration

Exécutez ces étapes sur l'interface de ligne de commande ASA ou FTD pour configurer une capture de paquets sur les interfaces de liaison ascendante de données.

Notez que le pare-feu sécurisé 1210, 1250, 3100 et 4200 (excepté 4245) et ne disposent que d'une seule interface de liaison ascendante active dans_data_uplink1.

Le pare-feu sécurisé 1200 (sauf 1210 et 1250) et 4245 ont plusieurs interfaces de liaison ascendante in_data_uplink1, in_data_uplink2 et ainsi de suite. Veillez toujours à inclure toutes les interfaces de liaison ascendante de données.

Ceci est un résultat du pare-feu sécurisé 1220 :

```
<#root>

>

cap capsw switch interface ?


Available interfaces to listen:

in_data_uplink1

 Capture packets on internal data uplink1 interface

in_data_uplink2

 Capture packets on internal data uplink2 interface

in_data_uplink3

 Capture packets on internal data uplink3 interface
...
```

1. Créez une session de capture :

<#root>

>

capture capsw switch interface in_data_uplink1

Le pare-feu sécurisé 1200/4200 prend en charge la directionnalité de capture :

<#root>

> capture capsw switch interface in_data_uplink1 direction ?

```
  both To capture switch bi-directional traffic
  egress To capture switch egressing traffic
  ingress To capture switch ingressing traffic
```

> capture capsw switch interface in_data_uplink1 direction both

2. Activez la session de capture :

<#root>

> 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 :

<#root>

>

show capture capsw detail

```
Packet Capture info
  Name:              capsw
  Session:           1
  Admin State:       enabled
```

```
  Oper State:        up


  Oper State Reason: Active


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

Total Physical ports involved in Packet Capture: 1

Physical port:

  Slot Id:           1


  Port Id:           18


  Pcapfile:          /mnt/disk0/packet-capture/sess-1-capsw-data-uplink1.pcap

  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 :

<#root>

>

connect fxos

…
firewall#

connect local-mgmt

firewall(local-mgmt)#

show portmanager switch status

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

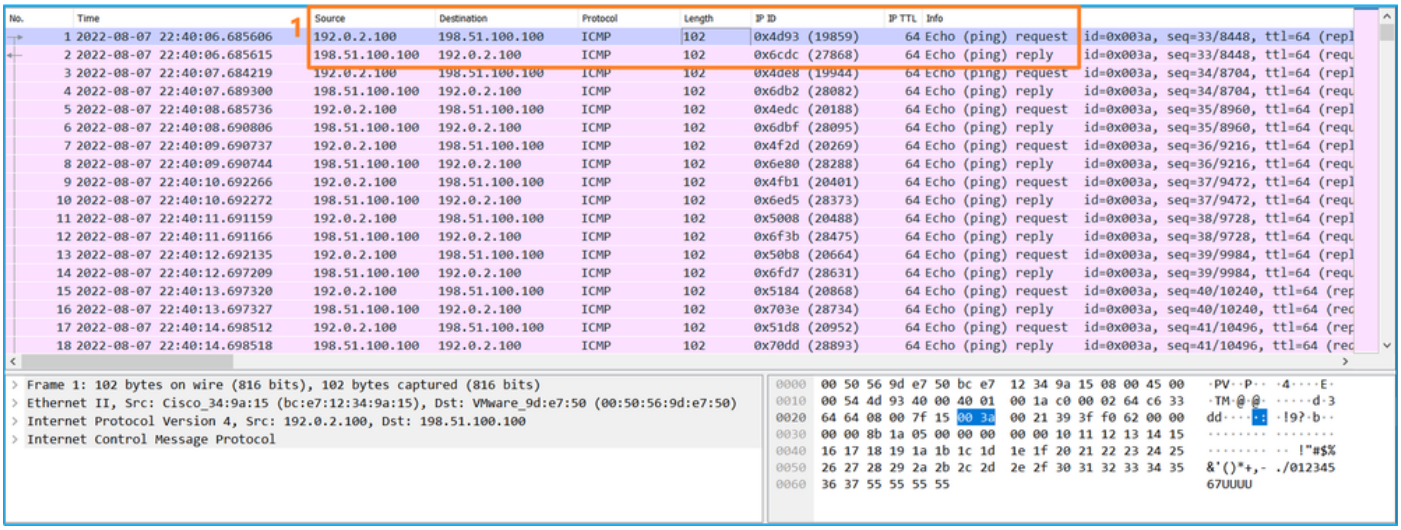
Collecter les fichiers de capture

Suivez les étapes de la section Collecter les fichiers de capture internes du commutateur du pare-feu sécurisé.

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_data_uplink1. Dans cet exemple, les paquets capturés sur le pare-feu sécurisé 3100 sont analysés.

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.



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

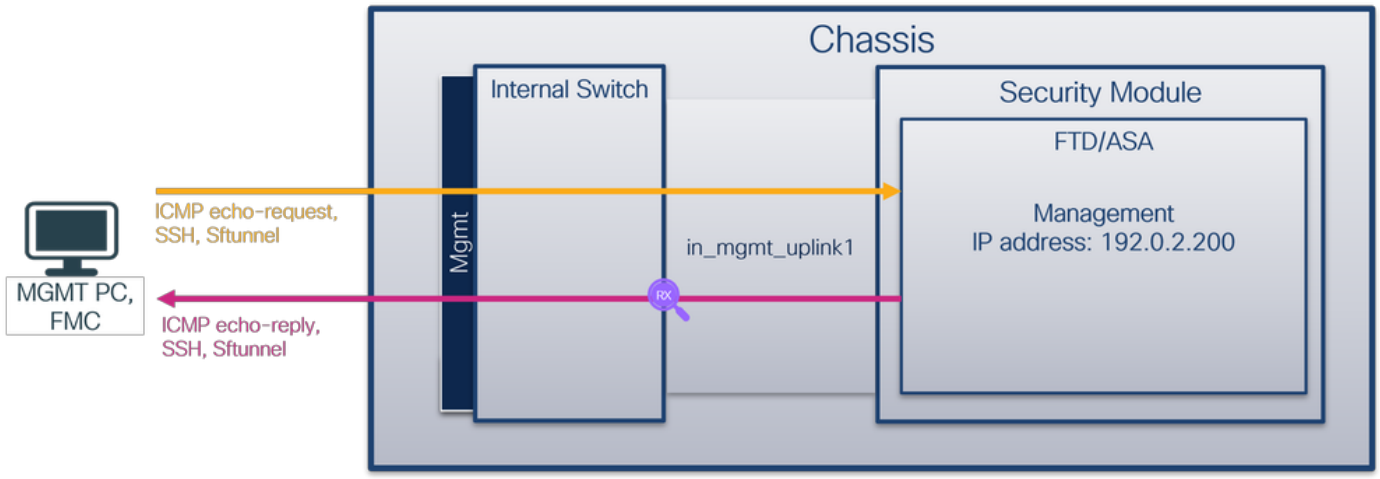
* Contrairement au modèle 3100, le pare-feu sécurisé 1200/4200 prend en charge les captures bidirectionnelles (entrée et sortie).

Tâche 2

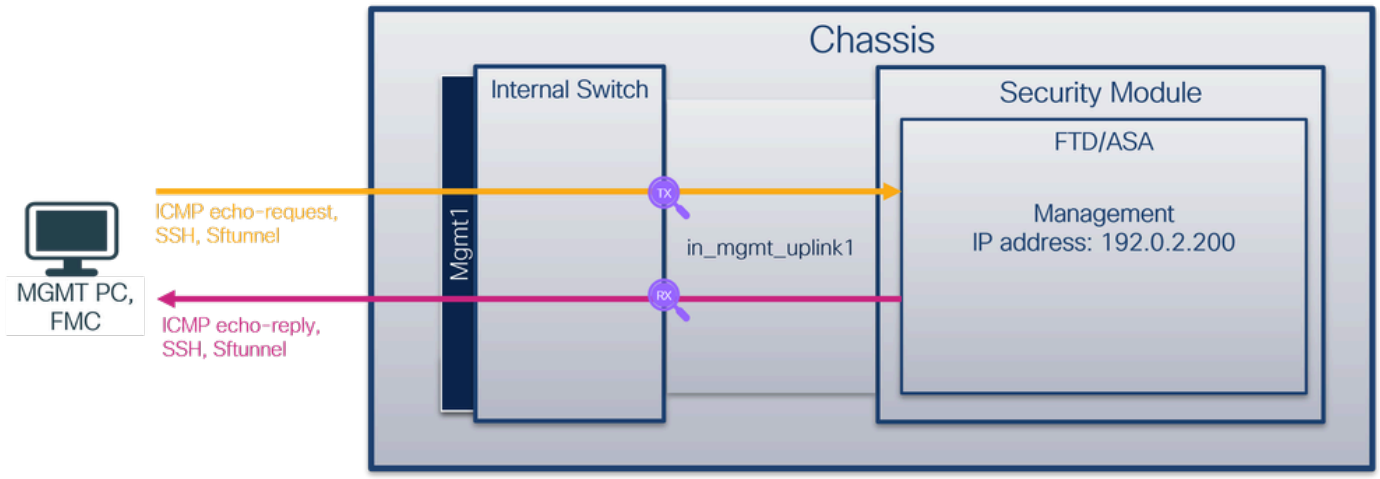
Utilisez l'interface de ligne de commande FTD ou ASA pour configurer et vérifier une capture de paquets sur l'interface de liaison ascendante in_mgmt_uplink1. Seuls les paquets des connexions du plan de gestion sont capturés.

Topologie, flux de paquets et points de capture

Secure Firewall 3100 :



Secure Firewall 4200 :



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 :

<#root>

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

Le pare-feu sécurisé 4200 prend en charge la directionnalité de capture :

<#root>

```
> capture capsw switch interface in_mgmt_uplink1 direction ?

  both To capture switch bi-directional traffic
  egress To capture switch egressing traffic
  ingress To capture switch ingressing traffic

> capture capsw switch interface in_mgmt_uplink1 direction both
```

2. Activez la session de capture :

<#root>

```
> 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 :

<#root>

```
> show capture capsw detail

Packet Capture info

Name:              capsw

  Session:           1

Admin State:       enabled

  Oper State:        up

  Oper State Reason: Active
```

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

Total Physical ports involved in Packet Capture: 1

Physical port:
  Slot Id:           1


  Port Id:           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 :

```
<#root>

>
```

```
connect fxos


…
firewall#
connect local-mgmt


firewall(local-mgmt)#
show portmanager switch status


Dev/Port         Mode        Link   Speed  Duplex  Loopback Mode  Port Manager
---------  ----------------  -----  -----  ------  -------------  ------------
0/1              SGMII         Up     1G     Full    None           Link-Up
0/2              SGMII         Up     1G     Full    None           Link-Up
0/3              SGMII         Up     1G     Full    None           Link-Up
0/4              SGMII         Up     1G     Full    None           Link-Up
0/5              SGMII       Down     1G     Half    None           Mac-Link-Down
0/6              SGMII       Down     1G     Half    None           Mac-Link-Down
0/7              SGMII       Down     1G     Half    None           Mac-Link-Down
0/8              SGMII       Down     1G     Half    None           Mac-Link-Down
0/9           1000_BaseX     Down     1G     Full    None           Link-Down
0/10          1000_BaseX     Down     1G     Full    None           Link-Down
0/11          1000_BaseX     Down     1G     Full    None           Link-Down
0/12          1000_BaseX     Down     1G     Full    None           Link-Down
0/13          1000_BaseX     Down     1G     Full    None           Link-Down
0/14          1000_BaseX     Down     1G     Full    None           Link-Down
0/15          1000_BaseX     Down     1G     Full    None           Link-Down
0/16          1000_BaseX     Down     1G     Full    None           Link-Down
0/17          1000_BaseX       Up     1G     Full    None           Link-Up
0/18             KR2           Up     50G    Full    None           Link-Up
0/19              KR           Up     25G    Full    None           Link-Up


0/20              KR           Up     25G    Full    None           Link-Up
0/21             KR4         Down     40G    Full    None           Link-Down
0/22             n/a         Down     n/a    Full    N/A            Reset
0/23             n/a         Down     n/a    Full    N/A            Reset
0/24             n/a         Down     n/a    Full    N/A            Reset
0/25          1000_BaseX     Down     1G     Full    None           Link-Down
0/26             n/a         Down     n/a    Full    N/A            Reset
0/27             n/a         Down     n/a    Full    N/A            Reset
0/28             n/a         Down     n/a    Full    N/A            Reset
0/29          1000_BaseX     Down     1G     Full    None           Link-Down
0/30             n/a         Down     n/a    Full    N/A            Reset
0/31             n/a         Down     n/a    Full    N/A            Reset
0/32             n/a         Down     n/a    Full    N/A            Reset
0/33          1000_BaseX     Down     1G     Full    None           Link-Down
0/34             n/a         Down     n/a    Full    N/A            Reset
0/35             n/a         Down     n/a    Full    N/A            Reset
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.

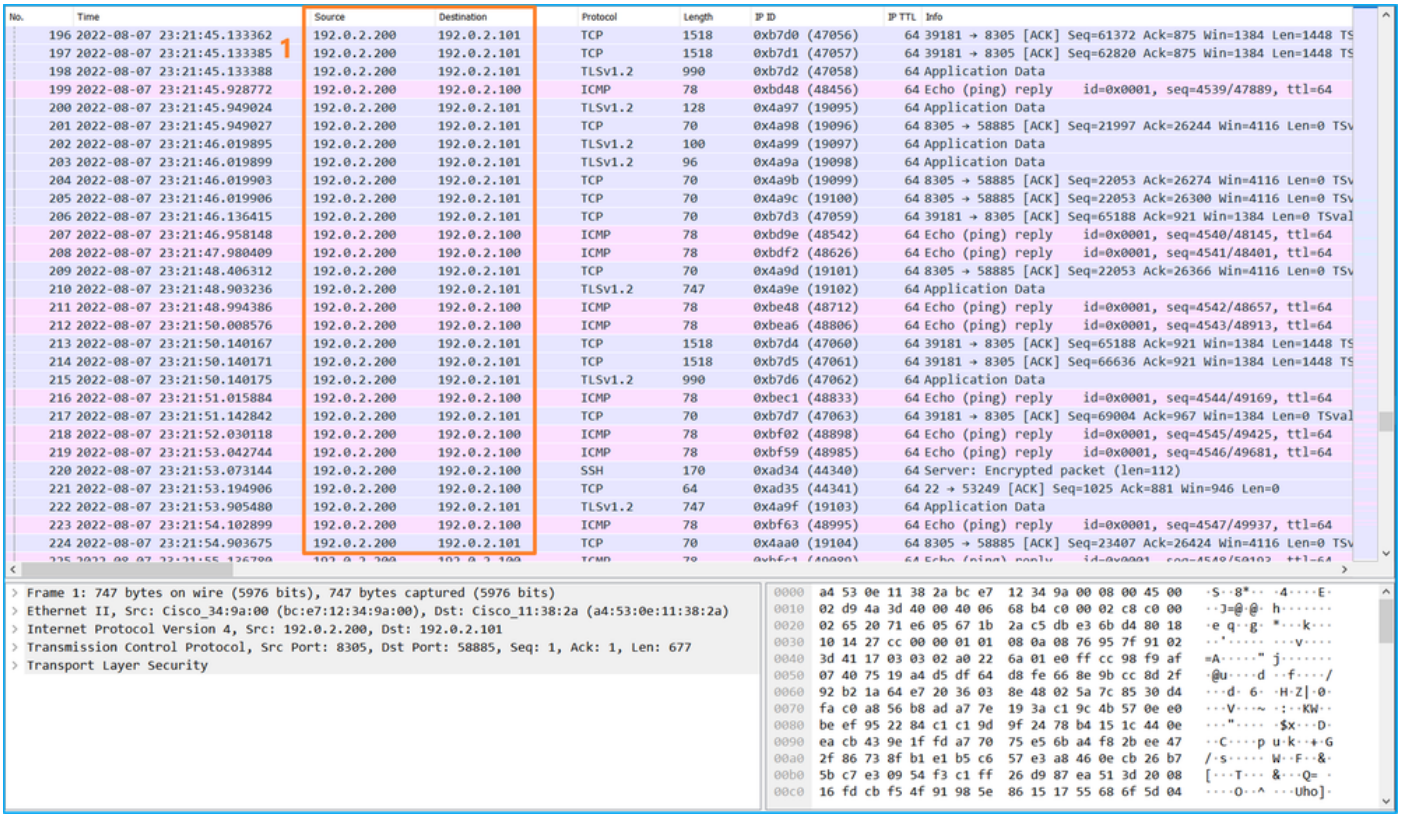
Collecter les fichiers de capture

Suivez les étapes de la section Collecter les fichiers de capture internes du commutateur du pare-feu sécurisé .

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. Dans cet exemple, les paquets capturés sur le pare-feu sécurisé 3100 sont analysés.

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.



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	in_mgmt_uplink1	Aucune	Entrée uniquement* (de l'interface de	Réponses d'écho ICMP de l'adresse IP de gestion FTD

capture de paquets sur l'interface de gestion de liaison ascendante			gestion au réseau via le commutateur interne)	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 192.0.2.101 SSH de l'adresse IP de gestion FTD 192.0.2.200 vers l'hôte 192.0.2.100

* Contrairement au modèle 3100, le pare-feu sécurisé 1200/4200 prend en charge les captures bidirectionnelles (entrées et sorties).

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

Exécutez 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 :

```
<#root>

>

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 :

```
<#root>

>

capture capsw switch interface inside ethernet-type arp
```

<#root>

> 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 :

<#root>

>

show capture capsw detail

```
Packet Capture info
 Name:              capsw

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

Total Physical ports involved in Packet Capture: 1

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

Filter:            capsw-1-1


Packet Capture Filter Info


  Name:              capsw-1-1


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

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

Ethertype:         2054


Total Physical breakout ports involved in Packet Capture: 0

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 le protocole ICMP :

```
<#root>

>

show capture capsw detail


Packet Capture info

Name:              capsw


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

Total Physical ports involved in Packet Capture: 1

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

Filter:            capsw-1-1



Packet Capture Filter Info
```

```
  Name:              capsw-1-1


Protocol:          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
```

Capture de paquets sur les interfaces de port de commutation L2

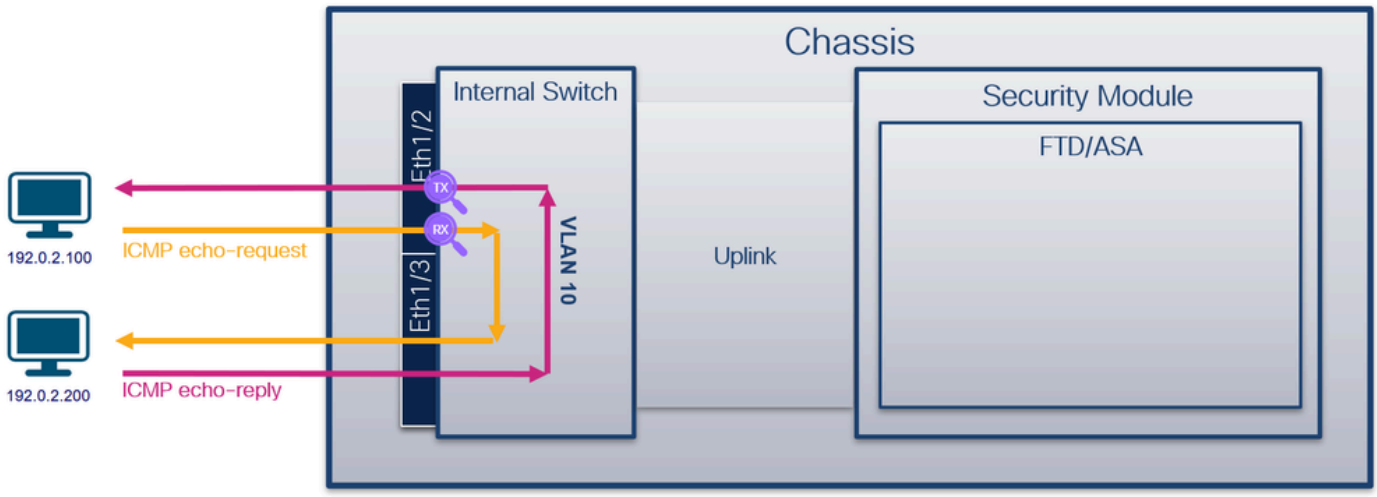
Les ports de commutateur transfèrent le trafic au niveau de la couche 2, en utilisant la fonction de commutation dans le matériel. Les ports de commutation d'un même VLAN peuvent communiquer entre eux à l'aide de la commutation matérielle, et le trafic n'est pas soumis à la politique de sécurité de défense contre les menaces. Les ports d'accès acceptent uniquement le trafic non étiqueté et vous pouvez les affecter à un seul VLAN. Les ports agrégés acceptent le trafic non balisé et balisé et peuvent appartenir à plusieurs VLAN. Par défaut, Ethernet 1/2 à 1/8 (1210) ou Ethernet 1/2 à 1/10 (1220) sont configurés en tant que ports de commutateur d’accès sur VLAN 1. Vous ne pouvez pas configurer l’interface de gestion en tant que port de commutateur.

Tâche 1

Utilisez l’interface de ligne de commande FTD ou ASA pour configurer et vérifier une capture de paquets sur les sous-interfaces Ethernet1/1 ou Ethernet1/2. Les deux interfaces sont des interfaces de commutateur affectées au VLAN 10.

Topologie, flux de paquets et points de capture

Pare-feu sécurisé 1200 :



Configuration

Procédez comme suit sur l'interface de ligne de commande ASA ou FTD pour configurer une capture de paquets sur l'interface Ethernet1/2 ou Ethernet1/3 :

1. Vérifiez les ports du commutateur L2 :

<#root>

>

show switch vlan

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    -                                down      E1/4, E1/5, E1/6, E1/7
                                                E1/8
10   VLAN-10                          up        E1/2, E1/3
```

2. Créez une session de capture, le commutateur 1200 prend en charge la directionnalité de capture :

<#root>

>

capture capsw switch interface switchport 2 direction ?

```
  both     To capture switch bi-directional traffic
  egress   To capture switch egressing traffic
  ingress  To capture switch ingressing traffic

>
```

capture capsw switch interface switchport 2 direction both

Remarque : Bien que le port soit étiqueté comme Ethernet1/2, lorsque vous effectuez une capture de commutateur de couche 2, vous ne pouvez pas le spécifier au format Ethernet1/2. Utilisez plutôt switchport 2.

3. Activez la session de capture

<#root>

>

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 :

<#root>

>

show capture capsw detail

```
Packet Capture info
  Name:
```

capsw

```
  Session:           2
  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

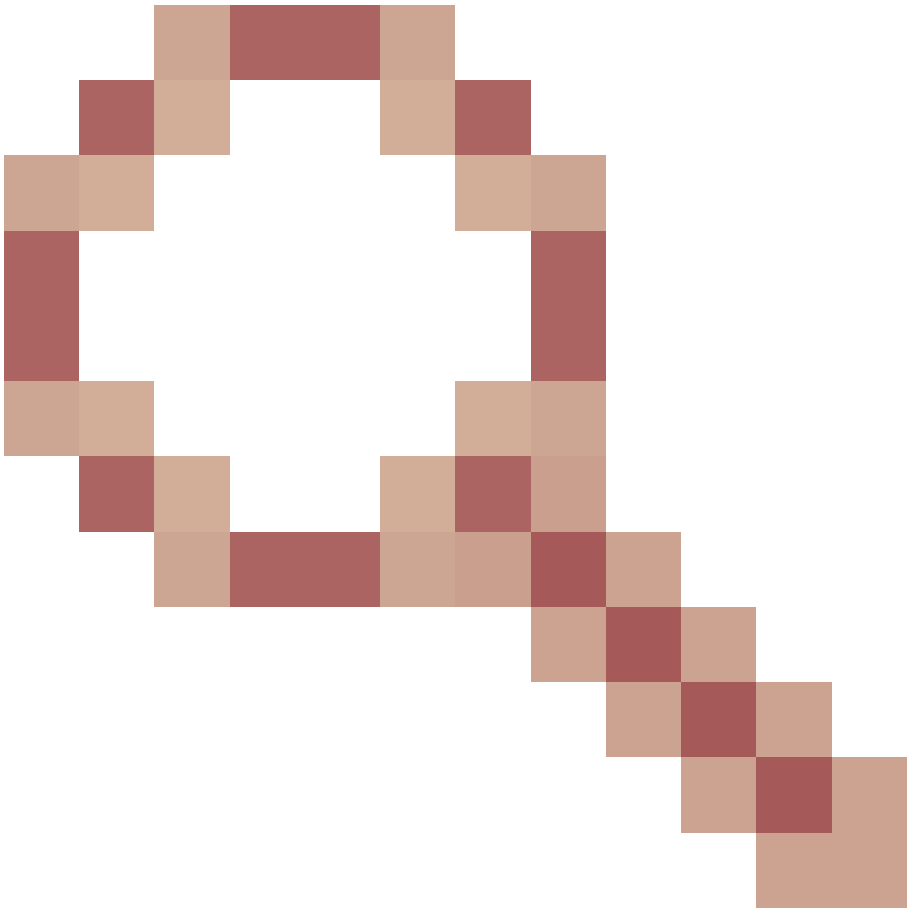
Physical port:
  Slot Id:           1
  Port Id:           2
  Pcapfile:          /mnt/disk0/packet-capture/sess-2-capsw-ethernet-1-2-0.pcap
  Pcapsize:          24
  Direction:         both
```

```
  Filter:           capsw-1-2

Packet Capture Filter Info
  Name:             capsw-1-2
  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

0 packet captured on disk using switch capture


Reading of capture file from disk is not supported
```



En raison du défaut CSCwq55508
, la taille et le nombre de paquets ne sont pas mis à jour dans le résultat des commandes show capture pour les captures de commutateur sur le pare-feu sécurisé 1200. Pour contourner le problème, ceci peut être vérifié dans l'interpréteur de commandes FXOS local-mgmt via la commande show portmanager switch pktcap-rules hardware :

<#root>

```
Firewall-1200(local-mgmt)#
```

```
show portmanager switch pktcap-rules hardware
```

```
Hardware DB rule: 1 /
```

```
Direction: egress
```

```
 HwIndex= 8196
 RuleId= 6144
 CounterIndex= 10
```

```
PacketCount= 38
```

```
 Slot= 1
 Interface= 2
 Protocol= 0
 EthertypeAtL2Offset= 0x0000
 EtherTypeAtL3Offset= 0x0000
 Ivlan= 0
 Ovlan= 0
 FlowId= 0
 SrcEport= 0
 TrgEport= 0
 SrcId= 0
 TcpUdpSrcPort= 0
 TcpUdpDstPort= 0
 SrcIpAddr= 0.0.0.0
 DstIpAddr= 0.0.0.0
 SrcIpv6Addr= ::
 DestIpv6Addr= ::
 SrcMacAddr= 00:00:00:00:00:00
 DestMacAddr= 00:00:00:00:00:00
```

```
Hardware DB rule: 2 /
```

```
Direction: ingress
```

```
 HwIndex= 4104
 RuleId= 5120
 CounterIndex= 0
```

```
PacketCount= 37
```

```
 Slot= 1
 Interface= 2
 Protocol= 0
 EthertypeAtL2Offset= 0x0000
 EtherTypeAtL3Offset= 0x0000
 Ivlan= 0
 Ovlan= 0
 FlowId= 0
 SrcEport= 0
 TrgEport= 0
 SrcId= 0
 TcpUdpSrcPort= 0
 TcpUdpDstPort= 0
 SrcIpAddr= 0.0.0.0
 DstIpAddr= 0.0.0.0
 SrcIpv6Addr= ::
```

```
DestIpv6Addr= ::
SrcMacAddr= 00:00:00:00:00:00
DestMacAddr= 00:00:00:00:00:00
```

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 du pare-feu sécurisé.

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 Ethernet 1/2 du commutateur L2. Dans cet exemple, les paquets capturés sur le pare-feu sécurisé 1210 sont analysés.

Vérifiez le point clé : dans ce cas, les paquets de requête et de réponse d'écho ICMP sont capturés.

No.	Time	Delta	Source	Destination	Protocol	Length	ICMP Type	ICMP Code	TTL	Info
1	0.000000	0.000000	192.0.2.100	192.0.2.200	ICMP	102	8	0	64	Echo (ping) request id=0x0018,
2	0.000022	0.000022	192.0.2.200	192.0.2.100	ICMP	102	0	0	64	Echo (ping) reply id=0x0018,
3	1.023909	1.023887	192.0.2.100	192.0.2.200	ICMP	102	8	0	64	Echo (ping) request id=0x0018,
4	1.023914	0.000005	192.0.2.200	192.0.2.100	ICMP	102	0	0	64	Echo (ping) reply id=0x0018,
5	2.045207	1.021293	192.0.2.100	192.0.2.200	ICMP	102	8	0	64	Echo (ping) request id=0x0018,
6	2.045217	0.000010	192.0.2.200	192.0.2.100	ICMP	102	0	0	64	Echo (ping) reply id=0x0018,
7	3.070763	1.025546	192.0.2.100	192.0.2.200	ICMP	102	8	0	64	Echo (ping) request id=0x0018,
8	3.070770	0.000007	192.0.2.200	192.0.2.100	ICMP	102	0	0	64	Echo (ping) reply id=0x0018,
9	4.094395	1.023625	192.0.2.100	192.0.2.200	ICMP	102	8	0	64	Echo (ping) request id=0x0018,
10	4.094401	0.000006	192.0.2.200	192.0.2.100	ICMP	102	0	0	64	Echo (ping) reply id=0x0018,
11	5.122298	1.027897	192.0.2.100	192.0.2.200	ICMP	102	8	0	64	Echo (ping) request id=0x0018,
12	5.122313	0.000015	192.0.2.200	192.0.2.100	ICMP	102	0	0	64	Echo (ping) reply id=0x0018,
13	6.142932	1.020619	192.0.2.100	192.0.2.200	ICMP	102	8	0	64	Echo (ping) request id=0x0018,
14	6.142941	0.000009	192.0.2.200	192.0.2.100	ICMP	102	0	0	64	Echo (ping) reply id=0x0018,
15	7.168917	1.025976	192.0.2.100	192.0.2.200	ICMP	102	8	0	64	Echo (ping) request id=0x0018,
16	7.168933	0.000016	192.0.2.200	192.0.2.100	ICMP	102	0	0	64	Echo (ping) reply id=0x0018,
17	8.192825	1.023892	192.0.2.100	192.0.2.200	ICMP	102	8	0	64	Echo (ping) request id=0x0018,
18	8.192840	0.000015	192.0.2.200	192.0.2.100	ICMP	102	0	0	64	Echo (ping) reply id=0x0018,

Explication

Ces paquets ne sont jamais transférés à l'application (FTD/ASA) car les deux hôtes sont connectés aux ports de commutation de couche 2 au sein du même VLAN.

Ce tableau récapitule la tâche :

Tâche	Point de capture	Filtre interne	Direction	Trafic capturé
Configurez et vérifiez une capture de paquets sur l'interface Ethernet1/2 du port de commutation L2	Ethernet1/2	Aucune	les deux	Requêtes d'écho ICMP de l'hôte 192.0.2.200 vers l'hôte 192.0.2.100 Réponses d'écho ICMP de

				l'hôte 192.0.2.100 à l'hôte 192.0.2.200

Capture de paquets sur un châssis à instances multiples

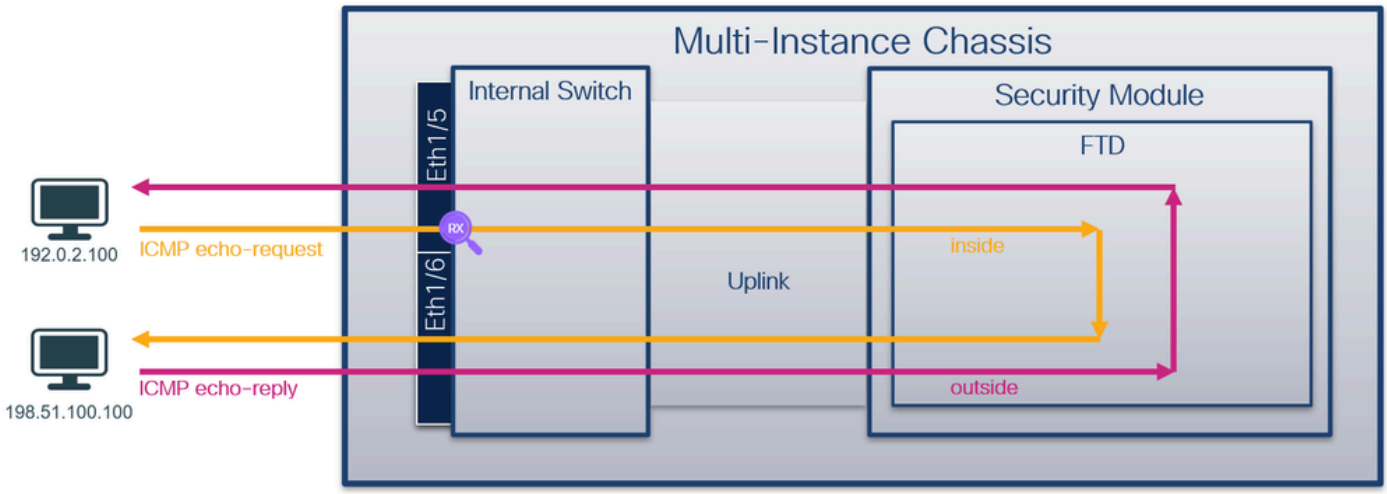
La capture de paquets de commutateur sur les plates-formes 3100/4200 en mode de déploiement multi-instance diffère de la capture de commutateur en mode natif. En mode multi-instance, la commande capture <name> switch n'est pas disponible sur les instances FTD. Au lieu de cela, les captures de paquets doivent être configurées à l'aide de l'interface de ligne de commande FXOS sur le châssis, comme pour les plates-formes 4100/9300, à l'aide de la commande scope packet-capture.

Tâche 1

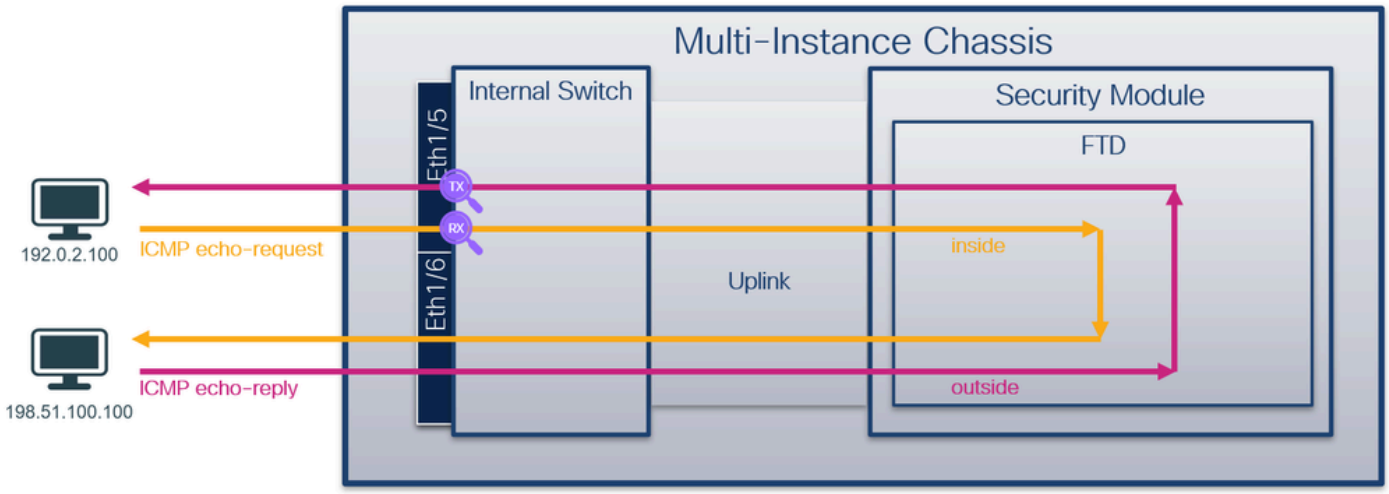
Utilisez l'interface de ligne de commande FXOS sur le châssis multi-instance pour configurer et vérifier une capture de paquets de commutateur sur l'interface Ethernet1/5.

Topologie, flux de paquets et points de capture

Secure Firewall 3100 :



Secure Firewall 4200 avec captures bidirectionnelles :



Configuration

CLI FXOS

Procédez comme suit sur l'interface de ligne de commande FXOS du châssis pour configurer une capture de paquets sur l'interface Ethernet1/5 :

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

```
<#root>

firepower-3120 #

scope ssa

firepower-3120 /ssa #

show app-instance

Application Name      Identifier           Slot ID     Admin State      Operational State     Running Versi
--------------------- -------------------- ---------- ---------------- --------------------- -------------

ftd

ftd1
                  1          Enabled         Online               7.7.0.89        7.7.0.89        Contai
```

2. Créez une session de capture :

```
<#root>

firepower-3120#

scope packet-capture
```

```
firepower-3120 /packet-capture #
create session cap1

firepower-3120 /packet-capture/session* #
create phy-port Eth1/5

firepower-3120 /packet-capture/session/phy-port* #
set app ftd

firepower-3120 /packet-capture/session/phy-port* #
set app-instance ftd1

firepower-3120 /packet-capture/session/phy-port* #
up

firepower-3120 /packet-capture/session* #
enable

firepower-3120 /packet-capture/session* #
commit-buffer

firepower-3120 /packet-capture/session #
```

Secure Firewall 4200 :

<#root>

```
firepower-4245#
scope packet-capture

firepower-4245 /packet-capture #
create session cap1

firepower-4245 /packet-capture/session* #
create phy-port Eth1/5

firepower-4245 /packet-capture/session/phy-port* #
set app ftd

firepower-4245 /packet-capture/session/phy-port* #
set app-instance ftd1
```

```
firepower-4245 /packet-capture/session/phy-port* #
set direction both

firepower-4245 /packet-capture/session/phy-port* #
up

firepower-4245 /packet-capture/session* #
enable

firepower-4245 /packet-capture/session* #
commit-buffer

firepower-4245 /packet-capture/session #
```

Vérification

CLI FXOS

Vérifiez les détails de la capture dans la portée packet-capture. Plus précisément, vérifiez le nom de la session de capture, l'état administratif et opérationnel, l'emplacement de l'interface et l'identificateur. Assurez-vous que la valeur Pcapsize en octets augmente et que le nombre de paquets capturés est différent de zéro :

<#root>

```
firepower-3120#
scope packet-capture

firepower-3120 /packet-capture #
show session cap1



SSP Traffic Monitoring 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
    Error Code: 0
    Drop Count: 0
```

Packet Count: 420

```
Physical ports involved in Packet Capture:
    Slot Id: 1
    Port Id: 5
    Pcapfile: /workspace/packet-capture/sess-1-cap1-ethernet-1-5-0.pcap
```

Pcapsize: 49128 bytes

```
    Filter:
    Sub Interface: 0
    Application Instance:
```

ftd1

```
    Application Name:
```

ftd

```
    Direction: Ingress
    Drop: Disable
```

Secure Firewall 4200 :

<#root>

```
firepower-4245#
```

scope packet-capture

```
firepower-4245 /packet-capture #
```

show session cap1

```
SSP Traffic Monitoring 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
    Error Code: 0
    Drop Count: 0

Packet Count: 95


Physical ports involved in Packet Capture:
    Slot Id: 1
    Port Id: 5
    Pcapfile: /workspace/packet-capture/sess-1-cap1-ethernet-1-5-0.pcap

Pcapsize: 11050  bytes


    Filter:
    Sub Interface: 0
    Application Instance:

 ftd1


    Application Name:

ftd



Direction: Both


    Drop: Disable
```

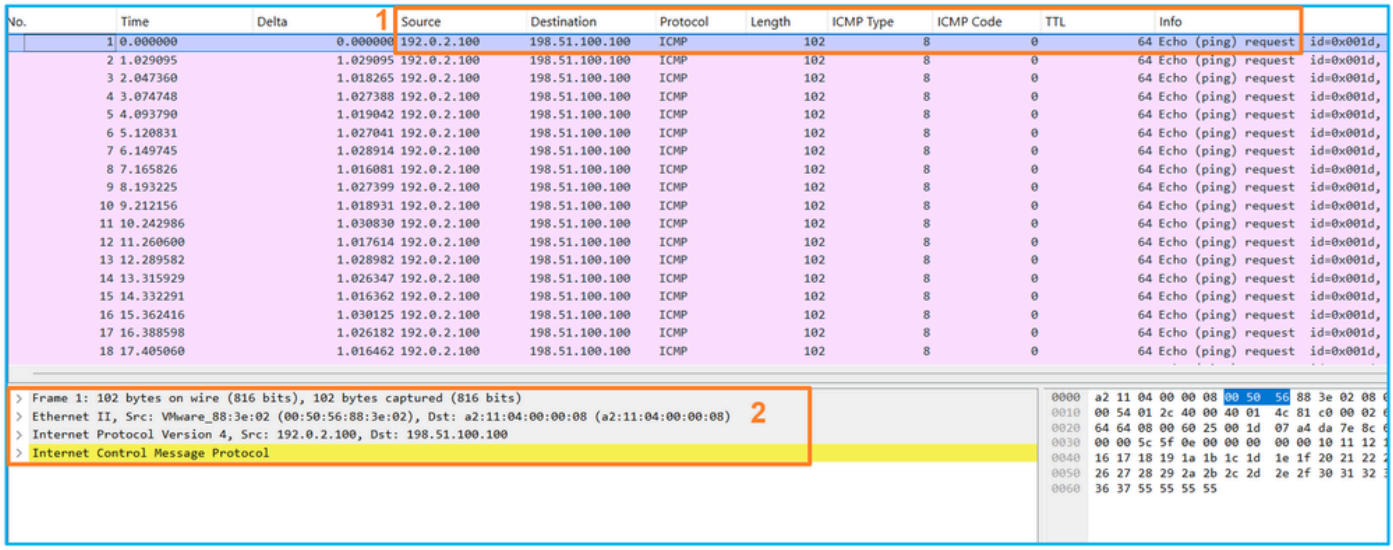
Collecter les fichiers de capture

Suivez les étapes de l'interface de ligne de commande FXOS dans la section Collecter les fichiers de capture de commutateur interne 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 pour Ethernet1/5. Dans cet exemple, les paquets capturés sur le pare-feu sécurisé 3100 sont analysés. 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 l'interface Ethernet1/5.

Ce tableau récapitule la tâche :

Tâche	Point de capture	Filtre interne	Direction	Trafic capturé
Configurer et vérifier une capture de paquets sur l'interface Ethernet1/5	Ethernet1/5	Aucune	Entrée uniquement*	Requêtes d'écho ICMP de l'hôte 192.0.2.100 vers l'hôte 198.51.100.100

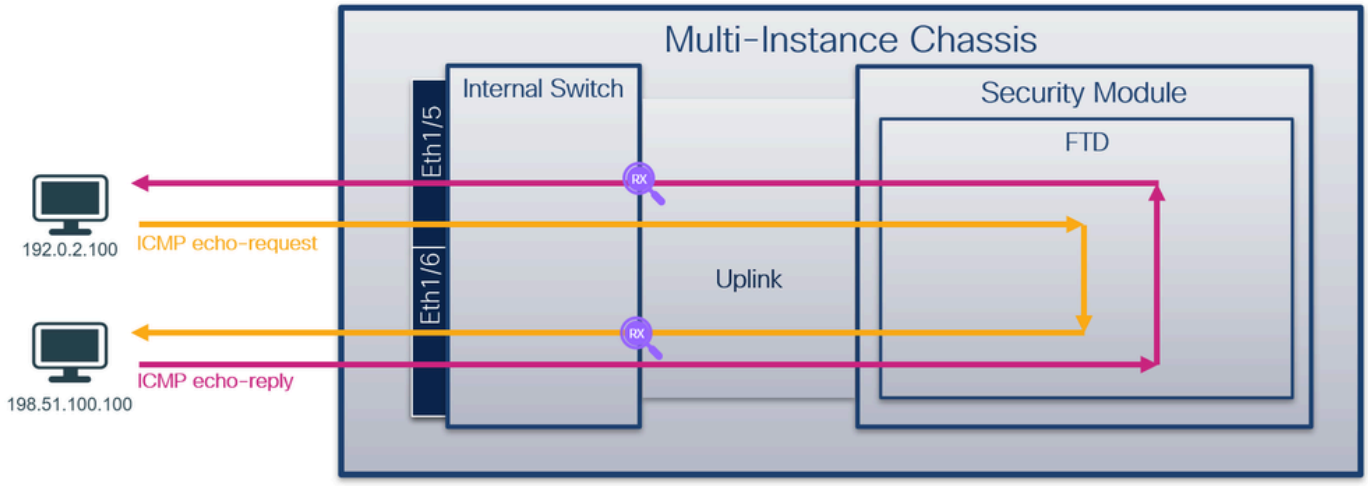
* Contrairement au modèle 3100, le Secure Firewall 4200 prend en charge les captures bidirectionnelles (entrée et sortie).

Tâche 2

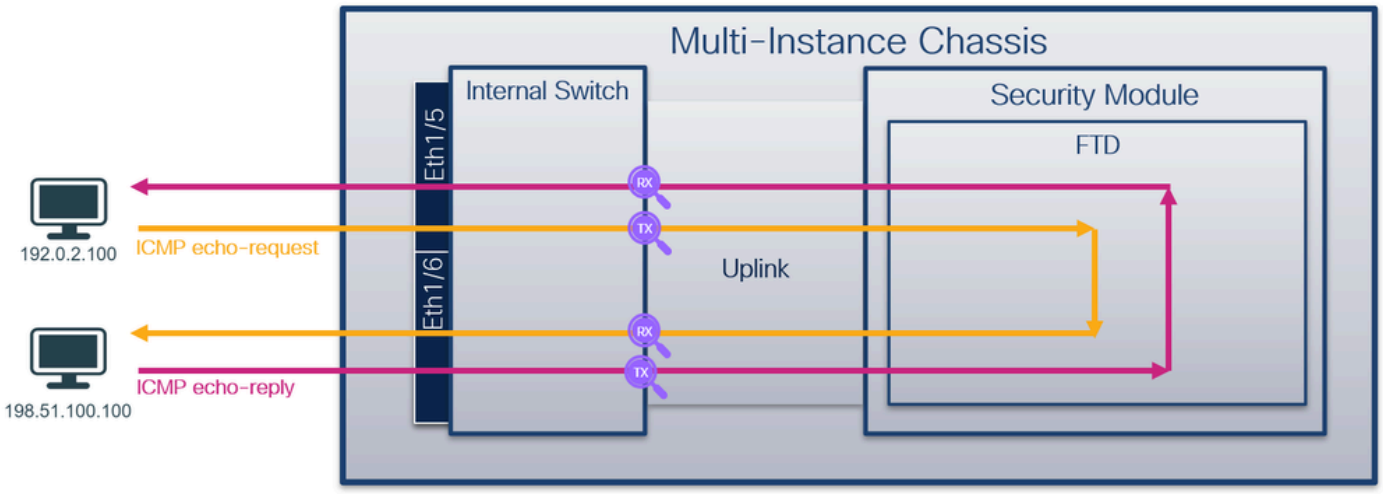
Utilisez l'interface de ligne de commande FXOS sur le châssis multi-instance pour configurer et vérifier une capture de paquets de commutation sur les interfaces de liaison ascendante de données.

Topologie, flux de paquets et points de capture

Secure Firewall 3100 :



Secure Firewall 4200 :



Configuration

CLI FXOS

Procédez comme suit sur l'interface de ligne de commande FXOS du châssis pour configurer une capture de paquets sur les interfaces de liaison ascendante de données :

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

<#root>

```
firepower-3120 /ssa #
```

show app-instance

```
Application Name      Identifier           Slot ID    Admin State     Operational State    Running Versi
-------------------- -------------------- ---------- --------------- -------------------- -------------
```

ftd

ftd1

```
                1          Enabled         Online                 7.7.0.89        7.7.0.89        Contai
```

2. Créez une session de capture :

<#root>

```
firepower-3120#
scope packet-capture

firepower-3120 /packet-capture #
create session cap1

firepower-3120 /packet-capture/session* #
create phy-port Eth1/18

firepower-3120 /packet-capture/session/phy-port* #
set app ftd

firepower-3120 /packet-capture/session/phy-port* #
set app-instance ftd1

firepower-3120 /packet-capture/session/phy-port* #
up

firepower-3120 /packet-capture/session* #
enable

firepower-3120 /packet-capture/session* #
commit-buffer

firepower-3120 /packet-capture/session #
```

Remarque : Contrairement au déploiement natif, en mode multi-instance, utilisez le numéro de port au lieu du nom de l'interface. Reportez-vous au tableau de la section Vue d'ensemble générale de l'architecture du système pour vérifier le mappage de port de commutateur interne.

Secure Firewall 4200 :

<#root>

```
firepower-4245#
scope packet-capture

firepower-4245 /packet-capture #
create session cap1

firepower-4245 /packet-capture/session* #
create phy-port Eth1/11

firepower-4245 /packet-capture/session/phy-port* #
set app ftd

firepower-4245 /packet-capture/session/phy-port* #
set app-instance ftd1

firepower-4245 /packet-capture/session/phy-port* #
set direction both

firepower-4245 /packet-capture/session/phy-port* #
up

firepower-4245 /packet-capture/session* #
create phy-port Eth1/12

firepower-4245 /packet-capture/session/phy-port* #
set app ftd

firepower-4245 /packet-capture/session/phy-port* #
set app-instance ftd1

firepower-4245 /packet-capture/session/phy-port* #
set direction both

firepower-4245 /packet-capture/session/phy-port* #
up

firepower-4245 /packet-capture/session* #
enable

firepower-4245 /packet-capture/session* #
commit-buffer
```

```
firepower-4245 /packet-capture/session #
```

Vérification

CLI FXOS

Vérifiez les détails de la capture dans la portée packet-capture. Plus précisément, vérifiez le nom de la session de capture, l'état administratif et opérationnel, l'emplacement de l'interface et l'identificateur. Assurez-vous que la valeur Pcapsize en octets augmente et que le nombre de paquets capturés est différent de zéro :

<#root>

```
firepower-3120#
```

scope packet-capture

```
firepower-3120 /packet-capture #
```

show session cap1

```
SSP Traffic Monitoring 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
    Error Code: 0
    Drop Count: 0
```

Packet Count: 171

```
Physical ports involved in Packet Capture:
    Slot Id: 1
    Port Id: 18
    Pcapfile: /workspace/packet-capture/sess-1-cap1-data-uplink1.pcap
```

Pcapsize: 19932 bytes

```
    Filter:
    Sub Interface: 0
    Application Instance:
```

ftd1

```
    Application Name:
```

ftd

```
    Direction:
```

Ingress

```
    Drop: Disable
```

Secure Firewall 4200 :

<#root>

```
firepower-4245#
```

scope packet-capture

```
firepower-4245 /packet-capture #
```

show session cap1

```
SSP Traffic Monitoring 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
    Error Code: 0
    Drop Count: 0
```

Packet Count: 70

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

```
    Slot Id:
 1
    Port Id:
11
    Pcapfile: /workspace/packet-capture/sess-1-cap1-data-uplink1.pcap
Pcapsize: 8320  bytes
    Filter:
    Sub Interface: 0
    Application Instance: ftd1
    Application Name: ftd
    D
irection: Both
    Drop: Disable
    Slot Id:
1
    Port Id:
12
    Pcapfile: /workspace/packet-capture/sess-1-cap1-data-uplink2.pcap
 Pcapsize: 172  bytes
    Filter:
    Sub Interface: 0
    Application Instance: ftd1
    Application Name: ftd
 Direction: Both
    Drop: Disable
```

Collecter les fichiers de capture

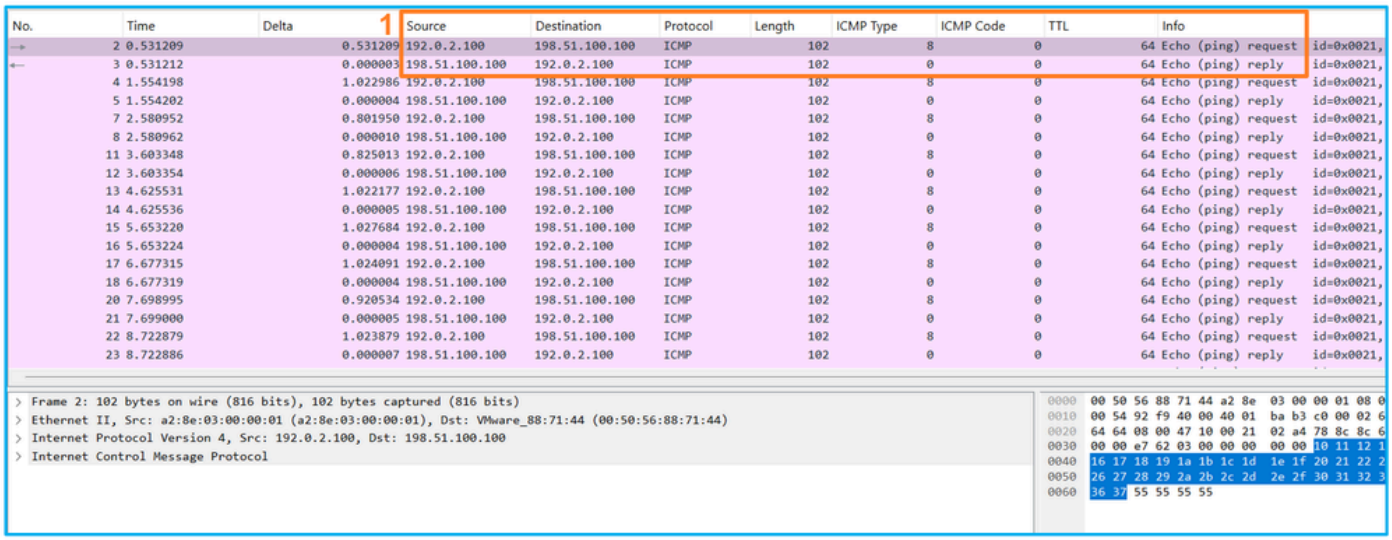
Suivez les étapes de l'interface de ligne de commande FXOS dans la section Collecter les fichiers de capture de commutateur interne Firepower 4100/9300.

Capturer l'analyse des fichiers

Utilisez une application de lecture de fichiers de capture de paquets pour ouvrir les fichiers de

capture pour l'interface in_data_uplink1. Dans cet exemple, les paquets capturés sur le pare-feu sécurisé 3100 sont analysés.

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.



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

* Contrairement au modèle 3100, le Secure Firewall 4200 prend en charge les captures bidirectionnelles (entrée et sortie).

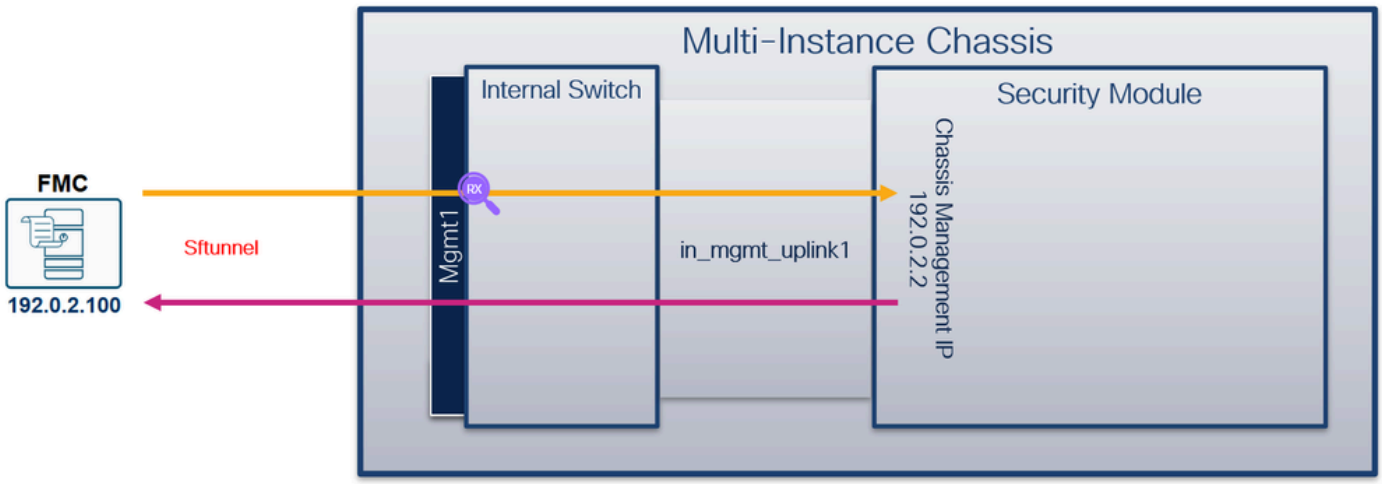
Tâche 3

Utilisez l'interface de ligne de commande FXOS sur le châssis multi-instance pour configurer et vérifier une capture de paquets de commutateur sur l'interface de gestion, capturant le trafic

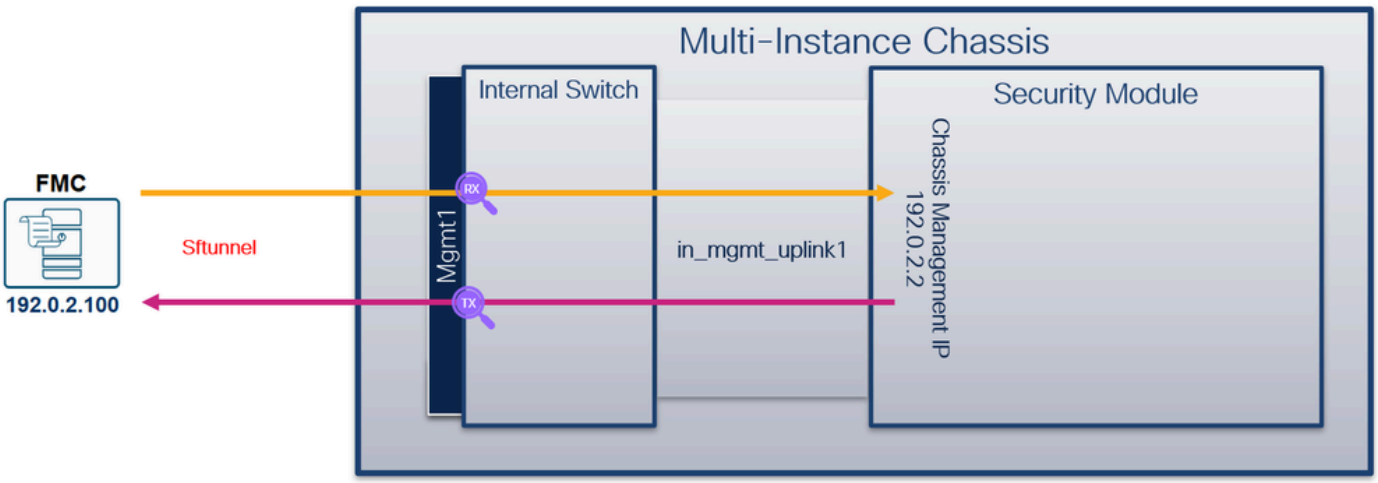
sftunnel entre le châssis et le FMC.

Topologie, flux de paquets et points de capture

Secure Firewall 3100 :



Secure Firewall 4200 avec captures bidirectionnelles :



Configuration

CLI FXOS

Procédez comme suit sur l'interface de ligne de commande FXOS du châssis pour configurer une capture de paquets pour le trafic sftunnel sur l'interface de gestion.

1. Créez un filtre de capture de paquets pour capturer uniquement le trafic TCP (numéro de protocole 6).

<#root>

```
firepower-4245#
```

```
scope packet-capture
```

```
firepower-4245 /packet-capture #
create filter filter1

firepower-4245 /packet-capture/filter* #
set protocol 6

firepower-4245 /packet-capture/filter* #
commit-buffer

firepower-4245 /packet-capture/filter #
up

firepower-4245 /packet-capture #
```

Remarque : Bien que le Secure Firewall 4200 supporte les captures de commutateur bidirectionnelles, en raison du bogue CSCwq64141 , il n'est pas possible de créer des filtres de capture de commutateur spécifiques avec des conditions de correspondance qui capturent le trafic dans les deux directions. Par conséquent, le filtre de cette tâche est configuré pour correspondre à tout le trafic TCP, ce qui permet la capture du trafic sftunnel dans les deux directions sur le pare-feu sécurisé 4200.

---

2. Créez une session de capture pour l'interface de gestion. Selon le tableau de la section Vue d'ensemble de haut niveau de l'architecture système, le port de gestion du pare-feu sécurisé 3100 est mappé au port de commutateur interne Eth1/17 :

```
<#root>
firepower-3120#
scope packet-capture
```

```
firepower-3120 /packet-capture #
create session cap1

firepower-3120 /packet-capture/session* #
create phy-port Eth1/17

firepower-3120 /packet-capture/session/phy-port* #
set filter filter1

firepower-3120 /packet-capture/session/phy-port* #
up

firepower-3120 /packet-capture/session* #
enable

firepower-3120 /packet-capture/session* #
up

firepower-3120 /packet-capture* #
commit-buffer

firepower-3120 /packet-capture #
```

Le port de gestion 1 du pare-feu sécurisé 4200 est mappé au port de commutation interne Eth1/9 :

<#root>

```
firepower-4245#
scope packet-capture

firepower-4245 /packet-capture #
create session cap1

firepower-4245 /packet-capture/session* #
create phy-port Eth1/9

firepower-4245 /packet-capture/session/phy-port* #
set direction both

firepower-4245 /packet-capture/session/phy-port* #
```

```
set filter filter1

firepower-4245 /packet-capture/session/phy-port* #
up

firepower-4245 /packet-capture/session* #
enable

firepower-4245 /packet-capture/session* #
commit-buffer
```

Vérification

CLI FXOS

Vérifiez les détails de la capture dans la portée packet-capture. Plus précisément, vérifiez le nom de la session de capture, l'état administratif et opérationnel, l'emplacement de l'interface, le filtre et l'identificateur. Assurez-vous que la valeur Pcapsize en octets augmente et que le nombre de paquets capturés est différent de zéro :

<#root>

```
firepower-3120#
scope packet-capture

firepower-3120 /packet-capture #
show session cap1


SSP Traffic Monitoring 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
    Error Code: 0
    Drop Count: 0
    Packet Count:
```

694

Physical ports involved in Packet Capture:
    Slot Id:

1

    Port Id:

17

    Pcapfile:

/workspace/packet-capture/sess-1-cap1-management-1-1.pcap

    Pcapsize:

81093 bytes

    Filter:

filter1

    Sub Interface: 0
    Application Instance:
    Application Name:
    Direction:

Ingress

    Drop: Disable

Secure Firewall 4200 :

<#root>

firepower-4245#

scope packet-capture

firepower-4245 /packet-capture #

show session cap1

SSP Traffic Monitoring 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
    Error Code: 0
    Drop Count: 0
    Packet Count:
```

222

```
Physical ports involved in Packet Capture:
    Slot Id:
```

1

```
    Port Id:
```

9

```
    Pcapfile:
```

/workspace/packet-capture/sess-1-cap1-management-1-1.pcap

```
    Pcapsize:
```

40180 bytes

```
    Filter: filter1
    Sub Interface: 0
    Application Instance:
    Application Name:
    Direction:
```

Both

```
    Drop: Disable
```

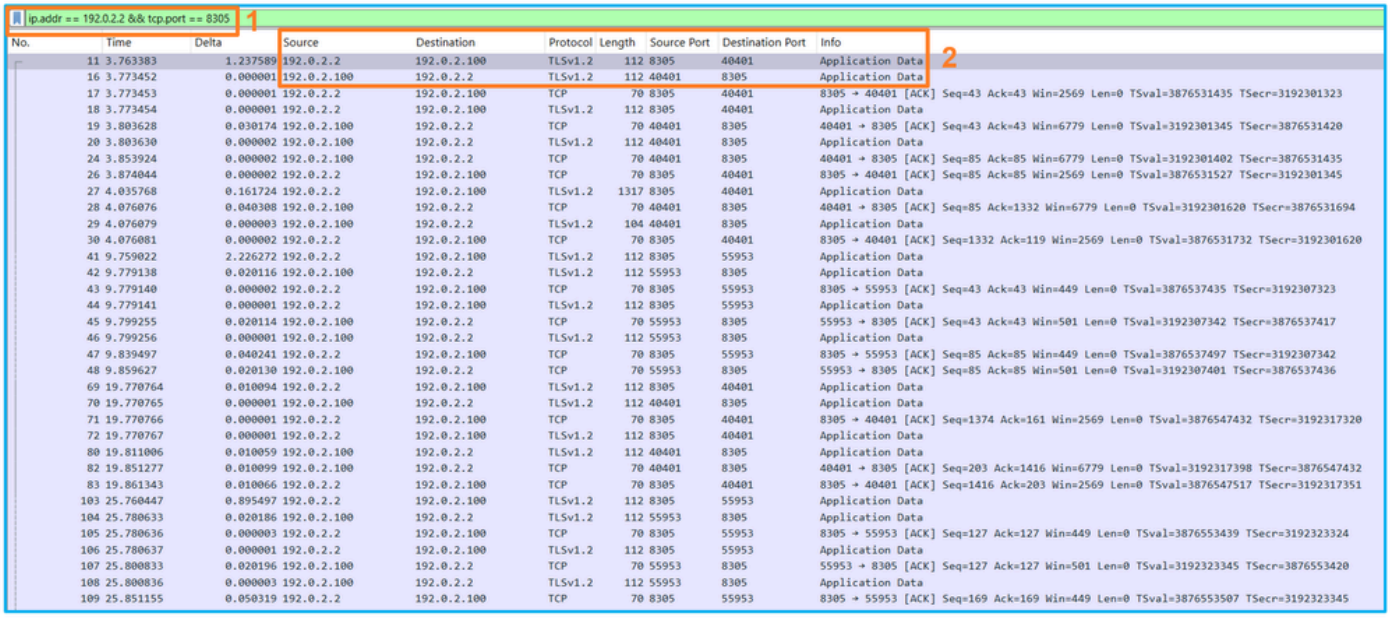
Collecter les fichiers de capture

Suivez les étapes de l'interface de ligne de commande FXOS dans la section Collecter les fichiers de capture de commutateur interne 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 pour l'interface de gestion. Dans cet exemple, les paquets capturés sur le pare-feu sécurisé 4200 sont analysés. Vérifiez les points clés :

1. Un filtre est nécessaire pour assainir la capture et afficher uniquement le trafic sftunnel.
2. Le trafic sftunnel est capturé dans les deux directions.



No.	Time	Delta	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
11	3.763383	1.237589	192.0.2.2	192.0.2.100	TLSv1.2	112	8305	40401	Application Data
16	3.773452	0.000001	192.0.2.100	192.0.2.2	TLSv1.2	112	40401	8305	Application Data
17	3.773453	0.000001	192.0.2.2	192.0.2.100	TCP	70	8305	40401	8305 → 40401 [ACK] Seq=43 Ack=43 Win=2569 Len=0 TSval=3876531435 TSecr=3192301323
18	3.773454	0.000001	192.0.2.2	192.0.2.100	TLSv1.2	112	8305	40401	Application Data
19	3.803628	0.030174	192.0.2.100	192.0.2.2	TCP	70	40401	8305	40401 → 8305 [ACK] Seq=43 Ack=43 Win=6779 Len=0 TSval=3192301345 TSecr=3876531420
20	3.803630	0.000002	192.0.2.100	192.0.2.2	TLSv1.2	112	40401	8305	Application Data
24	3.853924	0.000002	192.0.2.100	192.0.2.2	TCP	70	40401	8305	40401 → 8305 [ACK] Seq=85 Ack=85 Win=6779 Len=0 TSval=3192301402 TSecr=3876531435
26	3.874044	0.000002	192.0.2.2	192.0.2.100	TCP	70	8305	40401	8305 → 40401 [ACK] Seq=85 Ack=85 Win=2569 Len=0 TSval=3876531527 TSecr=3192301345
27	4.035768	0.161724	192.0.2.2	192.0.2.100	TLSv1.2	1317	8305	40401	Application Data
28	4.076076	0.040308	192.0.2.100	192.0.2.2	TCP	70	40401	8305	40401 → 8305 [ACK] Seq=85 Ack=1332 Win=6779 Len=0 TSval=3192301620 TSecr=3876531694
29	4.076079	0.000003	192.0.2.100	192.0.2.2	TLSv1.2	104	40401	8305	Application Data
30	4.076081	0.000002	192.0.2.2	192.0.2.100	TCP	70	8305	40401	8305 → 40401 [ACK] Seq=1332 Ack=119 Win=2569 Len=0 TSval=3876531732 TSecr=3192301620
41	9.759022	2.226272	192.0.2.2	192.0.2.100	TLSv1.2	112	8305	55953	Application Data
42	9.779138	0.020116	192.0.2.100	192.0.2.2	TLSv1.2	112	55953	8305	Application Data
43	9.779140	0.000002	192.0.2.2	192.0.2.100	TCP	70	8305	55953	8305 → 55953 [ACK] Seq=43 Ack=43 Win=449 Len=0 TSval=3876537435 TSecr=3192307323
44	9.779141	0.000001	192.0.2.2	192.0.2.100	TLSv1.2	112	8305	55953	Application Data
45	9.799255	0.020114	192.0.2.100	192.0.2.2	TCP	70	55953	8305	55953 → 8305 [ACK] Seq=43 Ack=43 Win=501 Len=0 TSval=3192307342 TSecr=3876537417
46	9.799256	0.000001	192.0.2.100	192.0.2.2	TLSv1.2	112	55953	8305	Application Data
47	9.839497	0.040241	192.0.2.2	192.0.2.100	TCP	70	8305	55953	8305 → 55953 [ACK] Seq=85 Ack=85 Win=449 Len=0 TSval=3876537497 TSecr=3192307342
48	9.859627	0.020130	192.0.2.100	192.0.2.2	TCP	70	55953	8305	55953 → 8305 [ACK] Seq=85 Ack=85 Win=501 Len=0 TSval=3192307401 TSecr=3876537436
69	19.770764	0.010094	192.0.2.2	192.0.2.100	TLSv1.2	112	8305	40401	Application Data
70	19.770765	0.000001	192.0.2.100	192.0.2.2	TLSv1.2	112	40401	8305	Application Data
71	19.770766	0.000001	192.0.2.2	192.0.2.100	TCP	70	8305	40401	8305 → 40401 [ACK] Seq=1374 Ack=161 Win=2569 Len=0 TSval=3876547432 TSecr=3192317320
72	19.770767	0.000001	192.0.2.2	192.0.2.100	TLSv1.2	112	8305	40401	Application Data
80	19.811006	0.010059	192.0.2.100	192.0.2.2	TLSv1.2	112	40401	8305	Application Data
82	19.851277	0.010099	192.0.2.100	192.0.2.2	TCP	70	40401	8305	40401 → 8305 [ACK] Seq=203 Ack=1416 Win=6779 Len=0 TSval=3192317398 TSecr=3876547432
83	19.861343	0.010066	192.0.2.2	192.0.2.100	TCP	70	8305	40401	8305 → 40401 [ACK] Seq=1416 Ack=203 Win=2569 Len=0 TSval=3876547517 TSecr=3192317351
103	25.760447	0.895497	192.0.2.2	192.0.2.100	TLSv1.2	112	8305	55953	Application Data
104	25.780633	0.020186	192.0.2.100	192.0.2.2	TLSv1.2	112	55953	8305	Application Data
105	25.780636	0.000003	192.0.2.2	192.0.2.100	TCP	70	8305	55953	8305 → 55953 [ACK] Seq=127 Ack=127 Win=449 Len=0 TSval=3876553439 TSecr=3192323324
106	25.780637	0.000001	192.0.2.2	192.0.2.100	TLSv1.2	112	8305	55953	Application Data
107	25.800833	0.020196	192.0.2.100	192.0.2.2	TCP	70	55953	8305	55953 → 8305 [ACK] Seq=127 Ack=127 Win=501 Len=0 TSval=3192323345 TSecr=3876553420
108	25.800836	0.000003	192.0.2.100	192.0.2.2	TLSv1.2	112	55953	8305	Application Data
109	25.851155	0.050319	192.0.2.2	192.0.2.100	TCP	70	8305	55953	8305 → 55953 [ACK] Seq=169 Ack=169 Win=449 Len=0 TSval=3876553507 TSecr=3192323345

Explication

Les captures du commutateur sont configurées sur l'interface de gestion.

Ce tableau récapitule la tâche :

Tâche	Point de capture	Filtre interne	Direction	Trafic capturé
Configurer et vérifier une capture de paquets pour le trafic sftunnel sur l'interface de gestion	*Ethernet1/9	trafic TCP	**les deux	Trafic Sftunnel (port TCP 8305) entre l'hôte 192.0.2.100 et l'hôte 192.0.2.2

* Reportez-vous au tableau de la section Vue d'ensemble générale de l'architecture système pour vérifier le mappage des ports de commutateur internes.

** Contrairement au modèle 3100, le Secure Firewall 4200 prend en charge les captures bidirectionnelles (entrée et sortie).

Collecter les fichiers de capture internes du commutateur Secure Firewall

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

Suivez ces étapes pour collecter les fichiers de capture de commutateur interne sur l'interface de ligne de commande ASA :

1. Arrêtez la capture :

<#root>

asa#

capture capsw switch stop

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

<#root>

asa#

show capture capsw detail

```
Packet Capture info

Name:              capsw

  Session:           1

Admin State:       disabled


  Oper State:        down


  Oper State Reason: Session_Admin_Shut


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

Total Physical ports involved in Packet Capture: 1

Physical port:
  Slot Id:           1
  Port Id:           1
```

```
  Pcapfile:

/mnt/disk0/packet-capture/

sess-1-capsw-ethernet-1-1-0.pcap


  Pcapsize:          139826
  Filter:            capsw-1-1

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

```
<#root>

asa#

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


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

asa#

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


Source filename [/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap]?
Destination filename [sess-1-capsw-ethernet-1-1-0.pcap]?
Copy in progress...C
```

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

FTD

Procédez comme suit pour collecter les fichiers de capture de commutateurs internes 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 :

```
<#root>

>

system support diagnostic-cli


Attaching to Diagnostic CLI ... Click 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower>

enable


Password:

<-- Enter


firepower#
```

2. Arrêtez la capture :

```
<#root>

firepower#

capture capi switch stop
```

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

```
<#root>

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.

<#root>

```
firepower#
```

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

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

```
firepower#
```

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

```
Source filename [/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap]?
Destination filename [sess-1-capsw-ethernet-1-1-0.pcap]?
Copy in progress...C
```

139826 bytes copied in 0.532 secs

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

1. Arrêtez la capture :

<#root>

```
>
```

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 :

<#root>

```
>
```

show capture capsw detail

```
Packet Capture info
```

Name: capsw

```
  Session:           1

Admin State:       disabled


  Oper State:        down


  Oper State Reason: Session_Admin_Shut


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

Total Physical ports involved in Packet Capture: 1

Physical port:
  Slot Id:           1
  Port Id:           1

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


  Pcapsize:          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 :

```
<#root>

>

expert
```

```
admin@firepower:~$
sudo su

root@firepower:/home/admin
```

4. Copiez le fichier de capture dans /ngfw/var/common/:

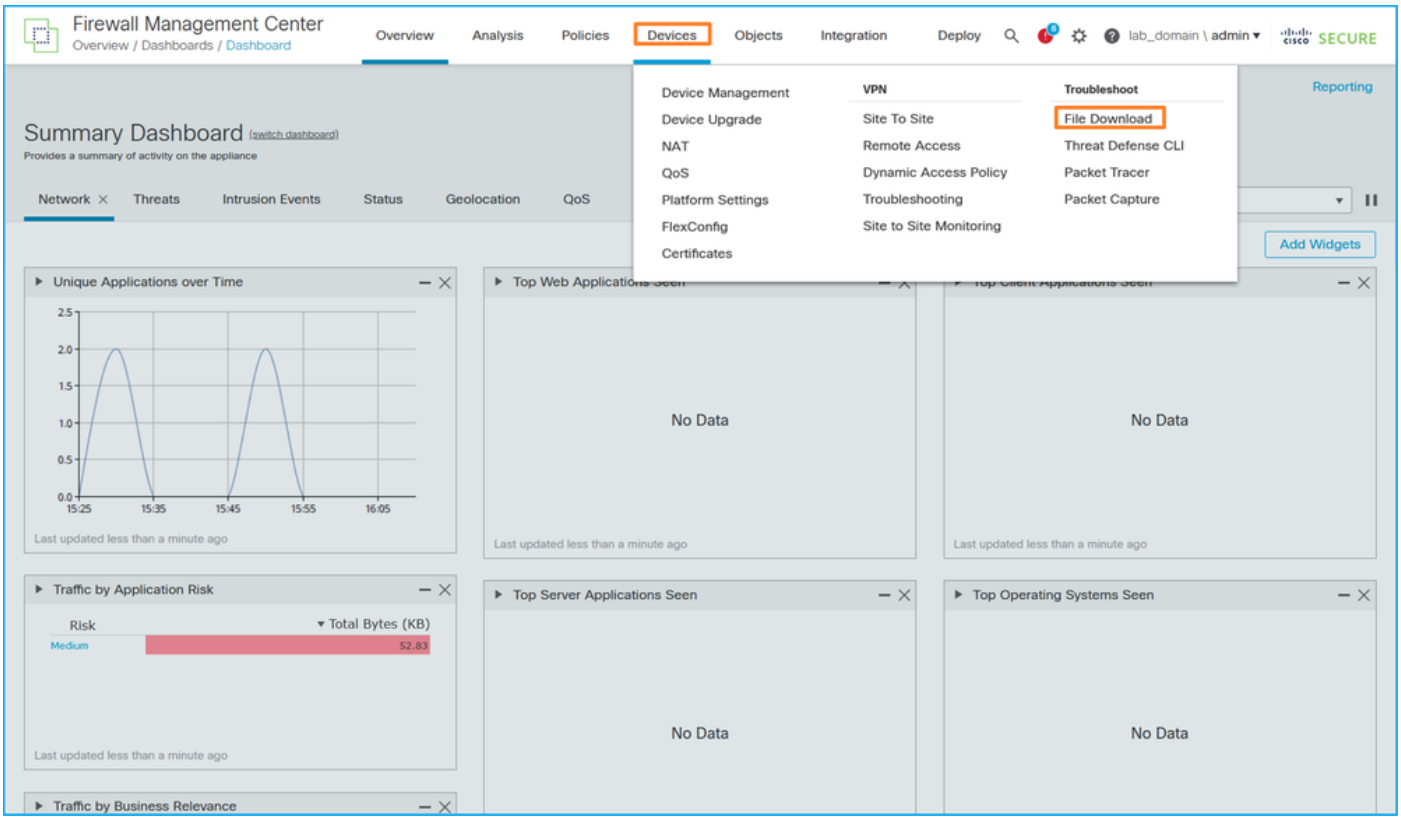
```
<#root>
root@KSEC-FPR3100-1:/home/admin
cp /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap /ngfw/var/common/

root@KSEC-FPR3100-1:/home/admin
ls -l /ngfw/var/common/sess*

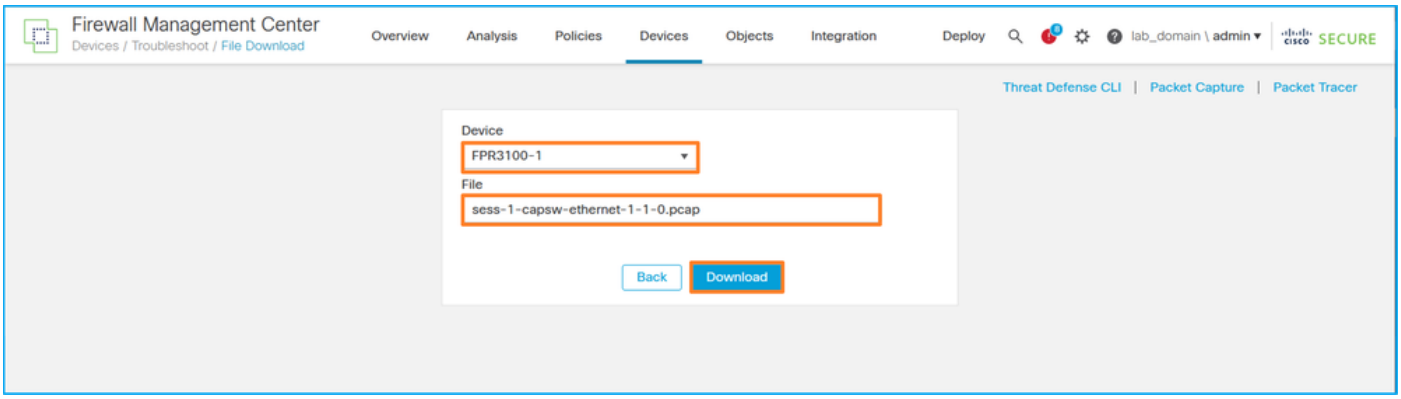
-rwxr-xr-x 1 root admin 139826 Aug  7 20:14
/ngfw/var/common/sess-1-capsw-ethernet-1-1-0.pcap

-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, sélectionnez Devices > File Download :



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



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

Lignes directrices 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 si nécessaire.
- 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 de nombre d'abandons 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.