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

Contenu

Introduction

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

Conditions préalables

Conditions requises

Connaissances de base du produit, analyse de capture.

Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

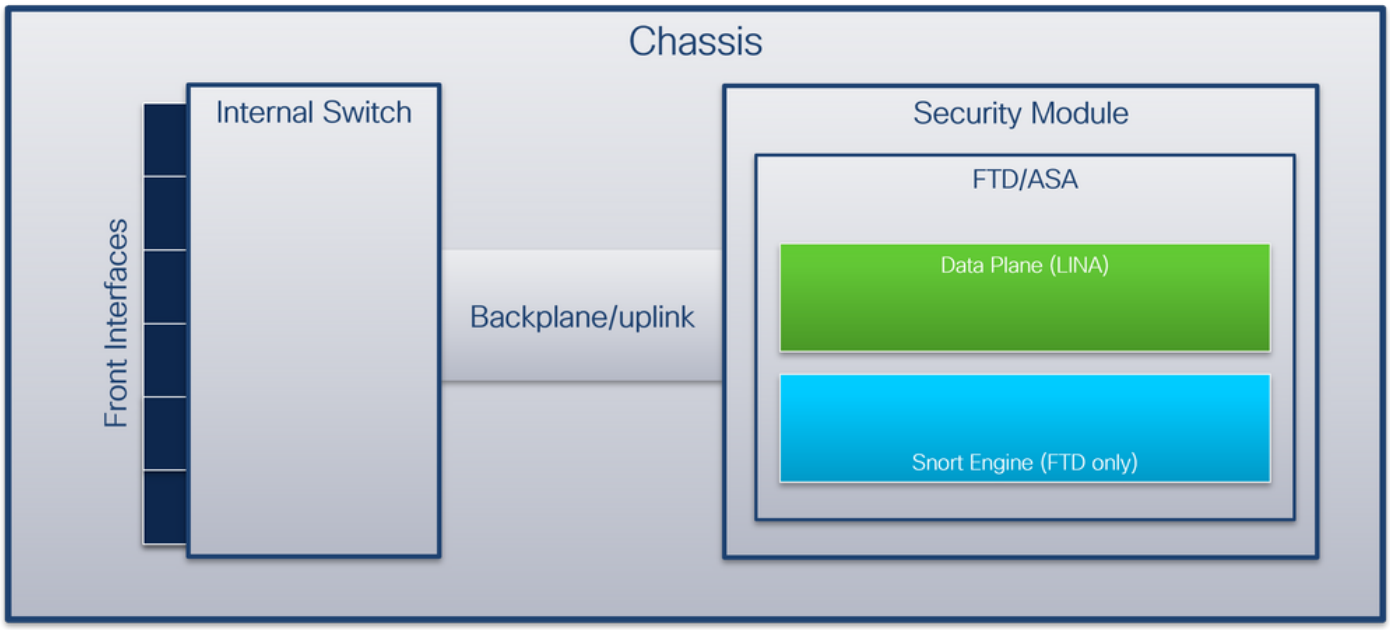
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Pare-feu sécurisé 31xx
- Firepower 41xx
- Firepower 93xx
- Système d'exploitation extensible sécurisé Cisco (FXOS) 2.12.0.x
- Cisco Secure Firewall Threat Defense (FTD) 7.2.0.x
- Cisco Secure Firewall Management Center (FMC) 7.2.0.x
- Cisco Secure Firewall Device Manager (FDM) 7.2.0.x
- Appareil de sécurité adaptatif (ASA) 9.18(1)x
- Adaptive Security Appliance Device Manager (ASDM) 7.18.1.x
- Wireshark 3.6.7 (https://www.wireshark.org/download.html)

Informations générales

Présentation générale de l'architecture système

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



Le châssis comprend les composants suivants :

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

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

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

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

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

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

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

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

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

Présentation générale du fonctionnement des commutateurs internes

Firepower 4100/9300

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

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

```
firepower# connect fxos
…
firepower(fxos)# show run int e1/2
!Command: show running-config interface Ethernet1/2
!Time: Tue Jul 12 22:32:11 2022

version 5.0(3)N2(4.120)

interface Ethernet1/2
 description U: Uplink
 no lldp transmit
 no lldp receive
 no cdp enable
 switchport mode dot1q-tunnel
 switchport trunk native vlan 102
 speed 1000
 duplex full
 udld disable
 no shutdown
```

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

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

Pare-feu sécurisé 3100

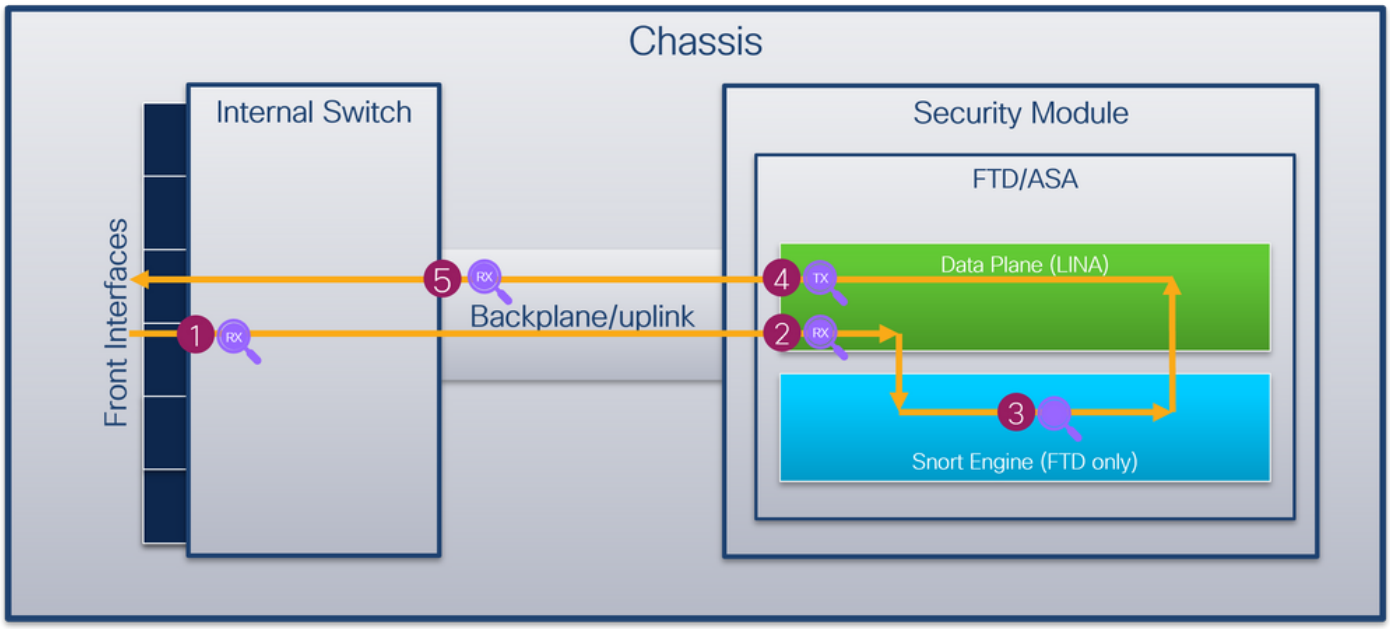
Comme dans Firepower 4100/9300, l'étiquette VLAN du port est utilisée par le commutateur interne pour identifier une interface.

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

Flux de paquets et points de capture

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

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



Les points de capture sont les suivants :

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

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

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

Configuration et vérification sur Firepower 4100/9300

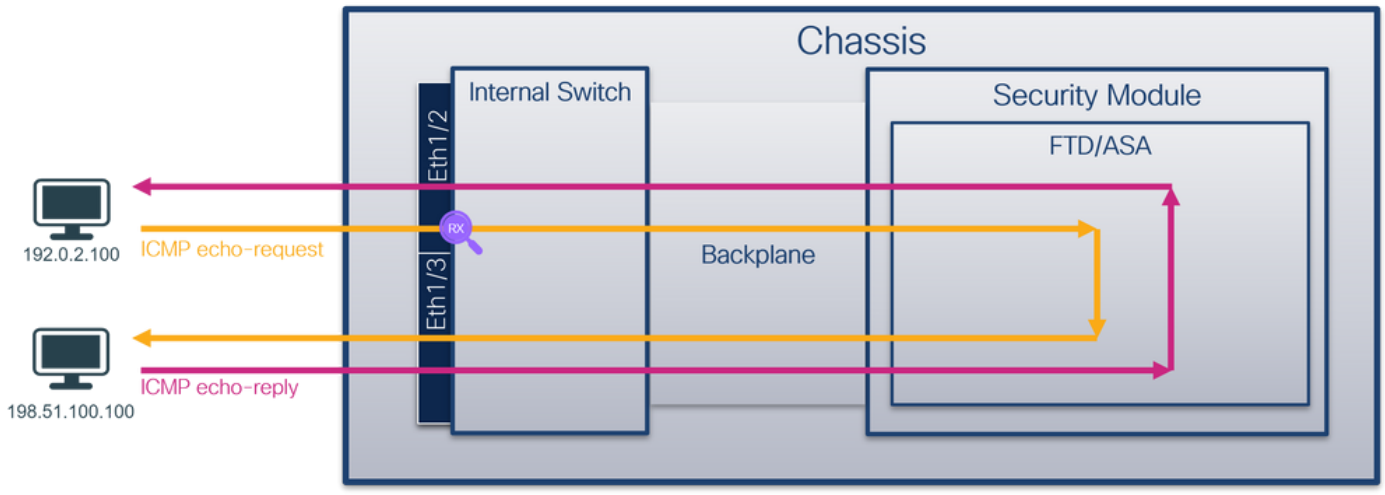
Les captures du commutateur interne Firepower 4100/9300 peuvent être configurées dans **Outils > Capture de paquets** sur FCM ou dans **capture de paquets de portée** dans l'interface de ligne de commande de FXOS**. Pour la description des options de capture de paquets, référez-vous au** *Guide de configuration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

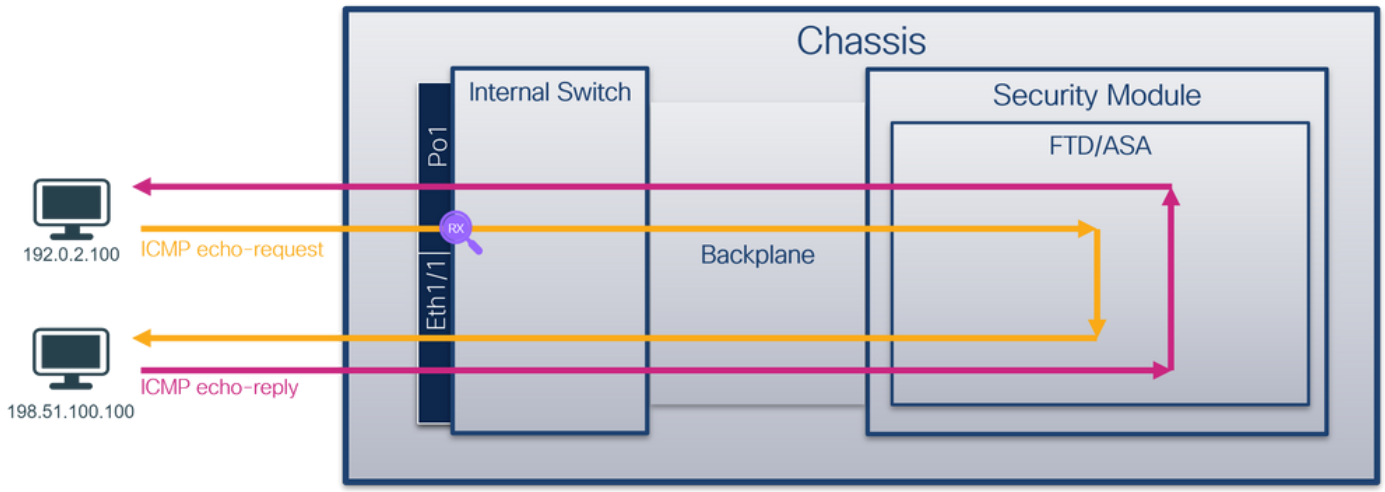
Ces scénarios couvrent les cas d'utilisation courants des captures de commutateur interne Firepower 4100/9300.

Capture de paquets sur une interface physique ou Port Channel

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

Topologie, flux de paquets et points de capture



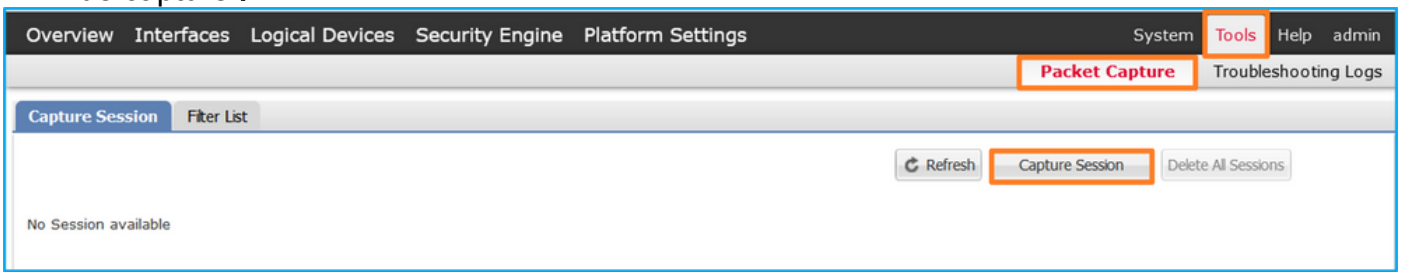


Configuration

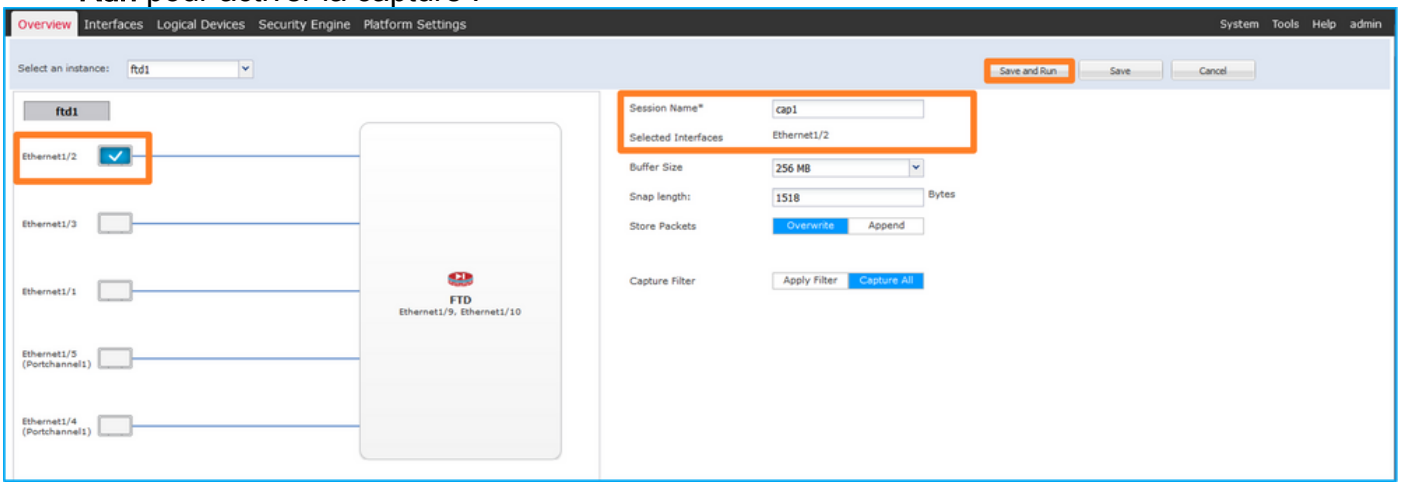
FCM

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

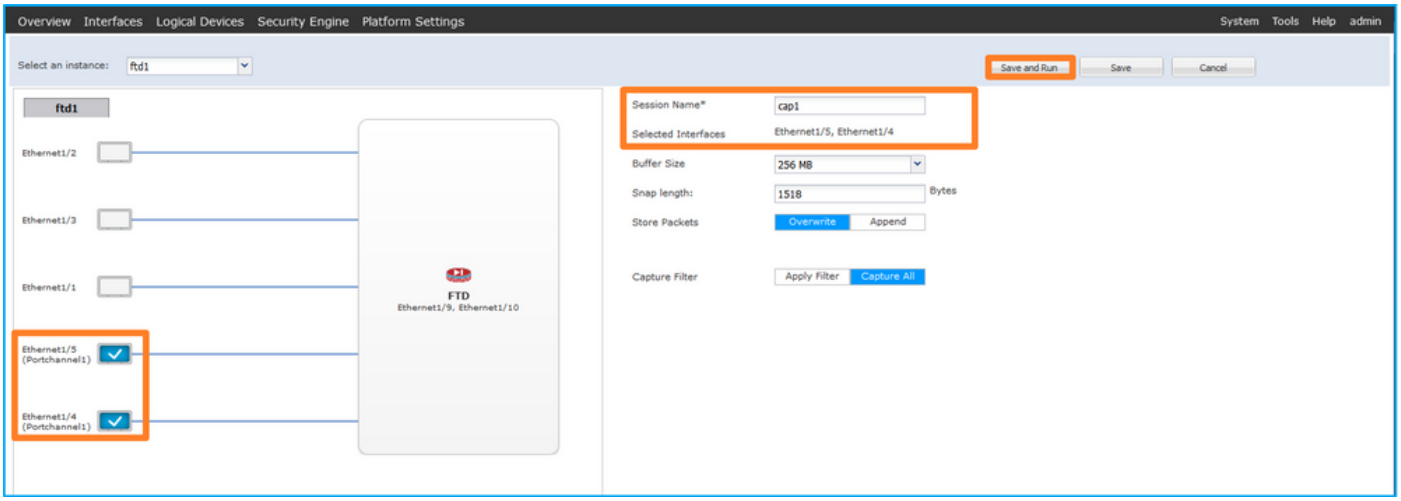
1. Utilisez **Outils > Capture de paquets > Session de capture** pour créer une nouvelle session de capture **:**



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



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



CLI FXOS

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

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

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

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

```
firepower# connect fxos
<output skipped>
firepower(fxos)# show port-channel summary
Flags:  D - Down         P - Up in port-channel (members)
        I - Individual   H - Hot-standby (LACP only)
        s - Suspended    r - Module-removed
        S - Switched     R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
1     Po1(SU)     Eth      LACP      Eth1/4(P)    Eth1/5(P)
```

3. Créez une session de capture :

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

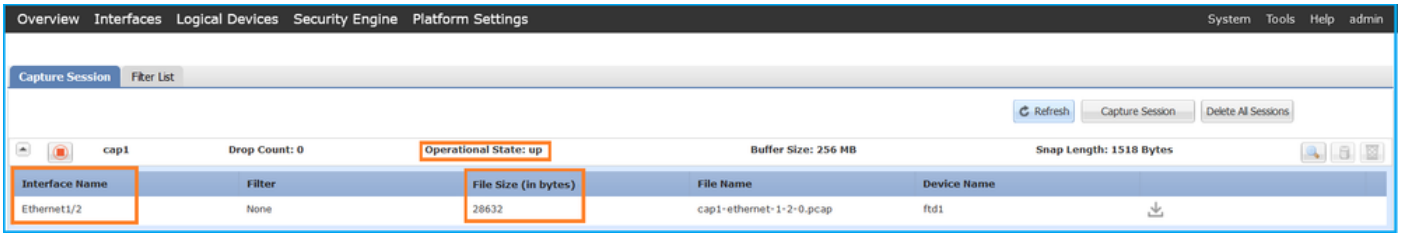
Pour les interfaces port-channel, une capture distincte est configurée pour chaque interface membre :

```
firepower# scope packet-capture
firepower /packet-capture # create session cap1
firepower /packet-capture/session* # create phy-port Eth1/4
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # set app-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 #
```

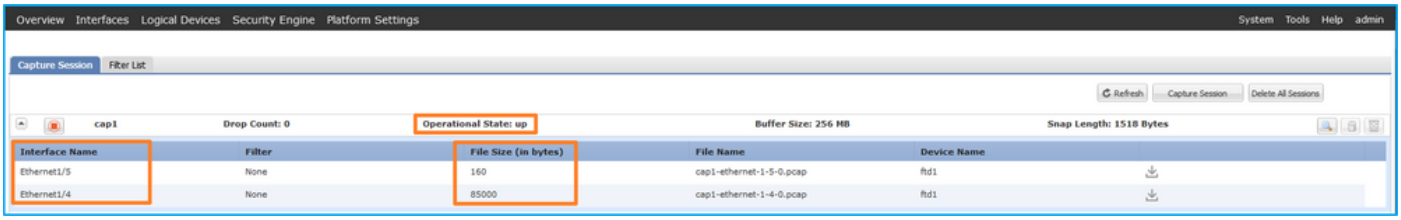
Vérification

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** :

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

Traffic Monitoring Session:
    Packet Capture Session Name: cap1
   Session: 1
    Admin State: Enabled
    Oper State: Up
    Oper State Reason: Active
   Config Success: Yes
   Config Fail Reason:
   Append Flag: Overwrite
   Session Mem Usage: 256  MB
```

```
   Session Pcap Snap Len: 1518  Bytes
   Error Code: 0
   Drop Count: 0

Physical ports involved in Packet Capture:
    Slot Id: 1
    Port Id: 2
    Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap
    Pcapsize: 75136  bytes
   Filter:
   Sub Interface: 0
    Application Instance Identifier: ftd1
    Application Name: ftd
```

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

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

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

Physical ports involved in Packet Capture:
   Slot Id: 1
    Port Id: 4
    Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-4-0.pcap
    Pcapsize: 310276  bytes
   Filter:
   Sub Interface: 0
    Application Instance Identifier: ftd1
    Application Name: ftd

   Slot Id: 1
    Port Id: 5
    Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-5-0.pcap
    Pcapsize: 160  bytes
   Filter:
   Sub Interface: 0
    Application Instance Identifier: ftd1
    Application Name: ftd
```

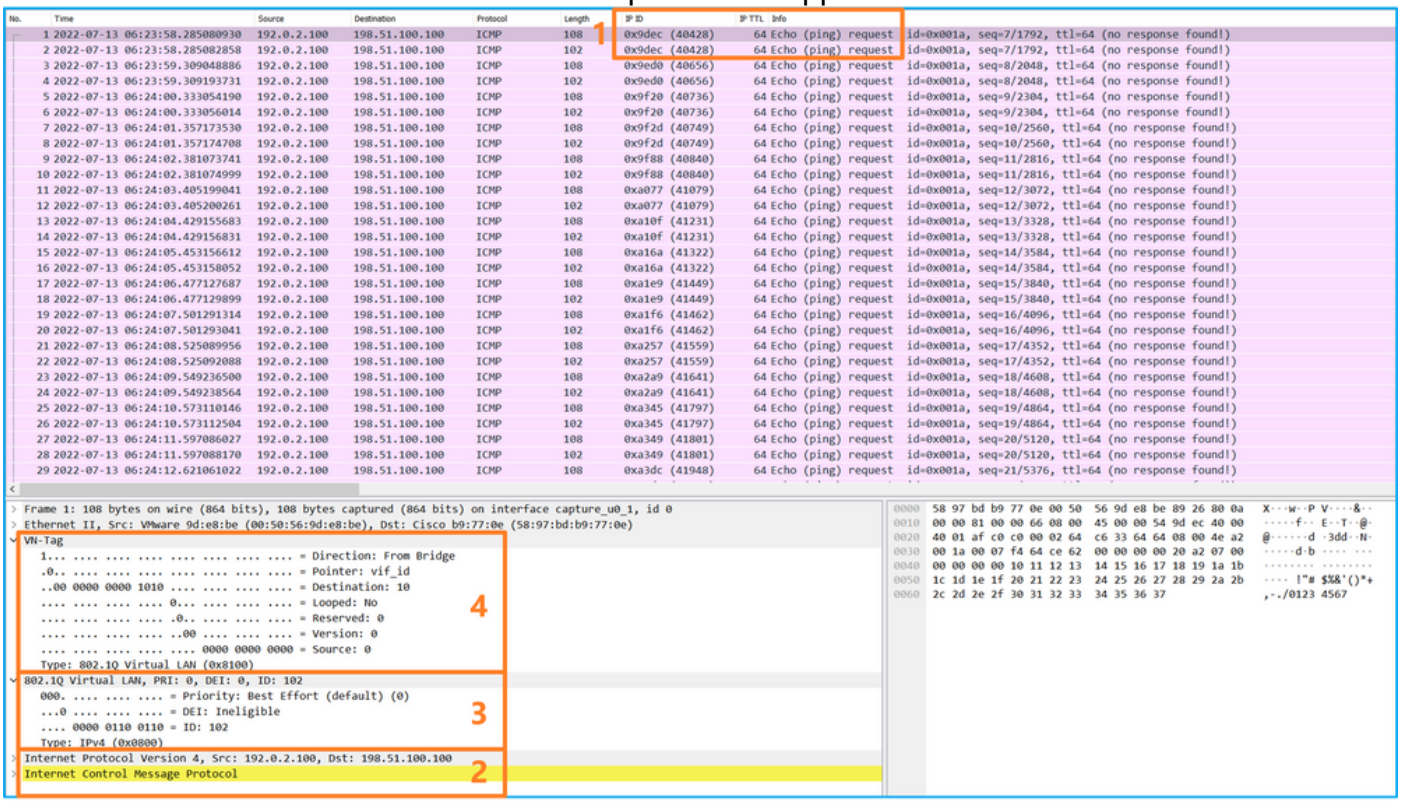
Collecter les fichiers de capture

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

Capturer l'analyse des fichiers

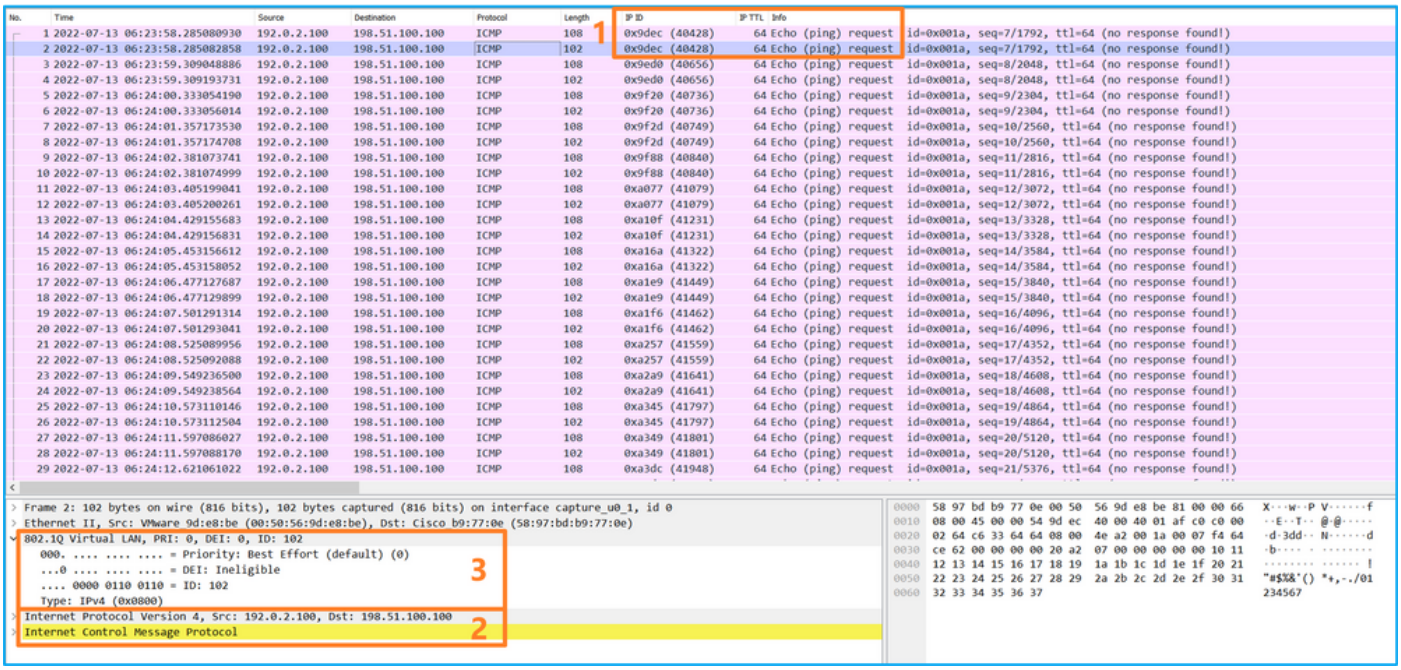
Utilisez une application de lecture de fichier de capture de paquets pour ouvrir le fichier de capture pour Ethernet1/2. Sélectionnez le premier paquet et vérifiez les points clés :

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



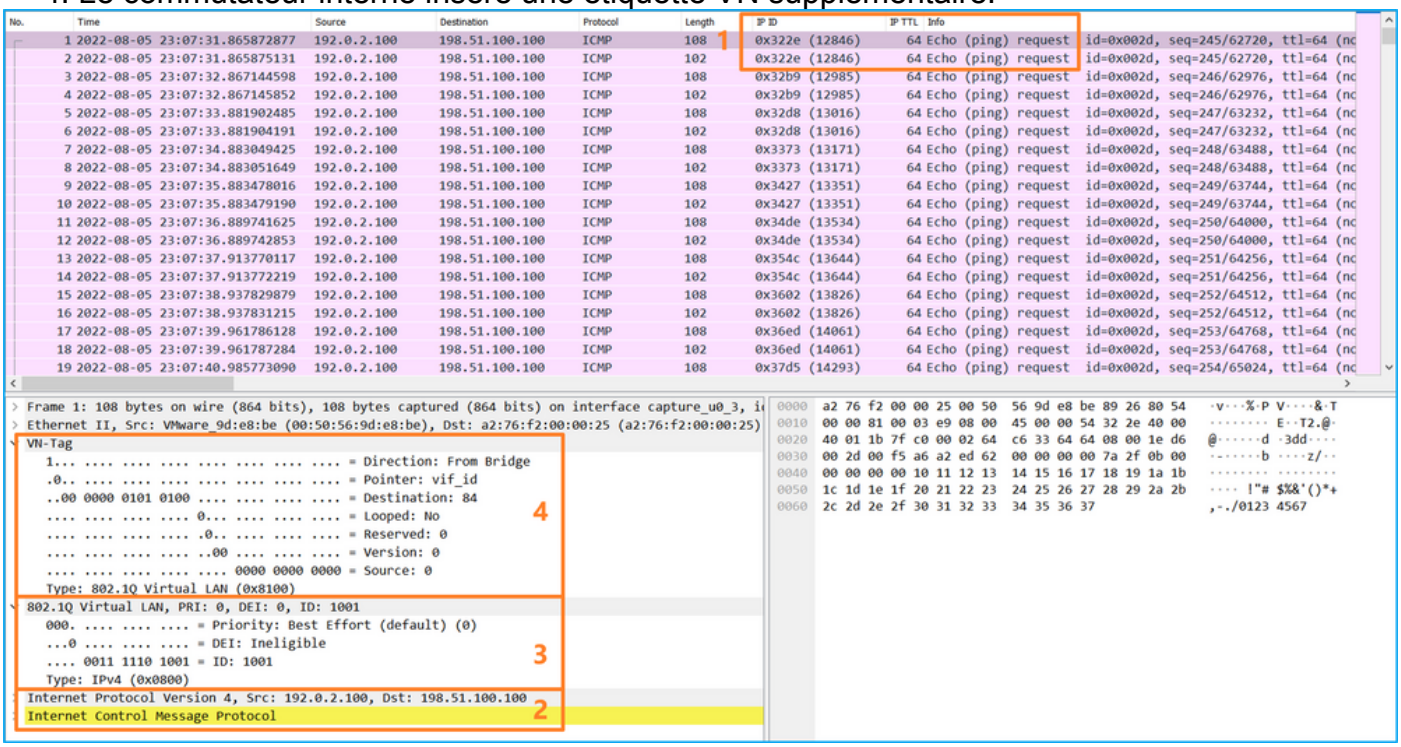
Sélectionnez le deuxième paquet et vérifiez les points clés :

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 :

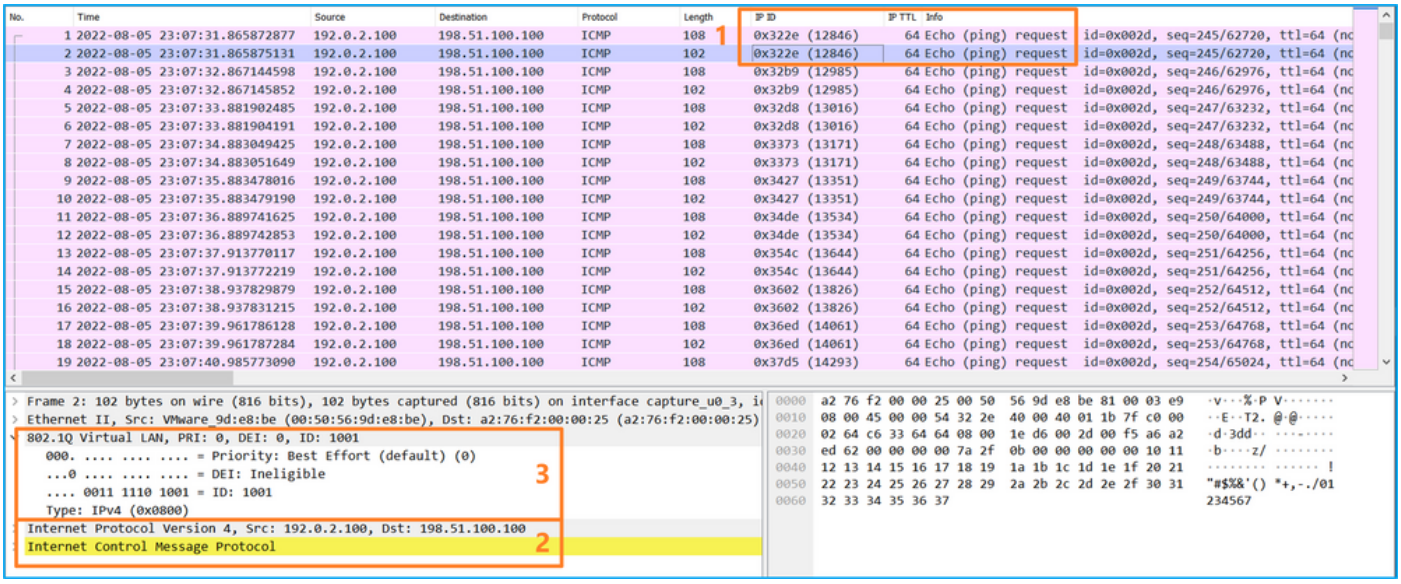
1. Seuls les paquets de requête d'écho ICMP sont capturés. Chaque paquet est capturé et affiché 2 fois.
2. L'en-tête de paquet d'origine est sans étiquette VLAN.
3. Le commutateur interne insère une étiquette VLAN de port supplémentaire **1001** qui identifie l'interface d'entrée Portchannel1.
4. Le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

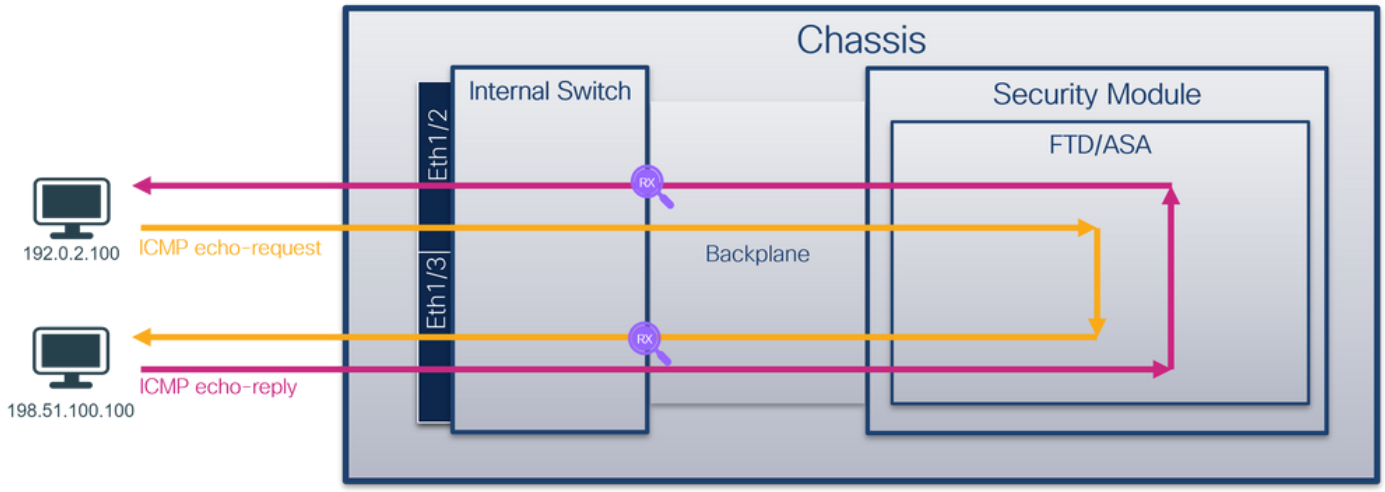
Ce tableau récapitule la tâche :

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

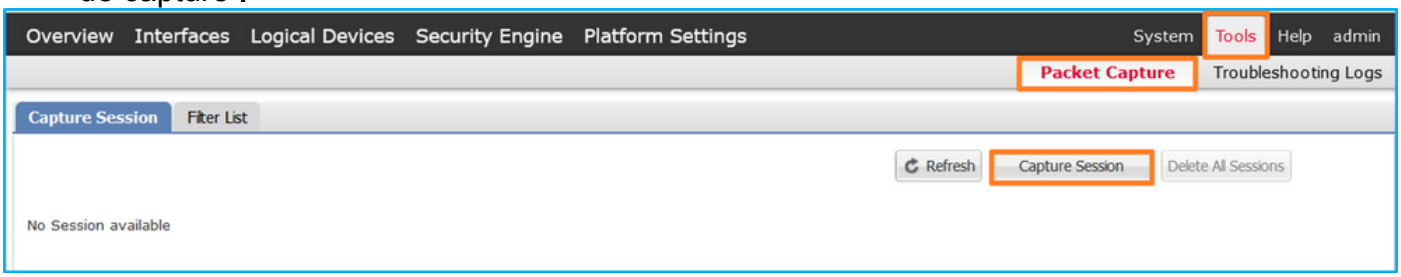


Configuration

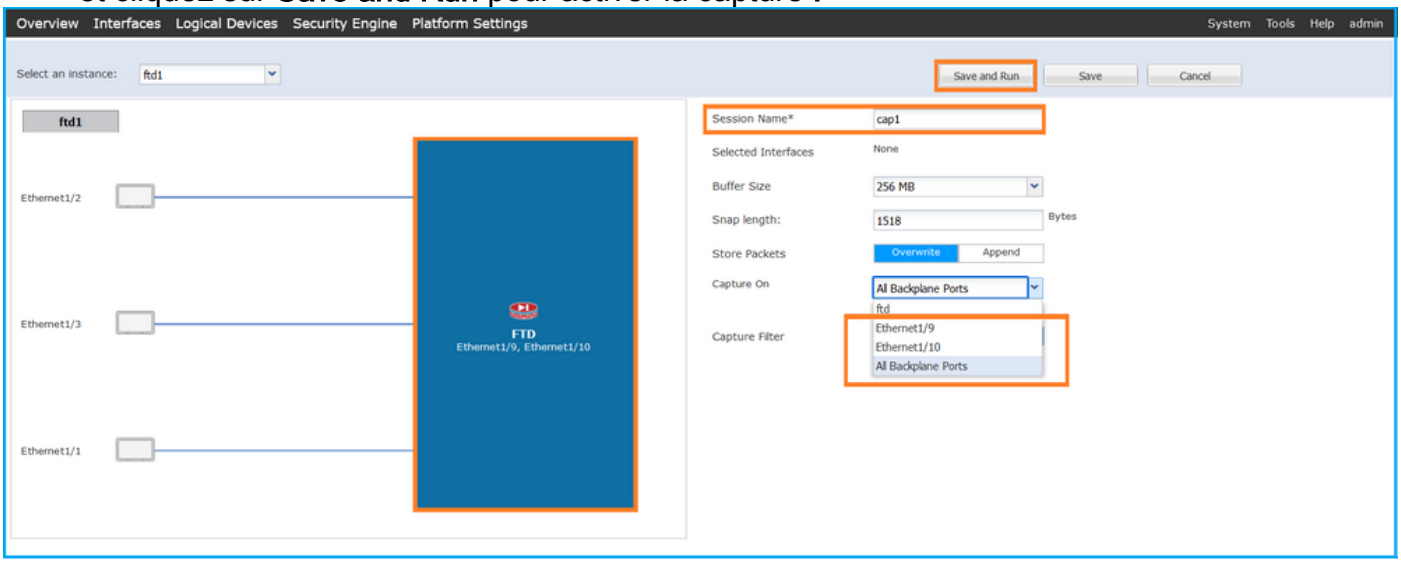
FCM

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 :

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

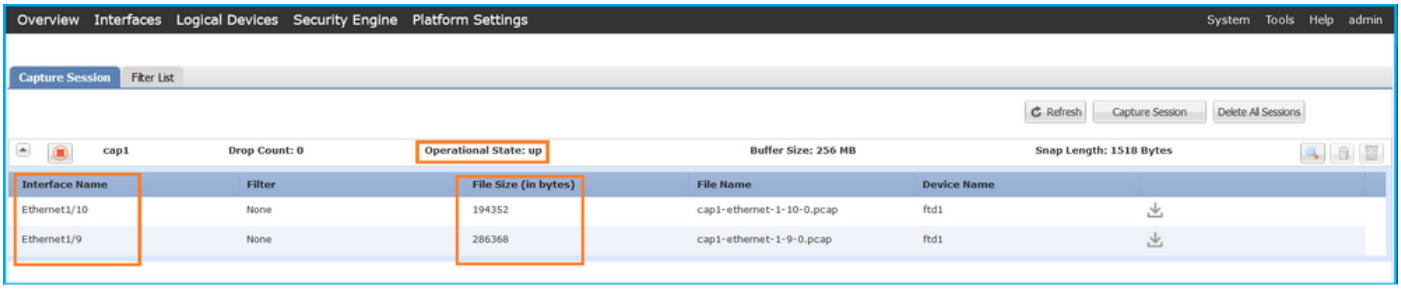
2. Créez une session de capture :

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

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

Traffic Monitoring Session:
    Packet Capture Session Name: cap1
   Session: 1
   Admin State: Enabled
    Oper State: Up
```

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

Physical ports involved in Packet Capture:
    Slot Id: 1
     Port Id: 10
     Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-10-0.pcap
     Pcapsize: 1017424  bytes
    Filter:
    Sub Interface: 0
     Application Instance Identifier: ftd1
     Application Name: ftd

     Slot Id: 1
     Port Id: 9
     Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-9-0.pcap
     Pcapsize: 1557432  bytes
    Filter:
    Sub Interface: 0
     Application Instance Identifier: ftd1
     Application Name: ftd
```

Collecter les fichiers de capture

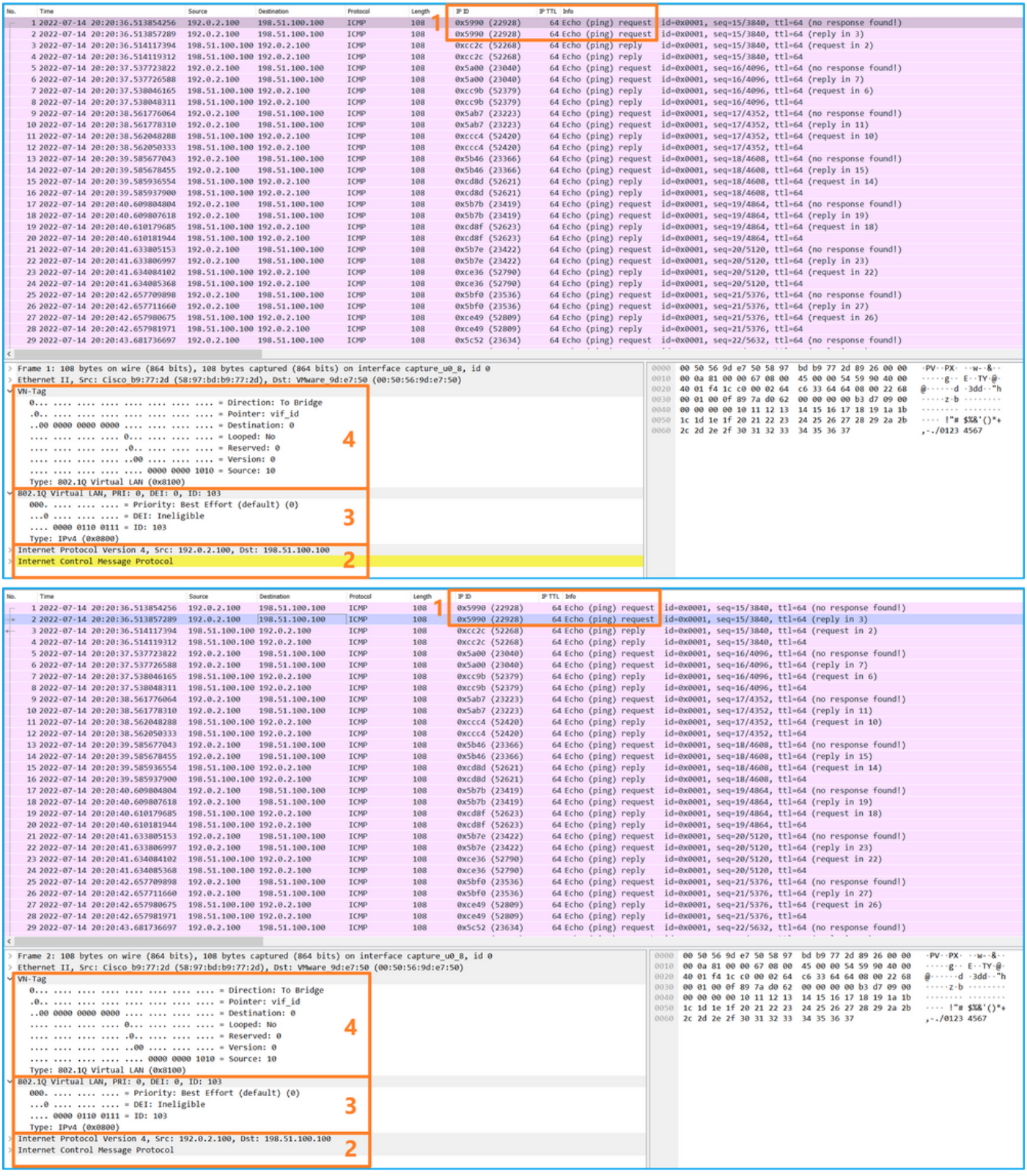
Suivez les étapes de la section **Collecter les fichiers de capture internes du commutateur Firepower 4100/9300**.

Capturer l'analyse des fichiers

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

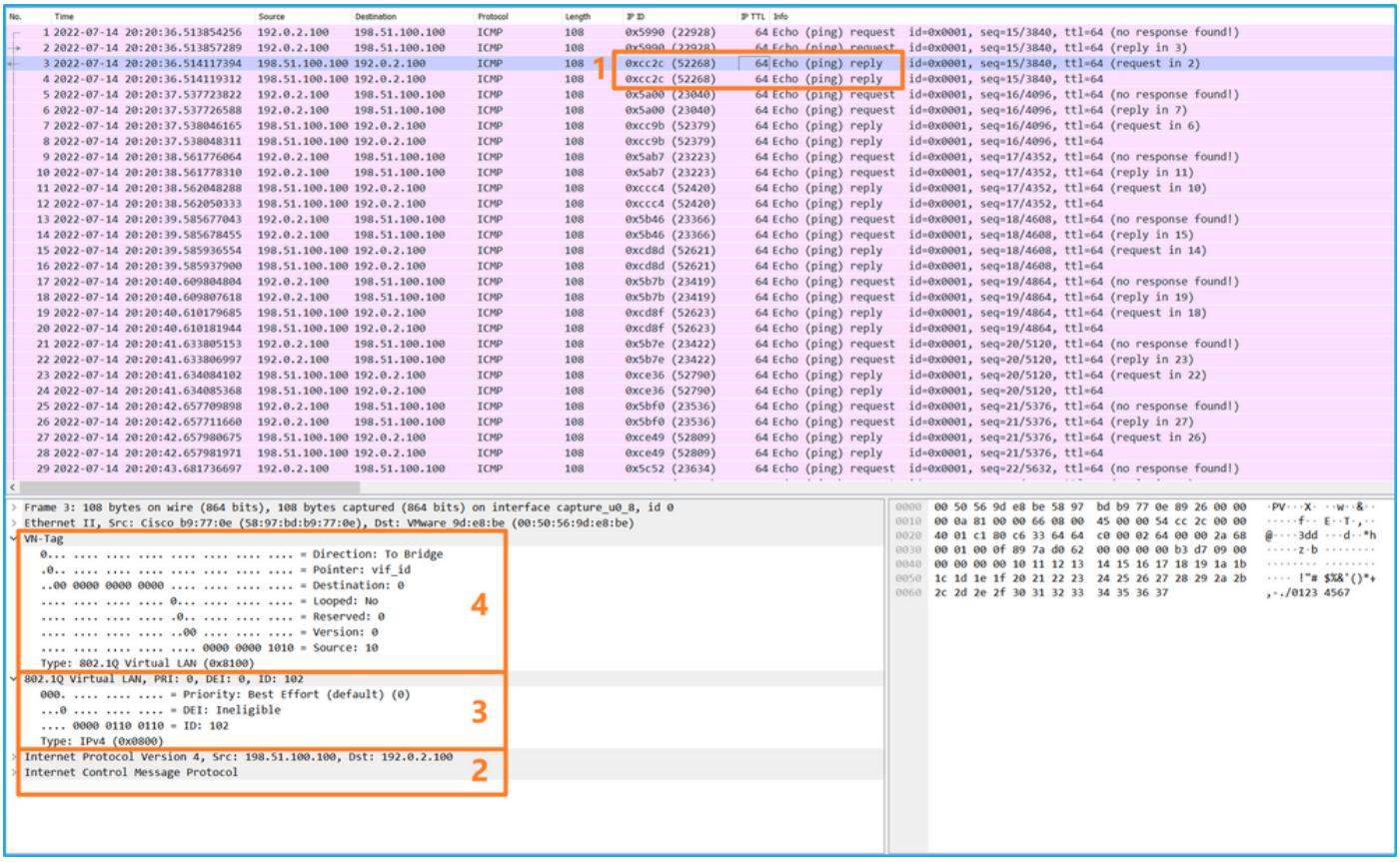
Sélectionnez le premier et le deuxième paquet, puis vérifiez les points clés :

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



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

Captures de paquets sur les ports des applications et des applications

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

Il existe principalement 2 cas d'utilisation :

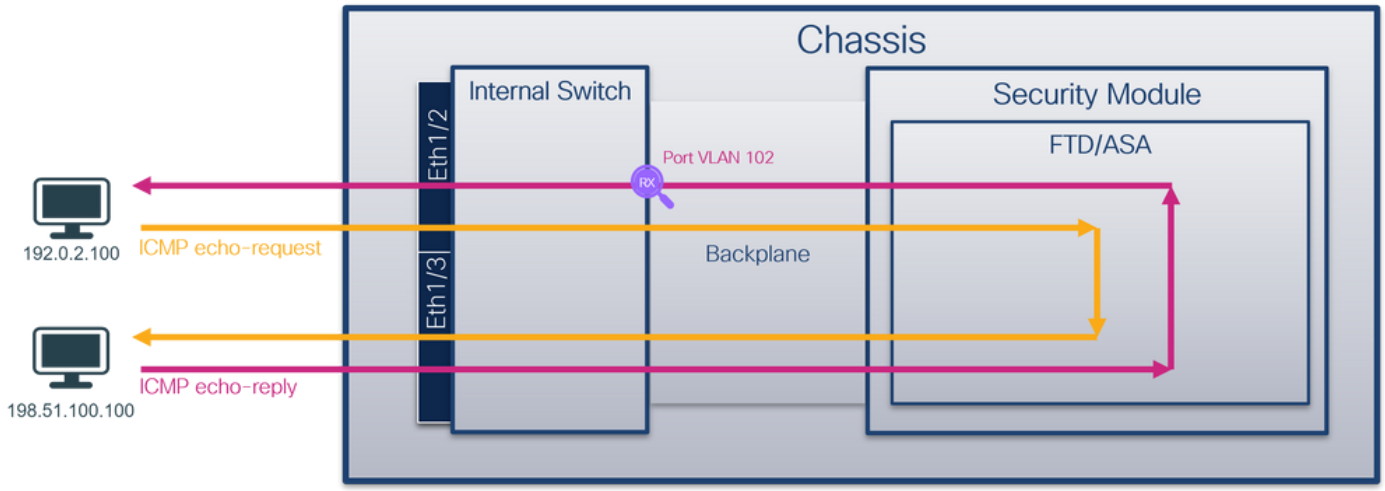
- Configurez les captures de paquets sur les interfaces de fond de panier pour les paquets qui quittent une interface avant spécifique. Par exemple, configurez les captures de paquets sur l'interface de fond de panier Ethernet1/9 pour les paquets qui quittent l'interface Ethernet1/2.
- Configurez des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

Cette section couvre les deux cas d'utilisation.

Tâche 1

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

Topologie, flux de paquets et points de capture

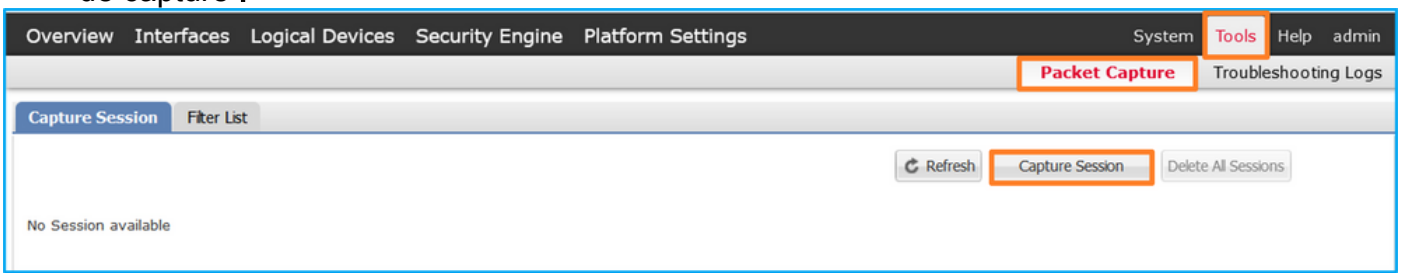


Configuration

FCM

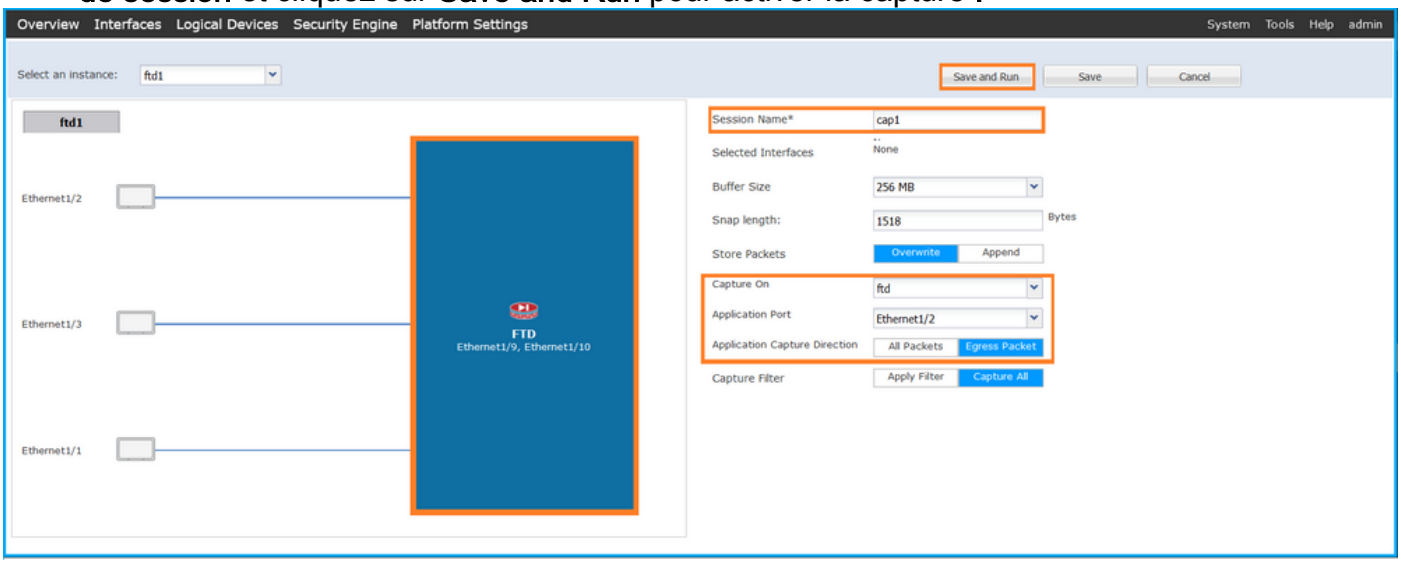
Procédez comme suit sur FCM pour configurer une capture de paquets sur l'application FTD et le port d'application Ethernet1/2 :

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



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

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



CLI FXOS

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

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

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

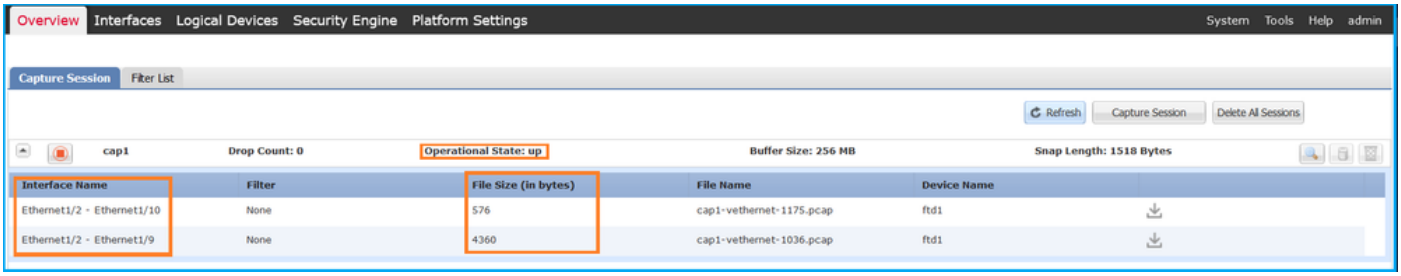
2. Créez une session de capture :

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

Vérification

FCM

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



CLI FXOS

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

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

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

Application ports involved in Packet Capture:
    Slot Id: 1
    Link Name: 112
    Port Name: Ethernet1/2
   App Name: ftd
   Sub Interface: 0
    Application Instance Identifier: ftd1

Application ports resolved to:
    Name: vnic1
    Eq Slot Id: 1
    Eq Port Id: 9
    Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1036.pcap
    Pcapsize: 53640  bytes
   Vlan: 102
   Filter:

   Name: vnic2
    Eq Slot Id: 1
    Eq Port Id: 10
    Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1175.pcap
    Pcapsize: 1824  bytes
   Vlan: 102
   Filter:
```

Collecter les fichiers de capture

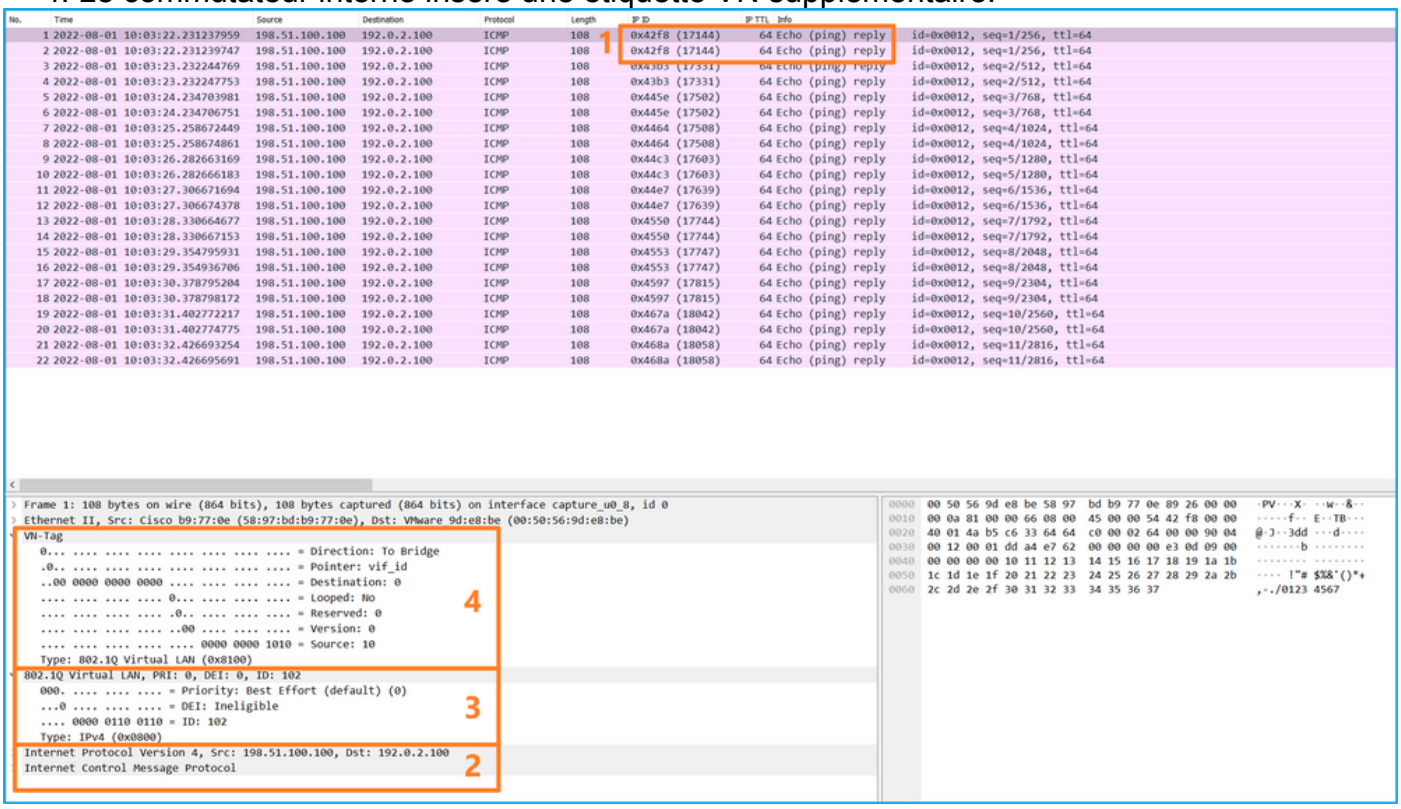
Suivez les étapes de la section **Collecter les fichiers de capture internes du commutateur Firepower 4100/9300**.

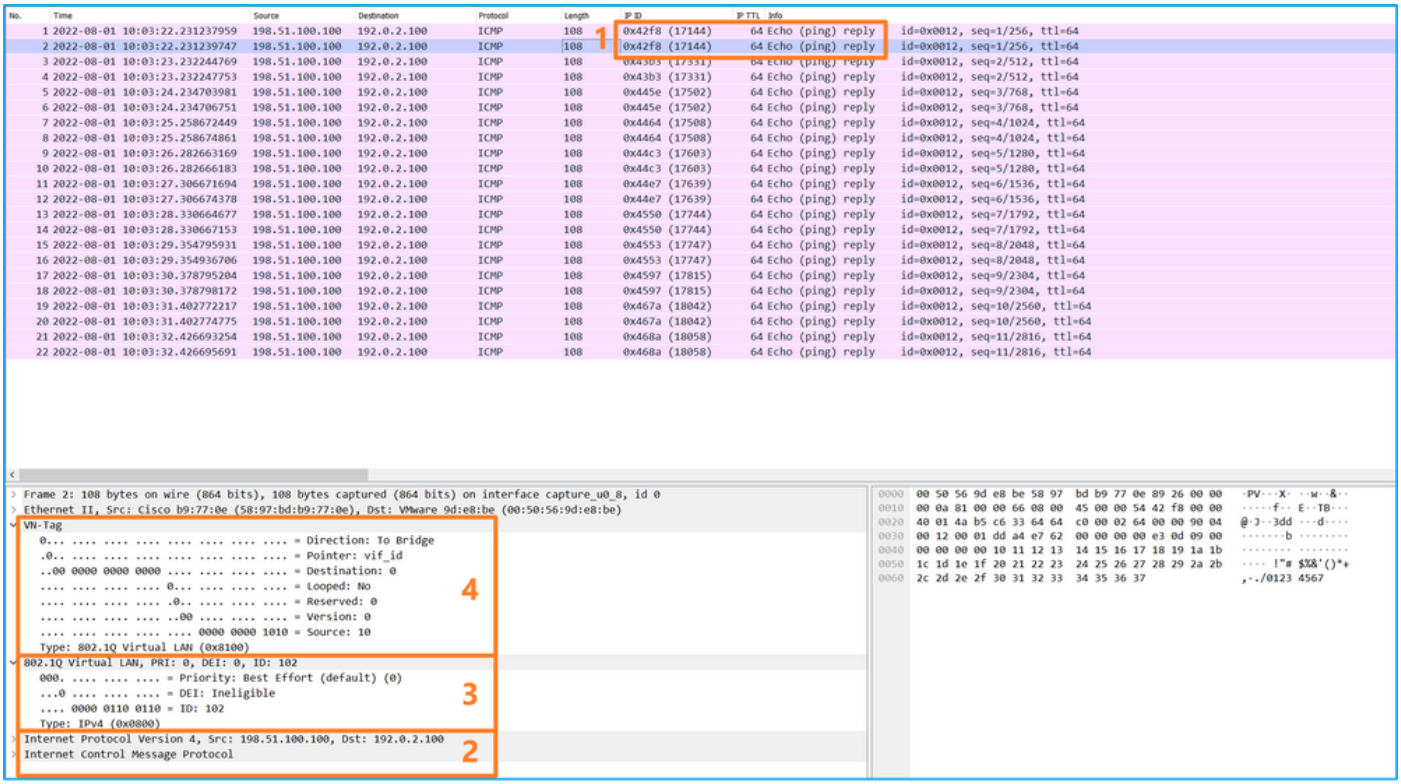
Capturer l'analyse des fichiers

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

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

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





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'h 198.51.100.100 à l'hôte 192.0.2.100

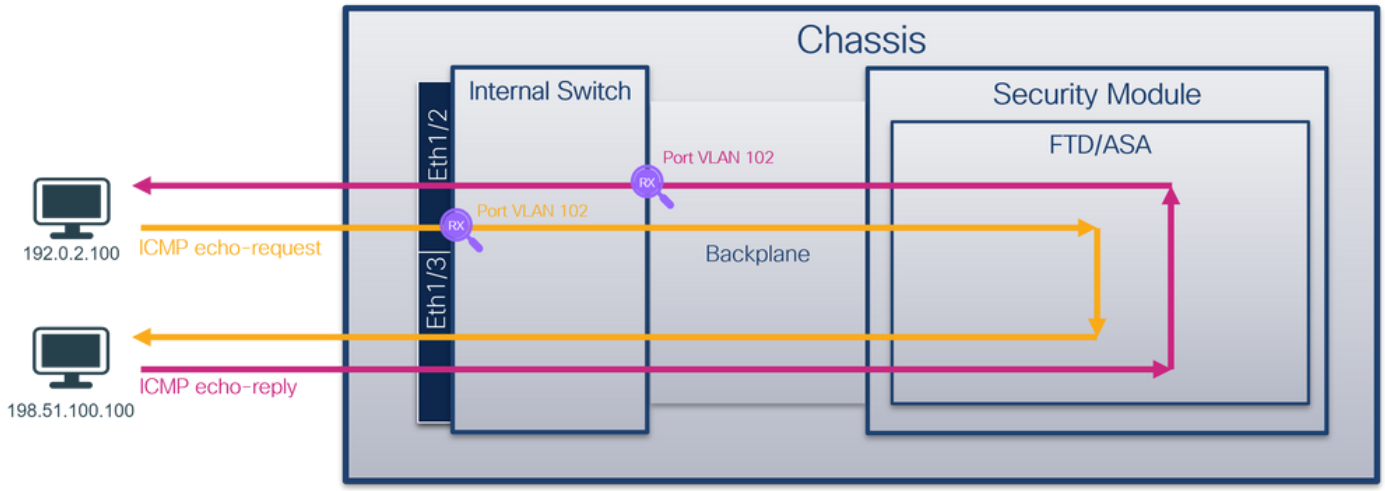
Tâche 2

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

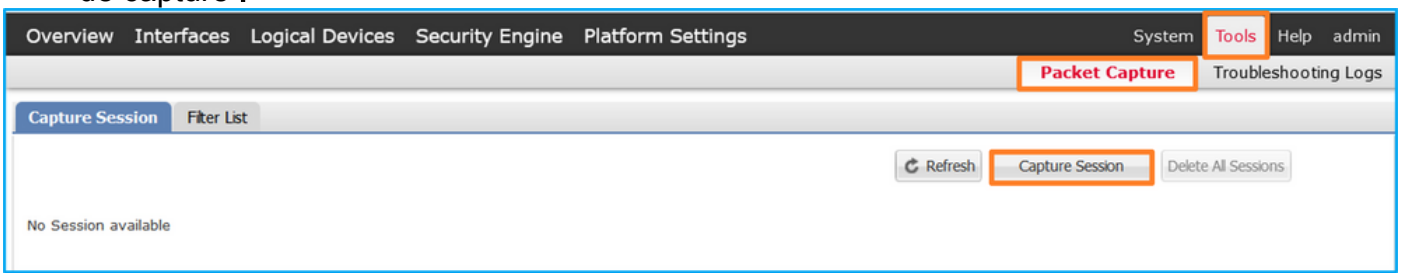


Configuration

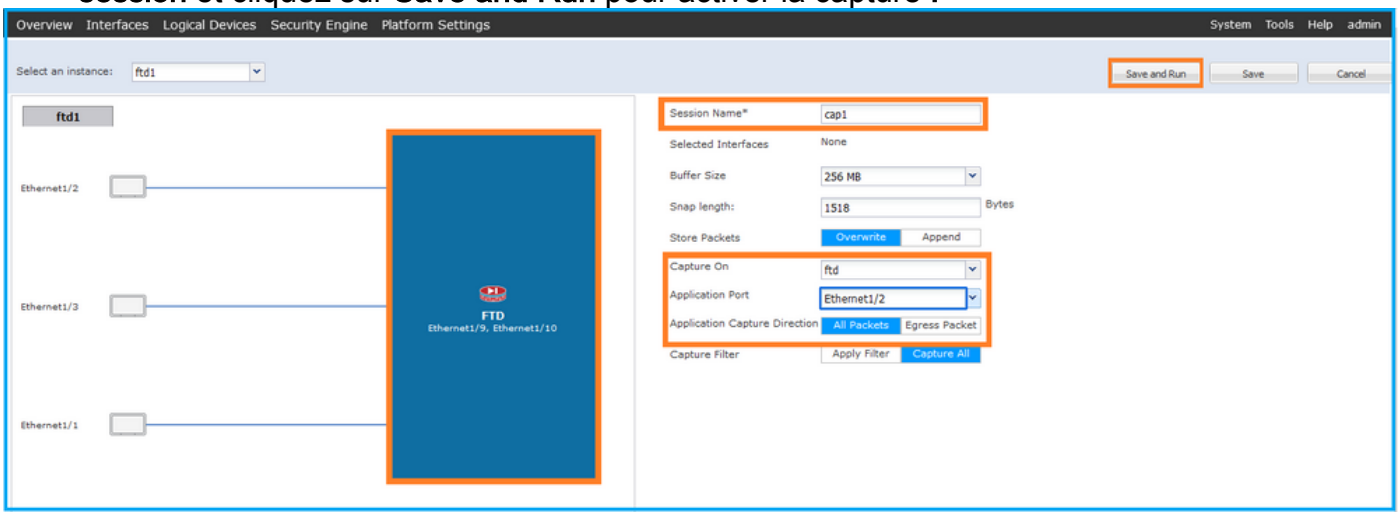
FCM

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 :

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

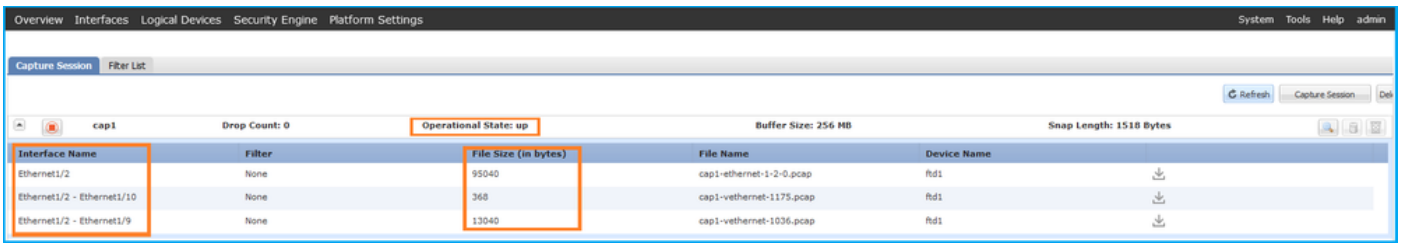
2. Créez une session de capture :

```
firepower# scope packet-capture
firepower /packet-capture # create session cap1
firepower /packet-capture/session* # create phy-port eth1/2
firepower /packet-capture/session/phy-port* # set app-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** :

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

Traffic Monitoring Session:
    Packet Capture Session Name: cap1
   Session: 1
    Admin State: Enabled
    Oper State: Up
    Oper State Reason: Active
   Config Success: Yes
   Config Fail Reason:
   Append Flag: Overwrite
```

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

Physical ports involved in Packet Capture:
    Slot Id: 1
    Port Id: 2
    Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap
    Pcapsize: 410444  bytes
   Filter:
   Sub Interface: 0
    Application Instance Identifier: ftd1
    Application Name: ftd

Application ports involved in Packet Capture:
   Slot Id: 1
    Link Name: link12
    Port Name: Ethernet1/2
    App Name: ftd
   Sub Interface: 0
    Application Instance Identifier: ftd1

Application ports resolved to:
   Name: vnic1
   Eq Slot Id: 1
    Eq Port Id: 9
    Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1036.pcap
    Pcapsize: 128400  bytes
    Vlan: 102
   Filter:

   Name: vnic2
   Eq Slot Id: 1
    Eq Port Id: 10
    Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1175.pcap
    Pcapsize: 2656  bytes
    Vlan: 102
   Filter:
```

Collecter les fichiers de capture

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

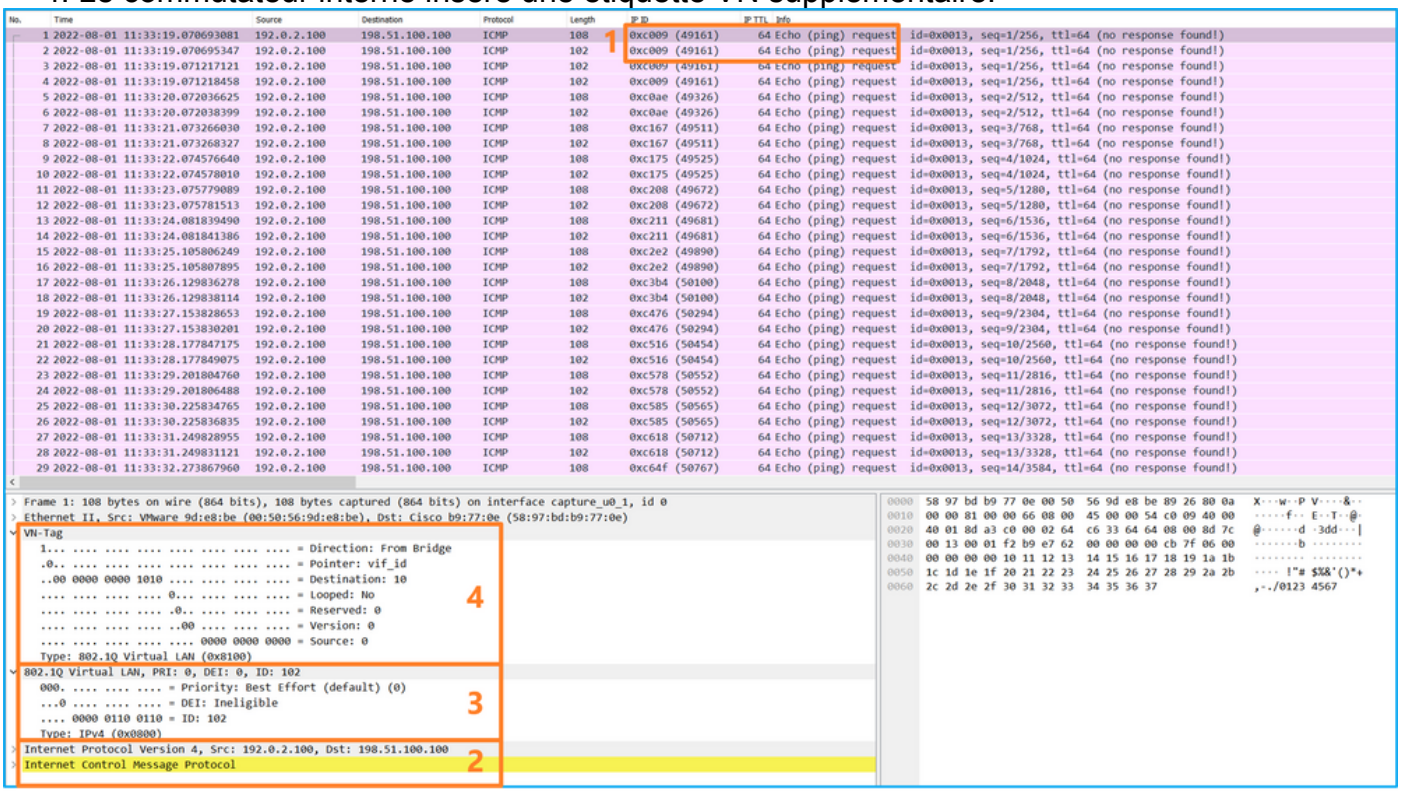
Capturer l'analyse des fichiers

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

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

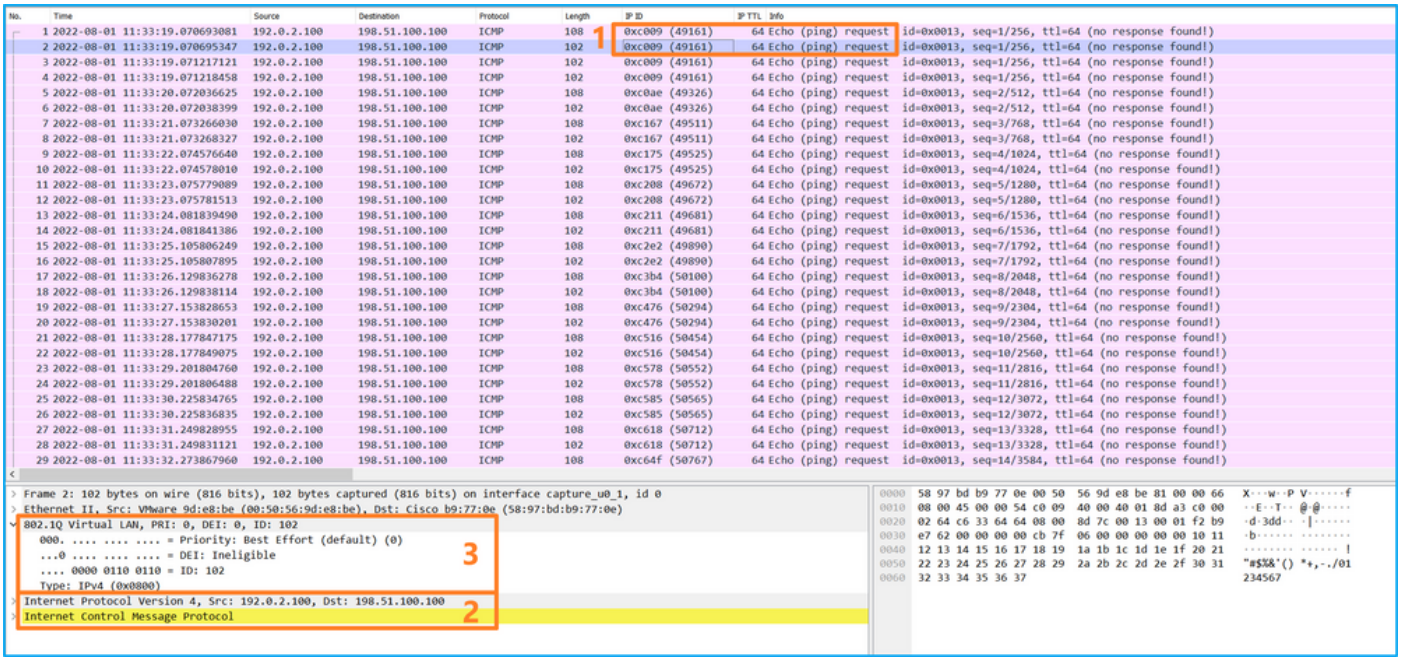
1. Seuls les paquets de requête d’écho ICMP sont capturés. Chaque paquet est capturé et affiché 2 fois.
2. L'en-tête de paquet d'origine est sans étiquette VLAN.
3. Le commutateur interne insère une étiquette VLAN de port supplémentaire **102** qui identifie l'interface d'entrée Ethernet1/2.

4. Le commutateur interne insère une étiquette VN supplémentaire.



Sélectionnez le deuxième paquet et vérifiez les points clés :

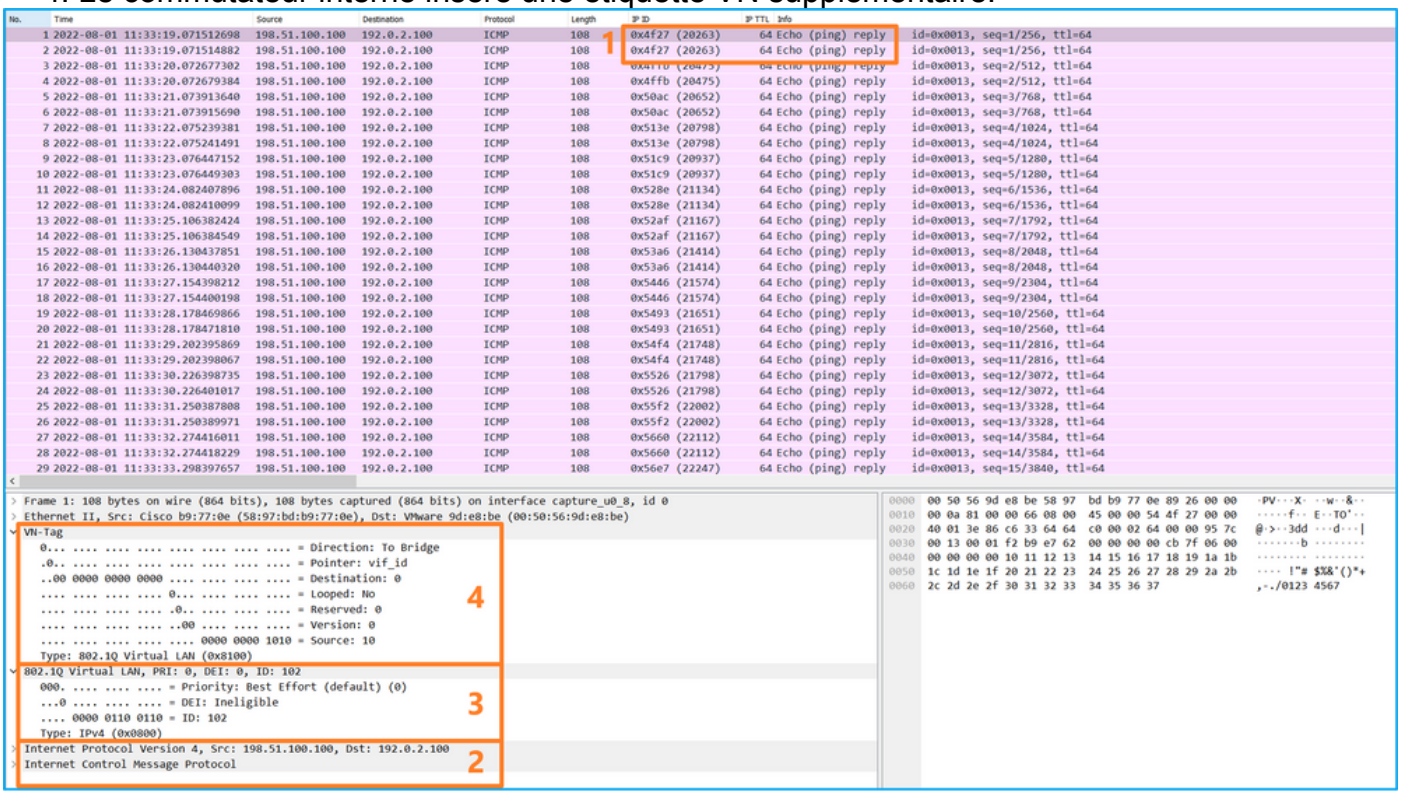
1. Seuls les paquets de requête d'écho ICMP sont capturés. Chaque paquet est capturé et affiché 2 fois.
2. L'en-tête de paquet d'origine est sans étiquette VLAN.
3. Le commutateur interne insère une étiquette VLAN de port supplémentaire **102** qui identifie l'interface d'entrée Ethernet1/2.

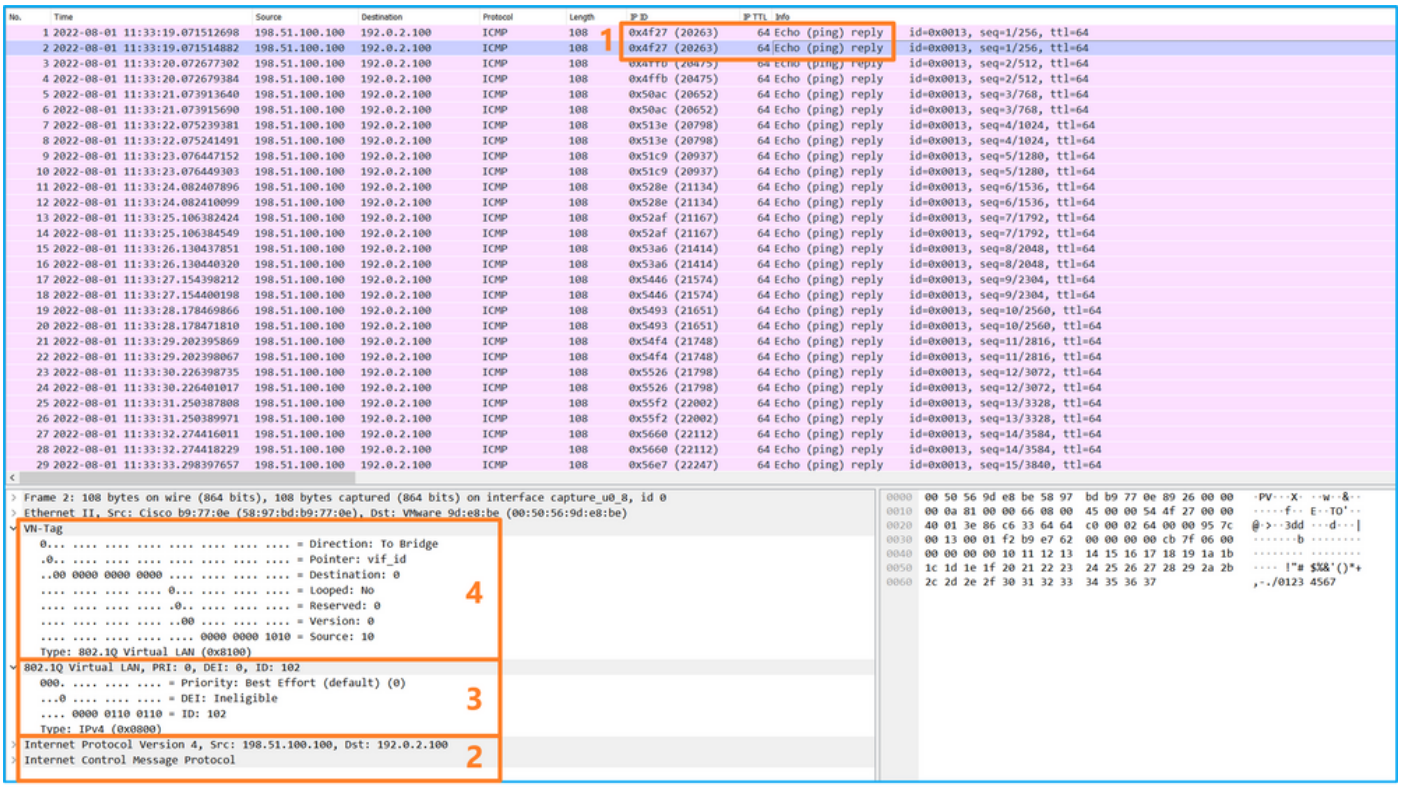


Ouvrez le fichier de capture pour l'interface Ethernet1/9, sélectionnez le premier et le deuxième paquet, puis vérifiez les points clés :

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.

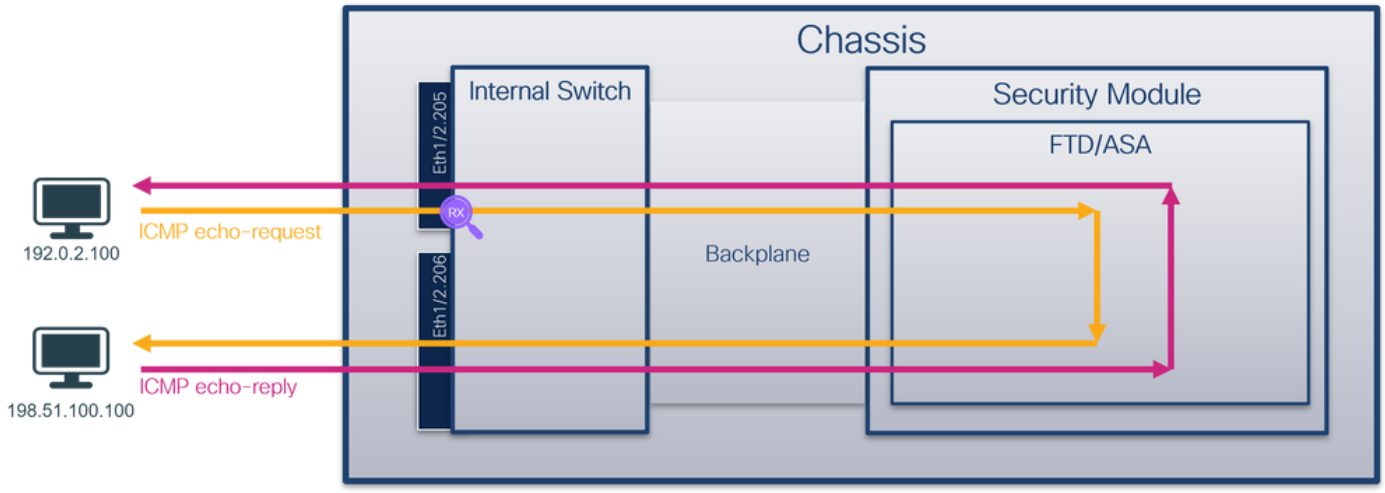
Ce tableau récapitule la tâche :

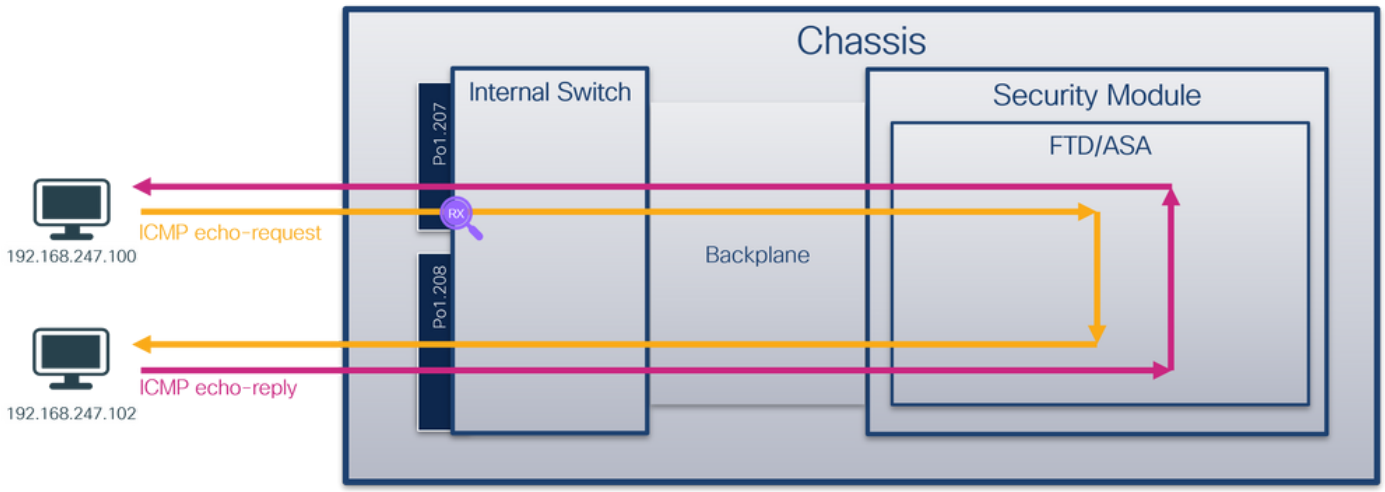
Tâche	Point de capture	VLAN de port interne dans les paquets capturés	Direction	Trafic capturé
Configuration et vérification des captures sur l'application et le port d'application Ethernet1/2	Interfaces du fond de panier	102	Entrée uniquement	Réponses d'écho ICMP de l'h 198.51.100.100 à l'hôte 192.0.2.100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



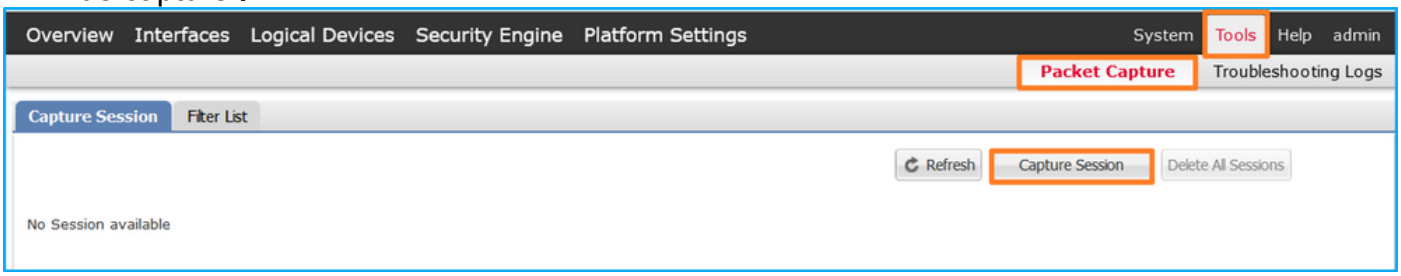


Configuration

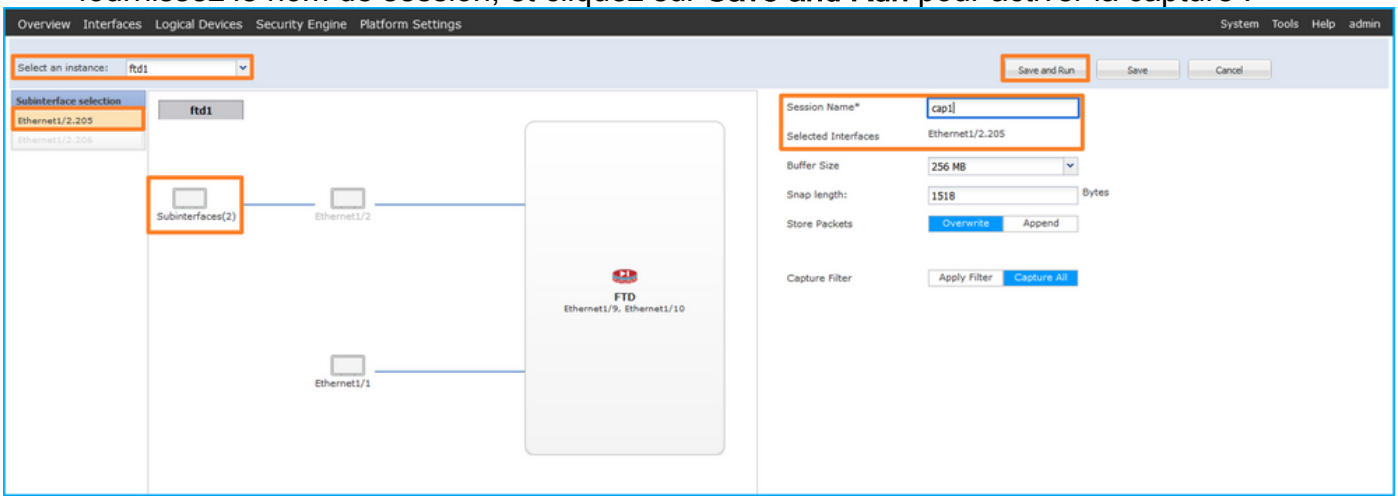
FCM

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 :

```
firepower# scope ssa
firepower /ssa #  show app-instance
App Name   Identifier Slot ID    Admin State Oper State       Running Version Startup Version
Deploy Type Turbo Mode Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- --------------- -------------- --------------- --
--------- ---------- ------------ --------------- ------------
ftd        ftd1       1          Enabled     Online          7.2.0.82       7.2.0.82
Container   No         RP20         Not Applicable  None
ftd        ftd2       1          Enabled     Online          7.2.0.82       7.2.0.82
Container   No         RP20         Not Applicable  None
```

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

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

3. Créez une session de capture :

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

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

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

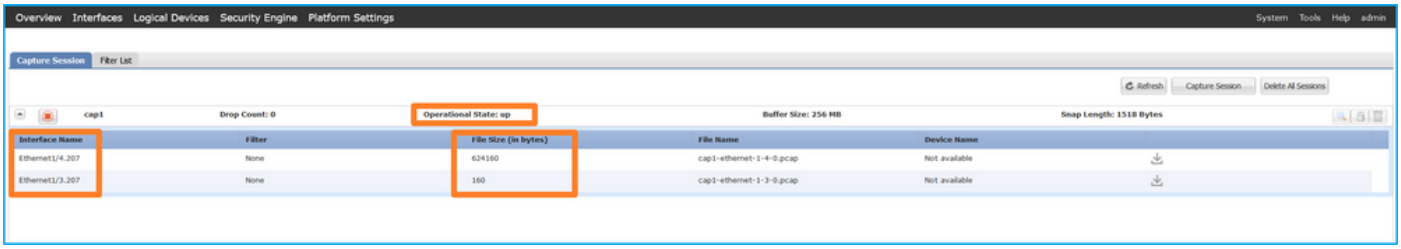
```
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # set app-identifier ftd1
firepower /packet-capture/session/phy-port* # set subinterface 207
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # enable
firepower /packet-capture/session* # commit
firepower /packet-capture/session #
```

Vérification

FCM

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

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** :

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

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

Physical ports involved in Packet Capture:
    Slot Id: 1
    Port Id: 2
    Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap
    Pcapsize: 9324  bytes
   Filter:
```

```
    Sub Interface: 205
    Application Instance Identifier: ftd1
    Application Name: ftd
```

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

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

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

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

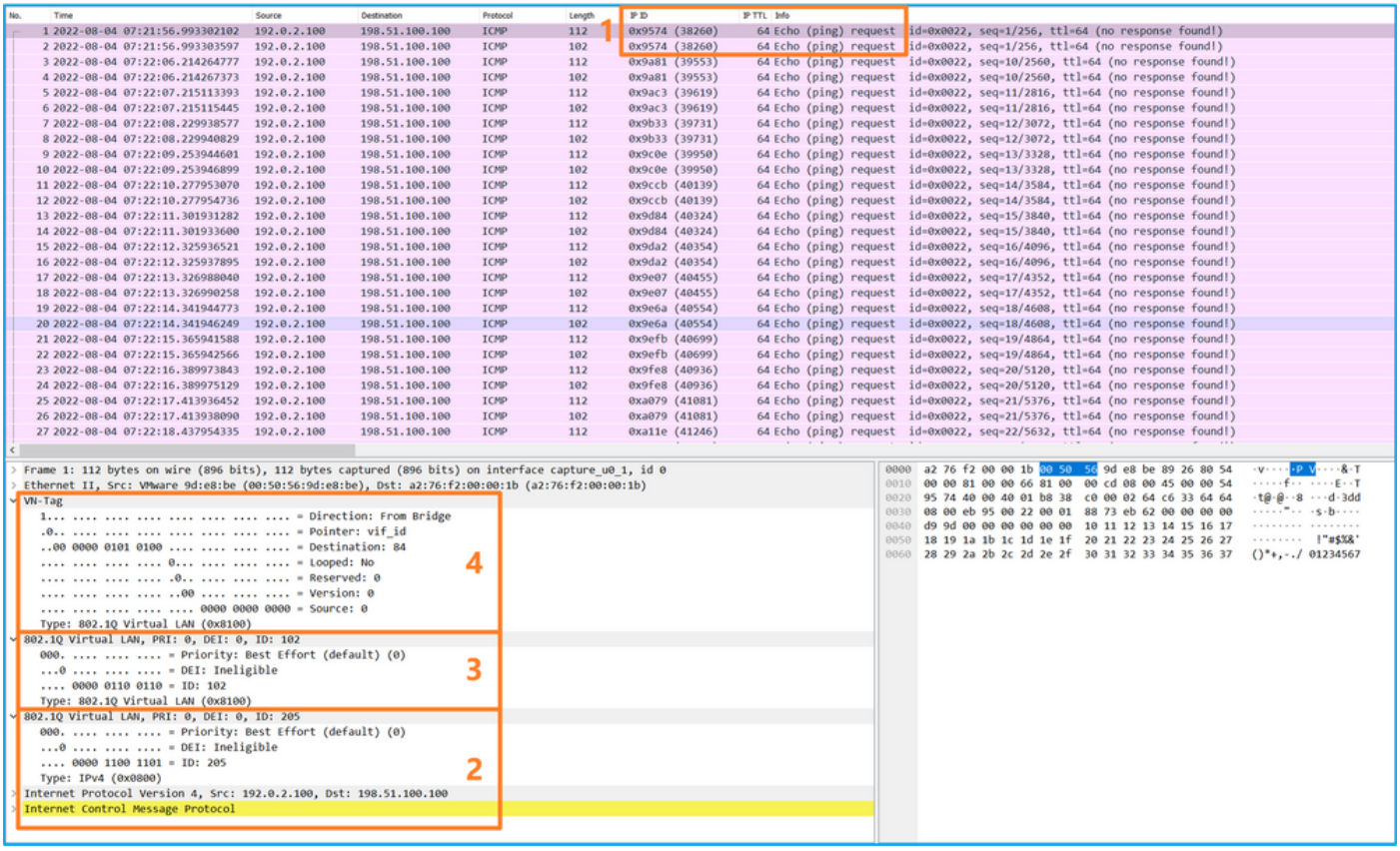
Collecter les fichiers de capture

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

Capturer l'analyse des fichiers

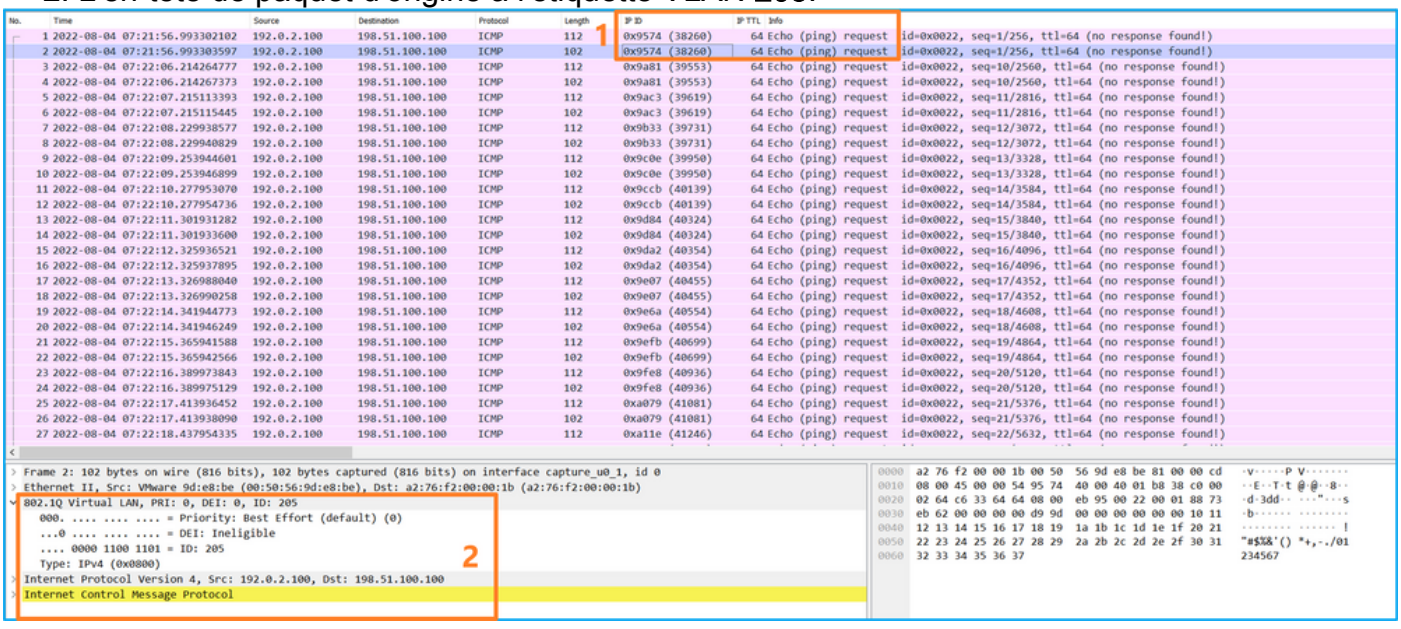
Utilisez une application de lecture de fichier de capture de paquets pour ouvrir le fichier de capture. Sélectionnez le premier paquet et vérifiez les points clés :

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



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**.

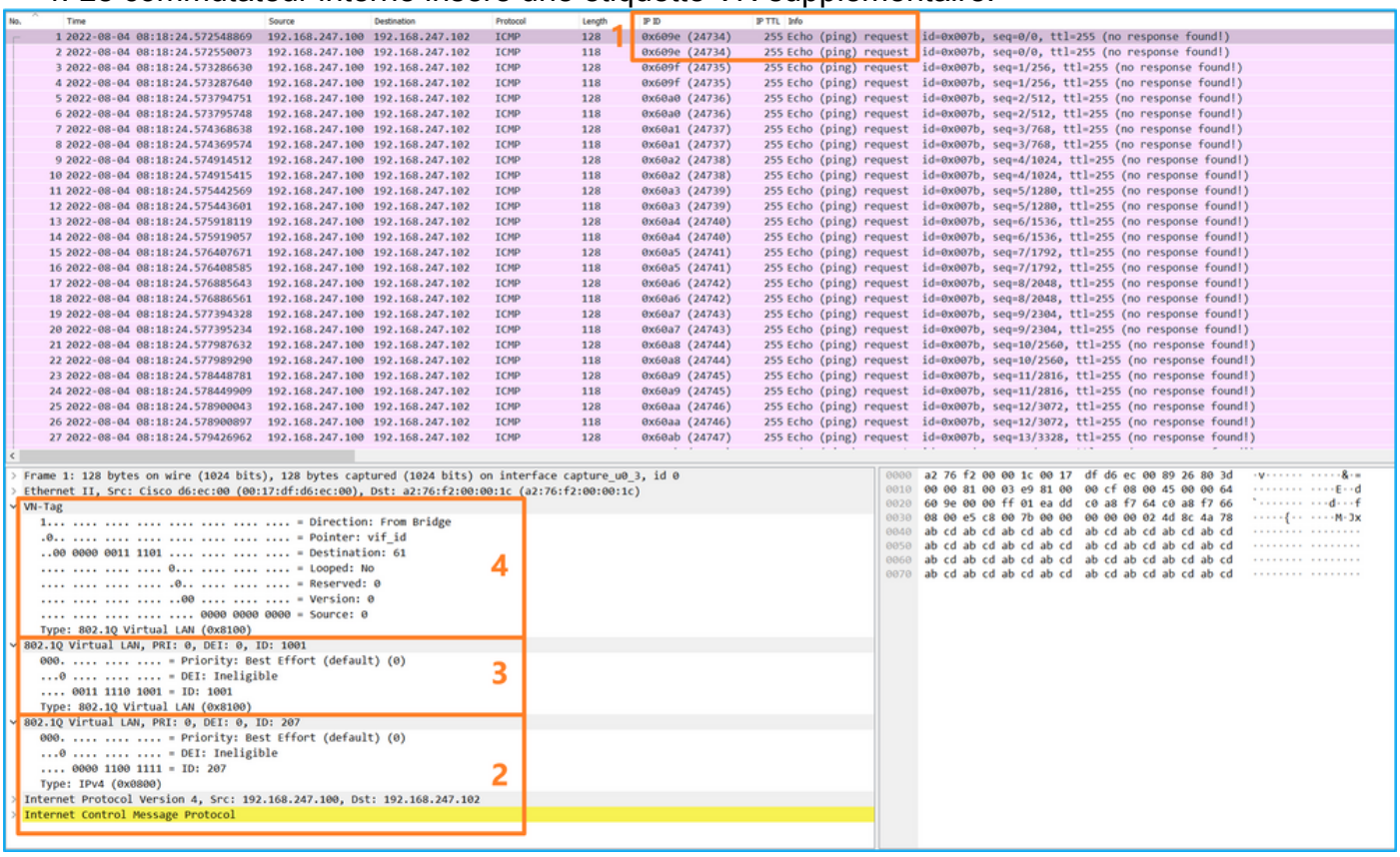


Ouvrez à présent les fichiers de capture pour Portchannel1.207. Sélectionnez le premier paquet et vérifiez les points clés

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

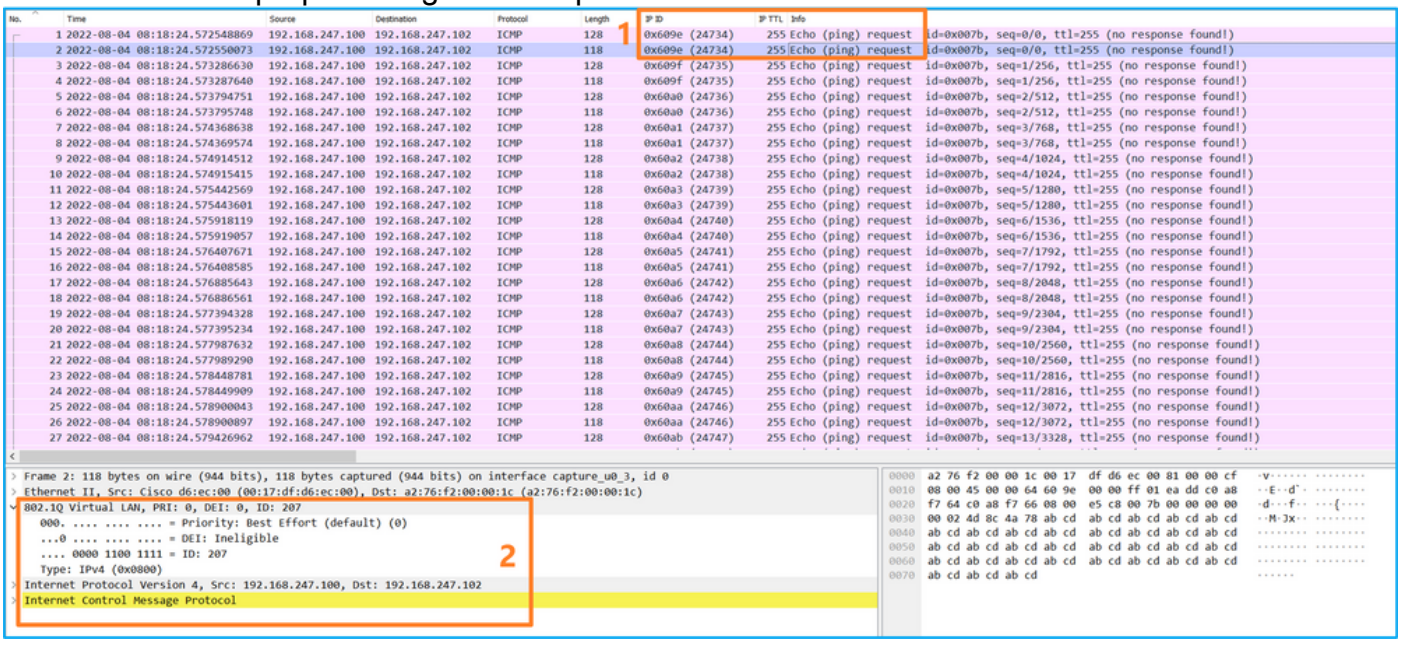
l'interface d'entrée Portchannel1.

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.

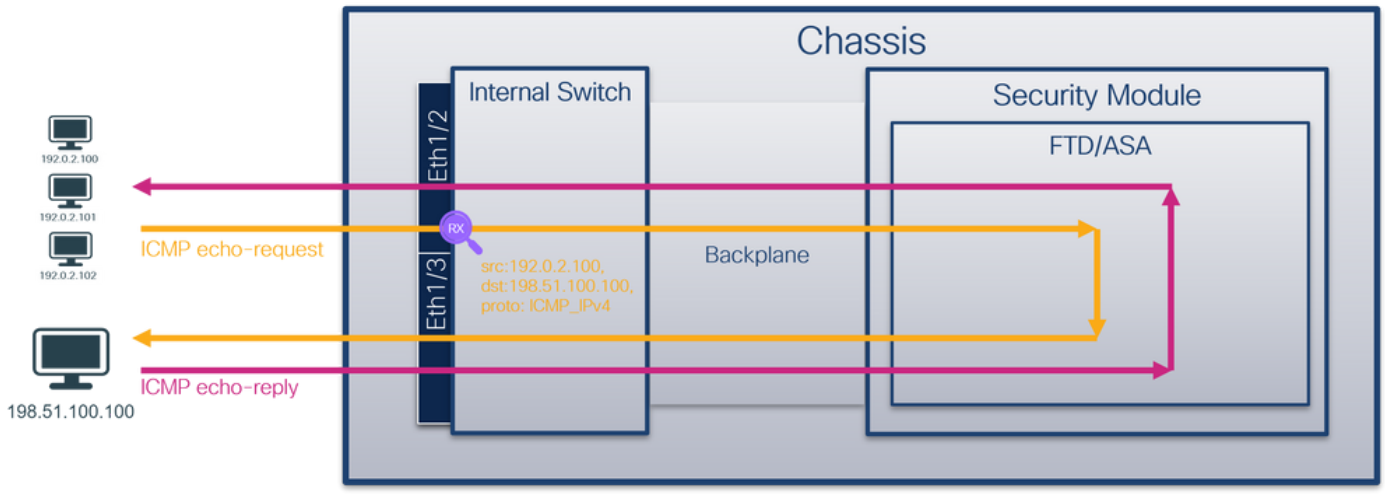
Ce tableau récapitule la tâche :

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

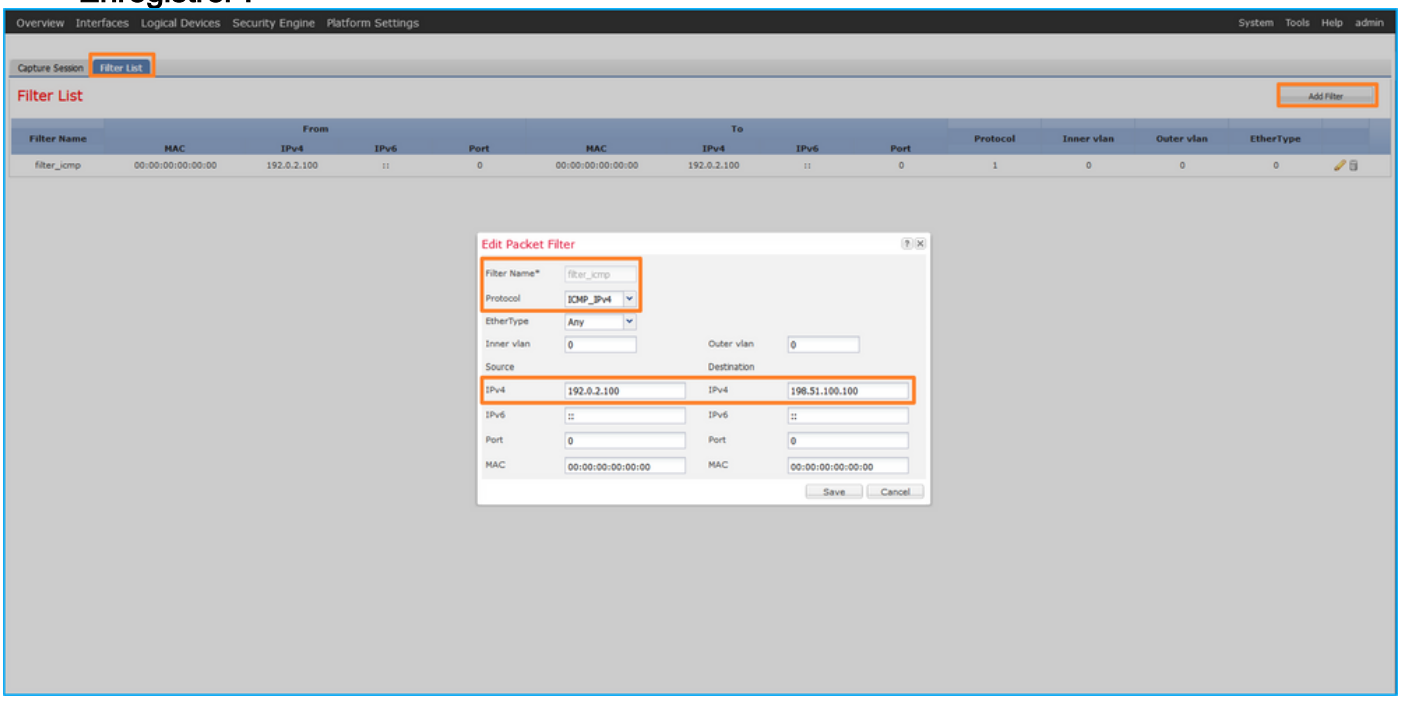


Configuration

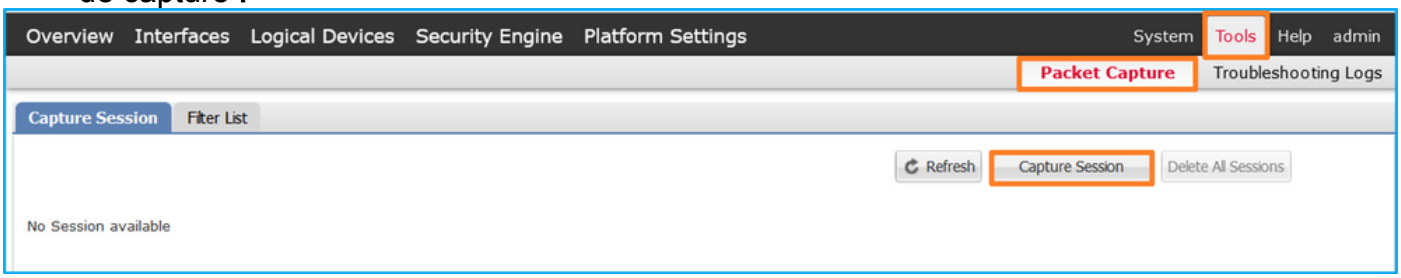
FCM

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

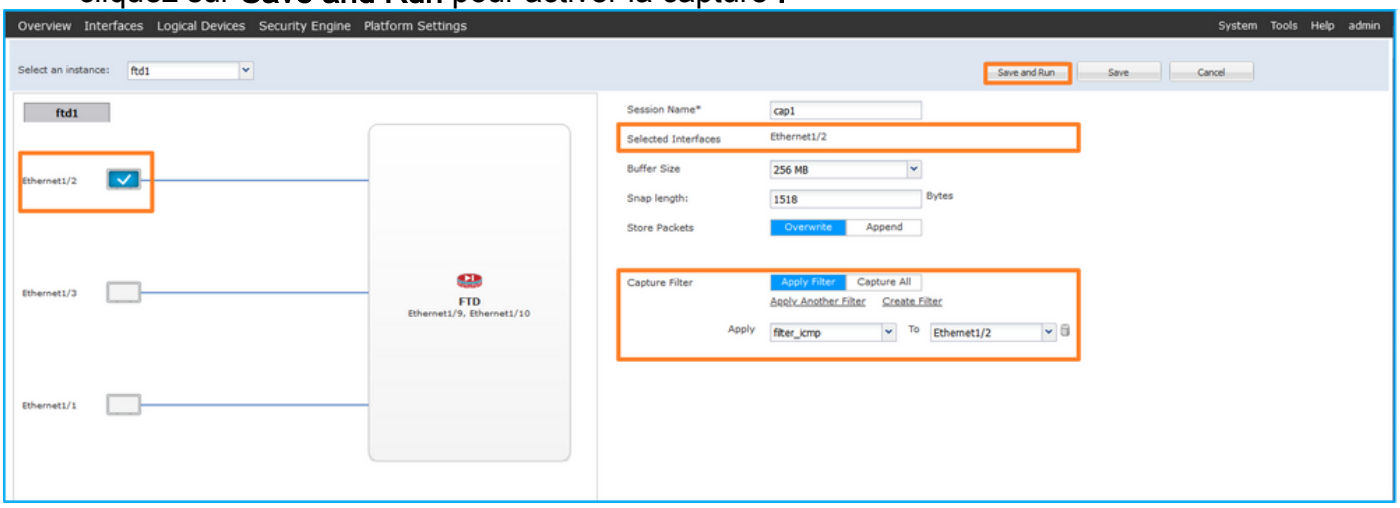
1. Utilisez **Outils > Capture de paquets > Liste de filtres > Ajouter un filtre** pour créer un filtre de capture.
2. Spécifiez le **nom** du **filtre, le protocole, l'IPv4 source, l'IPv4 de destination** et cliquez sur **Enregistrer :**



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



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



CLI FXOS

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

paquets sur les interfaces de fond de panier :

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

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

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

3. Créez une session de capture :

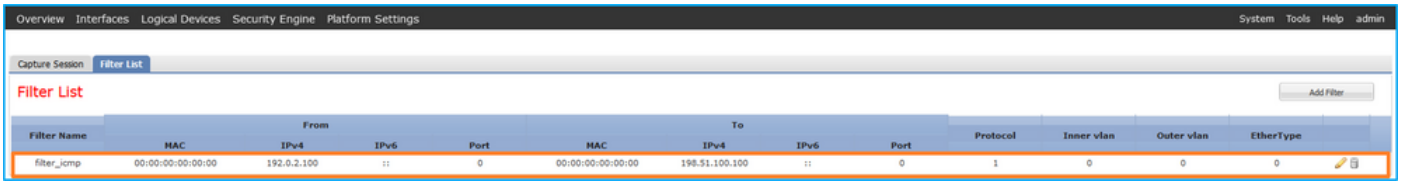
2.

```
firepower# scope packet-capture
firepower /packet-capture # create filter filter_icmp
firepower /packet-capture/filter* # set destip 198.51.100.100
firepower /packet-capture/filter* # set protocol 1
firepower /packet-capture/filter* # set srcip 192.0.2.100
firepower /packet-capture/filter* # exit
firepower /packet-capture* # create session cap1
firepower /packet-capture/session* # create phy-port Ethernet1/2
firepower /packet-capture/session/phy-port* # set app ftd
firepower /packet-capture/session/phy-port* # set app-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 #
```

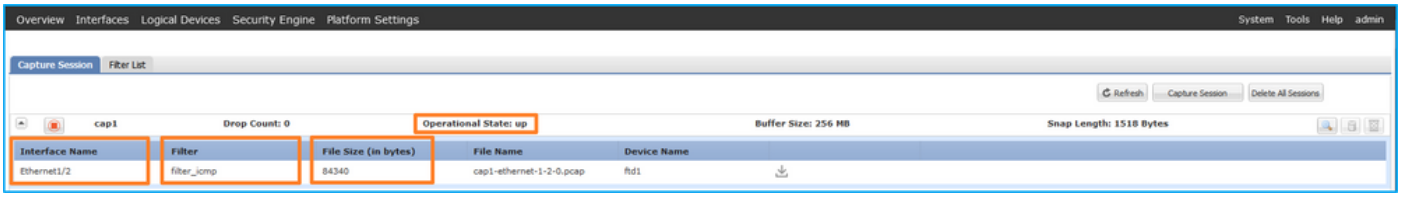
Vérification

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** :

```
firepower# scope packet-capture
firepower /packet-capture # show filter detail

Configure a filter for packet capture:
   Name: filter_icmp
    Protocol: 1
   Ivlan: 0
   Ovlan: 0
   Src Ip: 192.0.2.100
    Dest Ip: 198.51.100.100
   Src MAC: 00:00:00:00:00:00
   Dest MAC: 00:00:00:00:00:00
   Src Port: 0
   Dest Port: 0
   Ethertype: 0
   Src Ipv6: ::
   Dest Ipv6: ::
firepower /packet-capture # show session cap1

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

Physical ports involved in Packet Capture:
   Slot Id: 1
    Port Id: 2
    Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap
    Pcapsize: 213784  bytes
   Filter: filter_icmp
   Sub Interface: 0
    Application Instance Identifier: ftd1
    Application Name: ftd
```

Collecter les fichiers de capture

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

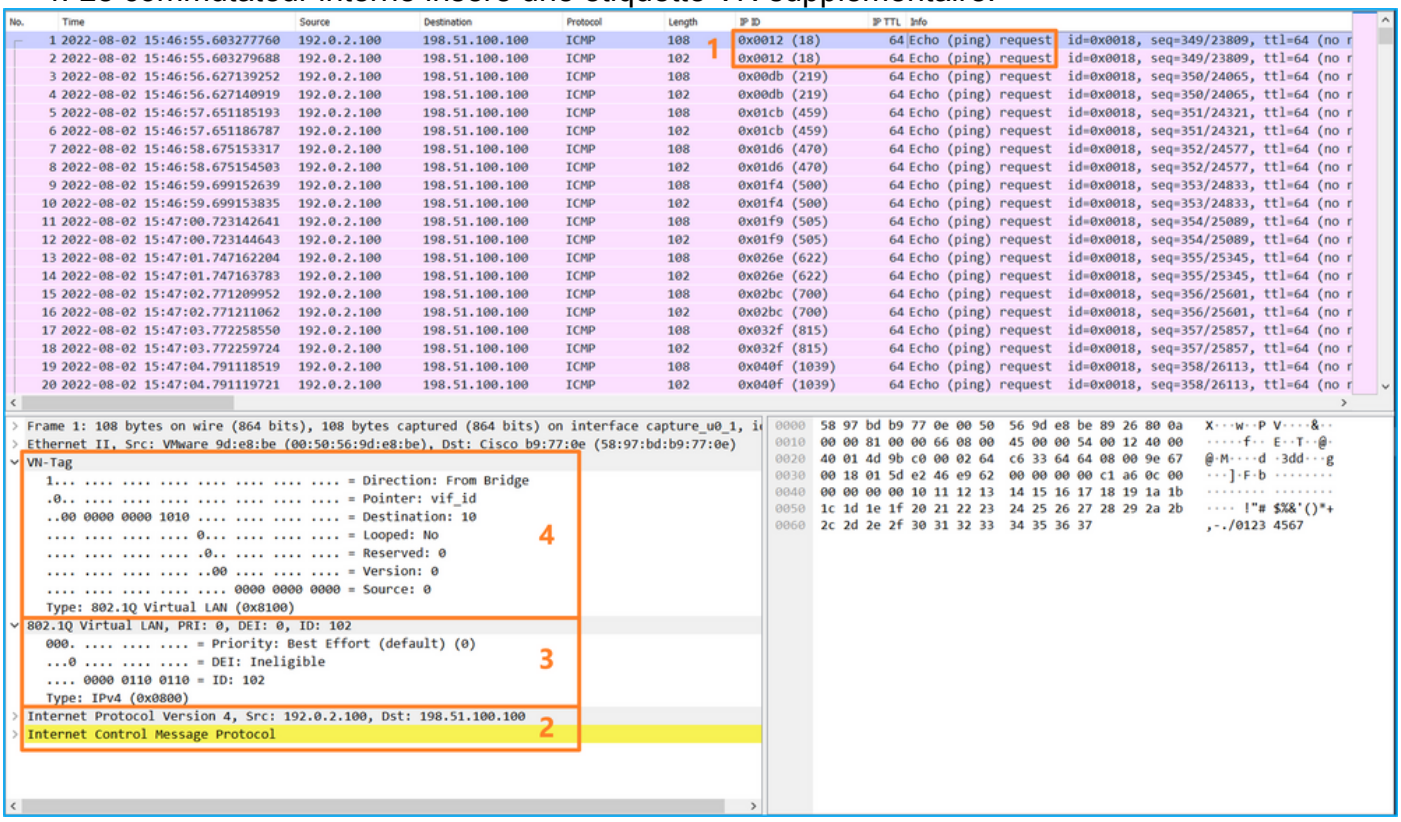
Capturer l'analyse des fichiers

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

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

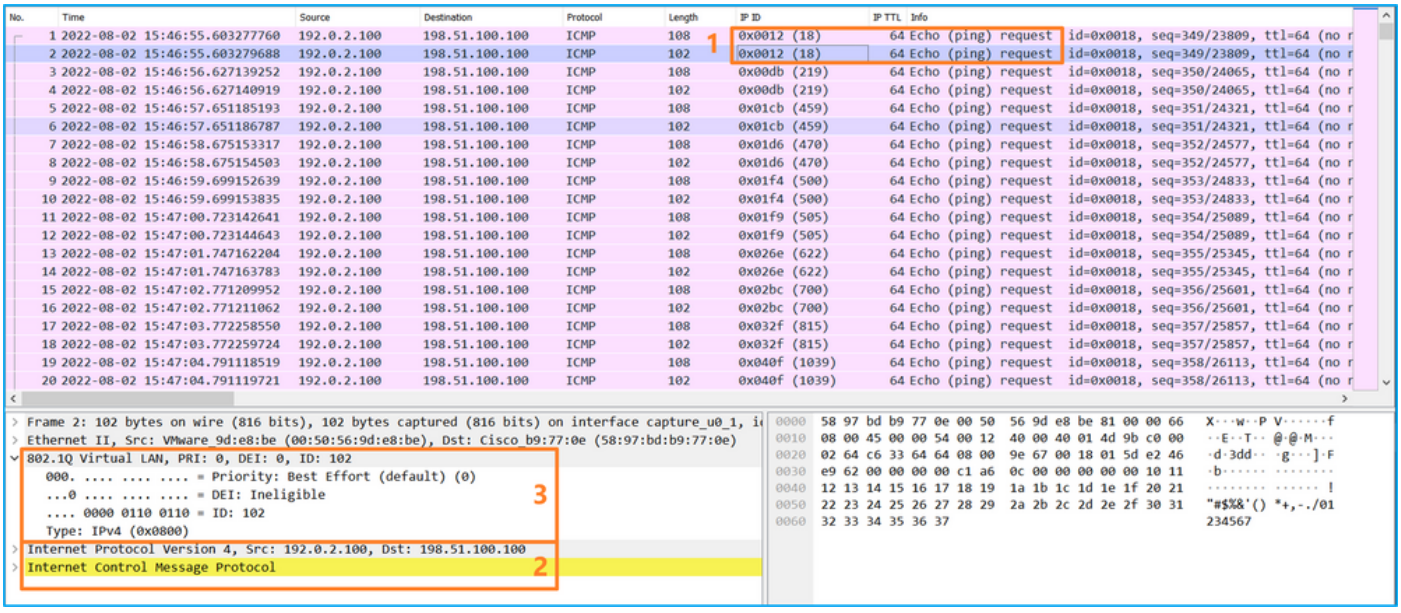
l'interface d'entrée Ethernet1/2.

4. Le commutateur interne insère une étiquette VN supplémentaire.



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 :

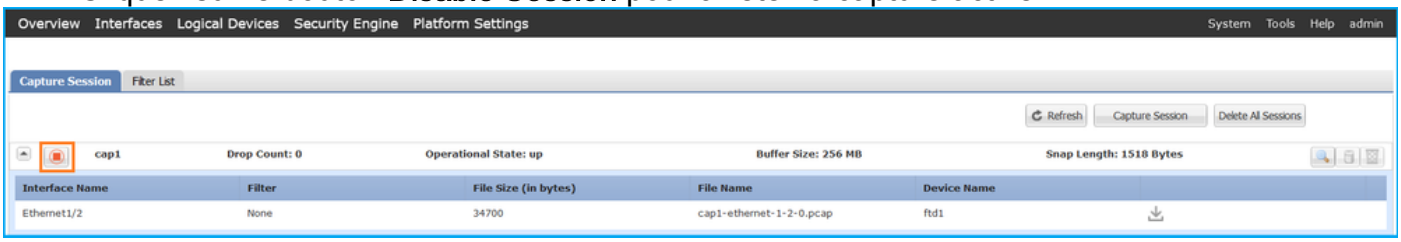
Tâche	Point de capture	VLAN de port interne dans les paquets capturés	Direction	Filtre utilisateur	Trafic capturé
Configurer et vérifier une capture de paquets avec un filtre sur l'interface avant Ethernet1/2	Ethernet1/2	102	Entrée uniquement	Protocole : ICMP Source : 192.0.2.100 Destination : 198.51.100.100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

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

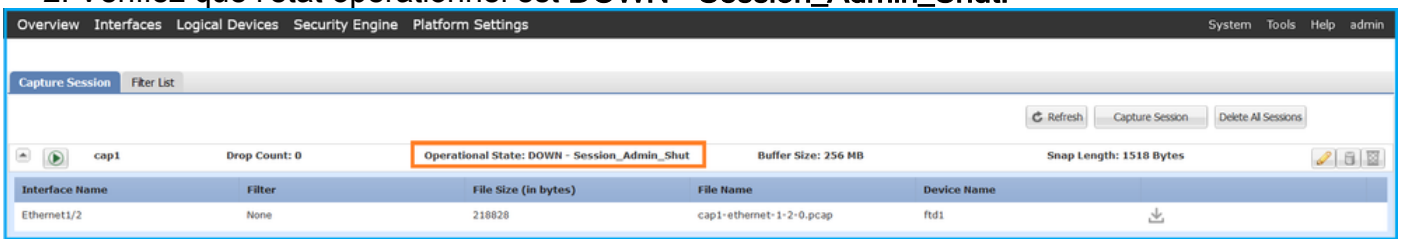
FCM

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

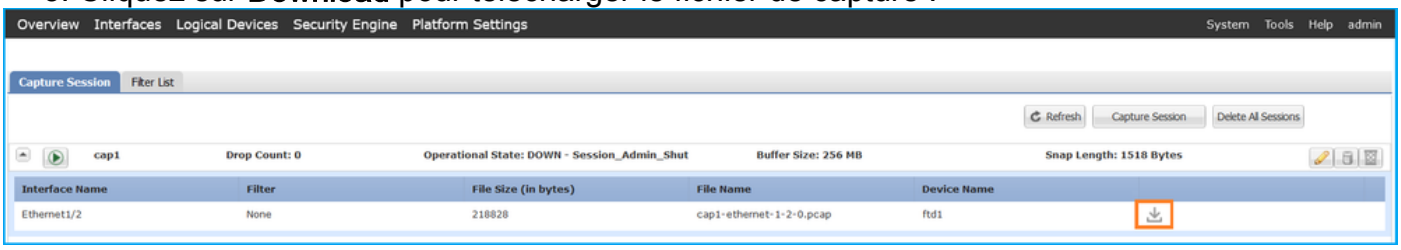
1. Cliquez sur le bouton **Disable Session** pour arrêter la capture active :



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



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



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

CLI FXOS

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

1. Arrêtez la capture active :

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

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

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

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

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

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

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

Recommandations, limites et meilleures pratiques pour Commutateur interne

Capture de paquets

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

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

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

Configuration et vérification sur Pare-feu sécurisé 3100

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

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

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

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

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

1. Spécifiez une interface d'entrée :

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

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

 management       Name of interface Management1/1
```

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

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

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

```
> capture capsw switch interface inside match ?
 <0-255>  Enter protocol number (0 - 255)
 ah
 eigrp
 esp
 gre
 icmp
 icmp6
 igmp
 igrp
 ip
 ipinip
 ipsec
 mac      Mac-address filter
```

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

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

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

6. Vérifiez les détails de la capture :

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

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

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

Total Physical ports involved in Packet Capture: 1
Physical port:
 Slot Id:           1
 Port Id:           1
 Pcapfile:          /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
  Pcapsize:          18838
 Filter:            capsw-1-1

Packet Capture Filter Info
```

```
  Name:              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 :

```
> 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 Secure Firewall 3100**.

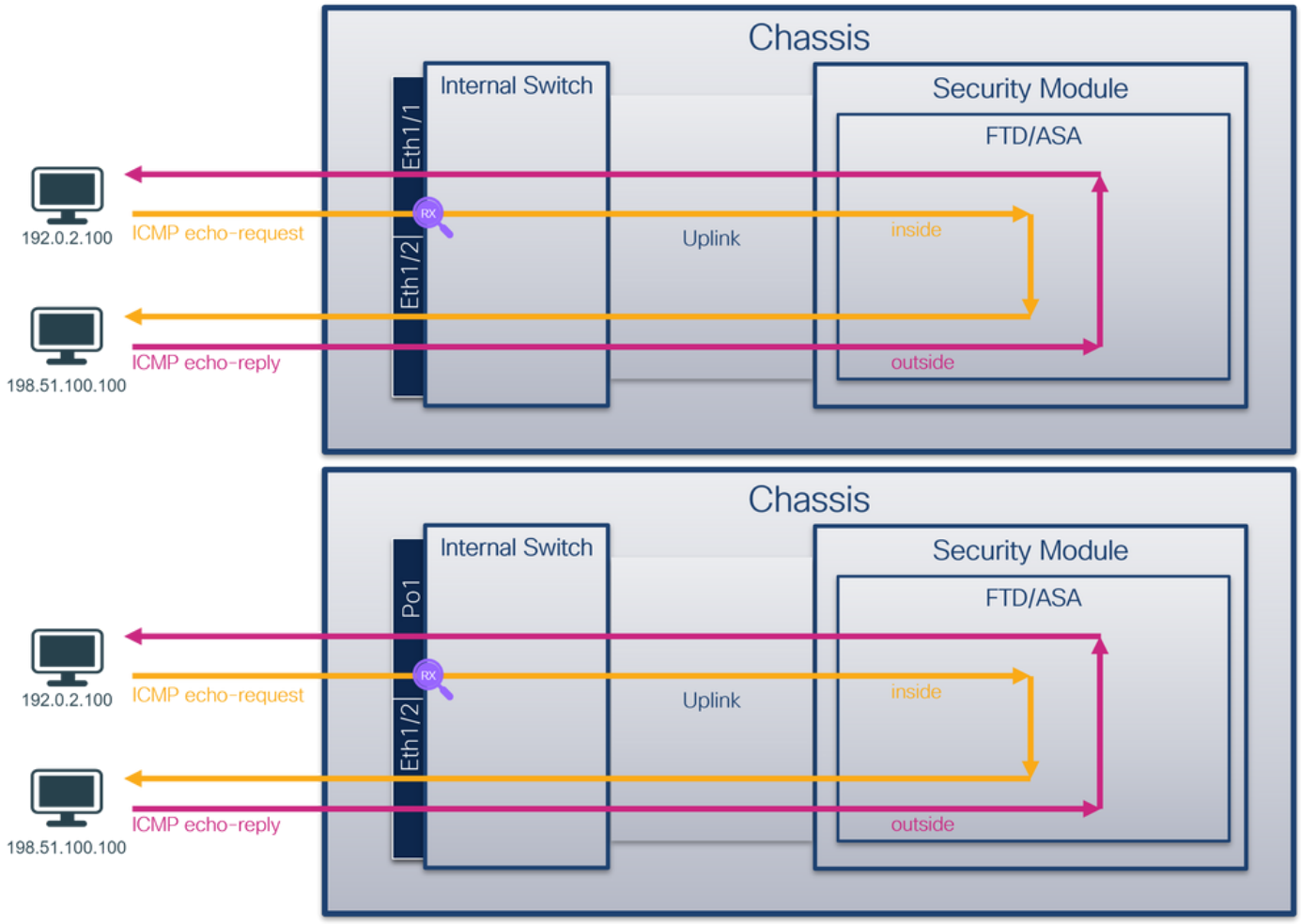
Dans la version 7.2, la configuration de capture interne du commutateur n'est pas prise en charge sur FMC ou FDM. Dans le cas du logiciel ASA version 9.18(1) et ultérieure, les captures de commutateurs internes peuvent être configurées dans ASDM versions 7.18.1.x et ultérieures.

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

Capture de paquets sur une interface physique ou Port Channel

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

Topologie, flux de paquets et points de capture



Configuration

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

1. Vérifiez le nom si :

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

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

2. Créez une session de capture :

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

3. Activez la session de capture :

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

Vérification

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

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

Total Physical ports involved in Packet Capture: 1

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

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

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

Total Physical breakout ports involved in Packet Capture: 0

79 packets captured on disk using switch capture

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

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

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

Total Physical ports involved in Packet Capture: 2

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

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

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

Packet Capture Filter Info
 Name:              capsw-1-3
 Protocol:          0
 Ivlan:             0
```

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

Total Physical breakout ports involved in Packet Capture: 0

56 packet captured on disk using switch capture

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

Les interfaces membres port-channel peuvent être vérifiées dans l'interpréteur de commandes FXOS **local-mgmt** via la commande **show portchannel summary :**

```
> connect fxos
…
KSEC-FPR3100-1 connect local-mgmt
KSEC-FPR3100-1(local-mgmt) show portchannel summary
Flags:  D - Down        P - Up in port-channel (members)
I - Individual  H - Hot-standby (LACP only)
s - Suspended   r - Module-removed
S - Switched    R - Routed
U - Up (port-channel)
M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
1     Po1(U)      Eth      LACP      Eth1/3(P)    Eth1/4(P)

LACP KeepAlive Timer:
--------------------------------------------------------------------------------
      Channel  PeerKeepAliveTimerFast
--------------------------------------------------------------------------------
1     Po1(U)      False

Cluster LACP Status:
--------------------------------------------------------------------------------
      Channel  ClusterSpanned  ClusterDetach  ClusterUnitID  ClusterSysID
--------------------------------------------------------------------------------
1     Po1(U)      False          False          0              clust
```

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

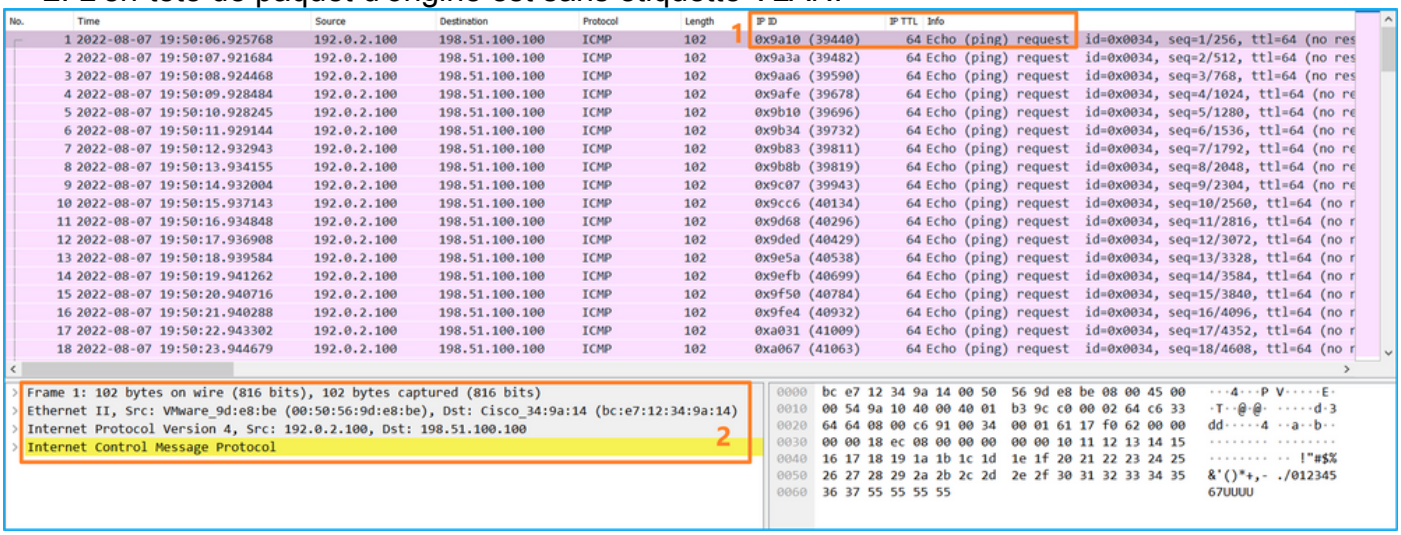
Collecter les fichiers de capture

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

Capturer l'analyse des fichiers

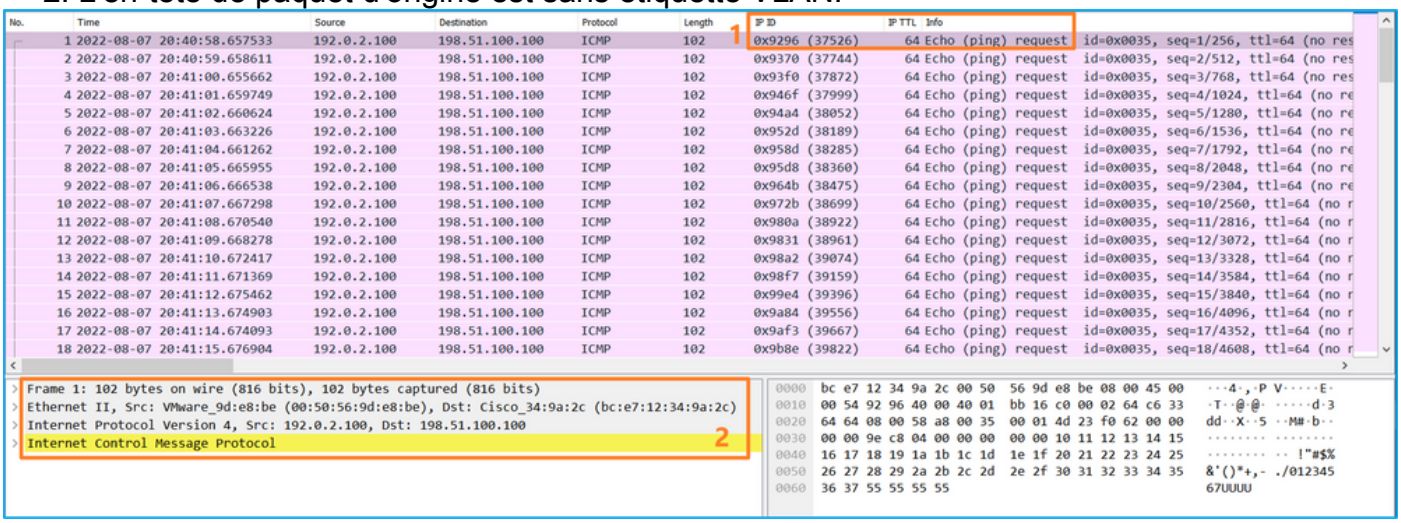
Utilisez une application de lecture de fichiers de capture de paquets pour ouvrir les fichiers de capture pour Ethernet1/1. Sélectionnez le premier paquet et vérifiez les points clés :

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



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

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



Explication

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

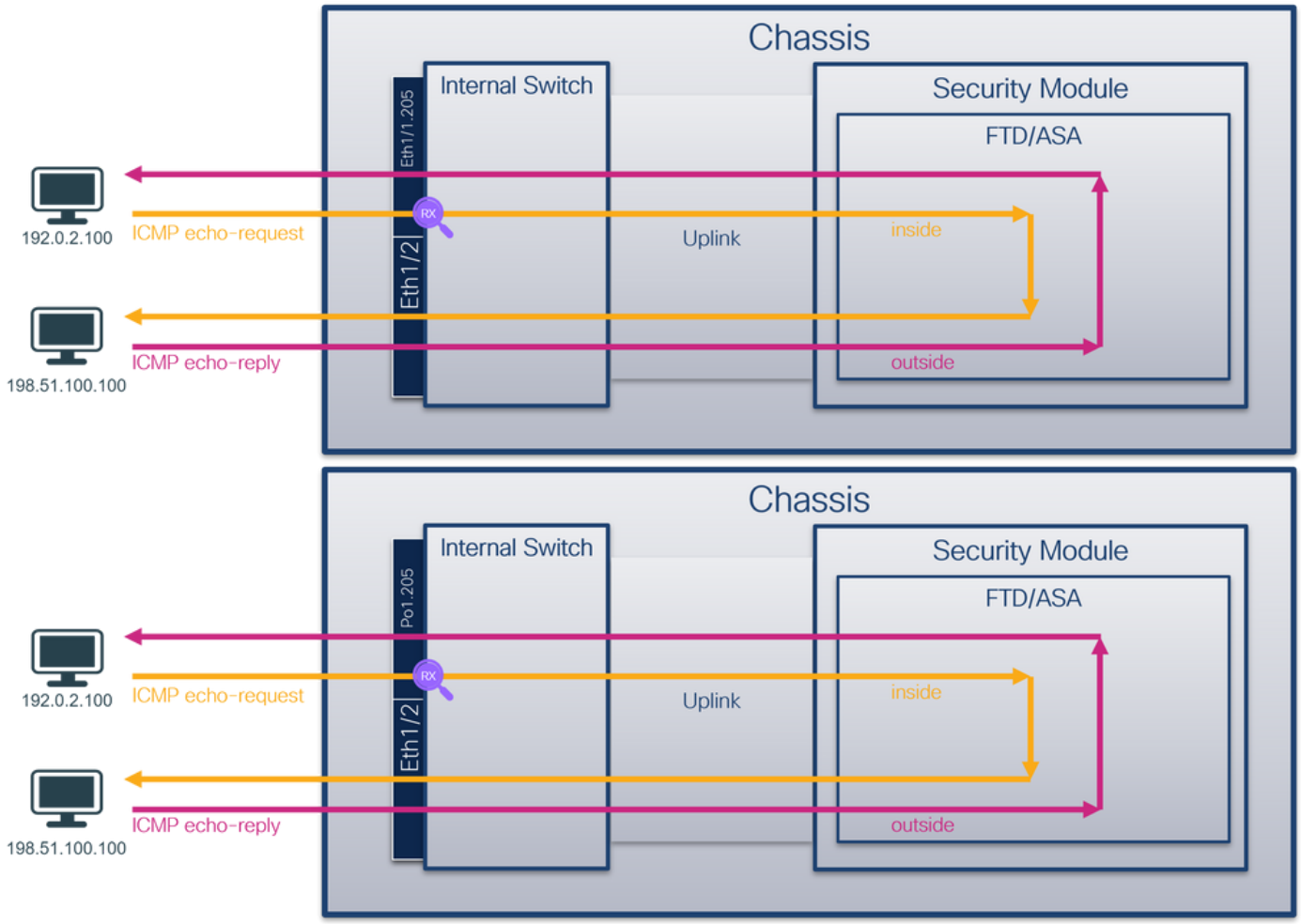
Ce tableau récapitule la tâche :

Tâche	Point de capture	Filtre interne	Direction	Trafic capturé
Configurer et vérifier une capture de paquets sur l’interface Ethernet1/1	Ethernet1/1	Aucune	Entrée uniquement	Requêtes d’écho ICMP de l’hôte 192.0.2.100 vers l’hôte 198.51.100.
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.

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

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

Topologie, flux de paquets et points de capture



Configuration

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

1. Vérifiez le nom si :

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

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

2. Créez une session de capture :

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

3. Activez la session de capture :

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

Vérification

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

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

Total Physical ports involved in Packet Capture: 1

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

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

Total Physical breakout ports involved in Packet Capture: 0

46 packets captured on disk using switch capture

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

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

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

interfaces membres :

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

Total Physical ports involved in Packet Capture: 2

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

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

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

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

```
Total Physical breakout ports involved in Packet Capture: 0

49 packet captured on disk using switch capture

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

Les interfaces membres port-channel peuvent être vérifiées dans l'interpréteur de commandes FXOS **local-mgmt** via la commande **show portchannel summary :**

```
> connect fxos
…
KSEC-FPR3100-1 connect local-mgmt
KSEC-FPR3100-1(local-mgmt) show portchannel summary
Flags:  D - Down        P - Up in port-channel (members)
I - Individual  H - Hot-standby (LACP only)
s - Suspended   r - Module-removed
S - Switched    R - Routed
U - Up (port-channel)
M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
     Channel
--------------------------------------------------------------------------------
1     Po1(U)      Eth      LACP      Eth1/3(P)    Eth1/4(P)

LACP KeepAlive Timer:
--------------------------------------------------------------------------------
     Channel  PeerKeepAliveTimerFast
--------------------------------------------------------------------------------
1     Po1(U)      False

Cluster LACP Status:
--------------------------------------------------------------------------------
     Channel  ClusterSpanned  ClusterDetach  ClusterUnitID  ClusterSysID
--------------------------------------------------------------------------------
1     Po1(U)      False          False          0            clust
```

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

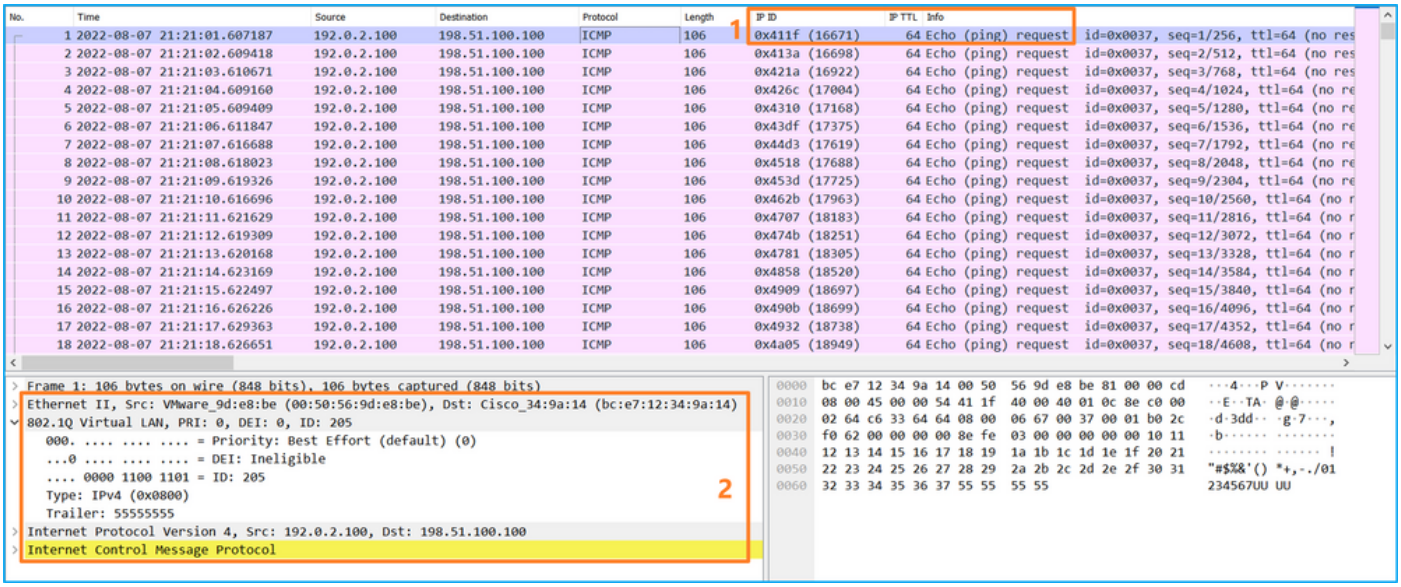
Collecter les fichiers de capture

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

Capturer l'analyse des fichiers

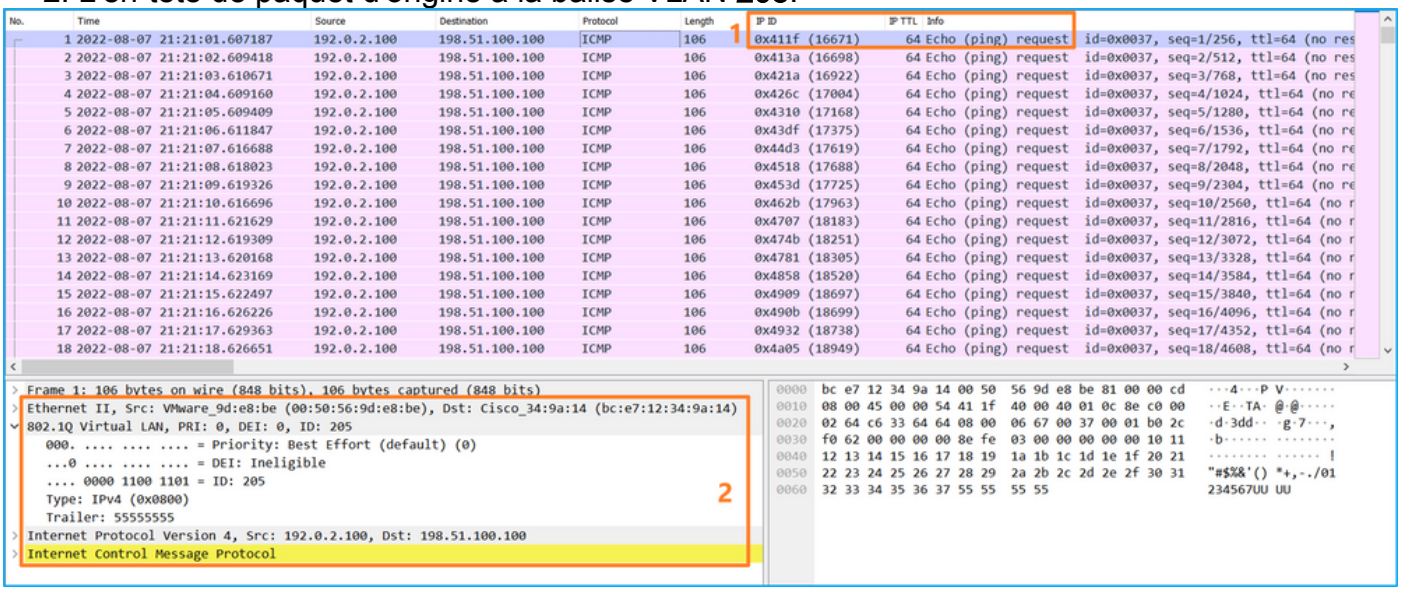
Utilisez une application de lecture de fichiers de capture de paquets pour ouvrir les fichiers de capture pour Ethernet1/1.205. Sélectionnez le premier paquet et vérifiez les points clés :

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



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	Ethernet 1/1	VLAN externe 205	Entrée uniquement	Requêtes d'écho ICMP de l'hôte 192.0.2.100 vers l'hôte 198.51.10
Configurez et vérifiez une capture de paquets sur la sous-interface Portchannel1.205 avec les interfaces membres Ethernet1/3 et Ethernet1/4	Ethernet 1/3 Ethernet 1/4	VLAN externe 205	Entrée uniquement	Requêtes d'écho ICMP de l'hôte 192.0.2.100 vers l'hôte 198.51.10

Capture de paquets sur des interfaces internes

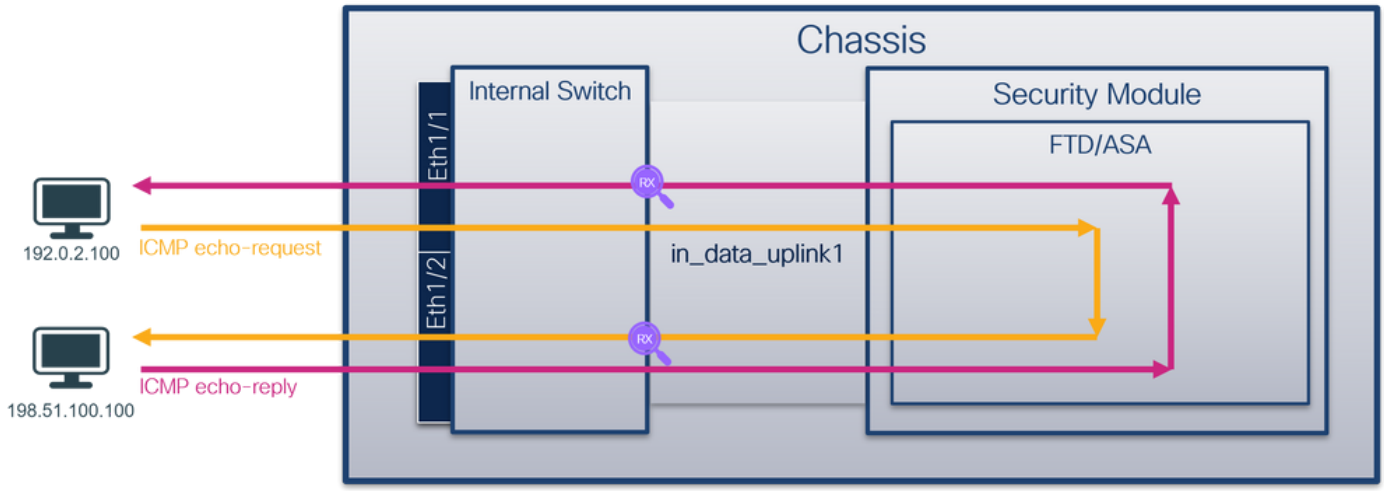
Le pare-feu sécurisé dispose de 2 interfaces internes :

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

Tâche 1

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

Topologie, flux de paquets et points de capture



Configuration

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

1. Créez une session de capture :

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

2. Activez la session de capture :

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

Vérification

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

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

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

Total Physical ports involved in Packet Capture: 1

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

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

Total Physical breakout ports involved in Packet Capture: 0

66 packets captured on disk using switch capture

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

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

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

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

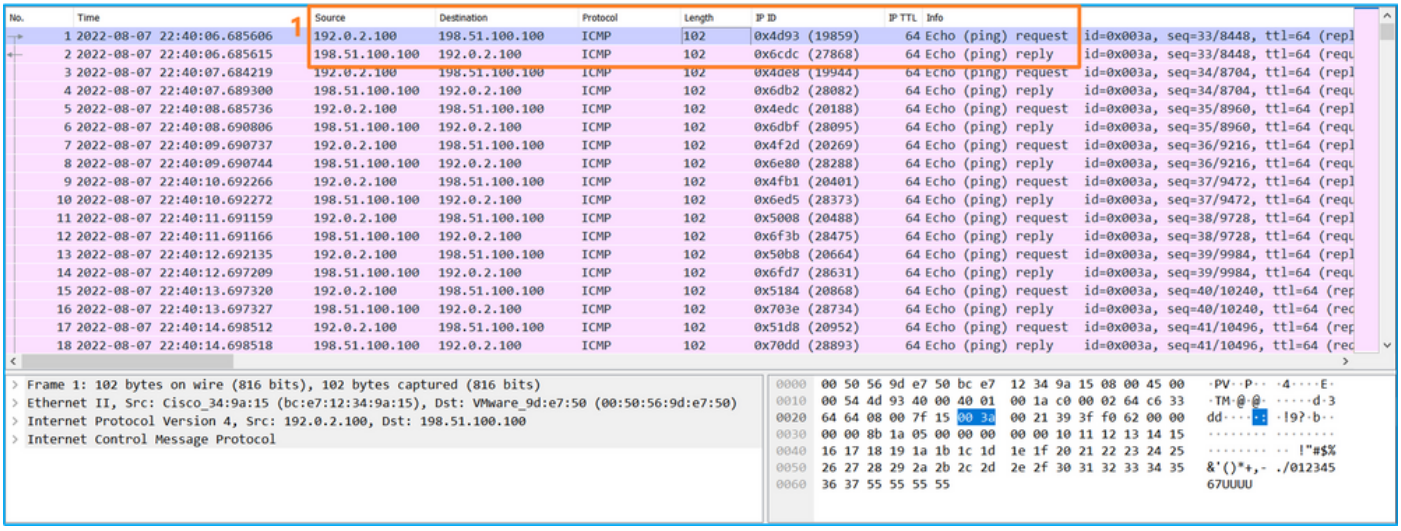
Pour accéder à FXOS sur ASA, exécutez la commande **connect fxos admin**. Dans le cas du multi-contexte, exécutez cette commande dans le contexte admin.

Collecter les fichiers de capture

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

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. 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.

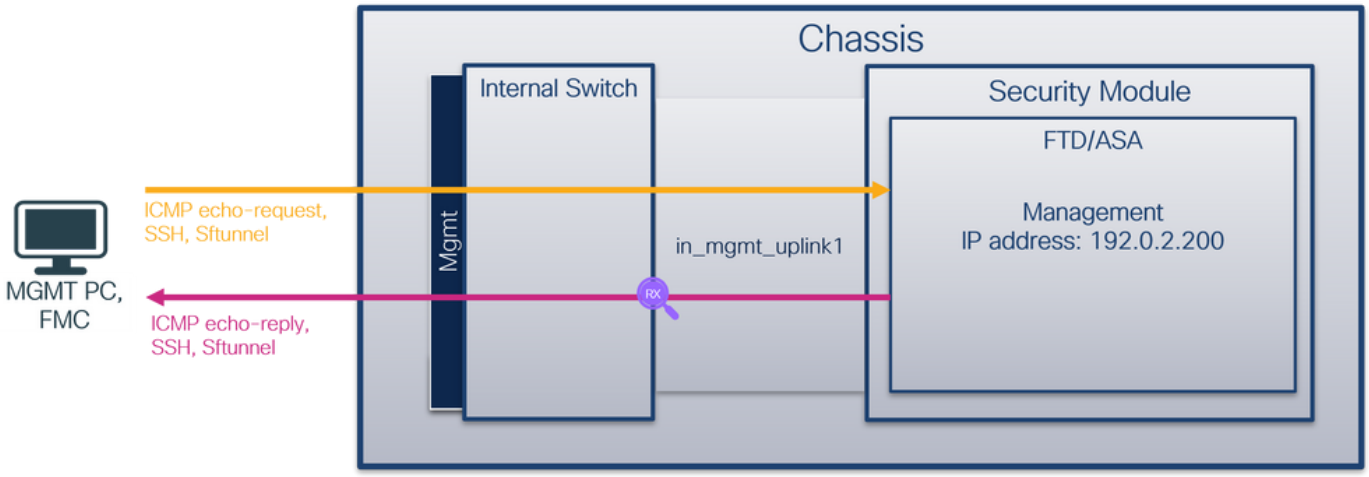
Ce tableau récapitule la tâche :

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 192.0.2.1

Tâche 2

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

Topologie, flux de paquets et points de capture



Configuration

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

1. Créez une session de capture :

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

2. Activez la session de capture :

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

Vérification

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

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

Total Physical ports involved in Packet Capture: 1

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

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

Total Physical breakout ports involved in Packet Capture: 0

281 packets captured on disk using switch capture

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

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

```
> connect fxos
…
KSEC-FPR3100-1 connect local-mgmt
KSEC-FPR3100-1(local-mgmt) show portmanager switch status
Dev/Port         Mode        Link   Speed  Duplex  Loopback Mode  Port Manager
---------  ----------------  -----  -----  ------  -------------  ------------
0/1             SGMII         Up     1G     Full    None           Link-Up
0/2             SGMII         Up     1G     Full    None           Link-Up
0/3             SGMII         Up     1G     Full    None           Link-Up
0/4             SGMII         Up     1G     Full    None           Link-Up
0/5             SGMII        Down    1G     Half    None           Mac-Link-Down
0/6             SGMII        Down    1G     Half    None           Mac-Link-Down
```

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

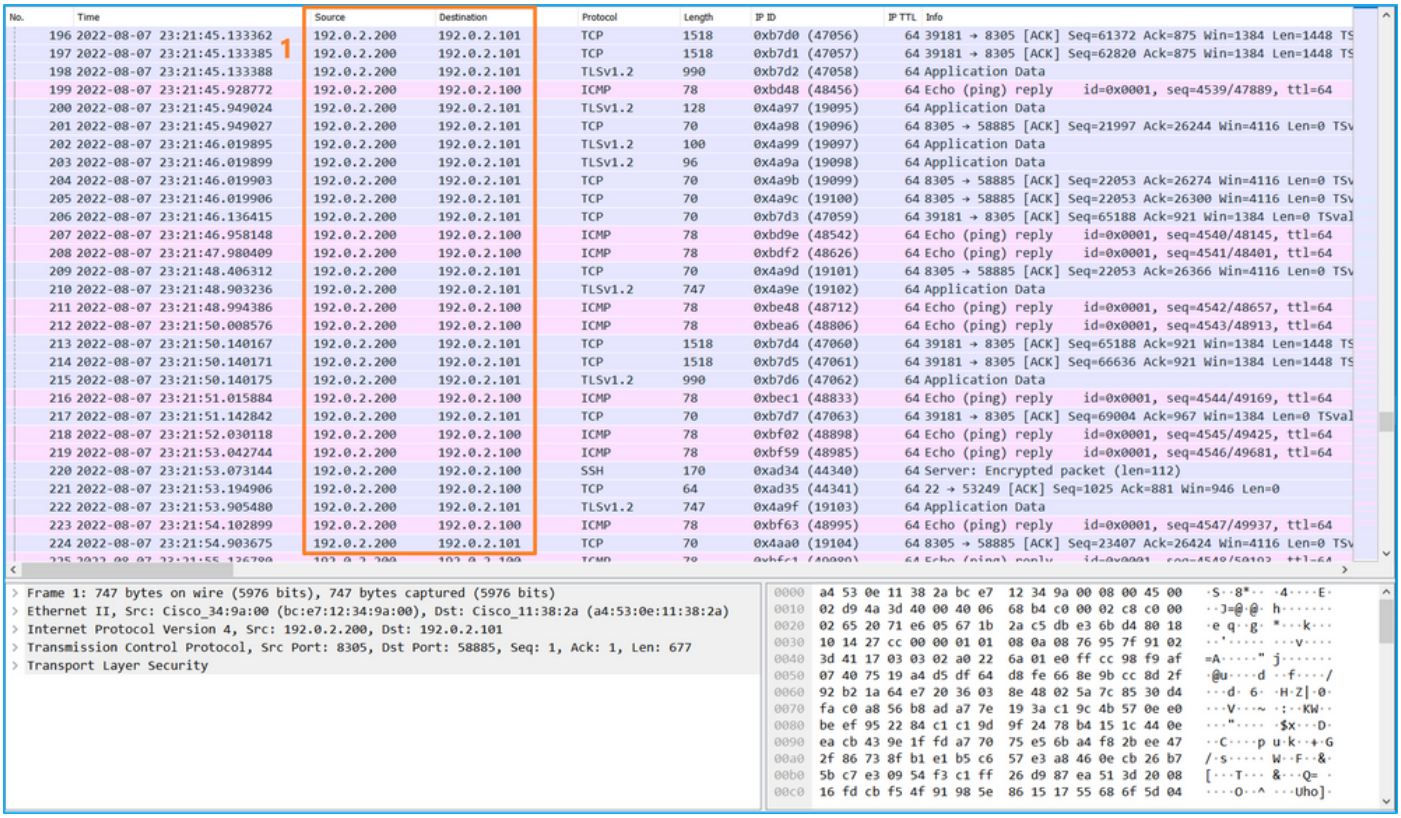
Pour accéder à FXOS sur ASA, exécutez la commande **connect fxos admin**. Dans le cas du multi-contexte, exécutez cette commande dans le contexte admin.

Collecter les fichiers de capture

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

Capturer l'analyse des fichiers

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



Explication

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

Ce tableau récapitule la tâche :

Tâche	Point de capture	Filtre interne	Direction	Trafic capturé
Configurer et vérifier une capture de paquets sur l'interface de gestion de liaison ascendante	in_mgmt_uplink1	Aucune	Entrée uniquement (de l'interface de gestion au réseau en passant par le commutateur interne)	Réponses d'écho ICMP de l'adresse IP d gestion FTD 192.0.2.200 à l'hôte 192.0.2 Sftunnel de l'adresse IP de gestion FTD 192.0.2.200 à l'adresse IP FMC 192.0.2.1 SSH de l'adresse IP de gestion FTD 192.0.2.200 vers l'hôte 192.0.2.100

Filtres de capture de paquets

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

Configuration

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

1. Vérifiez le nom si :

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

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

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

> capture capsw switch interface inside match icmp 198.51.100.100
```

Vérification

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

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

Total Physical ports involved in Packet Capture: 1

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

Packet Capture Filter Info
  Name:              capsw-1-1
 Protocol:          0
 Ivlan:             0
 Ovlan:             0
 Src Ip:            0.0.0.0
 Dest Ip:           0.0.0.0
 Src Ipv6:          ::
 Dest Ipv6:         ::
 Src MAC:           00:00:00:00:00:00
 Dest MAC:          00:00:00:00:00:00
 Src Port:          0
 Dest Port:         0
 Ethertype:         2054

Total Physical breakout ports involved in Packet Capture: 0
```

```
0 packet captured on disk using switch capture

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

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

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

Total Physical ports involved in Packet Capture: 1

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

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

Total Physical breakout ports involved in Packet Capture: 0

0 packets captured on disk using switch capture

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

Collecter les fichiers de capture internes du commutateur Secure Firewall 3100

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

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

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

paquets à partir de toutes les interfaces membres.

ASA

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

1. Arrêtez la capture :

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

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

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

Total Physical ports involved in Packet Capture: 1

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

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

Total Physical breakout ports involved in Packet Capture: 0

886 packets captured on disk using switch capture

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

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

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

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

FTD

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

1. Accédez à la CLI de diagnostic :

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

firepower> enable
Password: <-- Enter
firepower#
```

2. Arrêtez la capture :

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

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

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

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

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

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

Total Physical breakout ports involved in Packet Capture: 0

886 packets captured on disk using switch capture

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

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

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

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

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

1. Arrêtez la capture :

```
> capture capsw switch stop
```

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

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

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

Total Physical ports involved in Packet Capture: 1

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

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

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

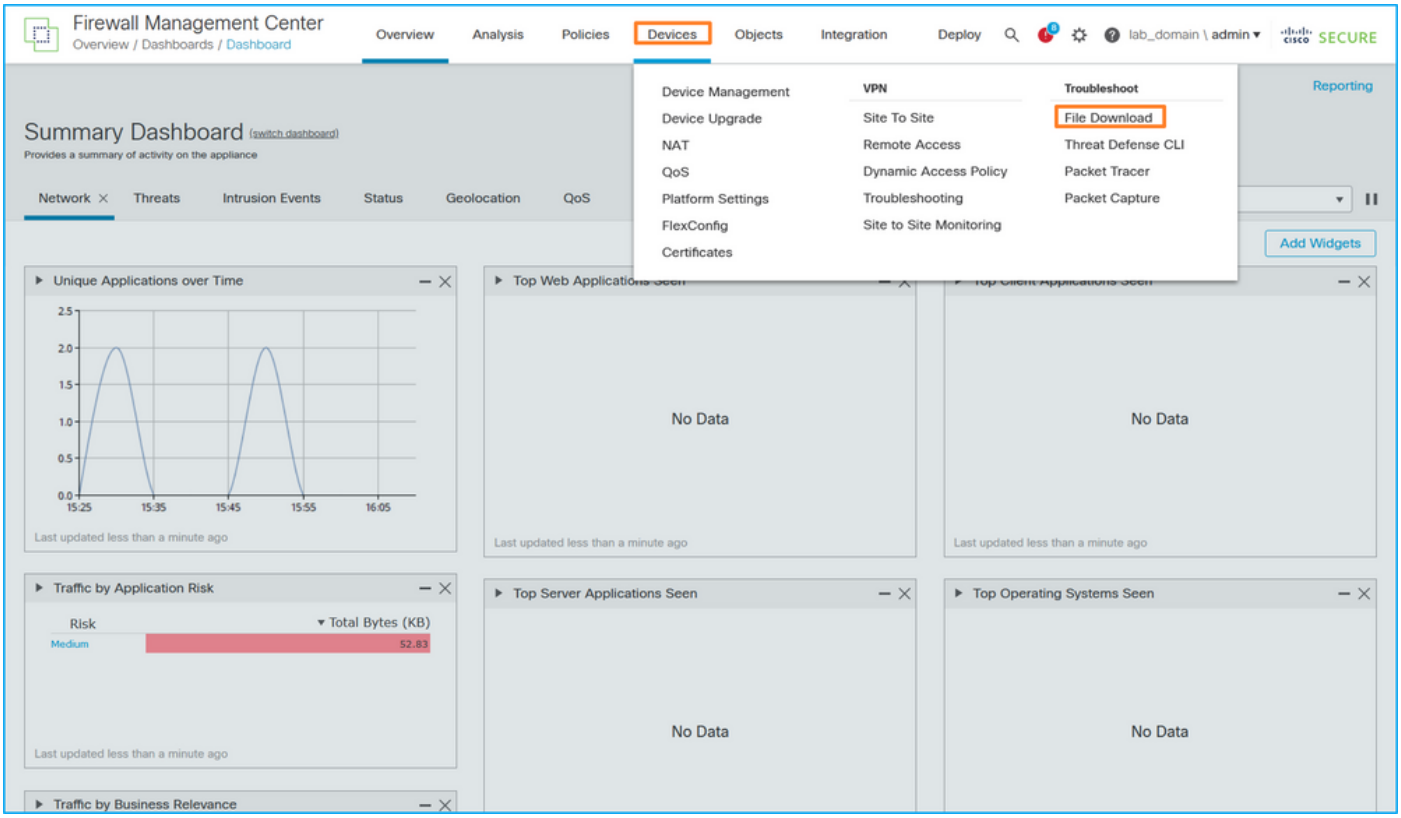
3. Passez en mode expert et passez en mode racine :

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

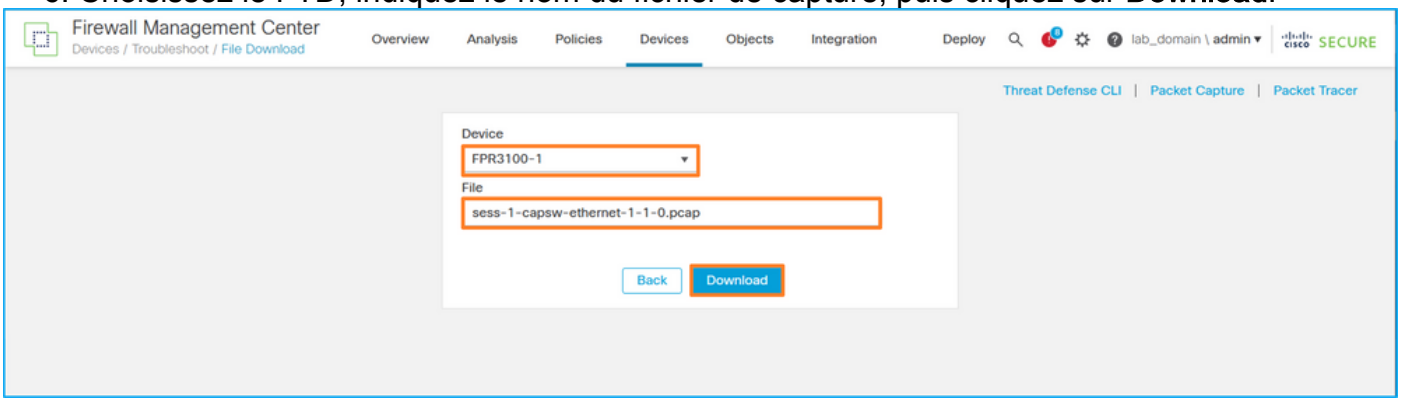
4. Copiez le fichier de capture dans /ngfw/var/common/:

```
root@KSEC-FPR3100-1:/home/admin cp /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
/ngfw/var/common/
root@KSEC-FPR3100-1:/home/admin ls -l /ngfw/var/common/sess*
-rwxr-xr-x 1 root admin 139826 Aug  7 20:14 /ngfw/var/common/sess-1-capsw-ethernet-1-1-0.pcap
-rwxr-xr-x 1 root admin     24 Aug  6 21:58 /ngfw/var/common/sess-1-capsw-ethernet-1-3-0.pcap
```

5. Sur FMC, choisissez **Devices > File Download** :



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

Directives et limites :

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

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

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

Informations connexes

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

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

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