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

# Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Informations générales
Présentation générale de l'architecture du système
Présentation générale du fonctionnement des commutateurs internes
Flux de paquets et points de capture
Configuration et vérification sur Firepower 4100/9300
Capture de paquets sur une interface physique ou Port Channel
Captures de paquets sur les interfaces de fond de panier
Captures de paquets sur les ports des applications et des applications
Capture de paquets sur une sous-interface d'une interface physique ou Port Channel
Filtres de capture de paquets
Collecter les fichiers de capture du commutateur interne Firepower 4100/9300
Recommandations, limites et meilleures pratiques pour la capture de paquets de commutateur interne
Configuration et vérification sur Secure Firewall 3100/4200
Capture de paquets sur une interface physique ou Port Channel
Capture de paquets sur une sous-interface d'une interface physique ou Port Channel
Capture de paquets sur des interfaces internes
Filtres de capture de paquets
Collecter les fichiers de capture internes du commutateur Secure Firewall
Recommandations, limites et meilleures pratiques pour la capture de paquets de commutateur interne
Informations connexes

# Introduction

Ce document décrit la configuration et la vérification de la puissance de feu, et le pare-feu sécurisé capture le commutateur interne.

# Conditions préalables

# Exigences

Connaissances de base sur les produits, analyse de capture.

# Composants utilisés

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

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

- Pare-feu sécurisé 31xx, 42xx
- 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, 7.4.1-172
- Cisco Secure Firewall Management Center (FMC) 7.2.0.x, 7.4.1-172
- Appareil de sécurité adaptatif (ASA) 9.18(1)x, 9.20(x)
- Wireshark 3.6.7 (<u>https://www.wireshark.org/download.html</u>)

# Informations générales

# Présentation générale de l'architecture du système

Du point de vue du flux de paquets, l'architecture des pare-feu Firepower 4100/9300 et Secure Firewall 3100/4200 peut être visualisée comme illustré dans cette figure :



Le châssis comprend les composants suivants :

- Commutateur interne transfère le paquet du réseau à l'application et vice versa. Le commutateur interne est connecté aux interfaces avant qui résident sur le module d'interface intégré ou les modules de réseau externes et se connectent à des périphériques externes, par exemple, des commutateurs. Ethernet 1/1, Ethernet 2/4, etc. sont des exemples d'interfaces avant. Le « front » n'est pas une définition technique forte. Dans ce document, il est utilisé pour distinguer les interfaces connectées aux périphériques externes des interfaces de fond de panier ou de liaison ascendante.
- Fond de panier ou liaison ascendante interface interne qui connecte le module de sécurité (SM) au commutateur interne.
- Liaison ascendante de gestion interface interne exclusive à Secure Firewall 3100/4200 qui fournit le chemin du trafic de gestion entre le commutateur interne et l'application.

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

Plateforme	Nombre de modules de sécurité pris en charge	Interfaces de fond de panier/liaison ascendante	Gestion des interfaces de liaison ascendante	Interfaces d'application mappées
Firepower 4100 (sauf Firepower 4110/4112)	1	SM1 : Ethernet1/9 Ethernet1/10	S/O	Internal-Data0/0 Données internes0/1
Firepower 4110/4112	1	Ethernet1/9	S/O	Internal-Data0/0 Données internes0/1
Firepower 9300	repower 9300 3		S/O	Internal-Data0/0 Données internes0/1 Internal-Data0/0 Données internes0/1 Internal-Data0/0 Données

		Ethernet1/14		internes0/1
Pare-feu sécurisé 3100	1	SM1 : in_data_uplink1	in_mgmt_uplink1	Données internes0/1 Gestion1/1
Pare-feu sécurisé 4200	1	SM1 : in_data_uplink1 SM1 : in_data_uplink2 (seulement 4245)	in_mgmt_uplink1 in_mgmt_uplink2	Données internes0/1 Internal-Data0/2 (seulement 4245) Gestion1/1 Gestion1/2

Dans le cas de Firepower 4100/9300 avec 2 interfaces de fond de panier par module ou de Secure Firewall 4245 avec 2 interfaces de liaison ascendante de données, le commutateur interne et les applications sur les modules effectuent un équilibrage de charge de trafic sur les 2 interfaces.

- Module de sécurité, moteur de sécurité ou lame : module dans lequel sont installées des applications telles que FTD ou ASA. Firepower 9300 prend en charge jusqu'à 3 modules de sécurité.
- Interface d'application mappée noms des interfaces de fond de panier ou de liaison ascendante dans les applications, telles que FTD ou ASA.

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

<#root>

>
show interface detail | grep Interface
Interface Internal-Control0/0 "ha\_ctl\_nlp\_int\_tap", is up, line protocol is up
Control Point Interface States:
 Interface number is 6
 Interface config status is active
Interface Internal-Data0/0 "", is up, line protocol is up
Control Point Interface States:
 Interface number is 2
 Interface config status is active
Interface state is active
Interface state is active
Interface Internal-Data0/1 "", is up, line protocol is up

Control Point Interface States: Interface number is 3 Interface config status is active Interface state is active Interface Internal-Data0/2 "nlp\_int\_tap", is up, line protocol is up Control Point Interface States: Interface number is 4 Interface config status is active Interface state is active Interface Internal-Data0/3 "ccl\_ha\_nlp\_int\_tap", is up, line protocol is up Control Point Interface States: Interface number is 5 Interface config status is active Interface state is active Interface Internal-Data0/4 "cmi\_mgmt\_int\_tap", is up, line protocol is up Control Point Interface States: Interface number is 7 Interface config status is active Interface state is active Interface Port-channel6.666 "", is up, line protocol is up Interface Ethernet1/1 "diagnostic", is up, line protocol is up Control Point Interface States: Interface number is 8 Interface config status is active Interface state is active

# Présentation générale du fonctionnement des commutateurs internes

Firepower 4100/9300

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

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

#### <#root>

firepower#

connect fxos

firepower(fxos)#

show run int e1/2

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

version 5.0(3)N2(4.120)

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

switchport trunk native vlan 102

speed 1000 duplex full udld disable no shutdown

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

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

Pare-feu sécurisé 3100/4200

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

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

Flux de paquets et points de capture

Firepower 4100/9300 et Secure Firewall 3100

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

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



Les points de capture sont les suivants :

- 1. Point de capture d'entrée de l'interface avant du commutateur interne. Une interface avant est une interface connectée aux périphériques homologues, tels que les commutateurs.
- 2. Point de capture d'entrée interface du plan de données
- 3. Point de capture Snort
- 4. Point de capture de sortie d'interface du plan de données
- 5. Fond de panier interne du commutateur ou point de capture d'entrée de liaison ascendante. Une interface de fond de panier ou de liaison ascendante connecte le commutateur interne à l'application.

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

Pare-feu sécurisé 4200

Les pare-feu Secure Firewall 4200 prennent en charge les captures de paquets sur les interfaces du commutateur interne. Cette figure montre les points de capture de paquets le long du chemin des paquets au sein du châssis et de l'application :



Les points de capture sont les suivants :

- 1. Point de capture d'entrée de l'interface avant du commutateur interne. Une interface avant est une interface connectée aux périphériques homologues, tels que les commutateurs.
- 2. Point de capture de sortie d'interface de fond de panier du commutateur interne.
- 3. Point de capture d'entrée interface du plan de données
- 4. Point de capture Snort
- 5. Point de capture de sortie d'interface du plan de données
- 6. Fond de panier interne du commutateur ou point de capture d'entrée de liaison ascendante. Une interface de fond de panier ou de liaison ascendante connecte le commutateur interne à l'application.
- 7. Point de capture de sortie de l'interface avant du commutateur interne.

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

# Configuration et vérification sur Firepower 4100/9300

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

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

# Capture de paquets sur une interface physique ou Port Channel

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

ou l'interface Portchannel1. Dans le cas d'une interface port-channel, assurez-vous de sélectionner toutes les interfaces membres physiques.

Topologie, flux de paquets et points de capture



# Configuration

FCM

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

1. Utilisez Tools > Packet Capture > Capture Session pour créer une nouvelle session de capture :

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

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

Overview Interfaces Logical Devices Security Engine Platform Settings		System Tools Help admin
Select an instance: ftd1 v		Save and Run Save Cancel
Ttd1	Session Name* Cap1 Selected Interfaces Ethernet1/2	
Ethernet1/2	Buffer Size 256 MB  Snap length: 1518 Bytes	
Ethernet1/3	Store Packets Overwrite Append	
Ethernet1/1 FTD Ethernet1/9, Ethernet1/10	Capture Filter Apply Filter Capture All	
Ethernet1/5 (Portchannel3)		
Ethernet1/4 (Portchannel1)		

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

Overview Interfaces Logical Devices Security Engine Platform Settings					System T	ools Help admin
Select an instance: ftd1 ¥			Save and Run	Save	Cancel	
ftd1	Session Name* Selected Interfaces	Cap1 Ethernet1/5, Ethernet1/4				
Ethernet1/2	Buffer Size Snap length:	256 MB 💙				
Ethernet1/3	Store Packets	Overwrite Append				
Ethernet1/1 FTD Ethernet1/9, Ethernet1/10	Capture Filter	Apply Filter Capture All				
Ethernet1/5						
Ebhernet1/4 (Portchannels)						

# **CLI FXOS**

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

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

<#root>			
firepower#			
scope ssa			
firepower show app-i	/ssa # nstance		
App Name	Identifier Slot ID	Admin State Oper State	Running Version Startup Version Deploy Ty
ftd	ftdl		

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

<#root>

firepower#

connect fxos

<output skipped>
firepower(fxos)#

show port-channel summary

Flags	: D - Down I - Individ s - Suspend S - Switche U - Up (por M - Not in	P - lual H - led r - ed R - t-channe use. Min	Up in pou Hot-stand Module-re Routed 1) -links not	rt-channel (me dby (LACP only emoved t met	embers) y)	
Group	Port- T Channel	уре	Protocol	Member Ports		
1	Pol(SU) E	:	LACP	Eth1/4(P)	Eth1/5(P)	

3. Créez une session de capture :

#### <#root>

firepower#

scope packet-capture

firepower /packet-capture #

create session cap1

firepower /packet-capture/session\* #

create phy-port Eth1/2

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

set app ftd

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

set app-identifier ftd1

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

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

firepower /packet-capture/session #

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

# <#root> firepower# scope packet-capture firepower /packet-capture # create session cap1 firepower /packet-capture/session\* # create phy-port Eth1/4 firepower /packet-capture/session/phy-port\* # set app ftd firepower /packet-capture/session/phy-port\* # up firepower /packet-capture/session/phy-port\* # up firepower /packet-capture/session\* # create phy-port Eth1/5 firepower /packet-capture/session/phy-port\* #

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 :

Overview Int	nterfaces	Logical Devices	Security Engine	Platform Settings				System	Tools H	telp a	admin
Capture Session	n Filter Lis	t									
							C Refresh Capture Sessi	Delete Al Se	ssions		
• (0) •	cap1	Drop Count	:: 0	Operational State: up	Buffer Size: 256 M	в	Snap Length: 1518 Byte	15			
Interface Name	e	Filter		File Size (in bytes)	File Name	Device Name					
Ethernet1/2		None		28632	cap1-ethernet-1-2-0.pcap	ftd1	⊻				

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

Overview Interfaces L	ogical Devices Security Engine F	Platform Settings			s	iystem Tools Help admin
Capture Session Filter List						
					C Refresh Capture Session	Delete All Sessions
a 👔 cap1	Drop Count: 0	Operational State: up	Buffer Size: 256 MB		Snap Length: 1518 Bytes	
Interface Name	Filter	File Size (in bytes)	File Name	Device Name		
Ethernet1/5	None	160	cap1-ethernet-1-5-0.pcap	ftd1	*	
Ethernet1/4	None	85000	cap1-ethernet-1-4-0.pcap	ftd1	<u>*</u>	

## **CLI FXOS**

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

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

show session cap1

```
Traffic Monitoring Session:
    Packet Capture Session Name: cap1
    Session: 1
    Admin State: Enabled
    Oper State: Up
    Oper State Reason: Active
    Config Success: Yes
    Config Fail Reason:
    Append Flag: Overwrite
    Session Mem Usage: 256 MB
    Session Pcap Snap Len: 1518 Bytes
    Error Code: 0
    Drop Count: 0
Physical ports involved in Packet Capture:
    Slot Id: 1
    Port Id: 2
    Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap
    Pcapsize: 75136 bytes
    Filter:
    Sub Interface: 0
    Application Instance Identifier: ftd1
    Application Name: ftd
```

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

<#root>

firepower#

scope packet-capture

firepower /packet-capture #

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

```
Pcapsize: 160 bytes
Filter:
Sub Interface: 0
Application Instance Identifier: ftd1
```

Application Name: ftd

Collecter les fichiers de capture

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

Capturer l'analyse des fichiers

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

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

No.	Time	Source	Destination	Protocol	Length	19 ID	IP TTL Info		
F	1 2022-07-13 06:23:58.285080930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (48428)	64 Echo (ping)	request	id=0x001a, seq=7/1792, ttl=64 (no response found!)
	2 2022-07-13 06:23:58.285082858	192.0.2.100	198.51.100.100	ICMP	102	0x9dec (40428)	64 Echo (ping)	request	id=0x001a, seq=7/1792, ttl=64 (no response found!)
	3 2022-07-13 06:23:59.309048886	192.0.2.100	198.51.100.100	ICMP	108	0x9ed0 (40656)	64 Echo (ping)	request	id=0x001a, seq=8/2048, ttl=64 (no response found!)
	4 2022-07-13 06:23:59.309193731	192.0.2.100	198.51.100.100	ICMP	102	0x9ed0 (40656)	64 Echo (ping)	request	id=0x001a, seq=8/2048, ttl=64 (no response found!)
	5 2022-07-13 06:24:00.333054190	192.0.2.100	198.51.100.100	ICMP	108	0x9f20 (40736)	64 Echo (ping)	request	id=0x001a, seq=9/2304, ttl=64 (no response found!)
	6 2022-07-13 06:24:00.333056014	192.0.2.100	198.51.100.100	ICMP	102	0x9f20 (40736)	64 Echo (ping)	request	id=0x001a, seq=9/2304, ttl=64 (no response found!)
	7 2022-07-13 06:24:01.357173530	192.0.2.100	198.51.100.100	ICMP	108	0x9f2d (40749)	64 Echo (ping)	request	id=0x001a, seq=10/2560, ttl=64 (no response found!)
	8 2022-07-13 06:24:01.357174708	192.0.2.100	198.51.100.100	ICMP	102	0x9f2d (40749)	64 Echo (ping)	request	id=0x001a, seq=10/2560, ttl=64 (no response found!)
	9 2022-07-13 06:24:02.381073741	192.0.2.100	198.51.100.100	ICMP	108	0x9f88 (40840)	64 Echo (ping)	request	id=0x001a, seq=11/2816, ttl=64 (no response found!)
	10 2022-07-13 06:24:02.381074999	192.0.2.100	198.51.100.100	ICMP	102	0x9f88 (40840)	64 Echo (ping)	request	id=0x001a, seq=11/2816, ttl=64 (no response found!)
	11 2022-07-13 06:24:03.405199041	192.0.2.100	198.51.100.100	ICMP	108	0xa077 (41079)	64 Echo (ping)	request	id=0x001a, seq=12/3072, ttl=64 (no response found!)
	12 2022-07-13 06:24:03.405200261	192.0.2.100	198.51.100.100	ICMP	102	0xa077 (41079)	64 Echo (ping)	request	<pre>id=0x001a, seq=12/3072, ttl=64 (no response found!)</pre>
	13 2022-07-13 06:24:04.429155683	192.0.2.100	198.51.100.100	ICMP	108	0xa10f (41231)	64 Echo (ping)	request	id=0x001a, seq=13/3328, ttl=64 (no response found!)
	14 2022-07-13 06:24:04.429156831	192.0.2.100	198.51.100.100	ICMP	102	0xa10f (41231)	64 Echo (ping)	request	id=0x001a, seq=13/3328, ttl=64 (no response found!)
	15 2022-07-13 06:24:05.453156612	192.0.2.100	198.51.100.100	ICMP	108	0xa16a (41322)	64 Echo (ping)	request	id=0x001a, seq=14/3584, ttl=64 (no response found!)
	16 2022-07-13 06:24:05.453158052	192.0.2.100	198.51.100.100	ICMP	102	0xa16a (41322)	64 Echo (ping)	request	id=0x001a, seq=14/3584, ttl=64 (no response found!)
	17 2022-07-13 06:24:06.477127687	192.0.2.100	198.51.100.100	ICMP	108	0xa1e9 (41449)	64 Echo (ping)	request	id=0x001a, seq=15/3840, ttl=64 (no response found!)
	18 2022-07-13 06:24:06.477129899	192.0.2.100	198.51.100.100	ICMP	102	0xa1e9 (41449)	64 Echo (ping)	request	id=0x001a, seq=15/3840, ttl=64 (no response found!)
	19 2022-07-13 06:24:07.501291314	192.0.2.100	198.51.100.100	ICMP	108	0xa1f6 (41462)	64 Echo (ping)	request	id=0x001a, seq=16/4096, ttl=64 (no response found!)
	20 2022-07-13 06:24:07.501293041	192.0.2.100	198.51.100.100	ICMP	102	0xa1f6 (41462)	64 Echo (ping)	request	id=0x001a, seq=16/4096, ttl=64 (no response found!)
	21 2022-07-13 06:24:08.525089956	192.0.2.100	198.51.100.100	ICMP	108	0xa257 (41559)	64 Echo (ping)	request	id=0x001a, seq=17/4352, ttl=64 (no response found!)
	22 2022-07-13 06:24:08.525092088	192.0.2.100	198.51.100.100	ICMP	102	0xa257 (41559)	64 Echo (ping)	request	id=0x001a, seq=17/4352, ttl=64 (no response found!)
	23 2022-07-13 06:24:09.549236500	192.0.2.100	198.51.100.100	ICMP	108	0xa2a9 (41641)	64 Echo (ping)	request	<pre>id=0x001a, seq=18/4608, ttl=64 (no response found!)</pre>
	24 2022-07-13 06:24:09.549238564	192.0.2.100	198.51.100.100	ICMP	102	0xa2a9 (41641)	64 Echo (ping)	request	id=0x001a, seq=18/4608, ttl=64 (no response found!)
	25 2022-07-13 06:24:10.573110146	192.0.2.100	198.51.100.100	ICMP	108	0xa345 (41797)	64 Echo (ping)	request	id=0x001a, seq=19/4864, ttl=64 (no response found!)
	26 2022-07-13 06:24:10.573112504	192.0.2.100	198.51.100.100	ICMP	102	0xa345 (41797)	64 Echo (ping)	request	<pre>id=0x001a, seq=19/4864, ttl=64 (no response found!)</pre>
	27 2022-07-13 06:24:11.597086027	192.0.2.100	198.51.100.100	ICMP	108	0xa349 (41801)	64 Echo (ping)	request	id=0x001a, seq=20/5120, ttl=64 (no response found!)
	28 2022-07-13 06:24:11.597088170	192.0.2.100	198.51.100.100	ICMP	102	0xa349 (41801)	64 Echo (ping)	request	<pre>id=0x001a, seq=20/5120, tt1=64 (no response found!)</pre>
	29 2022-07-13 06:24:12.621061022	192.0.2.100	198.51.100.100	ICMP	108	0xa3dc (41948)	64 Echo (ping)	request	1d=0x001a, seq=21/5376, ttl=64 (no response found!)
<									
> F	rame 1: 108 bytes on wire (864 bit	s), 108 bytes (	captured (864 bits)	on interface	capture_u	0_1, id 0		0	000 58 97 bd b9 77 0e 00 50 56 9d e8 be 89 26 80 0a X···w··P V····&··
> E	thernet II, Src: VMware 9d:e8:be (	00:50:56:9d:e8	:be), Dst: Cisco b9	77:0e (58:97:	bd:b9:77:	0e)		0	010 00 00 81 00 00 66 08 00 45 00 00 54 9d ec 40 00 ·····f·· E··T··@·
<b>~</b> N	/N-Tag							0	020 40 01 af c0 c0 00 02 64 c6 33 64 64 08 00 4e a2 @·····d ·3dd··N·
	1	= Direc	tion: From Bridge					0	030 00 1a 00 07 f4 64 ce 62 00 00 00 00 20 a2 07 00d.b
	.0	= Point	er: vif_id						340 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 10
		= Desti	nation: 10						250 IC IG IE IT 20 21 22 23 24 25 20 27 28 29 24 20 1 # \$46 ()-+
	···· ··· ··· ··· ··· 0··· ···	= Loope	d: No	41					,.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
	···· ··· ··· ··· ··· ···	= Reser	ved: 0	- I -					
	00	= Versi	on: 0						
	0000 000	00 0000 = Sourc	e: 0						
L	Type: 802.10 Virtual LAN (0x8100	)							
×٤	02.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 102							
	000 = Priority: H	Best Effort (de	fault) (0)	-					
	0 = DEI: Ineli	gible		31					
	0000 0110 0110 = ID: 102			-					
	Type: IPv4 (0x0800)			_					
> 1	internet Protocol Version 4, Src: 1	92.0.2.100, Dst	t: 198.51.100.100	2					
> 1	Internet Control Message Protocol			2					

Sélectionnez le deuxième paquet et vérifiez les points clés :

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

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info		
Г	1 2022-07-13 06:23:58.285080930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (48428)	64 Echo (ping) reque	id=0x001a, seq=7/1792, ttl=64 (no response found!)	
	2 2022-07-13 06:23:58.285082858	192.0.2.100	198.51.100.100	ICMP	102	0x9dec (48428)	64 Echo (ping) reque	id=0x001a, seq=7/1792, ttl=64 (no response found!)	
	3 2022-07-13 06:23:59.309048886	192.0.2.100	198.51.100.100	ICMP	108	0x9ed0 (40656)	64 Echo (ping) reque	id=0x001a, seq=8/2048, ttl=64 (no response found!)	
	4 2022-07-13 06:23:59.309193731	192.0.2.100	198.51.100.100	ICMP	102	0x9ed0 (40656)	64 Echo (ping) reque	id=0x001a, seq=8/2048, ttl=64 (no response found!)	
	5 2022-07-13 06:24:00.333054190	192.0.2.100	198.51.100.100	ICMP	108	0x9f20 (40736)	64 Echo (ping) reque	id=0x001a, seq=9/2304, ttl=64 (no response found!)	
	6 2022-07-13 06:24:00.333056014	192.0.2.100	198.51.100.100	ICMP	102	0x9f20 (40736)	64 Echo (ping) reque	id=0x001a, seq=9/2304, ttl=64 (no response found!)	
	7 2022-07-13 06:24:01.357173530	192.0.2.100	198.51.100.100	ICMP	108	0x9f2d (40749)	64 Echo (ping) reque	id=0x001a, seq=10/2560, ttl=64 (no response found!)	
	8 2022-07-13 06:24:01.357174708	192.0.2.100	198.51.100.100	ICMP	102	0x9f2d (40749)	64 Echo (ping) reque	id=0x001a, seq=10/2560, ttl=64 (no response found!)	
	9 2022-07-13 06:24:02.381073741	192.0.2.100	198.51.100.100	ICMP	108	0x9f88 (40840)	64 Echo (ping) reque	id=0x001a, seq=11/2816, ttl=64 (no response found!)	
	10 2022-07-13 06:24:02.381074999	192.0.2.100	198.51.100.100	ICMP	102	0x9f88 (40840)	64 Echo (ping) reque	id=0x001a, seq=11/2816, ttl=64 (no response found!)	
	11 2022-07-13 06:24:03.405199041	192.0.2.100	198.51.100.100	ICMP	108	0xa077 (41079)	64 Echo (ping) reque	id=0x001a, seq=12/3072, ttl=64 (no response found!)	
	12 2022-07-13 06:24:03.405200261	192.0.2.100	198.51.100.100	ICMP	102	0xa077 (41079)	64 Echo (ping) reque	id=0x001a, seq=12/3072, ttl=64 (no response found!)	
	13 2022-07-13 06:24:04.429155683	192.0.2.100	198.51.100.100	ICMP	108	0xa10f (41231)	64 Echo (ping) reque	id=0x001a, seq=13/3328, ttl=64 (no response found!)	
	14 2022-07-13 06:24:04.429156831	192.0.2.100	198.51.100.100	ICMP	102	0xa10f (41231)	64 Echo (ping) reque	id=0x001a, seq=13/3328, ttl=64 (no response found!)	
	15 2022-07-13 06:24:05.453156612	192.0.2.100	198.51.100.100	ICMP	108	0xa16a (41322)	64 Echo (ping) reque	id=0x001a, seq=14/3584, ttl=64 (no response found!)	
	16 2022-07-13 06:24:05.453158052	192.0.2.100	198.51.100.100	ICMP	102	0xa16a (41322)	64 Echo (ping) reque	id=0x001a, seq=14/3584, ttl=64 (no response found!)	
	17 2022-07-13 06:24:06.477127687	192.0.2.100	198.51.100.100	ICMP	108	0xa1e9 (41449)	64 Echo (ping) reque	id=0x001a, seq=15/3840, ttl=64 (no response found!)	
	18 2022-07-13 06:24:06.477129899	192.0.2.100	198.51.100.100	ICMP	102	0xa1e9 (41449)	64 Echo (ping) reque	id=0x001a, seq=15/3840, ttl=64 (no response found!)	
	19 2022-07-13 06:24:07.501291314	192.0.2.100	198.51.100.100	ICMP	108	0xa1f6 (41462)	64 Echo (ping) reque	id=0x001a, seq=16/4096, ttl=64 (no response found!)	
	20 2022-07-13 06:24:07.501293041	192.0.2.100	198.51.100.100	ICMP	102	0xa1f6 (41462)	64 Echo (ping) reque	id=0x001a, seq=16/4096, ttl=64 (no response found!)	
	21 2022-07-13 06:24:08.525089956	192.0.2.100	198.51.100.100	ICMP	108	0xa257 (41559)	64 Echo (ping) reque	id=0x001a, seq=17/4352, ttl=64 (no response found!)	
	22 2022-07-13 06:24:08.525092088	192.0.2.100	198.51.100.100	ICMP	102	0xa257 (41559)	64 Echo (ping) reque	id=0x001a, seq=17/4352, ttl=64 (no response found!)	
	23 2022-07-13 06:24:09.549236500	192.0.2.100	198.51.100.100	ICMP	108	0xa2a9 (41641)	64 Echo (ping) reque	id=0x001a, seq=18/4608, ttl=64 (no response found!)	
	24 2022-07-13 06:24:09.549238564	192.0.2.100	198.51.100.100	ICMP	102	0xa2a9 (41641)	64 Echo (ping) reque	id=0x001a, seq=18/4608, ttl=64 (no response found!)	
	25 2022-07-13 06:24:10.573110146	192.0.2.100	198.51.100.100	ICMP	108	0xa345 (41797)	64 Echo (ping) reque	id=0x001a, seq=19/4864, ttl=64 (no response found!)	
	26 2022-07-13 06:24:10.573112504	192.0.2.100	198.51.100.100	ICMP	102	0xa345 (41797)	64 Echo (ping) reque	id=0x001a, seq=19/4864, ttl=64 (no response found!)	
	27 2022-07-13 06:24:11.597086027	192.0.2.100	198.51.100.100	ICMP	108	0xa349 (41801)	64 Echo (ping) reque	id=0x001a, seq=20/5120, ttl=64 (no response found!)	
	28 2022-07-13 06:24:11.597088170	192.0.2.100	198.51.100.100	ICMP	102	0xa349 (41801)	64 Echo (ping) reque	id=0x001a, seq=20/5120, ttl=64 (no response found!)	
	29 2022-07-13 06:24:12.621061022	192.0.2.100	198.51.100.100	ICMP	108	0xa3dc (41948)	64 Echo (ping) reque	id=0x001a, seq=21/5376, ttl=64 (no response found!)	
¢.								en de la desta de la companya de la	
1	Forme 2, 102 button on vine (015 bit	<ol> <li>102 but es a</li> </ol>	anturned (015 bits)	an intenface				00 50 07 bd b0 77 00 00 50 56 0d o0 bo 01 00 00 66 . V.	
1	Frame 2: 102 Dytes on wire (816 Dit	s), 102 bytes c	aptured (816 Dits)	on interface (	capture_u	0_1, 10 0		10 00 00 45 00 00 54 0d or 40 00 40 01 of c0 c0 00	E.T. 0.0
í,	Ethernet II, Srt: Whare Suiesbe (	00:50:56:90:08:	be), Dst: Cisco_b9:	77:00 (58:97:	00:09:77:	oe)		20 02 64 c6 33 64 64 08 00 4e a2 00 1a 00 07 f4 64 d	3dd ·· N·····d
۲	802.10 VIPtual LAN, PRI: 0, DEI: 0,	10: 102	(au1t) (a)					30 ce 62 00 00 00 00 20 a2 07 00 00 00 00 00 10 11 b	
	000 Priority; t	Sest Errort (de	rault) (0)	<b>2</b>				40 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21	
		çible.		וכ				50 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 "#1	\$%8'() *+,/01
	0000 0110 0110 = 1D: 102							60 32 33 34 35 36 37 234	4567
	Type: 1994 (0x0800)	02 0 2 100 Det	. 100 51 100 100	_					
13	Internet Protocol Version 4, Src: 1	92.0.2.100, Dst	: 198.51.100.100	2					
1	internet control Message Protocol			6					

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.

No.	Time	Source	Destination	Protocol	Length	IP ID		IP TTL Info		1			^
-	1 2022-08-05 23:07:31.865872877	192.0.2.100	198.51.100.100	ICMP	108	Øx322e (	(12846)	64 Echo (ping)	request	id=0x002d,	seq=245/62720,	ttl=64 (n	nc
	2 2022-08-05 23:07:31.865875131	192.0.2.100	198.51.100.100	ICMP	102	Øx322e (	(12846)	64 Echo (ping)	request	id=0x002d,	seq=245/62720,	ttl=64 (n	10
	3 2022-08-05 23:07:32.867144598	192.0.2.100	198.51.100.100	ICMP	108	Øx32b9 (	(12985)	64 Echo (ping)	request	id=0x002d,	seq=246/62976,	ttl=64 (n	1C
	4 2022-08-05 23:07:32.867145852	192.0.2.100	198.51.100.100	ICMP	102	Øx32b9 (	(12985)	64 Echo (ping)	request	id=0x002d,	seq=246/62976,	ttl=64 (n	10
	5 2022-08-05 23:07:33.881902485	192.0.2.100	198.51.100.100	ICMP	108	Øx32d8 (	(13016)	64 Echo (ping)	request	id=0x002d,	seq=247/63232,	ttl=64 (n	10
	6 2022-08-05 23:07:33.881904191	192.0.2.100	198.51.100.100	ICMP	102	0x32d8 (	(13016)	64 Echo (ping)	request	id=0x002d,	seq=247/63232,	ttl=64 (n	ic
	7 2022-08-05 23:07:34.883049425	192.0.2.100	198.51.100.100	ICMP	108	Øx3373 (	(13171)	64 Echo (ping)	request	id=0x002d,	seq=248/63488,	ttl=64 (n	ic
	8 2022-08-05 23:07:34.883051649	192.0.2.100	198.51.100.100	ICMP	102	Øx3373 (	(13171)	64 Echo (ping)	request	id=0x002d,	seq=248/63488,	ttl=64 (n	1C
	9 2022-08-05 23:07:35.883478016	192.0.2.100	198.51.100.100	ICMP	108	0x3427 (	(13351)	64 Echo (ping)	request	id=0x002d,	seq=249/63744,	ttl=64 (n	ic
	10 2022-08-05 23:07:35.883479190	192.0.2.100	198.51.100.100	ICMP	102	0x3427 (	(13351)	64 Echo (ping)	request	id=0x002d,	seq=249/63744,	ttl=64 (n	ic
	11 2022-08-05 23:07:36.889741625	192.0.2.100	198.51.100.100	ICMP	108	Øx34de (	(13534)	64 Echo (ping)	request	id=0x002d,	seq=250/64000,	ttl=64 (n	ic
	12 2022-08-05 23:07:36.889742853	192.0.2.100	198.51.100.100	ICMP	102	Øx34de (	(13534)	64 Echo (ping)	request	id=0x002d,	seq=250/64000,	ttl=64 (n	ic
	13 2022-08-05 23:07:37.913770117	192.0.2.100	198.51.100.100	ICMP	108	0x354c (	(13644)	64 Echo (ping)	request	id=0x002d,	seq=251/64256,	ttl=64 (n	ic
	14 2022-08-05 23:07:37.913772219	192.0.2.100	198.51.100.100	ICMP	102	0x354c	(13644)	64 Echo (ping)	request	id=0x002d,	seq=251/64256,	ttl=64 (n	ic
	15 2022-08-05 23:07:38.937829879	192.0.2.100	198.51.100.100	ICMP	108	0x3602 (	(13826)	64 Echo (ping)	request	id=0x002d,	seq=252/64512,	ttl=64 (n	ic
	16 2022-08-05 23:07:38.937831215	192.0.2.100	198.51.100.100	ICMP	102	0x3602 (	(13826)	64 Echo (ping)	request	id=0x002d,	seq=252/64512,	ttl=64 (n	IC I
	17 2022-08-05 23:07:39.961786128	192.0.2.100	198.51.100.100	ICMP	108	Øx36ed (	(14061)	64 Echo (ping)	request	id=0x002d,	seq=253/64768,	ttl=64 (n	ic
	18 2022-08-05 23:07:39.961787284	192.0.2.100	198.51.100.100	ICMP	102	Øx36ed (	(14061)	64 Echo (ping)	request	id=0x002d,	seq=253/64768,	ttl=64 (n	IC I
	19 2022-08-05 23:07:40.985773090	192.0.2.100	198.51.100.100	ICMP	108	Øx37d5 (	(14293)	64 Echo (ping)	request	id=0x002d,	seq=254/65024,	ttl=64 (n	ic v
<												>	>
>	Frame 1: 108 bytes on wire (864 bits)	), 108 bytes cap	tured (864 bits) on	interface	capture_u0_3,	i 0000	a2 76	f2 00 00 25 00 50	56 9d e8	be 89 26 80	54 · v · · · % · P	V · · · · & · T	
>	Ethernet II, Src: VMware_9d:e8:be (00	ð:50:56:9d:e8:be	), Dst: a2:76:f2:00	:00:25 (a2	:76:f2:00:00:25	5) 0010	00 00	81 00 03 e9 08 00	45 00 00	54 32 2e 40	00	ET2.@-	
	VN-Tag					0020	40 01	1b 7f c0 00 02 64	c6 33 64	64 08 00 1e	d6 @·····d	- 3dd	
ш	1	= Directio	n: From Bridge			0030	00 20	00 T5 a6 a2 ed 62	14 15 16	00 /a 21 00	00 ·-···D		
	.0	= Pointer:	vif_id			0040	10 10	10 1f 20 21 22 22	24 25 26	17 18 19 1a 27 28 20 25	2b 1"#	\$78.1/1*+	
	00 0000 0101 0100	<pre> = Destinat</pre>	ion: 84			0050	2c 2d	20 2f 30 31 32 33	34 35 36	37	/0123	4567	
	0	<pre> = Looped:</pre>	No 4				LC LO	EC ET DO DE DE DO	54 55 50	57	, , , , , , , , , , , , , , , , , , , ,	4507	
	0	= Reserved	1: 0										
	00	= Version:	0										
ш	0000 0000	0000 = Source:	0										
II-	Type: 802.10 Virtual LAN (0x8100)												
	802.1Q Virtual LAN, PRI: 0, DEI: 0, 1	ID: 1001											
ш	000 Be	st Effort (defau	lt) (0)										
	0 = DEI: Ineligi	ble	2										
	0011 1110 1001 = ID: 1001		2										
	Type: IPv4 (0x0800)												
1E	Internet Protocol Version 4, Src: 192	2.0.2.100, Dst:	198.51.100.100										
	Internet Control Message Protocol		2										

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.

No	Time	Source	Destination	Protocol	Length	IP ID		IP TT	L Info			1				^
C.	1 2022-08-05 23:07:31.865872877	192.0.2.100	198.51.100.100	ICMP	108	0x322e (1	2846)	6	4 Echo	(ping)	request	id=0x002d,	seq=245/62720	, ttl=64	(nc	
	2 2022-08-05 23:07:31.865875131	192.0.2.100	198.51.100.100	ICMP	102	Øx322e (1	2846)	6	4 Echo	(ping)	request	id=0x002d,	seq=245/62720	, ttl=64	(nc	
	3 2022-08-05 23:07:32.867144598	192.0.2.100	198.51.100.100	ICMP	108	0x32b9 (1	2985)	6	4 Echo	(ping)	request	id=0x002d,	seq=246/62976	, ttl=64	(nc	
	4 2022-08-05 23:07:32.867145852	192.0.2.100	198.51.100.100	ICMP	102	0x32b9 (1	2985)	6	4 Echo	(ping)	request	id=0x002d,	seq=246/62976	, ttl=64	(nc	
	5 2022-08-05 23:07:33.881902485	192.0.2.100	198.51.100.100	ICMP	108	0x32d8 (1	3016)	6	4 Echo	(ping)	request	id=0x002d,	seq=247/63232	, ttl=64	(nc	
	6 2022-08-05 23:07:33.881904191	192.0.2.100	198.51.100.100	ICMP	102	0x32d8 (1	3016)	6	4 Echo	(ping)	request	id=0x002d,	seq=247/63232	, ttl=64	(nc	
	7 2022-08-05 23:07:34.883049425	192.0.2.100	198.51.100.100	ICMP	108	Øx3373 (1	3171)	6	4 Echo	(ping)	request	id=0x002d,	seq=248/63488	, ttl=64	(nc	
	8 2022-08-05 23:07:34.883051649	192.0.2.100	198.51.100.100	ICMP	102	Øx3373 (1	3171)	6	4 Echo	(ping)	request	id=0x002d,	seq=248/63488	, ttl=64	(nc	
	9 2022-08-05 23:07:35.883478016	192.0.2.100	198.51.100.100	ICMP	108	0x3427 (1	3351)	6	4 Echo	(ping)	request	id=0x002d,	seq=249/63744	, ttl=64	(nc	
	10 2022-08-05 23:07:35.883479190	192.0.2.100	198.51.100.100	ICMP	102	0x3427 (1	3351)	6	4 Echo	(ping)	request	id=0x002d,	seq=249/63744	, ttl=64	(nc	
	11 2022-08-05 23:07:36.889741625	192.0.2.100	198.51.100.100	ICMP	108	0x34de (1	3534)	6	4 Echo	(ping)	request	id=0x002d,	seq=250/64000	, ttl=64	(nc	
	12 2022-08-05 23:07:36.889742853	192.0.2.100	198.51.100.100	ICMP	102	0x34de (1	3534)	6	4 Echo	(ping)	request	id=0x002d,	seq=250/64000	, ttl=64	(nc	
	13 2022-08-05 23:07:37.913770117	192.0.2.100	198.51.100.100	ICMP	108	0x354c (1	3644)	6	4 Echo	(ping)	request	id=0x002d,	seq=251/64256	, ttl=64	(nc	
	14 2022-08-05 23:07:37.913772219	192.0.2.100	198.51.100.100	ICMP	102	0x354c (1	3644)	6	4 Echo	(ping)	request	id=0x002d,	seq=251/64256	, ttl=64	(nc	
	15 2022-08-05 23:07:38.937829879	192.0.2.100	198.51.100.100	ICMP	108	0x3602 (1	3826)	6	4 Echo	(ping)	request	id=0x002d,	seq=252/64512	, ttl=64	(nc	
	16 2022-08-05 23:07:38.937831215	192.0.2.100	198.51.100.100	ICMP	102	0x3602 (1	3826)	6	4 Echo	(ping)	request	id=0x002d,	seq=252/64512	, ttl=64	(nc	
	17 2022-08-05 23:07:39.961786128	192.0.2.100	198.51.100.100	ICMP	108	0x36ed (1	4061)	6	4 Echo	(ping)	request	id=0x002d,	seq=253/64768	, ttl=64	(nc	
	18 2022-08-05 23:07:39.961787284	192.0.2.100	198.51.100.100	ICMP	102	0x36ed (1	4061)	6	4 Echo	(ping)	request	id=0x002d,	seq=253/64768	, ttl=64	(nc	
	19 2022-08-05 23:07:40.985773090	192.0.2.100	198.51.100.100	ICMP	108	0x37d5 (1	4293)	6	4 Echo	(ping)	request	id=0x002d,	seq=254/65024	, ttl=64	(nc	~
<															>	
>	Frame 2: 102 bytes on wire (816 bits	), 102 bytes capt	tured (816 bits) on	interface o	apture_u0_3,	i 0000	a2 76	f2 00	00 25 0	0 50	56 9d e8	be 81 00 03	e9 ·v··%·P	v		
>	Ethernet II, Src: VMware_9d:e8:be (0	0:50:56:9d:e8:be)	), Dst: a2:76:f2:00	:00:25 (a2:7	6:f2:00:00:2	5) 0010	08 00	45 00	00 54 3	32 2e	40 00 40	01 1b 7f c0	00 ··E··T2.	0.0		
ł	802.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 1001				0020	02 64	c6 33	64 64 6	00 80	1e d6 00	2d 00 f5 a6	a2 ·d·3dd··			
н	000 Be	st Effort (defau	lt) (0)			0030	ed 62	00 00	00 00 7	a 2f	0b 00 00	00 00 00 10	11 ·b····z/			
н	0 = DEI: Ineligi	ble	3			0040	12 13	14 15	16 17 1	18 19	1a 1b 1c	1d 1e 1f 20	21			
н	0011 1110 1001 = ID: 1001		-			0050	22 23	24 25	26 27 2	8 29	2a 20 2C	2d 2e 2f 30	31 "#\$%&"()	*+,/01		
П	Type: IPv4 (0x0800)					0000	52 33	54 35	30 37				23450/			
H	Internet Protocol Version 4, Src: 19	2.0.2.100, Dst: 1	198.51.100.100													
	Internet Control Message Protocol		2													
1 L																

# 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 Tools > Packet Capture > Capture Session pour créer une nouvelle session de capture :

Overview	Interfaces	Logical Devices	Security Engine	Platform Settings		System	Tools Help admin
						Packet Capture	Troubleshooting Logs
Capture Ses	sion Filter	List					
					C Refresh	Capture Session Dek	te All Sessions
No Session av	vailable						

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 :

Overview Interfaces Logical Devices Security Engine Platform Settings		System Tools Help admin
Select an instance: ftd1		Save and Run Save Cancel
ftd1	Session Name*	cap1
	Selected Interfaces	None
Ethernet1/2	Buffer Size	256 MB
	Snap length:	1518 Bytes
	Store Packets	Overwrite Append
	Capture On	Al Backplane Ports
Ethernet1/3 FTD	Capture Filter	Ethernet1/9
Ethernet1/9, Ethernet1/10		Ethernet1/10 Al Backplane Ports
Ethernet1/1		

## **CLI FXOS**

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

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

<#root>								
firepower#								
scope ssa								
firepower / show app-in	'ssa# nstance							
App Name	Identifier Slot ID	Admin State	Oper State	Running Version	Startup	Version	Deploy	Ty
ftd	ftdl							
1	Enabled	Online	7.2.0.82	7.2.0.82	Native	No		

2. Créez une session de capture :

<#root>

firepower#

scope packet-capture

firepower /packet-capture #

create session cap1

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

commit

firepower /packet-capture/session #

Vérification

FCM

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

Overview Interfa	ces Logical Devices Security Engine	Platform Settings			Sys	tem Tools Help admin
Capture Session	iter List					
				Ċ R	efresh Capture Session De	elete All Sessions
🔺 🧵 cap1	Drop Count: 0	Operational State: up	Buffer Size: 256 MB	Sna	p Length: 1518 Bytes	
Interface Name	Filter	File Size (in bytes)	File Name	Device Name		
Ethernet1/10	None	194352	cap1-ethernet-1-10-0.pcap	ftd1	$_{\pm}$	
Ethernet1/9	None	286368	cap1-ethernet-1-9-0.pcap	ftd1	*	

# **CLI FXOS**

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

<#root> firepower#

scope packet-capture

firepower /packet-capture #

show session cap1

Traffic Monitoring Session:

Packet Capture Session Name: cap1

Session: 1

Admin State: Enabled

Oper State: Up

Oper State Reason: Active

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

Physical ports involved in Packet Capture:

Slot Id: 1

Port Id: 10

```
Pcapsize: 1017424 bytes
Filter:
Sub Interface: 0
Application Instance Identifier: ftd1
Application Name: ftd
Slot Id: 1
Port Id: 9
Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-9-0.pcap
Pcapsize: 1557432 bytes
Filter:
Sub Interface: 0
Application Instance Identifier: ftd1
Application Name: ftd
```

Collecter les fichiers de capture

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

Capturer l'analyse des fichiers

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

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

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

l'interface de sortie Ethernet1/3.

4. Le commutateur interne insère une étiquette VN supplémentaire.

No. Time	Source	Destination	Protocol	Length	PD	IP TTL Info		
1 2022-07-14 20:20:36.513854256	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64 Echo (ping) requ	est i	d=0x0001, seq=15/3840, ttl=64 (no response found!)
2 2022-07-14 20:20:36.513857289	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64 Echo (ping) requ	est i	ld=0x0001, seq=15/3840, ttl=64 (reply in 3)
3 2022-07-14 20:20:36.514117394	198.51.100.100	9 192.0.2.100	ICMP	108	Øxcc2c (52268)	64 Echo (ping) repl	y i	id=0x0001, seq=15/3840, ttl=64 (request in 2)
4 2022-07-14 20:20:36.514119312	198.51.100.100	192.0.2.100	ICMP	108	Øxcc2c (52268)	64 Echo (ping) repl	y i	ld=0x0001, seq=15/3840, ttl=64
5 2022-07-14 20:20:37.537723822	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040)	64 Echo (ping) requ	est i	id=0x0001, seq=16/4096, ttl=64 (no response found!)
6 2022-07-14 20:20:37.537726588	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040)	64 Echo (ping) requ	est i	id=0x0001, seq=16/4096, ttl=64 (reply in 7)
7 2022-07-14 20:20:37.538046165	198.51.100.100	192.0.2.100	ICMP	108	0xcc9b (52379)	64 Echo (ping) repl	y i	id=0x0001, seq=16/4096, ttl=64 (request in 6)
8 2022-07-14 20:20:37.538048311	198.51.100.100	192.0.2.100	ICMP	108	Øxcc9b (52379)	64 Echo (ping) repl	y i	id=0x0001, seq=16/4096, ttl=64
9 2022-07-14 20:20:38.561776064	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64 Echo (ping) requ	est i	id=0x0001, seq=17/4352, ttl=64 (no response found!)
10 2022-07-14 20:20:38.561778310	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64 Echo (ping) requ	est i	id=0x0001, seq=17/4352, ttl=64 (reply in 11)
11 2022-07-14 20:20:38.562048288	198.51.100.100	192.0.2.100	ICMP	108	0xccc4 (52420)	64 Echo (ping) repl	y i	id=0x0001, seq=17/4352, ttl=64 (request in 10)
12 2022-07-14 20:20:38.562050333	198.51.100.100	192.0.2.100	ICMP	108	0xccc4 (52420)	64 Echo (ping) repl	y i	id=0x0001, seq=17/4352, ttl=64
13 2022-07-14 20:20:39.585677043	192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366)	64 Echo (ping) requ	est i	id=0x0001, seq=18/4608, ttl=64 (no response found!)
14 2022-07-14 20:20:39.585678455	192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366)	64 Echo (ping) requ	est i	id=0x0001, seq=18/4608, ttl=64 (reply in 15)
15 2022-07-14 20:20:39.585936554	198.51.100.100	192.0.2.100	ICMP	108	0xcd8d (52621)	64 Echo (ping) repl	y i	id=0x0001, seq=18/4608, ttl=64 (request in 14)
16 2022-07-14 20:20:39.585937900	198.51.100.100	9 192.0.2.100	ICMP	108	Øxcd8d (52621)	64 Echo (ping) repl	y i	id=0x0001, seq=18/4608, ttl=64
17 2022-07-14 20:20:40.609804804	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (23419)	64 Echo (ping) requ	est i	id=0x0001, seq=19/4864, ttl=64 (no response found!)
18 2022-07-14 20:20:40.609807618	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (23419)	64 Echo (ping) requ	est i	id=0x0001, seq=19/4864, ttl=64 (reply in 19)
19 2022-07-14 20:20:40.610179685	198.51.100.100	192.0.2.100	ICMP	108	0xcd8f (52623)	64 Echo (ping) repl	y i	id=0x0001, seq=19/4864, ttl=64 (request in 18)
20 2022-07-14 20:20:40.610181944	198.51.100.100	192.0.2.100	ICMP	108	Øxcd8f (52623)	64 Echo (ping) repl	y i	id=0x0001, seq=19/4864, ttl=64
21 2022-07-14 20:20:41.633805153	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64 Echo (ping) requ	est i	id=0x0001, seq=20/5120, ttl=64 (no response found!)
22 2022-07-14 20:20:41.633806997	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64 Echo (ping) requ	est i	id=0x0001, seq=20/5120, ttl=64 (reply in 23)
23 2022-07-14 20:20:41.634084102	198.51.100.100	192.0.2.100	ICMP	108	0xce36 (52790)	64 Echo (ping) repl	y i	id=0x0001, seq=20/5120, ttl=64 (request in 22)
24 2022-07-14 20:20:41.634085368	198.51.100.100	192.0.2.100	ICMP	108	0xce36 (52790)	64 Echo (ping) repl	y i	id=0x0001, seq=20/5120, ttl=64
25 2022-07-14 20:20:42.657709898	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64 Echo (ping) requ	est i	id=0x0001, seq=21/5376, ttl=64 (no response found!)
26 2022-07-14 20:20:42.657711660	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64 Echo (ping) requ	est i	id=0x0001, seq=21/5376, ttl=64 (reply in 27)
27 2022-07-14 20:20:42.657980675	198.51.100.100	192.0.2.100	ICMP	108	0xce49 (52809)	64 Echo (ping) repl	y i	id=0x0001, seq=21/5376, ttl=64 (request in 26)
28 2022-07-14 20:20:42.657981971	198.51.100.100	192.0.2.100	ICMP	108	0xce49 (52809)	64 Echo (ping) repl	y i	id=0x0001, seq=21/5376, ttl=64
29 2022-07-14 20:20:43.681736697	192.0.2.100	198.51.100.100	ICMP	108	0x5c52 (23634)	64 Echo (ping) requ	est i	id=0x0001, seq=22/5632, ttl=64 (no response found!)
c					1 1			
> Frame 1: 100 butes on wine (064 bit	<li>(c) 100 botos </li>	antured (064 hits)	on interface	canture u	0.0 (4.0			an an sa sa sa na ar sa sa na bi ba rr ri an sa na an
> Frame 1. 108 bytes on wire (804 bit	9-07-bd-b0-77-7	d) Det: Whare of	011 Incertace	capcure_u	50)		001	10 00 00 10 00 07 08 00 45 00 00 54 59 00 40 00
/ Ethernet 11, SPC: CISCO_09:77:20 (5	8:97:00:09:77:2	(d), USC: VHware_90	.07.50 (00.50.	501901e71	50)		003	20 40 01 f4 1c c0 00 02 64 c6 33 64 64 08 00 22 68 @d .3dd"h
v vn-tag	- Dines	tion. To Deidao					00	30 00 01 00 0f 89 7a d0 62 00 00 00 00 b3 d7 09 00z.b
o	- Direc	cion: To Bridge					004	10 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b
00 0000 0000 0000	- Docti	er: vir_io					003	ie 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ···· !"# \$%&'()"+
		di No					000	0 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,/0123 4567
	- Record	u. no	4					
	- Weser	veu; o						
	······ ····· ·························	01:0						
	00 1010 = Sourc	e: 10						
Type: 802.10 Virtual LAN (0x8100)	)		_					
802.10 VITUAL LAN, PRI: 0, DEI: 0,	10: 103	(a)						
000 = Priority: E	sest Effort (de	raure) (0)	2					
	gible		5					
0000 0110 0111 = 1D: 103								
Type: IPV4 (0x0800)			_					
Internet Protocol Version 4, Src: 1	92.0.2.100, Dst	: 198.51.100.100	2					
Internet Control Message Protocol			2					

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.

1       1022-07-14       2022-07-14
2 202-07-14 2012/03.51837289       120.2.7.100       190.31.00.100       100
3 202:07:14 202:03:6.3411794         99:51.100.100 120.0.7.100         ICOP         100         0xcccc (3226)         64 Cho (ping) reply         10-0x001. seq:13/3840, t11-44           5 202:07:14 202:03:5.5172322         150.0.100 195.5.1.00.100 120.0.7.100         1COP         100         0xcccc (3226)         64 Cho (ping) reply         10-0x001. seq:13/3840, t11-44         (request in 2)           7 202:07:14 202:03:7.5372322         150.0.100 192.0.7.100         1COP         100         0xcccb (3237)         64 Cho (ping) reply         10-0x001. seq:13/4800, t11-44         (request in 6)           7 202:07:14 202:03:7.538411         105.51.100.100 122.0.7.100         1COP         100         0xccb (3237)         64 Cho (ping) reply         10-0x001. seq:13/4800, t11-44         (request in 6)           9 202:07:14 202:03:5507664         150.0.100 122.0.7.100         1COP         100         0xccb (3237)         64 Cho (ping) reply         10-0x001. seq:13/4800, t11-44         (request in 10)           10 202:07:14 202:03:15:050203         105.51.100.100         1COP         100         0xccc (5248)         64 Cho (ping) reply         10-0x001. seq:13/4800, t11-44         (request in 10)           10 202:07:14 202:03:05:0503         105.51.100.100         1COP         100         0xccc (5248)         64 Cho (ping) reply         10-0x001. seq:13/4800, t11-44         (request in 12)
4 202-07-14 20220:55.1419312       109.51.100.100 192.0.2.100       ICPP 100       0x5360 (2386)       64 Etch (ping) Preput       1d-0x0001, seq-15/386, t11-64       (reply in 7)         5 202-07-14 202:017.53726581       120.6.2.100       109.53.1.00.100       ICPP 108       0x5360 (2386)       64 Etch (ping) Preput       id-0x0001, seq-15/4005, t11-64 (reply in 7)         7 202-07-14 202:017.53726581       120.6.2.100       109.53.1.00.100       ICPP 108       0x5367 (2323)       64 Etch (ping) Preput       id-0x0001, seq-15/4005, t11-64 (reply in 7)         9 2022-07-14 202:017.5372641       120.6.2.100       109.53.1.00.100       ICPP 108       0x5367 (2323)       64 Etch (ping) Preput       id-0x0001, seq-15/332, t11-64 (no response found)         10 2022-07-14 202:018.56428428       106.10.10.010 19.0.0.100       ICPP 108       0x5267 (2323)       64 Etch (ping) Preput       id-0x0001, seq-15/332, t11-64 (no response found)         12 2022-07-14 202:018.56425731       19.6.2.100       109.10.100       ICPP 108       0x5267 (2324)       64 Etch (ping) Preput       id-0x0001, seq-15/4000, seq-
5 202-07-14 20:20:17,5772822       102.0.100       108.51.100.100       TCP       108       0x5400 (23040)       64 Etch (ping) request       d-0x8001, seq=16/4005, tt1-64 (no response found))         7 202-07-14 20:20:17,5738411       105.51.100.100       109.0.2.100       TCP       108       0x5400 (23040)       64 Etch (ping) reput       d-0x8001, seq=16/4005, tt1-64 (no response found))         9 202-07-14 20:20:17,5738411       105.51.100.100       109.0.2.100       TCP       108       0x5407 (2323)       64 Etch (ping) reput       d-0x8001, seq=16/4005, tt1-64 (no response found))         10 202-07-14 20:20:31.56177864       192.0.2.100       TCP       108       0x5407 (2323)       64 Etch (ping) reput       d-0x8001, seq=17/4332, tt1-64 (no response found))         11 202-07-14 20:20:31.56457841       193.51.100.100       109.0.2.100       TCP       108       0x5407 (2323)       64 Etch (ping) reput       d-0x8001, seq=17/4332, tt1-64 (no response found))         12 202-07-14 20:20:31.56458784       193.51.100.100       109.0.2.100       TCP       108       0x5407 (2323)       64 Etch (ping) reput       d-0x8001, seq=17/4332, tt1-64 (no response found))         12 202-07-14 20:20:30.640887614       194.51.100.100       109.0.2.100       TCP       108       0x5476 (2323)       64 Etch (ping) reput       d-0x8001, seq=17/4333, tt1-64 (no response found))       100.100       100.100
6 2022-07-14 20:2017.537726588 122.0.2.100 198.5.1.00.100 122.0.2.100 1019 108 0xco09 (23040) 64 Echo (ping) reput 160x0001, seq-16/4069, ttl-46 (request in 6) 8 2022-07-14 20:2017.538468151 198.5.1.00.100 122.0.2.100 1019 108 0xco09 (53279) 64 Echo (ping) reput 160x0001, seq-16/4069, ttl-46 (request in 6) 9 2022-07-14 20:2018.561776815 192.0.2.100 109.5.1.00.100 1019 108 0xco09 (53279) 64 Echo (ping) request 160x0001, seq-16/4069, ttl-46 (request in 6) 10 2022-07-14 20:2018.56277831 192.0.2.100 109.2.0.100 1019 108 0xco19 (23232) 64 Echo (ping) request 160x0001, seq-17/4532, ttl-46 (request in 10) 11 2022-07-14 20:2018.56277831 192.0.2.100 109.2.0.2.100 1019 108 0xcc4 (53240) 64 Echo (ping) request 160x0001, seq-17/4532, ttl-46 (request in 10) 12 2022-07-14 20:2019.56277831 192.0.2.100 109.2.0.2.100 1019 108 0xcc4 (53240) 64 Echo (ping) request 160x0001, seq-18/4069, ttl-46 (request in 10) 14 2022-07-14 20:2019.56577831 192.0.2.100 109.2.0.2.100 1019 108 0xcd6 (3366) 64 Echo (ping) request 160x0001, seq-18/4069, ttl-46 (request in 14) 16 5022-07-14 20:2019.58595534 198.5.100.100 120.2.100 1019 108 0xcd6 (3261) 64 Echo (ping) request 160x0001, seq-18/4069, ttl-46 (request in 14) 16 5022-07-14 20:2019.58595545 198.5.100.100 120.2.100 1019 108 0xcd6 (3261) 64 Echo (ping) request 160x0001, seq-18/4069, ttl-46 (request in 14) 16 5022-07-14 20:2019.58593790 198.5.100.100 120.2.100 1019 108 0xcd6 (5262) 64 Echo (ping) request 160x0001, seq-18/4069, ttl-46 (request in 14) 17 2022-07-14 20:2019.58593790 198.5.100.100 1020 108 0xcd6 (5262) 64 Echo (ping) request 160x0001, seq-18/4069, ttl-46 (request in 14) 10 20 202-07-14 20:2019.58593790 198.5.100.100 1020 108 0xcd6 (5262) 64 Echo (ping) request 160x0001, seq-18/4089, ttl-46 (request in 12) 20 202-07-14 20:2014.604801194 192.0.2.100 1019 108 0xcd6 (5262) 64 Echo (ping) request 160x0001, seq-18/4089, ttl-64 (request in 20) 20 202-07-14 20:2014.60311392.0.2.100 1019 108 0xcd6 (5262) 64 Echo (ping) request 160x0001, seq-20/5138, ttl-64 (request in 20) 20 20
7 2022-07-14 20:20:17.53846465       198.51.100.100 192.0.2.100       1029       108       0xcc0b (5237)       64 Echo (ping) reply       id=0x0001, seq=16/4069, til=64       (request in 6)         9 2022-07-14 20:20:18.56177664       192.0.2.100       198.51.100.100       1029       108       0xcc0b (5237)       64 Echo (ping) request       id=0x0001, seq=16/4069, til=64       (request in 10)         10 2022-07-14 20:20:18.5627831       198.51.100.100       192.0.2.100       108.51.100.100       192.0.2.100       108       0xccc1 (52420)       64 Echo (ping) request       id=0x0001, seq=17/4352, til=64       (request in 10)         12 2022-07-14 20:20:18.56278453       192.0.2.100       108.51.100.100       1079       108       0xccc1 (52420)       64 Echo (ping) request       id=0x0001, seq=17/4352, til=64       (request in 13)         12 2022-07-14 20:20:19.585774533       192.0.2.100       108.51.100.100       1079       108       0xcd6 (52621)       64 Echo (ping) request       id=0x0001, seq=18/4068, til=64       (request in 14)         16 2022-07-14 20:20:30.585775435       192.0.2.100       1079       108       0xcd6 (52622)       64 Echo (ping) request       id=0x0001, seq=18/4068, til=64       (request in 14)       id=0x0001, seq=18/4068, til=64       (request in 14)       id=0x001, seq=18/4068, til=64       (request in 14)       id=0x0001, seq=18/4068, til=64       (request
8 202-07-14 20:20:37.538048211       190.5.1.000 100 192.0.2.100       TOPP       108       0xc2ob (52297)       64 Echo (ping) reply       id-ox0001, seq-1/4335, ttl-44 (reply in 11)         10 2022-07-14 20:20:38.56177861       192.0.2.100       198.51.100.100       TOPP       108       0xc2ob (52237)       64 Echo (ping) request       id-ox0001, seq-1/4335, ttl-46 (reply in 11)         11 2022-07-14 20:20:38.56277861       192.0.2.100       TOPP       108       0xcccd (52420)       64 Echo (ping) reply       id-ox0001, seq-1/4335, ttl-46 (reply in 13)         12 2022-07-14 20:20:38.55677841       192.0.2.100       TOP       108       0xccd (52420)       64 Echo (ping) reply       id-ox0001, seq-1/4354, ttl-46 (reply in 16)         13 2022-07-14 20:20:39.555777841       192.0.2.100       TOP       108       0xcdd (52201)       64 Echo (ping) reply       id-ox0001, seq-1/4364, ttl-44 (reply in 15)         15 2022-07-14 20:20:39.555937564       193.0.100.100       102.0.2.010       TOP       108       0xcdd (52201)       64 Echo (ping) reply       id-ox0001, seq-1/4364, ttl-44 (reply in 15)         15 2022-07-14 20:20:34.66080718       192.0.2.100       TOP       108       0xcdd (52201)       64 Echo (ping) reply       id-ox0001, seq-1/4364, ttl-44 (reply in 12)         16 2022-07-14 20:20:46.61081544       193.51.100.100       192.0.2.100       TOP       108       0xcc
9 2022-07-14 20:21:8.56177604       192.0.2.00       198.51.100.100       1CVP       108       0053b7 (2222)       64 (cho (ping) request id-dx0001, seq-17/452; ttl-64 (request in 1a)         11 2022-07-14 20:21:8.56274328       198.51.100.100       1CVP       108       0053b7 (2222)       64 (cho (ping) request id-dx0001, seq-17/452; ttl-64 (request in 1a)         12 2022-07-14 20:21:8.56274328       198.51.100.100       1CVP       108       0053b7 (2223)       64 (cho (ping) request id-dx0001, seq-17/452; ttl-64 (request in 1a)         12 2022-07-14 20:21:8.56274328       198.51.100.100       1CVP       108       0053b6 (23366)       64 (cho (ping) request id-dx0001, seq-18/4608; ttl-64 (request in 14)         14 2022-07-14 20:21:9.565767455       192.0.2.100       108       0053b6 (23366)       64 (cho (ping) request id-dx0001, seq-18/4608; ttl-64 (reqly in 15)         15 2022-07-14 20:21:9.565767455       192.0.2.100       108       0053b7 (22419)       64 (cho (ping) request id-dx0001, seq-18/4608; ttl-64 (reqly in 19)         16 2022-07-14 20:21:04.600807618       192.0.2.100       108       0053b7 (22419)       64 (cho (ping) request id-dx0001, seq-19/4604; ttl-64 (reqly in 18)         18 202-07-14 20:21:04.60101954       192.0.2.100       108       0053b7 (22419)       64 (cho (ping) request id-dx0001, seq-19/4604; ttl-64 (reqly in 12)         19 2022-07-14 20:21:04.6101954       198.51.100.100       102.0.2.100       <
10 2022-07-14 202:08:.61778310       192.0.2.100       100:09       100:08       00:5057 (23223)       64 6tho (ping) request i d-000001, seq-17/4332, ttl-64 (request in 10)         12 2022-07-14 202:08:.50408283       109:51.100.100       102:0.2.100       100:09       108       00:5057 (23223)       64 6tho (ping) reqly id-000001, seq-17/4332, ttl-64         13 2022-07-14 202:08:.50408333       109:51.100.100       102:0.2.100       108:0       00:5067 (23263)       64 6tho (ping) reqly id-000001, seq-17/4068, ttl-64 (no response found)         14 2022-07-14 202:08:.50407043       10:20.2.0.100       10:20
112022-07-14 20:218.56204328       196.51.100.100 192.0.2.100       10/P       108       0xccc4 (52420)       64 tho (ping) reply       id=0x0001, seq=17/4332, ttl=64 (request in 10)         122022-07-14 20:218.5620433       192.0.2.100       108.51.100.100       10/P       188       0xcbd (23366)       64 tho (ping) request id=0x0001, seq=13/4688, ttl=64 (no response found)         142022-07-14 20:218.58570455       192.0.2.100       198.51.100.100       10.29       188       0xcbd (23366)       64 tho (ping) request id=0x0001, seq=13/4688, ttl=64 (request in 14)         152022-07-14 20:218.58570455       192.0.2.100       192.0.2.100       1029       188       0xcbd (23366)       64 tho (ping) request id=0x0001, seq=13/4688, ttl=64 (request in 14)         16202-07-14 20:218.60908064       192.0.2.100       192.0.2.100       1029.0.2.100
12 2022-07-14 202:13.5620*0313       196.51.100.100       10*P       108       0xccc4 (52240)       64 fcho (ping) requit       id=0x0001, seq=17/452; tl=-44         13 2022-07-14 202:19.585674455       192.0.2.100       198.51.100.100       10*P       108       0xccd4 (52240)       64 fcho (ping) requit       id=0x0001, seq=18/4608, tl=-64 (no response found))         14 2022-07-14 202:19.585674455       192.0.2.100       10*P       108       0xcdd (5261)       64 fcho (ping) requit       id=0x0001, seq=18/4608, tl=-64 (no response found))         15 2022-07-14 202:20.20.600898768       192.0.2.100       10*P       108       0xcdd (5261)       64 fcho (ping) requit       id=0x0001, seq=18/4608, tl=-64 (reply in 15)         12 2022-07-14 202:20.40.60897618       192.0.2.100       10*P       108       0xcdf (52623)       64 fcho (ping) requit       id=0x0001, seq=18/4608, tl=-64 (requits in 14)         12 2022-07-14 202:20.40.61017968       198.51.100.100       10*P       108       0xcdf (52623)       64 fcho (ping) requit       id=0x0001, seq=18/4608, tl=-64 (requits in 18)       20         12 2022-07-14 202:204.610179685       198.51.100.100       10*P       108       0xcdf (52623)       64 fcho (ping) requit       id=0x0001, seq=19/4864, tl=-64 (requits in 22)       20       20       20       20       20       20       20       20       20       20<
1 2 022-07-14 20:20:30.58567043       192.0.2.100       198.51.100.100       ICVP       108       0x5b6 (23366)       64 Echo (ping) request       id-0x0001, seq-18/4608, ttl-64 (reply in 15)         1 4 2022-07-14 20:20:30.58593654       198.51.100.100       ICVP       108       0x5b6 (23366)       64 Echo (ping) request       id-0x0001, seq-18/4608, ttl-64 (reply in 15)         1 5 2022-07-14 20:20:30.58593700       198.51.100.100       ICVP       108       0x5b6 (23366)       64 Echo (ping) request       id-0x0001, seq-18/4608, ttl-64 (reply in 15)         1 2 2022-07-14 20:20:40.60980484       192.0.2.100       ICVP       108       0x5b7b (23419)       64 Echo (ping) request       id-0x0001, seq-18/468, ttl-64         1 2 2022-07-14 20:20:40.60980484       12.0.2.100       ICVP       108       0x5b7b (23419)       64 Echo (ping) reply       id-0x0001, seq-19/4684, ttl-64
1 12 022-07-14 20:20:30.585936455 192.0.2.100       198.51.100.100       10.9P       108       0x5da6 (23366)       64 Echo (ping) repus       id-0x0001, seq=18/4608; ttl=64 (repus in 15)         1 5 2022-07-14 20:20:30.585937500       198.51.100.100       192.0.2.100       10.PP       108       0x5db6 (2340)       64 Echo (ping) repus       id-0x0001, seq=18/4608; ttl=64 (request in 14)         1 7 2022-07-14 20:20:30.585937500       198.51.100.100       10.PP       108       0x5db7 (23410)       64 Echo (ping) repus       id-0x0001, seq=18/4608; ttl=64 (request in 14)         1 2 2022-07-14 20:20:40.600980768       198.51.100.100       10.PP       108       0x5db7 (23410)       64 Echo (ping) repus       id-0x0001, seq=18/4608; ttl=64 (request in 14)         1 2 2022-07-14 20:20:40.60181944       199.51.100.100       10.PP       108       0x5db7 (23410)       64 Echo (ping) repus       id-0x0001, seq=18/4608; ttl=64 (request in 18)         2 2 2022-07-14 20:20:41.60181944       195.1100.100       10.PP       108       0x5db7 (23422)       64 Echo (ping) repus       id-0x0001, seq=28/5120; ttl=64 (repus in 22)         2 2 2022-07-14 20:20:41.633806971       199.51.100.100       10.PP       108       0x5db7 (23422)       64 Echo (ping) repus       id-0x0001, seq=28/5120; ttl=64 (request in 22)         2 2 2022-07-14 20:20:42.657780858       198.51.100.100       10.PP       108       0x5d
15 2022-07-14 20:20:30.58593564       198.51.100.100       192.0.2.100       TCMP       108       0xcd8d (\$2521)       64 Echo (ping) reply       id=0x0001, seq=18/4608, ttl=44 (request in 14)         16 2022-07-14 20:20:30.585937900       198.51.100.100       192.0.2.100       TCMP       108       0xcd8d (\$2521)       64 Echo (ping) reply       id=0x0001, seq=18/4608, ttl=44 (no response found1)         18 2022-07-14 20:20:40.60980404       192.0.2.100       10MP       108       0xcd8d (\$2521)       64 Echo (ping) request       id=0x0001, seq=18/4608, ttl=44 (no response found1)         19 2022-07-14 20:20:40.609804041       192.0.2.100       10MP       108       0xcd8f (\$2523)       64 Echo (ping) request       id=0x0001, seq=19/4864, ttl=44 (no response found1)         19 2022-07-14 20:20:40.61019055       192.0.2.100       10MP       108       0xcd8f (\$2523)       64 Echo (ping) request       id=0x0001, seq=19/4864, ttl=44 (no response found1)         21 2022-07-14 20:20:41.63106507       192.0.2.100       10MP       108       0xcd8f (\$2523)       64 Echo (ping) request       id=0x0001, seq=19/4864, ttl=44 (no response found1)         22 2022-07-14 20:20:41.631060507       192.0.2.100       10MP       108       0xcd8f (\$2523)       64 Echo (ping) request       id=0x0001, seq=19/4864, ttl=44 (no response found1)         22 2022-07-14 20:20:42.05711600       198.51.100.100       10MP
12 2022-07-14 20:20:30.589397800       198.51.100.100       109       108       0x5b7b (2341)       64 Echo (ping) reply       id=0x00001, seq=19/4864, tt1-64       (n response found1)         12 2022-07-14 20:20:40.609300761       192.0.2.100       198.51.100.100       ICMP       108       0x5b7b (2341)       64 Echo (ping) request       id=0x0001, seq=19/4864, tt1-64 (no response found1)         19 2022-07-14 20:20:40.609300761       198.51.100.100       ICMP       108       0x5b7b (2341)       64 Echo (ping) request       id=0x0001, seq=19/4864, tt1-64       (n response found1)         19 2022-07-14 20:20:40.60181944       198.51.100.100       ICMP       108       0xcd8f (5263)       64 Echo (ping) request       id=0x0001, seq=19/4864, tt1-64       (n response found1)         22 2022-07-14 20:20:41.63800571       198.51.100.100       ICMP       108       0xcd8f (5263)       64 Echo (ping) request       id=0x0001, seq=19/4864, tt1-64         22 2022-07-14 20:20:41.63800571       192.6.2.100       198.51.100.100       ICMP       108       0xc357 (23222)       64 Echo (ping) request       id=0x001, seq=20/5120, tt1-64       (request in 22)         24 2022-07-14 20:20:41.63400516       198.51.100.100       ICMP       108       0xc26 (52700)       64 Echo (ping) request       id=0x0001, seq=21/5376, tt1-64 (no response found1)       22 202-07-14 20:20:41.6340516       198.51.100.100
17 2022-07-14 20:20:40.609804804       192.0.2.100       109.51.100.100       ICMP       108       0x5b7b (23419)       64 Echo (ping) request id-ex0001, seq=19/4864, ttl-64 (no response found])         18 2022-07-14 20:20:40.609804804       192.0.2.100       100 192.0.2.100       ICMP       108       0x5b7b (23419)       64 Echo (ping) request id-ex0001, seq=19/4864, ttl-64 (request in 18)         20 2022-07-14 20:20:40.60187065       198.51.100.100       120.0.2.100       ICMP       108       0x5b7b (23419)       64 Echo (ping) request id-ex0001, seq=19/4864, ttl-64 (no response found])         21 2022-07-14 20:20:40.60187065       198.51.100.100       198.51.100.100       109.10.0.100       ICMP       108       0x5b7b (23422)       64 Echo (ping) request id-ex0001, seq=20/5120, ttl-64 (no response found])         22 2022-07-14 20:20:41.634065106       198.51.100.100       109.2.0.2.100       ICMP       108       0xc26 (52790)       64 Echo (ping) request id-ex0001, seq=20/5120, ttl-64 (no response found])         22 2022-07-14 20:20:41.634065106       198.51.100.100       109.2.0.2.100       ICMP       108       0xc26 (52790)       64 Echo (ping) request id-ex0001, seq=20/5120, ttl-64 (no response found])         22 2022-07-14 20:20:42.65771660       198.51.100.100       ICMP       108       0xc26 (52790)       64 Echo (ping) request id-ex0001, seq=20/5120, ttl-64 (no response found])         22 2022-07-14 20:20:42.65771660
19 2022-07-14 20:20:40.60909718       192.0.2.100       109       108       0x2db7 (23419)       64 Echo (ping) request id-0x0001, seq=19/4864, ttl-64 (request in 18)         19 2022-07-14 20:20:40.61017965       198.51.100.100       192.0.2.100       ICMP       108       0xcdBf (52623)       64 Echo (ping) request id-0x0001, seq=19/4864, ttl-64 (request in 18)         20 2022-07-14 20:20:40.61017965       198.51.100.100       192.0.2.100       ICMP       108       0xcdBf (52623)       64 Echo (ping) request id-0x0001, seq=19/4864, ttl-64         21 2022-07-14 20:20:41.63080533       192.0.2.100       109.51.100.100       192.0.2.100       ICMP       108       0x5b7c (23422)       64 Echo (ping) request id-0x0001, seq=20/5120, ttl-64 (request in 22)         22 2022-07-14 20:20:41.63408516       198.51.100.100       192.0.2.100       ICMP       108       0xc265 (52790)       64 Echo (ping) request id-0x001, seq=20/5120, ttl-64       reply id-0x0001, seq=20/5120, ttl-64         22 2022-07-14 20:20:41.63408516       198.51.100.100       102.0.2.100       ICMP       108       0xc266 (52790)       64 Echo (ping) request id-0x001, seq=21/5376, ttl-64 (request in 22)       22 202-07-14 20:20:24.2577166       108.01.00.100       102.0.2.100       ICMP       108       0xc266 (5280)       64 Echo (ping) request id-0x001, seq=21/5376, ttl-64 (request in 22)       22 202-07-14 20:20:42.65771660       108.01.00.100       109.100       109.100
19 2022-07-14 20:20:40.610179685       198.51.100.100       192.0.2.100       ICMP       108       0xcd8f (52623)       64 Echo (ping) reply       id=0x0001, seq=19/4864, ttl=64 (request in 18)         20 2022-07-14 20:20:41.633805153       198.51.100.100       192.0.2.100       ICMP       108       0xcd8f (52623)       64 Echo (ping) reply       id=0x0001, seq=19/4864, ttl=64 (request in 18)         21 2022-07-14 20:20:41.633805153       192.0.2.100       ICMP       108       0xcb7c (23422)       64 Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (no response found1)         22 2022-07-14 20:20:41.634804102       198.51.100.100       ICMP       108       0xcb7c (23422)       64 Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (request in 22)         24 2022-07-14 20:20:41.634804102       198.51.100.100       ICMP       108       0xc265 (52700)       64 Echo (ping) reply       id=0x0001, seq=20/5120, ttl=64 (request in 22)         24 2022-07-14 20:20:42.65770898       192.0.2.100       108.91.100.100       ICMP       108       0xc269 (52536)       64 Echo (ping) reply       id=0x0001, seq=21/5376, ttl=64       request in 22)         25 2022-07-14 20:20:42.657708988       192.0.2.100       1CMP       108       0xc269 (52809)       64 Echo (ping) reply       id=0x0001, seq=21/5376, ttl=64       request in 22)       id=0x0001, seq=21/5376, ttl=64       request in 22)       id=0x0001, seq=21/5376, ttl=6
20 2022-07-14 20:20:40.610181944 198.51.100.100 192.0.2.100 ICMP 108 0xcd8f (52623) 64 Echo (ping) reply id-ex0001, seq=20/5120, ttl-64 (no response found1) 22 2022-07-14 20:20:41.63380657 192.0.2.100 198.51.100.100 ICMP 108 0x5b7e (23422) 64 Echo (ping) reply id-ex0001, seq=20/5120, ttl-64 (request in 22) 23 2022-07-14 20:20:41.63408516 198.51.100.100 120.0.2.100 ICMP 108 0xc56 (52790) 64 Echo (ping) reply id-ex0001, seq=20/5120, ttl-64 (request in 22) 24 2022-07-14 20:20:41.63408516 198.51.100.100 120.0.2.100 ICMP 108 0xc56 (52790) 64 Echo (ping) reply id-ex0001, seq=20/5120, ttl-64 (request in 22) 24 2022-07-14 20:20:42.657909988 192.0.2.100 ICMP 108 0xc56 (52790) 64 Echo (ping) reply id-ex0001, seq=21/5376, ttl-64 (request in 22) 24 2022-07-14 20:20:42.657909988 192.0.2.100 ICMP 108 0xc56 (23536) 64 Echo (ping) reply id-ex0001, seq=21/5376, ttl-64 (reply in 27) 27 2022-07-14 20:20:42.657909867 192.0.2.100 ICMP 108 0xc56 (52790) 64 Echo (ping) reply id-ex0001, seq=21/5376, ttl-64 (reply in 27) 27 2022-07-14 20:20:42.657909867 192.0.2.100 ICMP 108 0xc56 (52809) 64 Echo (ping) reply id-ex0001, seq=21/5376, ttl-64 (request in 26) 28 2022-07-14 20:20:42.65790987 198.51.100.100 102.0.2.100 ICMP 108 0xc56 (52809) 64 Echo (ping) reply id-ex0001, seq=21/5376, ttl-64 (request in 26) 28 2022-07-14 20:20:42.65790987 198.51.100.100 102.0.2.100 ICMP 108 0xc52 (2630) 64 Echo (ping) reply id-ex0001, seq=21/5376, ttl-64 (reply in 26) 20 2022-07-14 20:20:42.65790807 198.51.100.100 102.0.2.100 ICMP 108 0xc52 (2630) 64 Echo (ping) reply id-ex0001, seq=21/5376, ttl-64 (request in 26) 28 2022-07-14 20:20:42.65790807 198.51.100.100 102.0.2.100 ICMP 108 0xc52 (2630) 64 Echo (ping) reply id-ex0001, seq=21/5376, ttl-64 (request in 26) 28 2022-07-14 20:20:42.65790807 198.51.100.100 102.0.2.100 ICMP 108 0xc52 (2630) 64 Echo (ping) reply id-ex0001, seq=21/5376, ttl-64 (request in 26) 28 2022-07-14 20:20:42.65790807 198.51.100.100 102.0.2.100 ICMP 108 0xc52 (2630) 64 Echo (ping) reply id-ex0001, seq=21/5376, ttl-64 (request in 26) 28 20
21 2022-07-14 20:20:41.633805153       192.0.2.100       108.51.100.100       ICMP       108       0x5b7e (23422)       64 Echo (ping) request       id=0x0001, seq=20/5120, ttl=64 (no response found!)         22 2022-07-14 20:20:41.63380597       192.0.2.100       109.51.100.100       ICMP       108       0x5b7e (23422)       64 Echo (ping) request       id=0x0001, seq=20/5120, ttl=64 (no response found!)         22 2022-07-14 20:20:41.634804597       192.0.2.100       109.51.100.100       ICMP       108       0xcce36 (52700)       64 Echo (ping) request       id=0x0001, seq=20/5120, ttl=64 (no response found!)         24 2022-07-14 20:20:41.63408105       198.51.100.100       100.100       102.0.2.100       ICMP       108       0xcce36 (52700)       64 Echo (ping) request       id=0x0001, seq=20/5120, ttl=64 (no response found!)         25 2022-07-14 20:20:42.657711660       192.0.2.100       108.51.100.100       ICMP       108       0xcce49 (52809)       64 Echo (ping) request       id=0x0001, seq=21/5376, ttl=64 (no response found!)         27 2022-07-14 20:20:42.657711660       192.0.2.100       1CMP       108       0xcce49 (52809)       64 Echo (ping) request       id=0x0001, seq=21/5376, ttl=64 (no response found!)         29 2022-07-14 20:20:42.657819137       198.51.100.100       ICMP       108       0xcce49 (52809)       64 Echo (ping) request       id=0x0001, seq=21/5376, ttl=64 (no response fo
22 2022-07-14 20:20:41.63380697       192.0.2.100       10P       108       0x557e (23422)       64 Echo (ping) request id-exeeds, seq-20/5120, tt1-64 (request in 22)         24 2022-07-14 20:20:41.63480508       198.51.100.100       10P       108       0xc265 (52790)       64 Echo (ping) request id-exeeds, seq-20/5120, tt1-64 (request in 22)         24 2022-07-14 20:20:41.63480508       198.51.100.100       10P       108       0xc265 (52790)       64 Echo (ping) request id-exeeds, seq-20/5120, tt1-64         25 2022-07-14 20:20:42.657718091       192.0.2.100       10P       108       0xc265 (52790)       64 Echo (ping) request id-exeeds, seq-21/5376, tt1-64 (request in 22)         26 2022-07-14 20:20:42.657718091       192.0.2.100       109.51.100.100       10P       108       0xc269 (52809)       64 Echo (ping) request id-exeeds, seq-21/5376, tt1-64 (request in 26)         28 2022-07-14 20:20:42.657780917       198.51.100.100       10P       108       0xc249 (52809)       64 Echo (ping) reply       id-exeeds, seq-21/5376, tt1-64 (request in 26)         28 2022-07-14 20:20:42.657781607       192.0.2.100       109.51.100.100       10P       108       0xc249 (52809)       64 Echo (ping) reply       id-exeeds, seq-21/5376, tt1-64       (request in 26)         28 2022-07-14 20:20:42.657781607       192.0.2.100       109.51.100.100       10P       108       0xc249 (52809)       64 Echo (ping) reply </td
23 2022-07-14 20:20:41.634084102       198.51.100.100 192.0.2.100       1CVP       108       0xce36 (5270)       64 Echo (ping) reply       id-0x0001, seq-20/5120, ttl-64       (request in 22)         24 2022-07-14 20:20:41.63408450       198.51.100.100 192.0.2.100       ICVP       108       0xce36 (5270)       64 Echo (ping) reply       id-0x0001, seq-20/5120, ttl-64       (request in 22)         25 2022-07-14 20:20:41.634084505       198.51.100.100 109.0.2.100       ICVP       108       0xc5b70 (2355)       64 Echo (ping) reply       id-0x0001, seq-21/5376, ttl-64 (no response foundl)         26 2022-07-14 20:20:42.657980807       192.0.2.100       ICVP       108       0xc249 (52809)       64 Echo (ping) request id-0x0001, seq-21/5376, ttl-64 (no response foundl)         27 2022-07-14 20:20:42.6579808075       192.0.2.100       ICVP       108       0xc249 (52809)       64 Echo (ping) request id-0x0001, seq-21/5376, ttl-64 (no response foundl)         28 2022-07-14 20:20:43.681736097       192.0.2.100       ICVP       108       0xc249 (52809)       64 Echo (ping) request id-0x0001, seq-21/5376, ttl-64 (no response foundl)         28 2022-07-14 20:20:43.681736097       192.0.2.100       ICVP       108       0xc249 (52809)       64 Echo (ping) request id-0x0001, seq-21/5376, ttl-64 (no response foundl)         28 2022-07-14 20:20:43.681736097       192.0.2.100       ICVP       108       0xc249 (52809) <t< td=""></t<>
24 2022-07-14 20:20:41.634083586 198.51.100.100 192.0.2.100       ICMP       108       0xce36 (5270)       64 Etcho (ping) request       id-0x0001, seq-21/5376, ttl-64       (request in 20)         25 2022-07-14 20:20:42.65790898 192.0.2.100       198.51.100.100       ICMP       108       0x5th0 (2556)       64 Etcho (ping) request       id-0x0001, seq-21/5376, ttl-64       (request in 22)         27 2022-07-14 20:20:42.65791600       198.51.100.100       ICMP       108       0x5th0 (2556)       64 Etcho (ping) request       id-0x0001, seq-21/5376, ttl-64       (request in 22)         27 2022-07-14 20:20:42.657908075       198.51.100.100       ICMP       108       0xcc49 (52809)       64 Etcho (ping) request       id-0x0001, seq-21/5376, ttl-64       (request in 26)         28 2022-07-14 20:20:42.657908075       198.51.100.100       ICMP       108       0xcc49 (52809)       64 Etcho (ping) request       id-0x0001, seq-21/5376, ttl-64       (request in 26)         29 2022-07-14 20:20:42.65791607       198.51.100.100       ICMP       108       0xcc49 (52809)       64 Etcho (ping) request       id-0x0001, seq-21/5376, ttl-64       (request in 26)         29 2022-07-14 20:20:43.681736697       192.0.2.100       ICMP       108       0xcc49 (52809)       64 Etcho (ping) request       id-0x0001, seq-21/5376, ttl-64       (request in 26)         2 Frame 3: 108 bytes on wire (864 bits),
25 2022-07-14 20:20:442.657709899       192.0.2.100       198.51.100.100       1CVP       188       0x5bf0 (2356)       64 Etcho (ping) request id=0x0001, seq=21/5376, ttl=64 (no response found!)         25 2022-07-14 20:20:442.657701660       192.0.2.100       1SVP       188       0x5bf0 (2356)       64 Etcho (ping) request id=0x0001, seq=21/5376, ttl=64 (no response found!)         27 2022-07-14 20:20:442.657701660       192.0.2.100       1SVP       188       0x5bf0 (2356)       64 Etcho (ping) request id=0x0001, seq=21/5376, ttl=64 (no response found!)         28 2022-07-14 20:20:42.657891971       198.51.100.100       1CVP       108       0xcc49 (52809)       64 Etcho (ping) request id=0x0001, seq=21/5376, ttl=64 (no response found!)         28 2022-07-14 20:20:42.657891971       198.51.100.100       1CVP       108       0xcc49 (52809)       64 Etcho (ping) request id=0x0001, seq=21/5376, ttl=64 (no response found!)         29 2022-07-14 20:20:43.68175697       192.0.2.100       ICVP       108       0xcc49 (52809)       64 Etcho (ping) request id=0x0001, seq=21/5376, ttl=64 (no response found!)         c       108       0xcc49 (52809)       64 Etcho (ping) request id=0x0001, seq=21/5376, ttl=64 (no response found!)       108         c       108       0xcc49 (52809)       64 Etcho (ping) request id=0x0001, seq=21/5376, ttl=64 (no response found!)       108       108       108       108       108       108
26 2022-07-14 20:2042.657711660       192.0.2.100       198.51.100.100       101       108       0x50f0 (2556)       64 Echo (ping) request       16-0x0001, seq-21/5376, ttl-64 (request in 26)         27 2022-07-14 20:2042.657711660       198.51.100.100       109.9.2100       1CMP       108       0xce49 (52809)       64 Echo (ping) request       16-0x0001, seq-21/5376, ttl-64 (request in 26)         28 2022-07-14 20:2042.65771607       198.51.100.100       120.9.2.100       ICMP       108       0xce49 (52809)       64 Echo (ping) request       16-0x0001, seq-21/5376, ttl-64 (request in 26)         29 2022-07-14 20:2043.681736697       198.51.100.100       ICMP       108       0xce49 (52809)       64 Echo (ping) request       16-0x0001, seq-21/5376, ttl-64 (request in 26)         5 Frame 3: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0.8, id 0       000       05 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00       PV - X - W - &
27 2022-07-14 20:2042.65798005       192.03.100.100 192.0.2.100       1CHP       108       0xcc49 (5280)       64 Echo (ping) request       104-000031, seq-21/5376, ttl-64 (request in 26)         28 2022-07-14 20:2043.65798005       192.0.2.100       1CHP       108       0xcc49 (5280)       64 Echo (ping) reqly       id-0x00031, seq-21/5376, ttl-64 (no response found1)         29 2022-07-14 20:2043.65798005       192.0.2.100       1CHP       108       0xcc49 (5280)       64 Echo (ping) reqly       id-0x00031, seq-21/5376, ttl-64 (no response found1)         29 2022-07-14 20:2043.65798005       198.51.100.100 198.51.100.100       ICHP       108       0xcc49 (5280)       64 Echo (ping) reqly       id-0x00031, seq-21/5376, ttl-64 (no response found1)         2       Frame 3: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0       64 Echo (ping) reqly       id-0x00031, seq-21/5376, ttl-64 (no response found1)         2       Frame 3: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0       64 Echo (ping) request       id-0x00031, seq-21/5376, ttl-64 (no response found1)         2       Viriag
2 2 2022-07-14 20:20:44.2657940973 198:51.100.100       1CMP       108       0xcc49 (52697)       64 Clink (hing) reply       10-0x0803, seq-21/536, Cli-64 (replets in to)         2 2 2022-07-14 20:20:44.657940973 198:51.100.100       1CMP       108       0xcc49 (52697)       64 Clink (hing) reply       10-0x0803, seq-21/536, Cli-64 (replets in to)         5       Frame 3: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id e       64 Clink (hing) reply       10-0x0801, seq-22/5632, tll-64 (no response found)         5       Frame 3: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id e       0000       00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00       •PV···X···w··&··         5       Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: Wware 9d:e8:be (00:50:56:9d:e8:be)       (00:50:56:9d:e8:be)       0000       00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00 ······························
25 2022-07-14 20:20:44.05/847366971 195:37:160:100 195 (3:1.00:100       1CP       106       0xccs52 (2634)       64 Ethol (ping) request id-example, signal provided, seq22/563, ttl-64 (no response found))         25 2022-07-14 20:20:44.0587366971 195:37:160:100 195 (3:1.00:100       1CP       108       0xccs52 (2634)       64 Ethol (ping) request id-example, seq22/563, ttl-64 (no response found))         25 Prame 3: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0       0000       00 50 56 56 46 8b 58 97. bd b7 77 68 26 60 00       PVX: -w&-         2 thermet 11, 5rc: Cisco b9:77:00 (51:97:bd:(51:97:bd:)77:00), Dst: Whare 9d:e8:be (00:50:56:9d:e8:be)       0010       00 50 56 9d 48 b 53 76 ad 62 00 00 24 66 <u>90 00 00 00 00 00 26 68 <u>90 00 00 00 00 00 00 00 00 00 00 00 00 0</u></u>
> Frame 3: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_ue_8, id e         > Frame 3: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_ue_8, id e         > 0000       00 50 56 69 de 8b 58 97 bd b9 77 0e 89 26 00 00       • PV···X· •·w·&··         > Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: Whare 9d:e8:be (00:56:56:9d:e8:be)       0000       00 50 56 69 de 8b 58 97 bd b9 77 0e 89 26 00 00       • PV···X· •·w·&·         > Wi-rag       0.000 00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00       • ······       • ······       • ·······       • ·······       • ·······       • ······       • ·······       • ······       • ·······       • ·······       • ·······       • ·······       • ·······       • ·······       • ·······       • ·······       • ·········       • ········       • ········       • ·············       • ················       • ·············       • ····································
C  Frame 3: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture u0.8, id 0 Frame 3: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture u0.8, id 0 Out of the second
> Frame 3: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture uo.s, id 0 00 00 50 55 9d e8 be 58 97 bd b9 77 0e 89 26 00 00 • Fthermet II, Src: Cisco b9:77:0e), Dst: Whare 9d:e8:be (00:50:55:9d:e8:be) 010 00 00 81 00 00 06 10 00 00 50 25 00 00 54 cc 20 00 0 • Fthermet II, Src: Cisco b9:77:0e), Dst: Whare 9d:e8:be (00:50:55:9d:e8:be) 010 00 00 81 00 00 00 11 12 13 14 15 16 77 18 19 1a 1b •
> Ethermet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: Whare 9d:e8:be (00:50:56:9d:e8:be)         001         00 0 a fi 10 00 06 60 80 00 45 00 00 5 4 cc 2 c0 00 00
VM-Tag       0020       40 01 c1 80 c6 33 64 64 c0 00 02 64 00 00 2 a 68 g/- 3d cdd -*h         0
0
$\begin{array}{c} 0.1 \\ 0.0 \\$
$\begin{array}{c} 0.000 \$
a second a
Type: 802.10 Virtual LAN (0x8100)
√ 802.10 Virtual LAN, PRI: 0, DEI: 0, ID: 102
000 Priority: Best Effort (default) (0)
0000 0110 0110 = ID: 102
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 198,51,100,100, Dst: 192.0.2.100
> Internet Control Message Protocol 2

# Explication

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

Ce tableau récapitule la tâche :

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

		192.0.2.100

Captures de paquets sur les ports des applications et des applications

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

Il existe principalement 2 cas d'utilisation :

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

Cette section couvre les deux cas d'utilisation.

Tâche 1

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

Topologie, flux de paquets et points de capture



Configuration

FCM

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

1. Utilisez Tools > Packet Capture > Capture Session pour créer une nouvelle session de capture :

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

 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 :

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

## **CLI FXOS**

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

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

<#root>			
firepower#			
scope ssa			
firepower show app-i:	/ssa# nstance		
App Name	Identifier Slot ID	Admin State Oper State	Running Version Startup Version Deploy Ty
ftd	ftdl		

1 Enabled Online 7.2.0.82 7.2.0.82 Native No
--

```
2. Créez une session de capture :
```

```
<#root>
firepower#
scope packet-capture
firepower /packet-capture #
create session cap1
firepower /packet-capture/session* #
create app-port 1 112 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 :

6	Overview	Interfaces	Logical Devices	Security Engine	Platform	n Settings				s	ystem	Tools	Help	admin
•	Capture Ses	ssion Filter Lis	st											
									C Refresh Capta	ure Session	Delete All S	Sessions		
6		cap1	Drop Cour	nt: 0	Operati	onal State: up	Buffer Size: 256 MB	1	Snap Length: 1518	Bytes				
Г	Interface Na	ame	Filter			File Size (in bytes)	File Name	Device Name						
	Ethernet1/2	- Ethernet1/10	None			576	cap1-vethemet-1175.pcap	ftd1		$\pm$				
Ŀ	Ethernet1/2	- Ethernet1/9	None			4360	cap1-vethernet-1036.pcap	ftd1		坐				

## **CLI FXOS**

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

<#root> firepower# scope packet-capture firepower /packet-capture # show session cap1 Traffic Monitoring Session: Packet Capture Session Name: cap1 Session: 1 Admin State: Enabled Oper State: Up Oper State Reason: Active Config Success: Yes Config Fail Reason: Append Flag: Overwrite Session Mem Usage: 256 MB Session Pcap Snap Len: 1518 Bytes Error Code: 0 Drop Count: 0 Application ports involved in Packet Capture: slot Id: 1 Link Name: 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 interne du commutateur Firepower 4100/9300.

Capturer l'analyse des fichiers

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

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

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

No. Time	Source	Destination	Protocol	Length	PD	IP TTL Info	
1 2022-08-01 10:03:22.231237959	198.51.100.100	192.0.2.100	ICMP	108 -	0x42f8 (17144)	64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64
2 2022-08-01 10:03:22.231239747	198.51.100.100	192.0.2.100	ICMP	108	0x42f8 (17144)	64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64
3 2022-08-01 10:03:23.232244769	198.51.100.100	192.0.2.100	ICMP	108	0X4303 (17331)	64 ECHO (DING) LEDIÀ	id=0x0012, seq=2/512, ttl=64
4 2022-08-01 10:03:23.232247753	198.51.100.100	192.0.2.100	ICMP	108	0x43b3 (17331)	64 Echo (ping) reply	id=0x0012, seq=2/512, ttl=64
5 2022-08-01 10:03:24.234703981	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64 Echo (ping) reply	id=0x0012, seq=3/768, ttl=64
6 2022-08-01 10:03:24.234706751	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64 Echo (ping) reply	id=0x0012, seq=3/768, ttl=64
7 2022-08-01 10:03:25.258672449	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64 Echo (ping) reply	id=0x0012, seq=4/1024, ttl=64
8 2022-08-01 10:03:25.258674861	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64 Echo (ping) reply	id=0x0012, seq=4/1024, ttl=64
9 2022-08-01 10:03:26.282663169	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64 Echo (ping) reply	id=0x0012, seq=5/1280, ttl=64
10 2022-08-01 10:03:26.282666183	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64 Echo (ping) reply	id=0x0012, seq=5/1280, ttl=64
11 2022-08-01 10:03:27.306671694	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64 Echo (ping) reply	id=0x0012, seq=6/1536, ttl=64
12 2022-08-01 10:03:27.306674378	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64 Echo (ping) reply	id=0x0012, seq=6/1536, ttl=64
13 2022-08-01 10:03:28.330664677	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64 Echo (ping) reply	id=0x0012, seq=7/1792, ttl=64
14 2022-08-01 10:03:28.330667153	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64 Echo (ping) reply	id=0x0012, seq=7/1792, ttl=64
15 2022-08-01 10:03:29.354795931	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64 Echo (ping) reply	id=0x0012, seq=8/2048, ttl=64
16 2022-08-01 10:03:29.354936706	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64 Echo (ping) reply	id=0x0012, seq=8/2048, ttl=64
17 2022-08-01 10:03:30.378795204	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64 Echo (ping) reply	id=0x0012, seq=9/2304, ttl=64
18 2022-08-01 10:03:30.378798172	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64 Echo (ping) reply	id=0x0012, seg=9/2304, ttl=64
19 2022-08-01 10:03:31.402772217	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64 Echo (ping) reply	id=0x0012, seg=10/2560, ttl=64
20 2022-08-01 10:03:31.402774775	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18842)	64 Echo (ping) reply	id=0x0012, seg=10/2560, ttl=64
21 2022-08-01 10:03:32.426693254	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64 Echo (ping) reply	id=0x0012, seg=11/2816, ttl=64
22 2022-08-01 10:03:32.426695691	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64 Echo (ping) reply	id=0x0012, seg=11/2816, ttl=64
<							
> Frame 1: 108 bytes on wire (864 bits > Ethernet II, Src: Cisco b9:77:0e (St VH-Tag 0	<ul> <li>s), 108 bytes ca</li> <li>8:97:bd:b9:77:0e</li> <li> = Directi</li> <li> = Pointer</li> <li> = Destini</li> <li> = Reserve</li> <li> = Reserve</li> <li> = Version</li> <li>0 1010 = Source:</li> <li>ID: 102</li> <li>est Effort (defa</li> <li>ible</li> <li>98.51.100.100, D</li> </ul>	ptured (864 bits) o ), Dst: VMware 9d:e ion: To Bridge r: vif_id ition: 0 i No d: 0 i: 10 sult) (0) st: 192.0.2.100	n interface ca 8:be (00:50:50	µpture_u@_ 5:9d∶e8:be	8, id 0 )		00000       00       50       56       9d       e8       95       06       00       97       06       89       26       00       00       00       00       00       10       00       06       08       00       06       54       24       76       06       00

Explication

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

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

Ce tableau récapitule la tâche :

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

# Tâche 2

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

Les captures de paquets simultanées sont configurées sur :

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

Topologie, flux de paquets et points de capture



# Configuration

# FCM

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

1. Utilisez Tools > Packet Capture > Capture Session pour créer une nouvelle session de

capture :

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

 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 :

Overview Interfaces	Logical Devices Security Engine P	latform Settings				System Tools Help admin
Select an instance: ftd1	*					Save and Run Save Cancel
ftd1			Session Name*	cap1	]	
			Selected Interfaces	None		
Ethernet1/2			Buffer Size	256 MB 👻	]	
			Snap length:	1518	Bytes	
			Store Packets	Overwrite Append	]	
			Capture On	ftd 🗸	]	
Ethernet1/3			Application Port	Ethernet1/2	]	
		Ethernet1/9, Ethernet1/10	Application Capture Directio	n All Packets Egress Packet	]	
			Capture Filter	Apply Filter Capture All	Γ	
Ethernet1/1						

# **CLI FXOS**

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

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

<#root>								
firepower#								
scope ssa								
firepower , show app-in	/ssa# nstance							
App Name	Identifier Slot ID	Admin State	Oper State	Running Version	Startup	Version	Deploy	Ty
ftd	ftdl							
1	Enabled	Online	7.2.0.82	7.2.0.82	Native	No		

```
2. Créez une session de capture :
```

```
<#root>
firepower#
scope packet-capture
firepower /packet-capture #
create session cap1
firepower /packet-capture/session* #
create phy-port eth1/2
firepower /packet-capture/session/phy-port* #
set app-identifier ftd1
firepower /packet-capture/session/phy-port* #
exit
firepower /packet-capture/session* #
create app-port 1 link12 Ethernet1/2 ftd
firepower /packet-capture/session/app-port* #
set app-identifier ftd1
firepower /packet-capture/session* #
enable
firepower /packet-capture/session* #
commit
firepower /packet-capture/session # commit
```

## Vérification

FCM

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

Overview Interfaces I	ogical Devices Security Engine Platfor	m Settings				System T	ools Help a	admin
Capture Session Filter List								
					6	C Refresh	Capture Session	Del
🔺 🔳 cap1	Drop Count: 0	Operational State: up	Buffer Size: 256 MB		Snap Length: 1518 Bytes			
Interface Name	Filter	File Size (in bytes)	File Name	Device Name				
Ethernet1/2	None	95040	cap1-ethernet-1-2-0.pcap	ftd1	±			
Ethernet1/2 - Ethernet1/10	None	368	cap1-vethernet-1175.pcap	ftd1	<u>+</u>			
Ethernet1/2 - Ethernet1/9	None	13040	cap1-vethernet-1036.pcap	ftd1	4			

# **CLI FXOS**

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

<#root>

firepower#

scope packet-capture

firepower /packet-capture #

show session cap1

Traffic Monitoring Session:

Packet Capture Session Name: cap1

Session: 1

Admin State: Enabled

Oper State: Up

Oper State Reason: Active

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

Physical ports involved in Packet Capture:

slot Id: 1

Port Id: 2
```
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
```

```
Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1175.pcap
Pcapsize: 2656 bytes
Vlan: 102
Filter:
```

Collecter les fichiers de capture

Eq Port Id: 10

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

Capturer l'analyse des fichiers

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

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

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

No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info	_	
-	1 2022-08-01 11:33:19.070693081	192.0.2.100	198.51.100.100	ICMP	108 1	0xc009 (49161	) 64 Echo (ping) r	request	id=0x0013, seq=1/256, ttl=64 (no response found!)
	2 2022-08-01 11:33:19.070695347	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161	) 64 Echo (ping) r	request	id=0x0013, seq=1/256, ttl=64 (no response found!)
	3 2022-08-01 11:33:19.071217121	192.0.2.100	198.51.100.100	ICMP	102	8XC089 (49161	) 64 ECR0 (ping) r	request	id=0x0013, seq=1/256, ttl=64 (no response found!)
	4 2022-08-01 11:33:19.071218458	192.0.2.100	198,51,100,100	ICMP	102	0xc009 (49161	64 Echo (ping) r	equest	id=0x0013, seg=1/256, ttl=64 (no response found!)
	5 2022-08-01 11:33:20.072036625	192.0.2.100	198.51.100.100	TCMP	108	8xc8ae (49326	64 Echo (ning) r	equest	id=0x0013, seq=2/512, ttl=64 (no response found1)
	6 2022-08-01 11:33:20.072038399	192.0.2.100	198.51.100.100	TCMP	102	BxcBae (49326	64 Echo (ning) n	equest	id=8x8813, seq=2/512, ttl=64 (no response found1)
	7 2022 00 01 11:22:21 072266020	102 0 2 100	100 51 100 100	TCMD	109	0xc167 (40511	64 Echo (ping) n	aquest	id=0x0013, seq=2/769, ++1=64 (no response found1)
	0 2022-00-01 11:33.21.073200030	192.0.2.100	100.51.100.100	TCMP	100	0xc167 (49511	64 Echo (ping) r	equest	id-0x0013, seq-3/760, ttl-64 (no response found)
	0 2022-00-01 11:33:21.0/320032/	192.0.2.100	198.51.100.100	TCHP	102	0xc107 (49511	ou cono (ping) r	equest	id exects, seq=3/768, cc1=64 (no response round))
	9 2022-08-01 11:33:22.0/45/6640	192.0.2.100	198.51.100.100	ICMP	108	0xc1/5 (49525	) 64 Echo (ping) r	equest	1d=0x0013, seq=4/1024, ttl=64 (no response round)
	10 2022-08-01 11:33:22.0/45/8010	192.0.2.100	198.51.100.100	ICMP	102	0xc1/5 (49525	) 64 Echo (ping) r	equest	1d=0x0013, seq=4/1024, ttl=64 (no response found))
	11 2022-08-01 11:33:23.075779089	192.0.2.100	198.51.100.100	ICMP	108	0xc208 (49672	64 Echo (ping) r	request	1d=0x0013, seq=5/1280, ttl=64 (no response found!)
	12 2022-08-01 11:33:23.075781513	192.0.2.100	198.51.100.100	ICMP	102	0xc208 (49672	) 64 Echo (ping) r	equest	1d=0x0013, seq=5/1280, ttl=64 (no response found!)
	13 2022-08-01 11:33:24.081839490	192.0.2.100	198.51.100.100	ICMP	108	Øxc211 (49681	) 64 Echo (ping) r	request	id=0x0013, seq=6/1536, ttl=64 (no response found!)
	14 2022-08-01 11:33:24.081841386	192.0.2.100	198.51.100.100	ICMP	102	0xc211 (49681	) 64 Echo (ping) r	request	id=0x0013, seq=6/1536, ttl=64 (no response found!)
	15 2022-08-01 11:33:25.105806249	192.0.2.100	198.51.100.100	ICMP	108	0xc2e2 (49890	) 64 Echo (ping) r	equest	id=0x0013, seq=7/1792, ttl=64 (no response found!)
	16 2022-08-01 11:33:25.105807895	192.0.2.100	198.51.100.100	ICMP	102	0xc2e2 (49890	) 64 Echo (ping) r	equest	id=0x0013, seq=7/1792, ttl=64 (no response found!)
	17 2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	ICMP	108	0xc3b4 (50100	) 64 Echo (ping) r	request	id=0x0013, seq=8/2048, ttl=64 (no response found!)
	18 2022-08-01 11:33:26.129838114	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100	64 Echo (ping) r	equest	id=0x0013, seq=8/2048, ttl=64 (no response found!)
	19 2022-08-01 11:33:27.153828653	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294	64 Echo (ping) r	equest	id=0x0013, seq=9/2304, ttl=64 (no response found!)
	20 2022-08-01 11:33:27.153830201	192.0.2.100	198.51.100.100	ICMP	102	0xc476 (50294	64 Echo (ping) r	equest	id=0x0013, seg=9/2304, ttl=64 (no response found!)
	21 2022-08-01 11:33:28,177847175	192.0.2.100	198,51,100,100	ICMP	108	0xc516 (50454	64 Echo (ping) r	equest	id=0x0013, seg=10/2560, ttl=64 (no response found!)
	22 2022-08-01 11:33:28.177849075	192.0.2.100	198,51,100,100	ICMP	102	0xc516 (50454	64 Echo (ping) r	equest	id=0x0013, seg=10/2560, ttl=64 (no response found!)
	23 2022-08-01 11:33:29.201804760	192.0.2.100	198,51,100,100	TCMP	108	8xc578 (58552	64 Echo (ning) r	equest	id=8x8013, seg=11/2816, ttl=64 (no response found!)
	24 2022-08-01 11:33:29 201806488	192.0.2.100	198.51.100.100	TCMP	102	Bxc578 (58552	64 Echo (ping) r	request	id=8x8013, seq=11/2816, ttl=64 (no response found!)
	25 2022-00-01 11:33:30 225834765	192.0.2.100	198.51.100.100	TCMP	102	BYC585 (58565	64 Echo (ping) r	request	id=0x0013, seq=12/3072, ttl=64 (no response found1)
	26 2022-00-01 11:33:30 225036705	192.0.2.100	100.51 100.100	TCMP	102	BYC595 (50565	64 Echo (ping) r	equest	id=0x0013, seq=12/3072, ttl=64 (no response found1)
	20 2022-00-01 11:33:30.223030055	192.0.2.100	100 51 100 100	TCHP	102	0x0303 (50303	(d teho (ping) r	equest	id-0x0013, seq-12/3320, ttl-64 (no response found)
	27 2022-08-01 11:33:31.249828933	192.0.2.100	198.51.100.100	TCHP	100	00018 (50712	(4 Cebe (ping) r	equest	id-oxoois, seq-15/5528, ((1-04 (no response found))
	28 2022-08-01 11:33:31.249831121	192.0.2.100	198.51.100.100	TCHP	102	0x0018 (50712	ou cono (ping) r	equest	id exects, seq=15/3528, ((1=64 (no response round))
	29 2022-08-01 11:33:32.2/386/960	192.0.2.100	198.51.100.100	ICMP	108	0XC64T (50/6/	) 64 Echo (ping) r	equest	1d=0x0013, seq=14/3584, tt1=64 (no response found)
×									
>	Frame 1: 108 bytes on wire (864 bit	s), 108 bytes ca	ptured (864 bits) o	n interface ca	pture_u0_	1, id 0		000	30 58 97 bd b9 77 8e 88 50 56 9d e8 be 89 26 88 8a X ··· w ·· P V ···· & ··
2	Ethernet II, Src: VMware 9d:e8:be (	00:50:56:9d:e8:b	e), Dst: Cisco b9:7	7:0e (58:97:bd	:b9:77:0e	)		001	.0 00 00 81 00 00 66 08 00 45 00 00 54 c0 09 40 00 ·····f··E··T··@·
× 1	VN-Tag							002	10 40 01 8d a3 c0 00 02 64 c6 33 64 64 08 00 8d 7c @·····d ·3dd···
	1	= Directi	on: From Bridge					00.	0 00 13 00 01 t2 b9 e7 62 00 00 00 00 cb 7t 06 00b
	.0	= Pointer	: vif_id						
		= Destina	tion: 10					00;	10 10 10 10 17 20 21 22 23 24 25 26 27 28 29 20 20 ····· ! # \$44 () **
	···· ··· ··· ··· ··· · ··· · ··· · ··· ·	= Looped:	No						10 20 20 20 21 30 31 32 33 34 33 30 37 j/0123 430/
	0	= Reserve	d: 0	· •					
		= Version	: 0						
	0000 000	00 0000 = Source:	0						
	Type: 802.10 Virtual LAN (0x8100)	)							
v 6	802.10 Virtual LAN, PRI: 0, DEI: 0,	ID: 102							
L Ľ	000 = Priority: [	Rest Effort (defa	ult) (0)						
	0 = DEI: Inelia	rible							
	0000 0110 0110 = ID: 102			·					
	Type: IPv4 (8x8888)								
	Internet Protocol Version 4. Src: 1	92.0.2.100. Dst:	198.51.100.100						
5	Internet Control Message Protocol								
1	and the control hassage frotocol								

Sélectionnez le deuxième paquet et vérifiez les points clés :

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

No	o. Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info		
r	1 2022-08-01 11:33:19.070693081	192.0.2.100	198.51.100.100	ICMP	108 1	0xc009 (49161)	64 Echo (ping) r	request i	d=0x0013, seq=1/256, ttl=64 (no response found!)
	2 2022-08-01 11:33:19.070695347	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping) r	request i	d=0x0013, seq=1/256, ttl=64 (no response found!)
	3 2022-08-01 11:33:19.071217121	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping) r	request i	d=0x0013, seq=1/256, ttl=64 (no response found!)
	4 2022-08-01 11:33:19.071218458	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping) r	request i	d=0x0013, seq=1/256, ttl=64 (no response found!)
	5 2022-08-01 11:33:20.072036625	192.0.2.100	198.51.100.100	ICMP	108	0xc0ae (49326)	64 Echo (ping) r	request i	d=0x0013, seq=2/512, ttl=64 (no response found!)
	6 2022-08-01 11:33:20.072038399	192.0.2.100	198.51.100.100	ICMP	102	0xc0ae (49326)	64 Echo (ping) r	request i	d=0x0013, seq=2/512, ttl=64 (no response found!)
	7 2022-08-01 11:33:21.073266030	192.0.2.100	198.51.100.100	ICMP	108	0xc167 (49511)	64 Echo (ping) r	request i	d=0x0013, seq=3/768, ttl=64 (no response found!)
	8 2022-08-01 11:33:21.073268327	192.0.2.100	198.51.100.100	ICMP	102	0xc167 (49511)	64 Echo (ping) r	request i	d=0x0013, seq=3/768, ttl=64 (no response found!)
	9 2022-08-01 11:33:22.074576640	192.0.2.100	198.51.100.100	ICMP	108	0xc175 (49525)	64 Echo (ping) r	request i	d=0x0013, seq=4/1024, ttl=64 (no response found!)
	10 2022-08-01 11:33:22.074578010	192.0.2.100	198.51.100.100	ICMP	102	0xc175 (49525)	64 Echo (ping) r	request i	d=0x0013, seq=4/1024, ttl=64 (no response found!)
	11 2022-08-01 11:33:23.075779089	192.0.2.100	198.51.100.100	ICMP	108	0xc208 (49672)	64 Echo (ping) r	request i	d=0x0013, seq=5/1280, ttl=64 (no response found!)
	12 2022-08-01 11:33:23.075781513	192.0.2.100	198.51.100.100	ICMP	102	0xc208 (49672)	64 Echo (ping) r	request i	d=0x0013, seq=5/1280, ttl=64 (no response found!)
	13 2022-08-01 11:33:24.081839490	192.0.2.100	198.51.100.100	ICMP	108	0xc211 (49681)	64 Echo (ping) r	request i	d=0x0013, seq=6/1536, ttl=64 (no response found!)
	14 2022-08-01 11:33:24.081841386	192.0.2.100	198.51.100.100	ICMP	102	0xc211 (49681)	64 Echo (ping) r	request i	d=0x0013, seq=6/1536, ttl=64 (no response found!)
	15 2022-08-01 11:33:25.105806249	192.0.2.100	198.51.100.100	ICMP	108	0xc2e2 (49890)	64 Echo (ping) r	request i	d=0x0013, seq=7/1792, ttl=64 (no response found!)
	16 2022-08-01 11:33:25.105807895	192.0.2.100	198.51.100.100	ICMP	102	0xc2e2 (49890)	64 Echo (ping) r	request i	d=0x0013, seq=7/1792, ttl=64 (no response found!)
	17 2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	ICMP	108	0xc3b4 (50100)	64 Echo (ping) r	request i	d=0x0013, seq=8/2048, ttl=64 (no response found!)
	18 2022-08-01 11:33:26.129838114	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100)	64 Echo (ping) r	request i	d=0x0013, seq=8/2048, ttl=64 (no response found!)
	19 2022-08-01 11:33:27.153828653	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294)	64 Echo (ping) r	request i	d=0x0013, seq=9/2304, ttl=64 (no response found!)
	20 2022-08-01 11:33:27.153830201	192.0.2.100	198.51.100.100	ICMP	102	0xc476 (50294)	64 Echo (ping) r	request i	d=0x0013, seq=9/2304, ttl=64 (no response found!)
	21 2022-08-01 11:33:28.177847175	192.0.2.100	198.51.100.100	ICMP	108	0xc516 (50454)	64 Echo (ping) r	request i	d=0x0013, seq=10/2560, ttl=64 (no response found!)
	22 2022-08-01 11:33:28.177849075	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (50454)	64 Echo (ping) r	request i	d=0x0013, seq=10/2560, ttl=64 (no response found!)
	23 2022-08-01 11:33:29.201804760	192.0.2.100	198.51.100.100	ICMP	108	0xc578 (50552)	64 Echo (ping) n	request i	d=0x0013, seq=11/2816, ttl=64 (no response found!)
	24 2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	102	0xc578 (50552)	64 Echo (ping) r	request i	d=0x0013, seq=11/2816, ttl=64 (no response found!)
	25 2022-08-01 11:33:30.225834765	192.0.2.100	198.51.100.100	ICMP	108	0xc585 (50565)	64 Echo (ping) r	request i	d=0x0013, seq=12/3072, ttl=64 (no response found!)
	26 2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (50565)	64 Echo (ping) r	request i	d=0x0013, seq=12/3072, ttl=64 (no response found!)
	27 2022-08-01 11:33:31.249828955	192.0.2.100	198.51.100.100	ICMP	108	0xc618 (50712)	64 Echo (ping) r	request i	d=0x0013, seq=13/3328, ttl=64 (no response found!)
	28 2022-08-01 11:33:31.249831121	192.0.2.100	198.51.100.100	ICMP	102	0xc618 (50712)	64 Echo (ping) r	request i	d=0x0013, seq=13/3328, ttl=64 (no response found!)
	29 2022-08-01 11:33:32.273867960	192.0.2.100	198.51.100.100	ICMP	108	0xc64f (50767)	64 Echo (ping) r	request i	d=0x0013, seq=14/3584, ttl=64 (no response found!)
<									
5	Frame 2: 102 bytes on wire (816 bit	s), 102 bytes car	otured (816 bits) or	interface ca	pture u0	1. id 0		0000	58 97 bd b9 77 0e 00 50 56 9d e8 be 81 00 00 66 Xw.P Vf
5	Ethernet II, Src; VMware 9d;e8;be (	00:50:56:9d:e8:b	e), Dst; Cisco b9:77	:0e (58:97:bd	:b9:77:00			0010	08 00 45 00 00 54 c0 09 40 00 40 01 8d a3 c0 00 ··E··T·· @·@····
4	802.10 Virtual LAN, PRI: 0, DEI: 0,	ID: 102				·		0020	02 64 c6 33 64 64 08 00 8d 7c 00 13 00 01 f2 b9 ·d·3dd···
	000 = Priority:	Best Effort (defa	ult) (0)					0030	e7 62 00 00 00 00 cb 7f 06 00 00 00 00 00 10 11
	0 = DEI: Inelia	zible	2					0040	12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21
	0000 0110 0110 = ID: 102		-	· •				0050	22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 "#\$%&"() "+,/01
	Type: IPv4 (0x0800)							0060	32 33 34 35 36 37 234567
>	Internet Protocol Version 4, Src: 1	92.0.2.100, Dst:	198.51.100.100						
>	Internet Control Message Protocol		6						
1									

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.

				L			
No. Time	Source	Destination	Protocol	Length	PD	PTTL Mo	li a anno stars ant sa
1 2022-08-01 11:33:19.071512698	198.51.100.100	192.0.2.100	ICMP	108	0x4†27 (20263)	64 Echo (ping) reply	1d=0x0013, seq=1/256, ttl=64
2 2022-08-01 11:33:19.071514882	198.51.100.100	192.0.2.100	ICMP	108	0x4†27 (20263)	64 Echo (ping) reply	1d=0x0013, seq=1/256, tt1=64
3 2022-08-01 11:33:20.072677302	198.51.100.100	192.0.2.100	ICMP	108	0X4110 (20475)	64 ECHO (ping) repry	1d=0x0013, seq=2/512, tt1=64
4 2022-08-01 11:33:20.072679384	198.51.100.100	192.0.2.100	ICMP	108	0x4110 (20475)	64 Echo (ping) reply	1d=0x0013, seq=2/512, ttl=64
5 2022-08-01 11:33:21.073913640	198.51.100.100	192.0.2.100	ICMP	108	0x50ac (20652)	64 Echo (ping) reply	1d=0x0013, seq=3/768, ttl=64
6 2022-08-01 11:33:21.073915690	198.51.100.100	192.0.2.100	ICMP	108	0x50ac (20652)	64 Echo (ping) reply	id=0x0013, seq=3/768, ttl=64
7 2022-08-01 11:33:22.075239381	198.51.100.100	192.0.2.100	ICMP	108	0x513e (20798)	64 Echo (ping) reply	id=0x0013, seq=4/1024, ttl=64
8 2022-08-01 11:33:22.075241491	198.51.100.100	192.0.2.100	ICMP	108	0x513e (20798)	64 Echo (ping) reply	id=0x0013, seq=4/1024, ttl=64
9 2022-08-01 11:33:23.076447152	198.51.100.100	192.0.2.100	ICMP	108	0x51c9 (20937)	64 Echo (ping) reply	id=0x0013, seq=5/1280, ttl=64
10 2022-08-01 11:33:23.076449303	198.51.100.100	192.0.2.100	ICMP	108	0x51c9 (20937)	64 Echo (ping) reply	id=0x0013, seq=5/1280, ttl=64
11 2022-08-01 11:33:24.082407896	198.51.100.100	192.0.2.100	ICMP	108	0x528e (21134)	64 Echo (ping) reply	id=0x0013, seq=6/1536, ttl=64
12 2022-08-01 11:33:24.082410099	198.51.100.100	192.0.2.100	ICMP	108	0x528e (21134)	64 Echo (ping) reply	id=0x0013, seq=6/1536, ttl=64
13 2022-08-01 11:33:25.106382424	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64 Echo (ping) reply	id=0x0013, seq=7/1792, ttl=64
14 2022-08-01 11:33:25.106384549	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64 Echo (ping) reply	id=0x0013, seq=7/1792, ttl=64
15 2022-08-01 11:33:26.130437851	198.51.100.100	192.0.2.100	ICMP	108	0x53a6 (21414)	64 Echo (ping) reply	id=0x0013, seq=8/2048, ttl=64
16 2022-08-01 11:33:26.130440320	198.51.100.100	192.0.2.100	ICMP	108	0x53a6 (21414)	64 Echo (ping) reply	id=0x0013, seq=8/2048, ttl=64
17 2022-08-01 11:33:27.154398212	198.51.100.100	192.0.2.100	ICMP	108	0x5446 (21574)	64 Echo (ping) reply	id=0x0013, seq=9/2304, ttl=64
18 2022-08-01 11:33:27.154400198	198.51.100.100	192.0.2.100	ICMP	108	0x5446 (21574)	64 Echo (ping) reply	id=0x0013, seq=9/2304, ttl=64
19 2022-08-01 11:33:28.178469866	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64 Echo (ping) reply	id=0x0013, seq=10/2560, ttl=64
20 2022-08-01 11:33:28.178471810	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64 Echo (ping) reply	id=0x0013, seq=10/2560, ttl=64
21 2022-08-01 11:33:29.202395869	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21748)	64 Echo (ping) reply	id=0x0013, seq=11/2816, ttl=64
22 2022-08-01 11:33:29.202398067	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21748)	64 Echo (ping) reply	id=0x0013, seq=11/2816, ttl=64
23 2022-08-01 11:33:30.226398735	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64 Echo (ping) reply	id=0x0013, seg=12/3072, ttl=64
24 2022-08-01 11:33:30.226401017	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64 Echo (ping) reply	id=0x0013, seg=12/3072, ttl=64
25 2022-08-01 11:33:31.250387808	198.51.100.100	192.0.2.100	ICMP	108	0x55f2 (22002)	64 Echo (ping) reply	id=0x0013, seg=13/3328, ttl=64
26 2022-08-01 11:33:31.250389971	198,51,100,100	192.0.2.100	ICMP	108	0x55f2 (22002)	64 Echo (ping) reply	id=0x0013, seg=13/3328, ttl=64
27 2022-08-01 11:33:32.274416011	198, 51, 100, 100	192.0.2.100	ICMP	108	0x5660 (22112)	64 Echo (ping) reply	id=0x0013, seg=14/3584, ttl=64
28 2022-08-01 11:33:32,274418229	198,51,100,100	192.0.2.100	ICMP	108	0x5660 (22112)	64 Echo (ping) reply	id=0x0013, seg=14/3584, ttl=64
29 2022-08-01 11:33:33,298397657	198, 51, 100, 100	192.0.2.100	ICMP	108	0x56e7 (22247)	64 Echo (ping) reply	id=0x0013, seg=15/3840, ttl=64
<	1,01,0111001100	19210121100	A CON	100	0000007 (222477)	or cone (brug) reby)	10-0/0015, 300-15/5040, 001-04
> Ename 1: 100 butes on vine (064 bit	<li>c) 100 buttos co</li>	ntuned (REA bits)	on intenface c	antuna un	e 14 e		0000 00 50 56 0d at ha 50 07 hd ha 77 as 20 76 00 00
> Frame 1, 100 bytes on wire (804 bit	9:07:bd:b0:77:00	) Det: Marana ad:	on incertace c	6:0d:00:b	_o, 10 0		0010 00 00 00 00 00 00 00 00 00 00 00 00
All Tag	0.97.00.09.77.00	), osc. wriware su.	60.06 (00.30.3	0.90.00.0	e)		0020 40 01 3e 86 c6 33 64 64 c0 00 02 64 00 00 95 7c @->3ddd1
• vn-tag	- Dinesti	ions To Doldan					0030 00 13 00 01 f2 b9 e7 62 00 00 00 cb 7f 06 00bb
0	- Direction	ion: To Bridge					0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b
	- Doction	r: VIT_10					0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ···· !"# \$%&"()"+
	= Destina	ation: 0					0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,/0123 4567
	= Loopea:	: NO	4				
	= Keserve	ea: 0					
	= Version	n: 0					
0000 000	00 1010 = Source:	: 10					
Type: 802.10 Virtual LAN (0x8100)	)		_				
802.10 VIPtual LAN, PRI: 0, DEI: 0,	10: 102						
000 = Priority: 1	Best Effort (defa	aurt) (0)	2				
0 = DEI: Inelig	g101ē		5				
0000 0110 0110 = ID: 102							
Type: IPv4 (0x0800)			_				
Internet Protocol Version 4, Src: 1	98.51.100.100, D	st: 192.0.2.100	2				
Internet Control Message Protocol			4				

## 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	Interfaces du fond de panier	102	Entrée uniquement	Réponses d'écho ICMP de l'hôte 198.51.100.100 à l'hôte 192.0.2.100
l'application et le port d'application Ethernet1/2	Interface Ethernet1/2	102	Entrée uniquement	Requêtes d'écho ICMP de l'hôte 192.0.2.100 vers l'hôte 198.51.100.100

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

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

Topologie, flux de paquets et points de capture



Configuration

#### FCM

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

1. Utilisez Tools > Packet Capture > Capture Session pour créer une nouvelle session de capture :

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

2. 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 :

Overview Interfaces Logical Devices Security Engine Platform Settings			System Tool	is Help admin
Select an instance: ftd1 v			Save and Run Save Cancel	
Subinterface selection Ethernet1/2.205 Ethernet1/2.206 Subinterfaces(2) Ethernet1/2		Session Name* Selected Interfaces Buffer Size Snap length: Store Packets	Cap1       Ethernet1/2.205       256 M8       1518       Overwrite       Append	
Ethernet1/1	FD Ethernet1/9, Ethernet1/10	Capture Filter	Apply Filter Cepture All	

3. Dans le cas d'une sous-interface port-channel, en raison de l'ID de bogue Cisco <u>CSCvq3119</u>, <u>les</u> sous-interfaces ne sont pas visibles dans le FCM. Utilisez l'interface de ligne de commande FXOS pour configurer les captures sur les sous-interfaces port-channel.

## CLI FXOS

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

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

## <#root>

firepower#

scope ssa

firepower /ssa #

show	app-	inst	tance

Арр	Name	Identifier	Slot	ID	Admin	State	0per	State	Running	Version	Startup	Version	Deploy	Ту
ftd		ftdl												
	1	Ena	bled	0n	line		7.2	2.0.82	7.2.0.3	82	Contair	ner No		R
ftd		ftd2	1		Enable	ed	Onli	ne	7.2.0.8	2	7.2.0.82	2	Contair	ıer

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

<#roo	t>				
firepo	ower#				
connec	et fxos				
<outpu firepc show p</outpu 	ut skipped> ower(fxos)# port-channel summa	ry			
Flags:	D - Down I - Individual s - Suspended S - Switched U - Up (port-ch M - Not in use.	P - Up in po H - Hot-stan r - Module-r R - Routed annel) Min-links no	ort-channel (m dby (LACP onl removed ot met	members) y)	
Group	Port- Type Channel	Protocol	Member Ports	;	_
1	Pol(SU) Eth	LACP	Eth1/3(P)	Eth1/3(P)	

3. Créez une session de capture :

<#root>
firepower#
scope packet-capture
firepower /packet-capture #
create session cap1
firepower /packet-capture/session\* #
create phy-port Eth1/2

```
firepower /packet-capture/session/phy-port* #
set app ftd
firepower /packet-capture/session/phy-port* #
set app-identifier ftd1
firepower /packet-capture/session/phy-port* #
set subinterface 205
firepower /packet-capture/session* #
enable
firepower /packet-capture/session* #
commit
```

firepower /packet-capture/session #

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

```
<#root>
firepower#
scope packet-capture
firepower /packet-capture #
create filter vlan207
firepower /packet-capture/filter* #
set ovlan 207
firepower /packet-capture/filter* #
up
firepower /packet-capture* #
create session cap1
firepower /packet-capture/session*
```

#### create phy-port Eth1/3

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

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

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

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

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

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

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

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

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

firepower /packet-capture/session\* #
enable

firepower /packet-capture/session\* #
commit

firepower /packet-capture/session #

Vérification

FCM

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

(en octets) augmente :

Overview Interfaces Logical Devices Security Engine Platform Set	tings				System Tools Help admin
Capture Session Piter List				A belieth Carture Section	Carlete Al Geospires
ant Bros Count 8	Operational State: up	Buffar Grav 356 MB		Shan Length: 1518 Bulles	
	operational state: up	00000 0000 200 Pt0		and conjust taxe of the	
Interface Name Filter	File Size (in bytes)	File Name	Device Name		
Ethernet1/2.205 None	233992	cap1-ethemet-1-2-0.pcap	ftd1	土	

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

Overview Interfaces Logici	al Devices Security Engine Platform Set	ttings				System Tools	Help admin
Capture Session Filter List							
					C Refresh Capture Session	Delete Al Sessions	
a 🔳 cap1	Drop Count: 0	Operational State: up	Buffer Size: 256 MB		Snap Length: 1518 Bytes		4.8.0
Interface Name	Filter	File Size (in bytes)	File Name	Device Name			
Ethernet1/4.207	None	624160	cap1-ethernet-1-4-0.pcap	Not available	4		
Ethernet1/3.207	None	160	cap1-ethernet-1-3-0.pcap	Not available	*		

## **CLI FXOS**

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

<#root>

firepower#

scope packet-capture

firepower /packet-capture #

show session cap1

Traffic Monitoring Session:

Packet Capture Session Name: cap1

Session: 1

Admin State: Enabled

Oper State: Up

Oper State Reason: Active

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

```
Drop Count: 0
Physical ports involved in Packet Capture:
   Slot Id: 1
   Port Id: 2
   Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap
   Pcapsize: 9324 bytes
    Filter:
    Sub Interface: 205
   Application Instance Identifier: ftd1
   Application Name: ftd
Port-channel 1 avec interfaces membres Ethernet1/3 et Ethernet1/4 :
<#root>
firepower#
scope packet-capture
```

firepower /packet-capture # show session cap1

Traffic Monitoring Session:

Packet Capture Session Name: cap1

Session: 1

Admin State: Enabled

Oper State: Up

Oper State Reason: Active

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

Session Mem Usage: 256 MB Session Pcap Snap Len: 1518 Bytes Error Code: 0 Drop Count: 0 Physical ports involved in Packet Capture: Slot Id: 1 Port Id: 3 Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-3-0.pcap Pcapsize: 160 bytes Filter: Sub Interface: 207 Application Instance Identifier: ftd1 Application Name: ftd Slot Id: 1 Port Id: 4 Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-4-0.pcap Pcapsize: 624160 bytes Filter: Sub Interface: 207 Application Instance Identifier: ftd1

Application Name: ftd

Collecter les fichiers de capture

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

Capturer l'analyse des fichiers

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

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

No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info	
-	1 2022-08-04 07:21:56.993302102	192.0.2.100	198.51.100.100	ICMP	112	0x9574 (38260)	64 Echo (ping) reques	id=0x0022, seq=1/256, ttl=64 (no response found!)
	2 2022-08-04 07:21:56.993303597	192.0.2.100	198.51.100.100	ICMP	102	0x9574 (38260)	64 Echo (ping) reques	id=0x0022, seq=1/256, ttl=64 (no response found!)
	3 2022-08-04 07:22:06.214264777	192.0.2.100	198.51.100.100	ICMP	112	0x9a81 (39553)	64 Echo (ping) reques	id=0x0022, seq=10/2560, ttl=64 (no response found!)
	4 2022-08-04 07:22:06.214267373	192.0.2.100	198.51.100.100	ICMP	102	0x9a81 (39553)	64 Echo (ping) reques	id=0x0022, seq=10/2560, ttl=64 (no response found!)
	5 2022-08-04 07:22:07.215113393	192.0.2.100	198.51.100.100	ICMP	112	0x9ac3 (39619)	64 Echo (ping) reques	id=0x0022, seq=11/2816, ttl=64 (no response found!)
	6 2022-08-04 07:22:07.215115445	192.0.2.100	198.51.100.100	ICMP	102	0x9ac3 (39619)	64 Echo (ping) reques	id=0x0022, seg=11/2816, ttl=64 (no response found!)
	7 2022-08-04 07:22:08.229938577	192.0.2.100	198.51.100.100	ICMP	112	0x9b33 (39731)	64 Echo (ping) reques	id=0x0022, seg=12/3072, ttl=64 (no response found!)
	8 2022-08-04 07:22:08.229940829	192.0.2.100	198.51.100.100	ICMP	102	0x9b33 (39731)	64 Echo (ping) reques	id=0x0022, seg=12/3072, ttl=64 (no response found!)
	9 2022-08-04 07:22:09.253944601	192.0.2.100	198.51.100.100	ICMP	112	0x9c0e (39950)	64 Echo (ping) reques	id=0x0022, seg=13/3328, ttl=64 (no response found!)
	10 2022-08-04 07:22:09.253946899	192.0.2.100	198,51,100,100	ICMP	102	0x9c0e (39950)	64 Echo (ping) reques	id=0x0022, seg=13/3328, ttl=64 (no response found!)
	11 2022-08-04 07:22:10.277953070	192.0.2.100	198,51,100,100	ICMP	112	0x9ccb (40139)	64 Echo (ping) reques	id=0x0022, sed=14/3584, ttl=64 (no response found!)
	12 2022-08-04 07:22:10.277954736	192.0.2.100	198,51,100,100	TCMP	102	0x9ccb (40139)	64 Echo (ping) reques	id=0x0022, seg=14/3584, ttl=64 (no response found))
	13 2022-08-04 07:22:11.301931282	192.0.2.100	198,51,100,100	TCMP	112	0x9d84 (40324)	64 Echo (ping) reques	id=0x0022, seg=15/3840, ttl=64 (no response found))
	14 2022-08-04 07:22:11.301933600	192.0.2.100	198.51.100.100	TCMP	102	0x9d84 (40324)	64 Echo (ning) reques	id=0x0022, seq=15/3840, ttl=64 (no response found1)
	15 2022-08-04 07:22:12 325036521	192.0.2.100	199.51.100.100	TCMP	112	exoda2 (40354)	64 Echo (ping) reques	id=0x0022, seg=16/4096, tt]=64 (no response found1)
	16 2022-00-04 07-22-12 225027005	102 0 2 100	100 51 100 100	TCMP	102	0x0da2 (40354)	64 Echo (ping) reques	id=0x0022, seq=16/4096, tt]=64 (no response found1)
	17 2022-08-04 07:22:13.326989040	192.0.2.100	198.51.100.100	TCMP	112	0x9002 (40354)	64 Echo (ping) reques	id=0x0022, seq=17/4352, ttl=64 (no response found1)
	10 2022-00-04 07:22:13:320300040	192.0.2.100	100 51 100 100	TCMD	102	0x9607 (40455)	64 Echo (ping) reques	id-0x0022, seq=17/4352, ttl=64 (no response found!)
	10 2022-00-04 07:22:15:520990256	192.0.2.100	100 51 100 100	TCHP	102	0x9007 (40455)	64 Echo (ping) reques	id-0x0022, seq=17/4532, ttl=64 (no response found!)
	19 2022-08-04 07:22:14.341944775	192.0.2.100	198.51.100.100	TCHP	102	0x900a (40554)	64 Echo (ping) reques	id-0x0022, seq=10/4600, ttl=64 (no response found!)
	20 2022-08-04 07:22:14.341946249	192.0.2.100	198.51.100.100	TCHP	102	0x900a (40554)	64 Echo (ping) reques	id-0x0022, seq=10/4008, ttl=04 (no response found!)
	21 2022-08-04 07:22:15.365941588	192.0.2.100	198.51.100.100	ICMP	112	0X90TD (40699)	64 Echo (ping) reques	1d=0x0022, seq=19/4864, ttl=64 (no response found!)
	22 2022-08-04 07:22:15.365942566	192.0.2.100	198.51.100.100	ICMP	102	0X90TD (40699)	64 Echo (ping) reques	1d=0x0022, seq=19/4864, ttl=64 (no response found)
	23 2022-08-04 07:22:16.389973843	192.0.2.100	198.51.100.100	ICMP	112	0X9Te8 (40936)	64 Ecno (ping) reques	1d=0x0022, seq=20/5120, ttl=64 (no response found!)
	24 2022-08-04 07:22:16.389975129	192.0.2.100	198.51.100.100	ICMP	102	0x9fe8 (40936)	64 Echo (ping) reques	1d=0x0022, seq=20/5120, ttl=64 (no response found!)
	25 2022-08-04 07:22:17.413936452	192.0.2.100	198.51.100.100	ICMP	112	0xa079 (41081)	64 Echo (ping) reques	1d=0x0022, seq=21/5376, ttl=64 (no response found!)
	26 2022-08-04 07:22:17.413938090	192.0.2.100	198.51.100.100	ICMP	102	0xa079 (41081)	64 Echo (ping) reques	1d=0x0022, seq=21/5376, ttl=64 (no response found!)
	27 2022-08-04 07:22:18.437954335	192.0.2.100	198.51.100.100	ICMP	112	0xa11e (41246)	64 Echo (ping) reques	1d=0x0022, seq=22/5632, ttl=64 (no response found!)
<								
> F	rame 1: 112 bytes on wire (896 bit	s), 112 bytes ca	ptured (896 bits)	on interface c	apture u0	1, id 0		100 a2 76 f2 00 00 1b 00 50 56 9d e8 be 89 26 80 54 ···································
> E	thernet II, Src: VMware 9d:e8:be (	00:50:56:9d:e8:b	e), Dst: a2:76:f2:	00:00:1b (a2:7	6:f2:00:00	0:1b)		10 00 00 81 00 00 66 81 00 00 cd 08 00 45 00 00 54 ·····f·····E··T
~ V	n-Tag							20 95 74 40 00 40 01 b8 38 c0 00 02 64 c6 33 64 64 ·t@·@··8 ···d·3dd
	1	= Directi	ion: From Bridge					30 08 00 eb 95 00 22 00 01 88 73 eb 62 00 00 00 00 ·····"···s·b····
	.0	= Pointer	r: vif id					40 d9 9d 00 00 00 00 00 00 10 11 12 13 14 15 16 17
	00 0000 0101 0100	= Destina	ation: 84					50 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 !"#\$3.8"
	0	= Looped:	: No	4				28 29 2a 20 2c 2d 2e 2t 30 31 32 33 34 35 36 37 ()*+,/ 01234567
		= Reserve	ed: 0	<b>T</b>				
		= Version	1: 0					
		30 0000 = Source:	. 0					
	Type: 802.10 Virtual LAN (0x8100)	)						
<b>V</b> 8	102.10 Virtual LAN, PRI: 0, DEI: 0.	ID: 102						
1	and = Priority' I	Rest Effort (def:	ault) (0)					
	a DET: Inelia	sible	MIC/ (0)	2				
	0000 0110 0110 - TD: 102	STORE						
	Tupor 902 10 Victual LAN (0v9100)	<b>`</b>						
	Type: abz.ig virtual LAN (6x8106)	101.305		_				
10	- Deiceitus I	10, 205	wilth (0)					
	o per rolling	sible	urc) (0)					
	0000 1100 1101 - TD: 205	gibie						
	0000 1100 1101 = 1D: 205			21				
	steppet Desteral Version ( fact t	03 0 3 100 0.4.	100 51 100 100					
	Internet Protocol Version 4, Src: 1	92.0.2.100, Dst:	198.51.100.100					
11	internet control Message Protocol							
-								
_								

Sélectionnez le deuxième paquet et vérifiez les points clés :

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

	o. Time	Source	Destination Pr	tocol Length	PD	IP TTL Info	
	1 2022-08-04 07:21:56.993302102	192.0.2.100	198.51.100.100 IC	MP 112	0x9574 (38260)	64 Echo (ping) request	id=0x0022, seq=1/256, ttl=64 (no response found!)
	2 2022-08-04 07:21:56.993303597	192.0.2.100	198.51.100.100 IC	MP 102	0x9574 (38260)	64 Echo (ping) request	id=0x0022, seq=1/256, ttl=64 (no response found!)
Г	3 2022-08-04 07:22:06.214264777	192.0.2.100	198.51.100.100 IC	MP 112	0x9a81 (39553)	64 Echo (ping) request	id=0x0022, seq=10/2560, ttl=64 (no response found!)
	4 2022-08-04 07:22:06.214267373	192.0.2.100	198.51.100.100 IC	MP 102	0x9a81 (39553)	64 Echo (ping) request	id=0x0022, seq=10/2560, ttl=64 (no response found!)
	5 2022-08-04 07:22:07.215113393	192.0.2.100	198.51.100.100 IC	MP 112	0x9ac3 (39619)	64 Echo (ping) request	id=0x0022, seq=11/2816, ttl=64 (no response found!)
	6 2022-08-04 07:22:07.215115445	192.0.2.100	198.51.100.100 IC	MP 102	0x9ac3 (39619)	64 Echo (ping) request	id=0x0022, seq=11/2816, ttl=64 (no response found!)
	7 2022-08-04 07:22:08.229938577	192.0.2.100	198.51.100.100 IC	MP 112	0x9b33 (39731)	64 Echo (ping) request	id=0x0022, seq=12/3072, ttl=64 (no response found!)
	8 2022-08-04 07:22:08.229940829	192.0.2.100	198.51.100.100 IC	MP 102	0x9b33 (39731)	64 Echo (ping) request	id=0x0022, seq=12/3072, ttl=64 (no response found!)
	9 2022-08-04 07:22:09.253944601	192.0.2.100	198.51.100.100 IC	MP 112	0x9c0e (39950)	64 Echo (ping) request	id=0x0022, seq=13/3328, ttl=64 (no response found!)
	10 2022-08-04 07:22:09.253946899	192.0.2.100	198.51.100.100 IC	MP 102	0x9c0e (39950)	64 Echo (ping) request	id=0x0022, seq=13/3328, ttl=64 (no response found!)
	11 2022-08-04 07:22:10.277953070	192.0.2.100	198.51.100.100 IC	MP 112	0x9ccb (40139)	64 Echo (ping) request	id=0x0022, seq=14/3584, ttl=64 (no response found!)
	12 2022-08-04 07:22:10.277954736	192.0.2.100	198.51.100.100 IC	MP 102	0x9ccb (40139)	64 Echo (ping) request	id=0x0022, seq=14/3584, ttl=64 (no response found!)
	13 2022-08-04 07:22:11.301931282	192.0.2.100	198.51.100.100 IC	MP 112	0x9d84 (40324)	64 Echo (ping) request	id=0x0022, seq=15/3840, ttl=64 (no response found!)
	14 2022-08-04 07:22:11.301933600	192.0.2.100	198.51.100.100 IC	MP 102	0x9d84 (40324)	64 Echo (ping) request	id=0x0022, seq=15/3840, ttl=64 (no response found!)
	15 2022-08-04 07:22:12.325936521	192.0.2.100	198.51.100.100 IC	MP 112	0x9da2 (40354)	64 Echo (ping) request	id=0x0022, seq=16/4096, ttl=64 (no response found!)
	16 2022-08-04 07:22:12.325937895	192.0.2.100	198.51.100.100 IC	MP 102	0x9da2 (40354)	64 Echo (ping) request	id=0x0022, seq=16/4096, ttl=64 (no response found!)
	17 2022-08-04 07:22:13.326988040	192.0.2.100	198.51.100.100 IC	MP 112	0x9e07 (40455)	64 Echo (ping) request	id=0x0022, seq=17/4352, ttl=64 (no response found!)
	18 2022-08-04 07:22:13.326990258	192.0.2.100	198.51.100.100 IC	MP 102	0x9e07 (40455)	64 Echo (ping) request	id=0x0022, seq=17/4352, ttl=64 (no response found!)
	19 2022-08-04 07:22:14.341944773	192.0.2.100	198.51.100.100 IC	MP 112	0x9e6a (40554)	64 Echo (ping) request	id=0x0022, seq=18/4608, ttl=64 (no response found!)
	20 2022-08-04 07:22:14.341946249	192.0.2.100	198.51.100.100 IC	MP 102	0x9e6a (40554)	64 Echo (ping) request	id=0x0022, seq=18/4608, ttl=64 (no response found!)
	21 2022-08-04 07:22:15.365941588	192.0.2.100	198.51.100.100 IC	MP 112	0x9efb (40699)	64 Echo (ping) request	id=0x0022, seq=19/4864, ttl=64 (no response found!)
	22 2022-08-04 07:22:15.365942566	192.0.2.100	198.51.100.100 IC	MP 102	0x9efb (40699)	64 Echo (ping) request	id=0x0022, seq=19/4864, ttl=64 (no response found!)
	23 2022-08-04 07:22:16.389973843	192.0.2.100	198.51.100.100 IC	MP 112	0x9fe8 (40936)	64 Echo (ping) request	id=0x0022, seq=20/5120, ttl=64 (no response found!)
	24 2022-08-04 07:22:16.389975129	192.0.2.100	198.51.100.100 IC	MP 102	0x9fe8 (40936)	64 Echo (ping) request	id=0x0022, seq=20/5120, ttl=64 (no response found!)
	25 2022-08-04 07:22:17.413936452	192.0.2.100	198.51.100.100 IC	MP 112	0xa079 (41081)	64 Echo (ping) request	id=0x0022, seq=21/5376, ttl=64 (no response found!)
	26 2022-08-04 07:22:17.413938090	192.0.2.100	198.51.100.100 IC	MP 102	0xa079 (41081)	64 Echo (ping) request	id=0x0022, seq=21/5376, ttl=64 (no response found!)
	27 2022-08-04 07:22:18.437954335	192.0.2.100	198.51.100.100 IC	MP 112	0xa11e (41246)	64 Echo (ping) request	id=0x0022, seq=22/5632, ttl=64 (no response found!)
					1 1		
E	forme 2, 102 butes on vine (016 bit	<li>a) 100 buttos co</li>	ntunod (Olf bits) on i	atonfoco contuno u	1. 14.0		20 27 76 £7 00 00 10 00 50 56 0d 28 ba 91 00 00 cd
	Sthemast II Encl Mhana OdiaBiba (	oorsorserodroph	ptured (816 01ts) on 1	aith (apropriate capture_ut	5_1, 10 0	00	10 08 00 45 00 00 50 57 40 00 40 01 b8 38 c0 00
	Page 10 virtual LAN DRT: 0 DET: 0	TD: 205	e), Ust. az./0.12.00.0	10 (az./0.12.00.0	50.10)	00	20 02 64 c6 33 64 64 08 00 eb 95 00 22 00 01 88 73 ·································
Г	and a priority in the second s	Bast Effort (daf:	(a)			00	30 eb 62 00 00 00 00 d9 9d 00 00 00 00 00 00 10 11 .b
L	a - DET: Tooli	sible	aurc) (0)			00	40 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21
Т	0000 1100 1101 - ID: 305	Giore	_			00	50 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 "#\$%&'() *+,/01
Т	Tupo: 1044 (0x0000)		2			00	60 32 33 34 35 36 37 234567
	Internet Destocal Version 4 Sec. 1	03 0 3 100 0/11	100 51 100 100				
	Internet Control Message Protocol	52.0.2.100, DSC:	190.31.100.100				
Г	internet control Message Protocol						

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

- 1. Seuls les paquets de requête d'écho ICMP sont capturés. Chaque paquet est capturé et affiché 2 fois.
- 2. L'en-tête de paquet d'origine a l'étiquette VLAN 207.
- 3. Le commutateur interne insère une étiquette VLAN de port supplémentaire 1001 qui identifie l'interface d'entrée Portchannel1.
- 4. Le commutateur interne insère une étiquette VN supplémentaire.

No. Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info		
- 1 2022-08-04 08:18:24.572548869	192.168.247.100	192.168.247.102	ICMP	128	0x609e (24734)	255 Echo (ping) r	equest	id=0x007b, seq=0/0, ttl=255 (no response found!)
2 2022-08-04 08:18:24.572550073	192.168.247.100	192.168.247.102	ICMP	118	0x609e (24734)	255 Echo (ping) r	equest	id=0x007b, seq=0/0, ttl=255 (no response found!)
3 2022-08-04 08:18:24.573286630	192.168.247.100	192.168.247.102	ICMP	128	0x609f (24735)	255 Echo (ping) r	equest	id=0x007b, seq=1/256, ttl=255 (no response found!)
4 2022-08-04 08:18:24.573287640	192.168.247.100	192.168.247.102	ICMP	118	0x609f (24735)	255 Echo (ping) r	equest	id=0x007b, seg=1/256, ttl=255 (no response found!)
5 2022-08-04 08:18:24,573794751	192.168.247.100	192.168.247.102	ICMP	128	0x60a0 (24736)	255 Echo (ping) r	equest	id=0x007b, seg=2/512, ttl=255 (no response found!)
6 2022-08-04 08:18:24,573795748	192.168.247.100	192.168.247.102	ICMP	118	0x60a0 (24736)	255 Echo (ping) r	equest	id=0x007b, seg=2/512, ttl=255 (no response found!)
7 2022-08-04 08:18:24.574368638	192.168.247.100	192,168,247,102	ICMP	128	0x60a1 (24737)	255 Echo (ping) r	equest	id=0x007b, seg=3/768, ttl=255 (no response found!)
8 2022-08-04 08:18:24.574369574	192.168.247.100	192.168.247.102	ICMP	118	0x60a1 (24737)	255 Echo (ping) r	equest	id=0x007b, seq=3/768, ttl=255 (no response found!)
9 2022-08-04 08:18:24.574914512	192.168.247.100	192.168.247.102	TCMP	128	0x60a2 (24738)	255 Echo (ping) r	equest	id=8x887h, seq=4/1824, ttl=255 (no response foundl)
10 2022-08-04 08:18:24.574915415	192.168.247.100	192.168.247.102	ICMP	118	0x60a2 (24738)	255 Echo (ping) r	equest	id=0x007b, seg=4/1024, ttl=255 (no response found1)
11 2022-08-04 08:18:24.575442569	192.168.247.100	192.168.247.102	TCMP	128	0x60a3 (24730)	255 Echo (ping) r	equest	id=8x887b, seq=5/1288, ttl=255 (no response found1)
12 2022-08-04 08:18:24 575443601	192.168.247.100	192.168.247.102	TCMP	118	0x60a3 (24730)	255 Echo (ping) n	equest	id=avaa7h, seq=5/1280, ttl=255 (no response foundl)
13 2022.08.04 08.18.24 575018110	102 168 247 100	102 168 247 102	TCMD	128	8x68a4 (24748)	255 Echo (ping) n	equest	id=0x007b, seq=6/1536 ttl=255 (no response found1)
14 2022-00-04 00:10:24:575010057	102 169 247 100	102 168 247 102	TCMD	119	0x60a4 (24740)	255 Echo (ping) n	equest	id-avaa7h seq=6/1536 ttl=255 (no response foundl)
15 2022-00-04 00:10:24.575407671	102 169 247 100	102 169 247 102	TCMD	129	0x60a5 (24740)	255 Echo (ping) n	equest	id-avaa7b seq=7/1702 ttl=255 (no response found1)
15 2022-00-04 00:10:24.570407071	102.108.247.100	102.108.247.102	TCMD	110	0x00a3 (24741)	255 Echo (ping) n	equest	id-0x007b, seq=7/1792, ttl=255 (no response found)
16 2022-08-04 08:18:24.5/6408585	192.108.247.100	192.108.247.102	ICMP	118	0x00a5 (24741)	255 Echo (ping) P	equest	id events are elected at a second country
1/ 2022-08-04 08:18:24.5/0885643	192.168.247.100	192.168.247.102	ICMP	128	0x00a6 (24742)	255 Echo (ping) P	equest	Id=0x007b, seq=8/2048, ttl=255 (no response found!)
18 2022-08-04 08:18:24.570880501	192.168.247.100	192.168.247.102	ICMP	118	0x60a6 (24742)	255 Echo (ping) r	equest	1d=0x007b, seq=8/2048, ttl=255 (no response found!)
19 2022-08-04 08:18:24.577394328	192.168.247.100	192.168.247.102	ICMP	128	0x60a7 (24743)	255 Echo (ping) r	equest	1d=0x007b, seq=9/2304, ttl=255 (no response found!)
20 2022-08-04 08:18:24.577395234	192.168.247.100	192.168.247.102	ICMP	118	0x60a7 (24743)	255 Echo (ping) r	equest	1d=0x007b, seq=9/2304, ttl=255 (no response found!)
21 2022-08-04 08:18:24.577987632	192.168.247.100	192.168.247.102	ICMP	128	0x60a8 (24744)	255 Echo (ping) r	equest	<pre>id=0x007b, seq=10/2560, ttl=255 (no response found!)</pre>
22 2022-08-04 08:18:24.577989290	192.168.247.100	192.168.247.102	ICMP	118	0x60a8 (24744)	255 Echo (ping) r	equest	id=0x007b, seq=10/2560, ttl=255 (no response found!)
23 2022-08-04 08:18:24.578448781	192.168.247.100	192.168.247.102	ICMP	128	0x60a9 (24745)	255 Echo (ping) r	equest	id=0x007b, seq=11/2816, ttl=255 (no response found!)
24 2022-08-04 08:18:24.578449909	192.168.247.100	192.168.247.102	ICMP	118	0x60a9 (24745)	255 Echo (ping) r	request	id=0x007b, seq=11/2816, ttl=255 (no response found!)
25 2022-08-04 08:18:24.578900043	192.168.247.100	192.168.247.102	ICMP	128	0x60aa (24746)	255 Echo (ping) r	equest	id=0x007b, seq=12/3072, ttl=255 (no response found!)
26 2022-08-04 08:18:24.578900897	192.168.247.100	192.168.247.102	ICMP	118	0x60aa (24746)	255 Echo (ping) r	equest	id=0x007b, seq=12/3072, ttl=255 (no response found!)
27 2022-08-04 08:18:24.579426962	192.168.247.100	192.168.247.102	ICMP	128	0x60ab (24747)	255 Echo (ping) r	equest	id=0x007b, seq=13/3328, ttl=255 (no response found!)
ć.								
> Frame 1: 128 bytes on wire (1024 bits	), 128 bytes cap	tured (1024 bits) o	n interface ca	pture u0	3, id 0			a2 76 f2 00 00 1c 00 17 df d6 ec 00 89 26 80 3d
> Ethernet II, Src: Cisco d6:ec:00 (00:	17:df:d6:ec:00).	Dst: a2:76:f2:00:0	0:1c (a2:76:f)	:00:00:10	)		0010	00 00 81 00 03 e9 81 00 00 cf 08 00 45 00 00 64E.d
VN-Tag					· · · · · · · · · · · · · · · · · · ·		0020	60 9e 00 00 ff 01 ea dd c0 a8 f7 64 c0 a8 f7 66 `df
1	Direction	: Ecom Bridge	_				0030	08 00 e5 c8 00 7b 00 00 00 00 00 02 4d 8c 4a 78 ·····{···M·Jx
	= Pointer:	vif id					0040	ab cd
00 0000 0011 1101	= Destinati	001 61					0050	ab cd
	= Looped: N	0	<b>1</b>				0060	ab cd
	- Posorwada	0	71				0070	ab cd
	- Version:	0						
	= version.	0						
Turnet 902 10 Victural LAN (0x9100)	oooo - source. o							
Type: 802.10 Virtual LAN (0X8100)	D: 1001		_					
✓ 802.10 VIPTUAI LAN, PKI: 0, DEI: 0, 1	D: 1001	(a)						
000 Priority: Bes	st Effort (defaul	t) (0)	2					
0 = DEI: Ineligit	01e		2					
0011 1110 1001 = ID: 1001								
Type: 802.10 Virtual LAN (0x8100)			_					
802.1Q Virtual LAN, PRI: 0, DEI: 0, I	D: 207							
000 Bes	st Effort (defaul	t) (0)						
0 = DEI: Ineligit	ble		-					
0000 1100 1111 = ID: 207			21					
Type: IPv4 (0x0800)			-					
Internet Protocol Version 4, Src: 192	.168.247.100, Dst	t: 192.168.247.102						
> Internet Control Message Protocol								
L								

Sélectionnez le deuxième paquet et vérifiez les points clés :

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

No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info		
-	1 2022-08-04 08:18:24,572548869	192,168,247,100	192,168,247,102	ICMP	128	0x609e (24734)	255 Echo (ping) rec	uest	id=0x007b, seg=0/0, ttl=255 (no response found!)
	2 2022-08-04 08:18:24.572550073	192,168,247,100	192,168,247,102	ICMP	118	0x609e (24734)	255 Echo (ping) rec	uest	id=0x007b, seg=0/0, ttl=255 (no response found!)
	3 2022-08-04 08:18:24.573286630	192.168.247.100	192.168.247.102	ICMP	128	0x609f (24735)	255 Echo (ping) rec	uest	id=0x007b, seg=1/256, ttl=255 (no response found!)
	4 2022-08-04 08:18:24.573287640	192.168.247.100	192.168.247.102	ICMP	118	0x609f (24735)	255 Echo (ping) rec	uest	id=0x007b, seq=1/256, ttl=255 (no response found!)
	5 2022-08-04 08:18:24.573794751	192.168.247.100	192.168.247.102	ICMP	128	0x60a0 (24736)	255 Echo (ping) rec	uest	id=0x007b, seq=2/512, ttl=255 (no response found!)
	6 2022-08-04 08:18:24.573795748	192.168.247.100	192.168.247.102	ICMP	118	0x60a0 (24736)	255 Echo (ping) rec	uest	id=0x007b, seg=2/512, ttl=255 (no response found!)
	7 2022-08-04 08:18:24.574368638	192.168.247.100	192.168.247.102	ICMP	128	0x60a1 (24737)	255 Echo (ping) red	uest	id=0x007b, seg=3/768, ttl=255 (no response found!)
	8 2022-08-04 08:18:24.574369574	192.168.247.100	192.168.247.102	ICMP	118	0x60a1 (24737)	255 Echo (ping) rec	uest	id=0x007b, seg=3/768, ttl=255 (no response found!)
	9 2022-08-04 08:18:24.574914512	192.168.247.100	192.168.247.102	ICMP	128	0x60a2 (24738)	255 Echo (ping) rec	uest	id=0x007b, seg=4/1024, ttl=255 (no response found!)
	10 2022-08-04 08:18:24.574915415	192.168.247.100	192.168.247.102	ICMP	118	0x60a2 (24738)	255 Echo (ping) rec	uest	id=0x007b, seg=4/1024, ttl=255 (no response found!)
	11 2022-08-04 08:18:24.575442569	192.168.247.100	192.168.247.102	ICMP	128	0x60a3 (24739)	255 Echo (ping) rec	uest	id=0x007b, seg=5/1280, ttl=255 (no response found!)
	12 2022-08-04 08:18:24.575443601	192.168.247.100	192.168.247.102	ICMP	118	0x60a3 (24739)	255 Echo (ping) rec	uest	id=0x007b, seg=5/1280, ttl=255 (no response found!)
	13 2022-08-04 08:18:24.575918119	192.168.247.100	192.168.247.102	ICMP	128	0x60a4 (24740)	255 Echo (ping) rec	uest	id=0x007b, seg=6/1536, ttl=255 (no response found!)
	14 2022-08-04 08:18:24.575919057	192.168.247.100	192.168.247.102	ICMP	118	0x60a4 (24740)	255 Echo (ping) rec	uest	id=0x007b, seq=6/1536, ttl=255 (no response found!)
	15 2022-08-04 08:18:24,576407671	192,168,247,100	192,168,247,102	ICMP	128	0x60a5 (24741)	255 Echo (ping) rec	uest	id=0x007b, seg=7/1792, ttl=255 (no response found!)
	16 2022-08-04 08:18:24.576408585	192.168.247.100	192.168.247.102	ICMP	118	0x60a5 (24741)	255 Echo (ping) rec	uest	id=0x007b, seq=7/1792, ttl=255 (no response found!)
	17 2022-08-04 08:18:24.576885643	192.168.247.100	192.168.247.102	ICMP	128	0x60a6 (24742)	255 Echo (ping) rec	uest	id=0x007b, seg=8/2048, ttl=255 (no response found!)
	18 2022-08-04 08:18:24.576886561	192.168.247.100	192.168.247.102	ICMP	118	0x60a6 (24742)	255 Echo (ping) rec	uest	id=0x007b, seq=8/2048, ttl=255 (no response found!)
	19 2022-08-04 08:18:24.577394328	192.168.247.100	192.168.247.102	ICMP	128	0x60a7 (24743)	255 Echo (ping) rec	quest	id=0x007b, seq=9/2304, ttl=255 (no response found!)
	20 2022-08-04 08:18:24.577395234	192.168.247.100	192.168.247.102	ICMP	118	0x60a7 (24743)	255 Echo (ping) rec	uest	id=0x007b, seq=9/2304, ttl=255 (no response found!)
	21 2022-08-04 08:18:24.577987632	192.168.247.100	192.168.247.102	ICMP	128	0x60a8 (24744)	255 Echo (ping) rec	quest	id=0x007b, seq=10/2560, ttl=255 (no response found!)
	22 2022-08-04 08:18:24.577989290	192.168.247.100	192.168.247.102	ICMP	118	0x60a8 (24744)	255 Echo (ping) rec	quest	id=0x007b, seq=10/2560, ttl=255 (no response found!)
	23 2022-08-04 08:18:24.578448781	192.168.247.100	192.168.247.102	ICMP	128	0x60a9 (24745)	255 Echo (ping) rec	uest	id=0x007b, seq=11/2816, ttl=255 (no response found!)
	24 2022-08-04 08:18:24.578449909	192.168.247.100	192.168.247.102	ICMP	118	0x60a9 (24745)	255 Echo (ping) rec	uest	id=0x007b, seq=11/2816, ttl=255 (no response found!)
	25 2022-08-04 08:18:24.578900043	192.168.247.100	192.168.247.102	ICMP	128	0x60aa (24746)	255 Echo (ping) rec	uest	id=0x007b, seq=12/3072, ttl=255 (no response found!)
	26 2022-08-04 08:18:24.578900897	192.168.247.100	192.168.247.102	ICMP	118	0x60aa (24746)	255 Echo (ping) rec	uest	id=0x007b, seq=12/3072, ttl=255 (no response found!)
	27 2022-08-04 08:18:24.579426962	192.168.247.100	192.168.247.102	ICMP	128	0x60ab (24747)	255 Echo (ping) rec	uest	id=0x007b, seq=13/3328, ttl=255 (no response found!)
<									and the first of the state
	and the second sec		and (and block as			11.0			
2 1	rame 2: 118 Dytes on wire (944 bits)	, 118 bytes capto	ured (944 bits) on	interface cap	ture_u0_3,	10 0		0000	az /6 TZ 00 00 10 00 1/ 0T 06 00 00 81 00 00 CT .V
	thernet II, Src: Cisco db:ec:00 (00:	1/:df:d6:ec:00),	DST: a2:76:12:00:0	0:1c (a2:/6:T	2:00:00:10	.)		0010	f7 64 c9 a8 f7 66 98 99 e5 c8 99 7h 99 99 99 99 99
<u>м</u> 8	02.10 Virtual LAN, PRI: 0, DEI: 0, I	D: 207	A) (A)					0030	98 92 4d 8c 4a 78 ab cd ab cd ab cd ab cd ab cd
	out Priority: Bes	st errort (defaul	(0)					0040	ab cd
	0 = DEI: Ineligit	ore		2				0050	ab cd
	0000 1100 1111 = 1D: 207			21				0060	ab cd
1.12	stoppet Destace] Marsian 4 Cost 103	160 347 100 04	. 103 160 347 103					0070	ab cd ab cd ab cd
1	atenant Control Message Destage	.100.247.100, DS	. 192.108.247.102						
1	internet control Hessage Protocol								

## Explication

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

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

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

Ce tableau récapitule la tâche :

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

Configurez et vérifiez une capture de paquets sur la sous- interface Portchannel1 avec les interfaces membres Ethernet1/3 et Ethernet1/4	Ethernet1/3 Ethernet1/4	1001	Entrée uniquement	Requêtes d'écho ICMP de 192.168.207.100 vers l'hôte 192.168.207.102
--	----------------------------	------	----------------------	---

## Filtres de capture de paquets

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

Topologie, flux de paquets et points de capture



## Configuration

## FCM

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

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

Overview Inter	faces Logical Devices Se	ecurity Engine Plat	form Settings									System Tools	Help admin
Capture Session	Filter List												_
Filter List												Ad	ld Filter
Filter House		From				То			Destand	Teneradan	Ordenudan	Distantions	
Filter Name	MAC	IPv4	IPv6	Port	MAC	IPv4	IPv6	Port	Protocol	Inner vian	Outer vian	ctnertype	
filter_icmp	00:00:00:00:00:00	192.0.2.100	П	0	00:00:00:00:00:00	192.0.2.100		0	1	0	0	0	/8
				Edit Packet	Filter								
				Filter Name* Protocol	filter_icmp ICMP_IPv4 ¥			_					
				EtherType	Any 👻								
				Inner vlan	0	Outer vlan	0						
				Source		Destination		_					
				IPv4	192.0.2.100	IPv4	198.51.100.100						
				IPv6	::	IPv6	::						
				Port	0	Port	0						
				MAC	00:00:00:00:00:00	MAC	00:00:00:00:00						
							Save	Cancel					

3. Utilisez Tools > Packet Capture > Capture Session pour créer une nouvelle session de capture :

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

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

Overview Interfaces Logical Devices Security Engine Platform Settings	System Tools Help admin
Select an instance: ftd1 v	Save and Run Save Cancel
ftd1	Session Name* Cap1 Selected Interfaces Ethernet1/2
Ethernet1/2	Buffer Size     256 MB       Snap length:     1518       Store Packets     Overwrite
Ethernet1/3 FTD FTD Ethernet1/9. Ethernet1/10	Capture Filter           Apply Filter         Capture All           Apply         Create Filter           Apply         To           Ethemet1/2         To
EthernetI/I	

## CLI FXOS

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

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

<#root>								
firepower#								
scope ssa								
firepower , show app-in	/ssa# nstance							
App Name	Identifier Slot ID	Admin	State Oper State	Running Version	Startup	Version	Deploy	Ту 
ftd	ftdl							
1	Enabled	Online	7.2.0.82	7.2.0.82	Native	No		

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

3. Créez une session de capture :

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

firepower /packet-capture #
create filter filter_icmp

firepower /packet-capture/filter* #
set destip 198.51.100.100

firepower /packet-capture/filter* #
set protocol 1

firepower /packet-capture/filter* #
set srcip 192.0.2.100

firepower /packet-capture/filter* #
exit

firepower /packet-capture/filter* #
```

```
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 :

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

#### **CLI FXOS**

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

<#root> firepower# scope packet-capture firepower /packet-capture # show filter detail Configure a filter for packet capture: Name: filter\_icmp Protocol: 1 Ivlan: 0 Ovlan: 0 Src Ip: 192.0.2.100 Dest Ip: 198.51.100.100 Src MAC: 00:00:00:00:00:00 Dest MAC: 00:00:00:00:00:00 Src Port: 0 Dest Port: 0 Ethertype: 0 Src Ipv6: :: Dest Ipv6: :: firepower /packet-capture # show session cap1 Traffic Monitoring Session: Packet Capture Session Name: cap1

Session: 1

Admin State: Enabled Oper State: Up Oper State Reason: Active Config Success: Yes Config Fail Reason: Append Flag: Overwrite Session Mem Usage: 256 MB Session Pcap Snap Len: 1518 Bytes Error Code: 0 Drop Count: 0 Physical ports involved in Packet Capture: Slot Id: 1 Port Id: 2 Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap Pcapsize: 213784 bytes Filter: filter\_icmp Sub Interface: 0 Application Instance Identifier: ftd1 Application Name: ftd Collecter les fichiers de capture

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

Capturer l'analyse des fichiers

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

1. Seuls les paquets de requête d'écho ICMP sont capturés. Chaque paquet est capturé et

affiché 2 fois.

- 2. L'en-tête de paquet d'origine est sans étiquette VLAN.
- 3. Le commutateur interne insère une étiquette VLAN de port supplémentaire 102 qui identifie l'interface d'entrée Ethernet1/2.
- 4. Le commutateur interne insère une étiquette VN supplémentaire.

-													_	_
1	No. Time	Source	Destination	Protocol	Length	PD		IP TTL Info					_	^
	1 2022-08-02 15:46:55.603277760	192.0.2.100	198.51.100.100	ICMP	108	0x0012	(18)	64 Echo (p	oing) request	id=0x0018, se	q=349/23809,	ttl=64 (	no r	
н	2 2022-08-02 15:46:55.603279688	192.0.2.100	198.51.100.100	ICMP	102	0x0012	(18)	64 Echo (p	oing) request	id=0x0018, se	q=349/23809,	ttl=64 (	no r	
L	3 2022-08-02 15:46:56.627139252	192.0.2.100	198.51.100.100	ICMP	108	0x00db	(219)	64 Echo (p	oing) request	id=0x0018, se	q=350/24065,	ttl=64 (	no r	
L	4 2022-08-02 15:46:56.627140919	192.0.2.100	198.51.100.100	ICMP	102	0x00db	(219)	64 Echo (p	oing) request	id=0x0018, se	q=350/24065,	ttl=64 (	no r	
L	5 2022-08-02 15:46:57.651185193	192.0.2.100	198.51.100.100	ICMP	108	0x01cb	(459)	64 Echo (p	oing) request	id=0x0018, se	q=351/24321,	ttl=64 (	no r	
н	6 2022-08-02 15:46:57.651186787	192.0.2.100	198.51.100.100	ICMP	102	0x01cb	(459)	64 Echo (p	oing) request	id=0x0018, se	q=351/24321,	ttl=64 (	no r	
н	7 2022-08-02 15:46:58.675153317	192.0.2.100	198.51.100.100	ICMP	108	0x01d6	(470)	64 Echo (p	oing) request	id=0x0018, se	q=352/24577,	ttl=64 (	no r	
L	8 2022-08-02 15:46:58.675154503	192.0.2.100	198.51.100.100	ICMP	102	0x01d6	(470)	64 Echo (p	oing) request	id=0x0018, se	q=352/24577,	ttl=64 (	no r	
н	9 2022-08-02 15:46:59.699152639	192.0.2.100	198.51.100.100	ICMP	108	0x01f4	(500)	64 Echo (p	oing) request	id=0x0018, se	q=353/24833,	ttl=64 (	no r	
н	10 2022-08-02 15:46:59.699153835	192.0.2.100	198.51.100.100	ICMP	102	0x01f4	(500)	64 Echo (p	oing) request	id=0x0018, se	q=353/24833,	ttl=64 (	no r	
L	11 2022-08-02 15:47:00.723142641	192.0.2.100	198.51.100.100	ICMP	108	0x01f9	(505)	64 Echo (p	oing) request	id=0x0018, se	q=354/25089,	ttl=64 (	no r	
L	12 2022-08-02 15:47:00.723144643	192.0.2.100	198.51.100.100	ICMP	102	0x01f9	(505)	64 Echo (p	oing) request	id=0x0018, se	q=354/25089,	ttl=64 (	no r	
L	13 2022-08-02 15:47:01.747162204	192.0.2.100	198.51.100.100	ICMP	108	0x026e	(622)	64 Echo (p	oing) request	id=0x0018, se	q=355/25345,	ttl=64 (	no r	
L	14 2022-08-02 15:47:01.747163783	192.0.2.100	198.51.100.100	ICMP	102	0x026e	(622)	64 Echo (p	oing) request	id=0x0018, se	q=355/25345,	ttl=64 (	no r	
L	15 2022-08-02 15:47:02.771209952	192.0.2.100	198.51.100.100	ICMP	108	0x02bc	(700)	64 Echo (p	oing) request	id=0x0018, se	q=356/25601,	ttl=64 (	no r	
L	16 2022-08-02 15:47:02.771211062	192.0.2.100	198.51.100.100	ICMP	102	0x02bc	(700)	64 Echo (p	oing) request	id=0x0018, se	q=356/25601,	ttl=64 (	no r	
L	17 2022-08-02 15:47:03.772258550	192.0.2.100	198.51.100.100	ICMP	108	0x032f	(815)	64 Echo (p	oing) request	id=0x0018, se	q=357/25857,	ttl=64 (	no r	
L	18 2022-08-02 15:47:03.772259724	192.0.2.100	198.51.100.100	ICMP	102	0x032f	(815)	64 Echo (p	oing) request	id=0x0018, se	q=357/25857,	ttl=64 (	no r	
Ľ	19 2022-08-02 15:47:04.791118519	192.0.2.100	198.51.100.100	ICMP	108	0x040f	(1039)	64 Echo (p	ing) request	id=0x0018, se	q=358/26113,	ttl=64 (	no r	
Ľ	20 2022-08-02 15:47:04.791119721	192.0.2.100	198.51.100.100	ICMP	102	0x040f	(1039)	64 Echo (p	oing) request	id=0x0018, se	q=358/26113,	ttl=64 (	no r	~
	c												>	
r	> Frame 1: 108 bytes on wire (864 bi	ts), 108 bytes c	aptured (864 bits)	on interfac	e capture u0	1. it 000	00 <b>58 9</b> 7	7 bd b9 77 0e (	00 50 56 9d e	8 be 89 26 80	0a Xw.	P V · · · · &		_
Т	> Ethernet II, Src: VMware 9d:e8:be	(00:50:56:9d:e8:	be), Dst: Cisco b9:	77:0e (58:9	7:bd:b9:77:0e	) 001	10 00 00	81 00 00 66 0	8 8 8 45 88 8	0 54 00 12 40	00 ·····f·	· E · · T · · (	<b>.</b>	
	VN-Tag					002	20 40 01	1 4d 9b c0 00 0	02 64 c6 33 6	4 64 08 00 9e	67 @·M····	d ·3dd··	g	
Т	1	= Direct	ion: From Bridge			003	30 <b>00 1</b> 8	8 01 5d e2 46 (	e9 62 00 00 0	0 00 c1 a6 0c	00 ···]·F·	b		
Т	.0	= Pointe	er: vif id			004	10 00 00	0 00 00 10 11	12 13 14 15 1	6 17 18 19 1a	1b			
Т		= Destin	nation: 10			003	50 1c 1c	d 1e 1f 20 21 3	22 23 24 25 2	6 27 28 29 2a	2b ···· !"	# \$%& ()	*	
Т	0 0	= Looped	i: No 🤞	1		000	50 2C 20	d 2e 2† 30 31 3	32 33 34 35 3	6 37	,/012	3 4567		
Т	0	= Reserv	ved: 0	·										
Т		= Versio	on: 0											
Т	0000 00	00 0000 = Source	: 0											
Т	Type: 802.10 Virtual LAN (0x8100	)												
	802.10 Virtual LAN, PRI: 0, DEI: 0	, ID: 102												
Т	000 = Priority:	Best Effort (def	ault) (0)											
Т	0 = DEI: Ineli	gible		3										
Т	0000 0110 0110 = ID: 102													
Т	Type: IPv4 (0x0800)													
Т	> Internet Protocol Version 4. Src:	192.0.2.100, Dst	: 198.51.100.100											
Т	> Internet Control Message Protocol			4										
L														
Т														
Т														
	<					>								

Sélectionnez le deuxième paquet et vérifiez les points clés :

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

No	o. Time	Source	Destination	Protocol	Length	IP ID		IP TTL In	fo						^
r	- 1 2022-08-02 15:46:55.603277760	192.0.2.100	198.51.100.100	ICMP	108 1	0x0012 (	(18)	64 E	cho (ping	) request	id=0x0018,	seq=349/23809,	ttl=64 (	(no r	
	2 2022-08-02 15:46:55.603279688	192.0.2.100	198.51.100.100	ICMP	102	0x0012 (	(18)	64 E	cho (ping	) request	id=0x0018,	seq=349/23809,	ttl=64 (	(no r	
	3 2022-08-02 15:46:56.627139252	192.0.2.100	198.51.100.100	ICMP	108	0x00db (	(219)	64 E	cho (ping	) request	id=0x0018,	seq=350/24065,	ttl=64 (	(no r	
	4 2022-08-02 15:46:56.627140919	192.0.2.100	198.51.100.100	ICMP	102	0x00db (	(219)	64 E	cho (ping	) request	id=0x0018,	seq=350/24065,	ttl=64 (	(no r	
	5 2022-08-02 15:46:57.651185193	192.0.2.100	198.51.100.100	ICMP	108	0x01cb (	(459)	64 E	cho (ping	) request	id=0x0018,	seq=351/24321,	ttl=64 (	(no r	
	6 2022-08-02 15:46:57.651186787	192.0.2.100	198.51.100.100	ICMP	102	0x01cb (	(459)	64 E	cho (ping	) request	id=0x0018,	seq=351/24321,	ttl=64 (	(no r	
	7 2022-08-02 15:46:58.675153317	192.0.2.100	198.51.100.100	ICMP	108	0x01d6 (	(470)	64 E	cho (ping	) request	id=0x0018,	seq=352/24577,	ttl=64 (	(no r	
	8 2022-08-02 15:46:58.675154503	192.0.2.100	198.51.100.100	ICMP	102	0x01d6 (	(470)	64 E	cho (ping	) request	id=0x0018,	seq=352/24577,	ttl=64 (	(no r	
	9 2022-08-02 15:46:59.699152639	192.0.2.100	198.51.100.100	ICMP	108	0x01f4 (	(500)	64 E	cho (ping	) request	id=0x0018,	seq=353/24833,	ttl=64 (	(no r	
	10 2022-08-02 15:46:59.699153835	192.0.2.100	198.51.100.100	ICMP	102	0x01f4 (	(500)	64 E	cho (ping	) request	id=0x0018,	seq=353/24833,	ttl=64 (	(no r	
	11 2022-08-02 15:47:00.723142641	192.0.2.100	198.51.100.100	ICMP	108	0x01f9 (	(505)	64 E	cho (ping	) request	id=0x0018,	seq=354/25089,	ttl=64 (	(no r	
	12 2022-08-02 15:47:00.723144643	192.0.2.100	198.51.100.100	ICMP	102	0x01f9 (	(505)	64 E	cho (ping	) request	id=0x0018,	seq=354/25089,	ttl=64 (	(no r	
	13 2022-08-02 15:47:01.747162204	192.0.2.100	198.51.100.100	ICMP	108	0x026e (	(622)	64 E	cho (ping	) request	id=0x0018,	seq=355/25345,	ttl=64 (	(no r	
	14 2022-08-02 15:47:01.747163783	192.0.2.100	198.51.100.100	ICMP	102	0x026e (	(622)	64 E	cho (ping	) request	id=0x0018,	seq=355/25345,	ttl=64 (	(no r	
	15 2022-08-02 15:47:02.771209952	192.0.2.100	198.51.100.100	ICMP	108	0x02bc (	(700)	64 E	cho (ping	) request	id=0x0018,	seq=356/25601,	ttl=64 (	(no r	
	16 2022-08-02 15:47:02.771211062	192.0.2.100	198.51.100.100	ICMP	102	0x02bc (	(700)	64 E	cho (ping	) request	id=0x0018,	seq=356/25601,	ttl=64 (	(no r	
	17 2022-08-02 15:47:03.772258550	192.0.2.100	198.51.100.100	ICMP	108	0x032f (	(815)	64 E	cho (ping	) request	id=0x0018,	seq=357/25857,	ttl=64 (	(no r	
	18 2022-08-02 15:47:03.772259724	192.0.2.100	198.51.100.100	ICMP	102	0x032f (	(815)	64 E	cho (ping	) request	id=0x0018,	seq=357/25857,	ttl=64 (	(no r	
	19 2022-08-02 15:47:04.791118519	192.0.2.100	198.51.100.100	ICMP	108	0x040f (	(1039)	64 E	cho (ping	) request	id=0x0018,	seq=358/26113,	ttl=64 (	(no r	
	20 2022-08-02 15:47:04.791119721	192.0.2.100	198.51.100.100	ICMP	102	0x040f (	(1039)	64 E	cho (ping	) request	id=0x0018,	seq=358/26113,	ttl=64 (	(no r	~
<														>	_
5	Frame 2: 102 bytes on wire (816 bit	s), 102 bytes ca	ptured (816 bits) or	interface ca	pture u0 1	, id 000	0 58 97	bd b9 7	7 0e 00 5	0 56 9d (	e8 be 81 00	00 66 X···w··	P V · · · ·	٠f	
>	Ethernet II, Src: VMware 9d:e8:be (	00:50:56:9d:e8:b	e), Dst: Cisco b9:77	:0e (58:97:bd	:b9:77:0e)	001	0 08 00	45 00 0	0 54 00 1	2 40 00 4	40 01 4d 9b	CO 00 ··E··T·	· @·@·M·		
~	802.10 Virtual LAN, PRI: 0, DEI: 0,	ID: 102			,	002	0 02 64	c6 33 6	4 64 08 0	0 9e 67 (	00 18 01 5d	e2 46 ·d·3dd·	· ·g···]	- F	
	000 = Priority:	Best Effort (defa	ault) (0)			003	e9 62	00 00 0	0 00 c1 a	6 0c 00 0	00 00 00 00	10 11 ·b·····			
	0 = DEI: Ineli	gible	3			004	10 12 13	14 15 1	6 17 18 1	9 1a 1b 1	lc 1d 1e 1f	20 21		1	
	0000 0110 0110 = ID: 102		-			005	0 22 23	24 25 2	6 27 28 2	9 2a 2b 2	2c 2d 2e 2f	30 31 "#\$%&'(	) *+,/(	01	
	Type: IPv4 (0x0800)					006	32 33	34 35 3	6 37			234567			
>	Internet Protocol Version 4, Src: 1	192.0.2.100, Dst:	198.51.100.100												
>	Internet Control Message Protocol		2												

## Explication

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

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

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

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

Ce tableau récapitule la tâche :

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

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

FCM

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

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

Overview	Interfaces	Logical Devices	Security Engine	Platform	n Settings					System	Tools	Help	admin
Capture Ses	sion Filter Lis	t											
								C Refresh Capt	ure Session	Delete Al S	essions		
	cap1	Drop Coun	t: 0	Operati	ional State: up	Buffer Size: 256 MB		Snap Length: 15	18 Bytes			۹ (	
Interface Na	ame	Filter			File Size (in bytes)	File Name	Device Name						
Ethernet1/2		None			34700	cap1-ethernet-1-2-0.pcap	ftd1		<u>+</u>				

2. Assurez-vous que l'état opérationnel est DOWN - Session\_Admin\_Shut:

Overview	Interfaces	Logical Devices Security Engine	Platform Settings			System	Tools Help admin
Capture Ses	sion Fiter Lis	t					
						Capture Session Delete A	I Sessions
	cap1	Drop Count: 0	Operational State: DOWN - Session_Admin_Shut	Buffer Size: 256 MB		Snap Length: 1518 Bytes	280
Interface N	ame	Filter	File Size (in bytes)	File Name	Device Name		
Ethernet1/2		None	218828	cap1-ethemet-1-2-0.pcap	ftd1	⊻	

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

Overview	Interfaces	Logical Devices	Security Engine	Platform Settings				System	Tools	Help a	admin
Capture Ses	sion Filter Lis	it									
							Capture Session	Delete All	Sessions		
	cap1	Drop Count	t: <b>0</b>	Operational State: DOWN - Session_Admin_Shu	at Buffer Size: 256 MB		Snap Length: 1518 Bytes			J 5	
Interface Na	me	Filter		File Size (in bytes)	File Name	Device Name					
Ethernet1/2		None		218828	cap1-ethemet-1-2-0.pcap	ftd1	土				

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

**CLI FXOS** 

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

1. Arrêtez la capture active :

<#root>

firepower#

scope packet-capture

firepower /packet-capture #

scope session cap1

firepower /packet-capture/session #

#### disable

firepower /packet-capture/session\* #

commit

firepower /packet-capture/session #

up

firepower /packet-capture #

show session cap1 detail

Traffic Monitoring Session: Packet Capture Session Name:

cap1

Session: 1

Admin State: Disabled

Oper State: Down

Oper State Reason: Admin Disable

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

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: O
Application Instance Identifier: ftd1
Application Name: ftd
```

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

#### <#root>

firepower#

connect local-mgmt

firepower(local-mgmt)#

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

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

firepower(local-mgmt)#

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

Password:

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

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

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

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

- Soyez conscient des directives et des limites.
- Capturez les paquets sur toutes les interfaces membres port-channel et analysez tous les fichiers de capture.
- Utiliser des filtres de capture.
- Tenez compte de l'impact de la fonction NAT sur les adresses IP des paquets lorsqu'un filtre de capture est configuré.
- Augmentez ou diminuez la lentille d'accrochage qui spécifie la taille de trame au cas où elle serait différente de la valeur par défaut de 1 518 octets. Une taille plus courte entraîne une augmentation du nombre de paquets capturés et vice versa.
- Réglez la taille de la mémoire tampon si nécessaire.

- Soyez conscient du nombre de pertes sur FCM ou FXOS CLI. Une fois la taille limite de la mémoire tampon atteinte, le compteur de nombre d'abandons augmente.
- Utilisez le filtre !vntag sur Wireshark pour afficher uniquement les paquets sans le VN-tag. Ceci est utile pour masquer les paquets étiquetés VN dans les fichiers de capture de paquets de l'interface avant.
- Utilisez le filtre frame.number&1 sur Wireshark pour afficher uniquement les trames impaires. Ceci est utile pour masquer les paquets en double dans les fichiers de capture de paquets de l'interface de fond de panier.
- Dans le cas de protocoles tels que TCP, Wireshark applique par défaut des règles de coloration qui affichent les paquets avec des conditions spécifiques dans différentes couleurs. Dans le cas de captures internes du commutateur dues à des paquets dupliqués dans des fichiers de capture, le paquet peut être coloré et marqué d'une manière faussement positive. Si vous analysez les fichiers de capture de paquets et appliquez un filtre, exportez les paquets affichés dans un nouveau fichier et ouvrez le nouveau fichier à la place.

# Configuration et vérification sur Secure Firewall 3100/4200

À la différence de Firepower 4100/9300, les captures du commutateur interne sur le pare-feu sécurisé 3100/4200 sont configurées sur l'interface de ligne de commande de l'application via la commande capture <name>switch, où l'option switch spécifie que les captures sont configurées sur le commutateur interne.

Voici la commande capture avec l'option switch :

<#root>

> capture cap\_sw switch

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

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

1. Spécifiez une interface d'entrée :

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

<#root>
>
capture capsw switch interface ?
Available interfaces to listen:
 in\_data\_uplink1 Capture packets on internal data uplink1 interface
 in\_mgmt\_uplink1 Capture packets on internal mgmt uplink1 interface
 inside Name of interface Ethernet1/1.205
management Name of interface Management1/1

Le Secure Firewall 4200 prend en charge les captures bidirectionnelles. La valeur par défaut est ingress, sauf indication contraire :

<#root>

>
capture capi switch interface inside direction
both To capture switch bi-directional traffic
egress To capture switch egressing traffic
ingress To capture switch ingressing traffic

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

<#root>

>

capture capsw switch interface

eventing Name of interface Management1/2 in\_data\_uplink1 Capture packets on internal data uplink1 interface in\_data\_uplink2 Capture packets on internal data uplink2 interface in\_mgmt\_uplink1 Capture packets on internal mgmt uplink1 interface in\_mgmt\_uplink2 Capture packets on internal mgmt uplink1 interface management Name of interface Management1/1 2. Spécifiez l'EtherType de trame Ethernet. L'EtherType par défaut est IP. Les valeurs de l'option ethernet-type spécifient l'EtherType :

<#root>

>

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

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

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

#### <#root>

<cr>

>

capture capsw switch interface inside match ? <0-255> Enter protocol number (0 - 255) ah eigrp esp gre icmp icmp6 igmp igrp ip ipinip ipsec Mac-address filter mac nos ospf рср pim pptp sctp snp SPI value spi tcp udp

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

```
<#root>
```

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

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

```
<#root>
```

Oper State:

```
>
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
```

up

Oper State Reason: Active			
Config Success:	yes		
Config Fail Reaso	n:		
Append Flag:	overwrite		
Session Mem Usage	: 256		
Session Pcap Snap	Len: 1518		
Error Code:	0		
Drop Count:	0		
Total Physical port	s involved in Packet Canture: 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 Filt	er Info		
Name:	capsw-1-1		
Protocol:	0		
Ivlan:	0		
Ovlan:	205		
Src Ip:	0.0.0.0		
Dest Ip:	0.0.0		
Src Ipv6:			
Dest Ipv6:	::		
Src MAC:	00:00:00:00:00		
Dest MAC:	00:00:00:00:00		
Src Port:	0		
Dest Port:	0		
Ethertype:	0		
Total Dhysical kass	kout ports involved in Dasket Conturns 0		

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

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 0 Drop Count: Total Physical ports involved in Packet Capture: 1 Physical port: Slot Id: 1 Port Id: 1 Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap 24 Pcapsize: Filter: capsw-1-1

Packet Capture	Filter Info
Name:	capsw-1-1
Protocol:	0
Ivlan:	0
Ovlan:	205
Src Ip:	0.0.0
Dest Ip:	0.0.0
Src Ipv6:	::
Dest Ipv6:	::
Src MAC:	00:00:00:00:00:00
Dest MAC:	00:00:00:00:00:00
Src Port:	0
Dest Port:	0
Ethertype:	0

Total Physical breakout ports involved in Packet Capture: 0 O packet captured on disk using switch capture Reading of capture file from disk is not supported 8. Collectez les fichiers de capture. Suivez les étapes de la section Collecter les fichiers de capture internes du commutateur du pare-feu sécurisé.

Dans la version 7.4 du logiciel Secure Firewall, la configuration de capture interne du commutateur n'est pas prise en charge sur le FMC ou le FDM. Dans le cas du logiciel ASA version 9.18(1) et ultérieure, les captures de commutateurs internes peuvent être configurées dans ASDM versions 7.18.1.x et ultérieures.

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

Capture de paquets sur une interface physique ou Port Channel

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

Topologie, flux de paquets et points de capture

Secure Firewall 3100 :



Secure Firewall 4200 avec captures bidirectionnelles :



## Configuration

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

1. Vérifiez le nom si :

## <#root>

>

```
show nameif
```

Interface	Name	Security
Ethernet1/1	inside	0
Ethernet1/2	outside	0
Management1/1	diagnostic	0

#### <#root>

>

#### show nameif

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

#### 2. Créer une session de capture

#### <#root>

>

capture capsw switch interface inside

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

#### <#root>

> capture capsw switch interface inside direction ?

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

> capture capsw switch interface inside direction both

3. Activez la session de capture :

<#root>

> no capture capsw switch stop

#### Vérification

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

<#root>	
>	
show capture capsw d	etail
Packet Canture info	
racket capture mito	
Name:	capsw
Session:	1
Admin State:	enabled
Oper States	
Oper State:	άĐ
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 Filte	r Info
Name:	capsw-1-1
Protocol:	0
Ivlan:	0
Ovlan:	0
Src Ip:	0.0.0.0
Dest Ip:	0.0.0.0
Src Ipv6:	::
Dest Ipv6:	::
Src MAC:	00:00:00:00:00
Dest MAC:	00:00:00:00:00
Src Port:	0
Dest Port:	0
Ethertype:	0

Total Physical breakout ports involved in Packet Capture: 0

79 packets captured on disk using switch capture

Reading of capture file from disk is not supported

Secure Firewall 4200 :

<#root>

>

show cap capsw detail

Packet Capture info

Name:	capsw
Session:	1
Admin State:	enabled
Oper State:	up

Oper State Reason: Active
Config Success: yes Config Fail Reason: Append Flag: overwrite Session Mem Usage: 256 Session Pcap Snap Len: 1518 Error Code: 0 Drop Count: 0 Total Physical ports involved in Packet Capture: 1 Physical port: Slot Id: 1 Port Id: 1 Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap Pcapsize: 0 Direction: both disable Drop: 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: :: 00:00:00:00:00:00 Src MAC: 00:00:00:00:00:00 Dest MAC: Src Port: 0 Dest Port: 0 0 Ethertype: Total Physical breakout ports involved in Packet Capture: 0 33 packet captured on disk using switch capture Reading of capture file from disk is not supported

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

#### <#root>

>

show capture capsw detail

Packet Capture info

Name: capsw

	Session:	1
	Admin State:	enabled
	Oper State:	up
	Oper State Reason:	Active
	Config Success:	yes
	Appond Elag:	ovorwrita
	Session Mem Usade	256
	Session Pcan Snan	en: 1518
	Frror Code:	0
	Drop Count:	0
_		
Т	otal Physical ports	involved in Packet Capture: 2
Р	hysical 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
P	acket Canture Filte	r Info
•	Name:	cansw-1-4
	Protocol:	0
	Tvlan:	0
	Ovlan:	0
	Src In:	
	Dest In:	
	Src Tryfe	
	Doct Tryfe	
	Dest ipvo:	
	SPC MAC:	
	Dest MAC:	00:00:00:00:00
	Src Port:	0
	Dest Port:	0
	Ethertype:	0
Р	hysical port:	
	Slot Id:	1
	Port Id:	٢

Pcapfile:	/mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-3-0.pcap
Pcapsize:	18399
Filter:	capsw-1-3
Packet Capture Fi	ilter 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
Dest MAC:	00:00:00:00:00
Src Port:	0
Dest Port:	0
Ethertype:	0

Total Physical breakout ports involved in Packet Capture: 0

56 packet captured on disk using switch capture

Reading of capture file from disk is not supported

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

```
<#root>
>
connect fxos
firewall#
connect local-mgmt
firewall(local-mgmt)#
show portchannel summary
               P - Up in port-channel (members)
Flags: D - Down
I - Individual H - Hot-standby (LACP only)
s - Suspended r - Module-removed
S - Switched R - Routed
U - Up (port-channel)
M - Not in use. Min-links not met
_____
Group Port- Type Protocol Member Ports
    Channel
```


#### 1 Pol(U) Eth LACP Eth1/3(P) Eth1/4(P)

LACP	KeepAlive	Timer:			
	Channel	PeerKeepAliveTi	merFast		
1	Po1(U)	False			
Clust	cer LACP St	tatus:			
	Channel	ClusterSpanned	ClusterDetach	ClusterUnitID	ClusterSysID
1	Po1(U)	False	False	0	clust

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

Collecter les fichiers de capture

Suivez les étapes de la section Collecter les fichiers de capture internes du commutateur du parefeu sécurisé.

Capturer l'analyse des fichiers

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

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

No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info	^
<b>F</b>	1 2022-08-07 19:50:06.925768	192.0.2.100	198.51.100.100	ICMP	102	0x9a10 (39440)	64 Echo (ping) request	id=0x0034, seq=1/256, ttl=64 (no res
	2 2022-08-07 19:50:07.921684	192.0.2.100	198.51.100.100	ICMP	102	0x9a3a (39482)	64 Echo (ping) request	id=0x0034, seq=2/512, ttl=64 (no res
	3 2022-08-07 19:50:08.924468	192.0.2.100	198.51.100.100	ICMP	102	0x9aa6 (39590)	64 Echo (ping) request	id=0x0034, seq=3/768, ttl=64 (no res
	4 2022-08-07 19:50:09.928484	192.0.2.100	198.51.100.100	ICMP	102	0x9afe (39678)	64 Echo (ping) request	id=0x0034, seq=4/1024, ttl=64 (no re
	5 2022-08-07 19:50:10.928245	192.0.2.100	198.51.100.100	ICMP	102	0x9b10 (39696)	64 Echo (ping) request	id=0x0034, seq=5/1280, ttl=64 (no re
	6 2022-08-07 19:50:11.929144	192.0.2.100	198.51.100.100	ICMP	102	0x9b34 (39732)	64 Echo (ping) request	id=0x0034, seq=6/1536, ttl=64 (no re
	7 2022-08-07 19:50:12.932943	192.0.2.100	198.51.100.100	ICMP	102	0x9b83 (39811)	64 Echo (ping) request	id=0x0034, seq=7/1792, ttl=64 (no re
	8 2022-08-07 19:50:13.934155	192.0.2.100	198.51.100.100	ICMP	102	0x9b8b (39819)	64 Echo (ping) request	id=0x0034, seq=8/2048, ttl=64 (no r€
	9 2022-08-07 19:50:14.932004	192.0.2.100	198.51.100.100	ICMP	102	0x9c07 (39943)	64 Echo (ping) request	id=0x0034, seq=9/2304, ttl=64 (no re
	10 2022-08-07 19:50:15.937143	192.0.2.100	198.51.100.100	ICMP	102	0x9cc6 (40134)	64 Echo (ping) request	id=0x0034, seq=10/2560, ttl=64 (no r
	11 2022-08-07 19:50:16.934848	192.0.2.100	198.51.100.100	ICMP	102	0x9d68 (40296)	64 Echo (ping) request	id=0x0034, seq=11/2816, ttl=64 (no r
	12 2022-08-07 19:50:17.936908	192.0.2.100	198.51.100.100	ICMP	102	0x9ded (40429)	64 Echo (ping) request	id=0x0034, seq=12/3072, ttl=64 (no r
	13 2022-08-07 19:50:18.939584	192.0.2.100	198.51.100.100	ICMP	102	0x9e5a (40538)	64 Echo (ping) request	id=0x0034, seq=13/3328, ttl=64 (no r
	14 2022-08-07 19:50:19.941262	192.0.2.100	198.51.100.100	ICMP	102	0x9efb (40699)	64 Echo (ping) request	id=0x0034, seq=14/3584, ttl=64 (no r
	15 2022-08-07 19:50:20.940716	192.0.2.100	198.51.100.100	ICMP	102	0x9f50 (40784)	64 Echo (ping) request	id=0x0034, seq=15/3840, ttl=64 (no r
	16 2022-08-07 19:50:21.940288	192.0.2.100	198.51.100.100	ICMP	102	0x9fe4 (40932)	64 Echo (ping) request	id=0x0034, seq=16/4096, ttl=64 (no r
	17 2022-08-07 19:50:22.943302	192.0.2.100	198.51.100.100	ICMP	102	0xa031 (41009)	64 Echo (ping) request	id=0x0034, seq=17/4352, ttl=64 (no r
	18 2022-08-07 19:50:23.944679	192.0.2.100	198.51.100.100	ICMP	102	0xa067 (41063)	64 Echo (ping) request	id=0x0034, seq=18/4608, ttl=64 (no r 🗸
<								>
En	ame 1: 102 bytes on wire (816 bits)	, 102 bytes capt	ured (816 bits)			0000 bc e7 12	34 9a 14 00 50 56 9d e8	be 08 00 45 00 ····4····P V·····E·
> Et	hernet II, Src: VMware 9d:e8:be (00	:50:56:9d:e8:be)	. Dst: Cisco 34:9a:	14 (bc:e7:12:	34:9a:14)	0010 00 54 98	10 40 00 40 01 b3 9c c0	00 02 64 c6 33 ·T··@·@· ·····d·3
> In	ternet Protocol Version 4, Src: 192	.0.2.100. Dst: 1	98.51.100.100		2	0020 64 64 08	00 c6 91 00 34 00 01 61	17 f0 62 00 00 dd · · · · 4 · · a · · b · ·
	ternet Control Message Protocol				2	0030 00 00 18	ec 08 00 00 00 00 00 10	11 12 13 14 15
						0040 16 17 18	19 1a 1b 1c 1d 1e 1f 20	21 22 23 24 25 !"#\$%
						0050 26 27 28	29 2a 2b 2c 2d 2e 2f 30	31 32 33 34 35 &'()*+,/012345
						0060 36 37 55	55 55 55	670000

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.

N	lo. Time	Source	Destination	Protocol	Length	PD	IP TTL Info		^
	1 2022-08-07 20:40:58.657533	192.0.2.100	198.51.100.100	ICMP	102	0x9296 (37526)	64 Echo (ping) request	id=0x0035, seq=1/256, ttl=64 (no re	s
	2 2022-08-07 20:40:59.658611	192.0.2.100	198.51.100.100	ICMP	102	0x9370 (37744)	64 Echo (ping) request	id=0x0035, seq=2/512, ttl=64 (no re	15
	3 2022-08-07 20:41:00.655662	192.0.2.100	198.51.100.100	ICMP	102	0x93f0 (37872)	64 Echo (ping) request	id=0x0035, seq=3/768, ttl=64 (no re	is in
	4 2022-08-07 20:41:01.659749	192.0.2.100	198.51.100.100	ICMP	102	0x946f (37999)	64 Echo (ping) request	id=0x0035, seq=4/1024, ttl=64 (no r	ie i
	5 2022-08-07 20:41:02.660624	192.0.2.100	198.51.100.100	ICMP	102	0x94a4 (38052)	64 Echo (ping) request	id=0x0035, seq=5/1280, ttl=64 (no r	ie i
	6 2022-08-07 20:41:03.663226	192.0.2.100	198.51.100.100	ICMP	102	0x952d (38189)	64 Echo (ping) request	id=0x0035, seq=6/1536, ttl=64 (no r	e i
	7 2022-08-07 20:41:04.661262	192.0.2.100	198.51.100.100	ICMP	102	0x958d (38285)	64 Echo (ping) request	id=0x0035, seq=7/1792, ttl=64 (no r	ie i
	8 2022-08-07 20:41:05.665955	192.0.2.100	198.51.100.100	ICMP	102	0x95d8 (38360)	64 Echo (ping) request	id=0x0035, seq=8/2048, ttl=64 (no r	ie i
	9 2022-08-07 20:41:06.666538	192.0.2.100	198.51.100.100	ICMP	102	0x964b (38475)	64 Echo (ping) request	id=0x0035, seq=9/2304, ttl=64 (no r	۰e
	10 2022-08-07 20:41:07.667298	192.0.2.100	198.51.100.100	ICMP	102	0x972b (38699)	64 Echo (ping) request	id=0x0035, seq=10/2560, ttl=64 (no	r
	11 2022-08-07 20:41:08.670540	192.0.2.100	198.51.100.100	ICMP	102	0x980a (38922)	64 Echo (ping) request	id=0x0035, seq=11/2816, ttl=64 (no	r
	12 2022-08-07 20:41:09.668278	192.0.2.100	198.51.100.100	ICMP	102	0x9831 (38961)	64 Echo (ping) request	id=0x0035, seq=12/3072, ttl=64 (no	r
	13 2022-08-07 20:41:10.672417	192.0.2.100	198.51.100.100	ICMP	102	0x98a2 (39074)	64 Echo (ping) request	id=0x0035, seq=13/3328, ttl=64 (no	r
	14 2022-08-07 20:41:11.671369	192.0.2.100	198.51.100.100	ICMP	102	0x98f7 (39159)	64 Echo (ping) request	id=0x0035, seq=14/3584, ttl=64 (no	r
	15 2022-08-07 20:41:12.675462	192.0.2.100	198.51.100.100	ICMP	102	0x99e4 (39396)	64 Echo (ping) request	id=0x0035, seq=15/3840, ttl=64 (no	r
	16 2022-08-07 20:41:13.674903	192.0.2.100	198.51.100.100	ICMP	102	0x9a84 (39556)	64 Echo (ping) request	id=0x0035, seq=16/4096, ttl=64 (no	r
	17 2022-08-07 20:41:14.674093	192.0.2.100	198.51.100.100	ICMP	102	0x9af3 (39667)	64 Echo (ping) request	id=0x0035, seq=17/4352, ttl=64 (no	r
	18 2022-08-07 20:41:15.676904	192.0.2.100	198.51.100.100	ICMP	102	0x9b8e (39822)	64 Echo (ping) request	id=0x0035, seq=18/4608, ttl=64 (no	r v
<								>	
	Frame 1: 102 bytes on wire (816 bits	), 102 bytes capt	ured (816 bits)			0000 bc e7 12	34 9a 2c 00 50 56 9d e8	be 08 00 45 00 ···4·, P V····E·	
	Ethernet II, Src: VMware 9d:e8:be (0	0:50:56:9d:e8:be)	, Dst: Cisco 34:9a:	2c (bc:e7:12:3	4:9a:2c)	0010 00 54 92	96 40 00 40 01 bb 16 c0	00 02 64 c6 33 ·T··@·@· ·····d·3	
	Internet Protocol Version 4, Src: 19	2.0.2.100, Dst: 1	98.51.100.100		_	0020 64 64 08	00 58 a8 00 35 00 01 4d	23 f0 62 00 00 dd · · X · · 5 · · M# · b · ·	
	Internet Control Message Protocol				2	0030 00 00 9e	c8 04 00 00 00 00 00 10	11 12 13 14 15	
L						0040 16 17 18	19 1a 1b 1c 1d 1e 1f 20	21 22 23 24 25 !"#\$%	
L						0050 26 27 28	29 2a 2b 2c 2d 2e 2f 30	31 32 33 34 35 &'()*+,/012345	
Т						0060 36 37 55	55 55 55	670000	

## Explication

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

Ce tableau récapitule la tâche :

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

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

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

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

Topologie, flux de paquets et points de capture

Secure Firewall 3100 :



Secure Firewall 4200 :

		Chassis				
	Internal Switch		Security Module			
	EH-17		FTD/ASA			
	RX					
192.0.2.100 ICMP echo-request		Uplink	inside			
198.51.100.100			outside			

# Configuration

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

1. Vérifiez le nom si :

<#root>		
>		
show nameif		
Interface	Name	Security
Ethernet1/1.205	inside	0
Ethernet1/2	outside	0

0

#### <#root>

>

show nameif

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

### 2. Créez une session de capture :

#### <#root>

>

capture capsw switch interface inside

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

#### <#root>

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

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

> capture capsw switch interface inside direction both

3. Activez la session de capture :

#### <#root>

> no capture capsw switch stop

### Vérification

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

<#root>	
>	
show capture capsw do	etail
Packet Capture info	
Name:	capsw
Session:	1
Admin State:	enabled
Oper State:	up
Oper State Reason:	Active
Config Success: Config Fail Reason Append Flag: Session Mem Usage: Session Pcap Snap Error Code: Drop Count:	yes : overwrite 256 Len: 1518 0 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 Filte	r Info
Name:	capsw-1-1
Protocol: Ivlan: Ovlan:	0 0 205

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

Total Physical breakout ports involved in Packet Capture: 0

46 packets captured on disk using switch capture

Reading of capture file from disk is not supported

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

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

```
<#root>
```

```
>
```

show capture capsw detail

#### Packet Capture info

Name:	capsw
Session:	1
Admin State:	enabled

Oper State: up

Oper State Reason: Active

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

Total Physical ports involved in Packet Capture: 2

Physical port:

Slot Id:	1
Port Id:	4
Pcapfile:	/mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-4-0.pcap
Pcapsize:	23442
Filter:	capsw-1-4
Packet Capture Fi	lter Info
Name:	capsw-1-4
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
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 Fi	lter Info
Name:	capsw-1-3
Protocol:	0
IVIAII.	0
Ovlan:	205
Src Ip:	0.0.0.0
Dest Ip:	0.0.0.0
Src Ipv6:	::
Dest Ipv6:	::
STC MAL: Dest MAC:	00:00:00:00:00
Src Port:	0
Dest Port:	0

```
Ethertype: 0
```

Total Physical breakout ports involved in Packet Capture: 0

49 packet captured on disk using switch capture

Reading of capture file from disk is not supported

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

```
<#root>
>
connect fxos
firewall#
connect local-mgmt
firewall(local-mgmt)#
show portchannel summary
Flags: D - Down
          P - Up in port-channel (members)
I - Individual H - Hot-standby (LACP only)
s - Suspended r - Module-removed
       R - Routed
S - Switched
U - Up (port-channel)
M - Not in use. Min-links not met
_____
Group Port- Type Protocol Member Ports
   Channel
_____
  Pol(U) Eth LACP Eth1/3(P) Eth1/4(P)
1
LACP KeepAlive Timer:
_____
   Channel PeerKeepAliveTimerFast
_____
  Po1(U)
1
         False
Cluster LACP Status:
      _____
   Channel ClusterSpanned ClusterDetach ClusterUnitID ClusterSysID
_____
  Po1(U) False False 0
1
                                 clust
```

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

Collecter les fichiers de capture

Suivez les étapes de la section Collecter les fichiers de capture internes du commutateur du parefeu sécurisé.

# Capturer l'analyse des fichiers

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

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

No	. Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info					^
-	1 2022-08-07 21:21:01.607187	192.0.2.100	198,51,100,100	ICMP	106	0x411f (1667	<ol> <li>64 Echo (ping)</li> </ol>	request	id=0x0037, seg=1	/256, ttl=64 (no	res	
	2 2022-08-07 21:21:02.609418	192.0.2.100	198.51.100.100	ICMP	106	0x413a (1669	<ol> <li>64 Echo (ping)</li> </ol>	request	id=0x0037, seg=2	/512, ttl=64 (no	res	
	3 2022-08-07 21:21:03.610671	192.0.2.100	198.51.100.100	ICMP	106	0x421a (1692	<ol> <li>64 Echo (ping</li> </ol>	request	id=0x0037, seq=3	/768, ttl=64 (no	res	
	4 2022-08-07 21:21:04.609160	192.0.2.100	198,51,100,100	ICMP	106	0x426c (1700	<ol> <li>64 Echo (ping)</li> </ol>	request	id=0x0037, seq=4	/1024. ttl=64 (no	OFE	
	5 2022-08-07 21:21:05.609409	192.0.2.100	198,51,100,100	ICMP	106	0x4310 (1716	<ol> <li>64 Echo (ping)</li> </ol>	request	id=0x0037, seq=5	/1280, ttl=64 (no	O FE	
	6 2022-08-07 21:21:06.611847	192.0.2.100	198,51,100,100	ICMP	106	0x43df (1737	5) 64 Echo (ping	request	id=0x0037, seq=6	/1536, ttl=64 (no	O FE	
	7 2022-08-07 21:21:07.616688	192.0.2.100	198,51,100,100	ICMP	106	0x44d3 (1761	9) 64 Echo (ping)	request	id=0x0037, seq=7	/1792, ttl=64 (no	O LE	
	8 2022-08-07 21:21:08.618023	192.0.2.100	198,51,100,100	ICMP	106	0x4518 (1768	<ol> <li>64 Echo (ping)</li> </ol>	request	id=0x0037, seq=8	/2048, ttl=64 (no	O LE	
	9 2022-08-07 21:21:09.619326	192.0.2.100	198,51,100,100	ICMP	106	0x453d (1772	5) 64 Echo (ping	request	id=0x0037, seq=9	/2304, ttl=64 (no	O FE	
	10 2022-08-07 21:21:10.616696	192.0.2.100	198,51,100,100	ICMP	106	0x462b (1796	<ol> <li>64 Echo (ping)</li> </ol>	request	id=0x0037, seg=1	0/2560, ttl=64 (	no r	
	11 2022-08-07 21:21:11.621629	192.0.2.100	198,51,100,100	ICMP	106	0x4707 (1818	<ol> <li>64 Echo (ping)</li> <li>64 Echo (ping)</li> </ol>	request	id=0x0037, seg=1	1/2816, ttl=64 (r	no r	
	12 2022-08-07 21:21:12.619309	192.0.2.100	198,51,100,100	ICMP	106	0x474b (1825	<ol> <li>64 Echo (ping)</li> </ol>	request	id=0x0037, seg=1	2/3072, ttl=64 (r	no r	
	13 2022-08-07 21:21:13.620168	192.0.2.100	198,51,100,100	ICMP	106	0x4781 (1830	5) 64 Echo (ping	request	id=0x0037, seg=1	3/3328, ttl=64 (r	no r	
	14 2022-08-07 21:21:14.623169	192.0.2.100	198,51,100,100	ICMP	106	0x4858 (1852	0) 64 Echo (ping)	request	id=0x0037, seg=1	4/3584, ttl=64 (	no r	
	15 2022-08-07 21:21:15.622497	192.0.2.100	198,51,100,100	ICMP	106	0x4909 (1869	7) 64 Echo (ping)	request	id=0x0037, seg=1	5/3840, ttl=64 (	no r	
	16 2022-08-07 21:21:16.626226	192.0.2.100	198,51,100,100	ICMP	106	0x490b (1869	<ol> <li>64 Echo (ping)</li> </ol>	request	id=0x0037, seg=1	6/4096, ttl=64 (	no r	
	17 2022-08-07 21:21:17.629363	192.0.2.100	198,51,100,100	ICMP	106	0x4932 (1873	<ol> <li>64 Echo (ping)</li> <li>64 Echo (ping)</li> </ol>	request	id=0x0037, seg=1	7/4352, ttl=64 (	no r	
	18 2022-08-07 21:21:18.626651	192.0.2.100	198,51,100,100	ICMP	106	0x4a05 (1894	<ol> <li>64 Echo (ping)</li> <li>64 Echo (ping)</li> </ol>	request	id=0x0037, seg=1	8/4608, ttl=64 (	no r	
<	TO LOLE OF OF EXTERIOR OF COM	10110121200	10010111001100		200		of cone (pang	request	a one of a	0,4000, 222 04 (	>	
	Free A. And hates an older (DAD hits	-) and hoter and	turned (one bits)			anna be	-7 42 24 05 44 00 50	FC od an	he 01 00 00 cd	4 D.V		
1	Frame 1: 106 Dytes on wire (848 Dits	s), 106 Dytes cap	Det: Gicco 24:0	2.14 /bc.c7	12.24.02.14	0000 00	e7 12 34 98 14 00 50 00 45 00 00 54 41 1f	10 00 40	De 81 00 00 C0			
1	Ethernet II, Src: VMware_90:08:De (	00:50:50:90:e8:De	e), DSC: CISCO_34:9	a:14 (bc:e/:	:12:34:98:14)	0020 02	64 66 33 64 64 08 00	06 67 00	37 00 01 b0 2c	·d·3dd·· · @.7···		
Ň	802.1Q VIPTUAI LAN, PKI: 0, DEI: 0,	IU: 205	14) (0)			0030 f0	62 00 00 00 00 8e fe	03 00 00	00 00 00 10 11	.b		
	000 = Priority: B	est Errort (dera	uit) (0)			0040 12	13 14 15 16 17 18 19	1a 1b 1c	1d 1e 1f 20 21		1	
		101e				0050 22	23 24 25 26 27 28 29	2a 2b 2c	2d 2e 2f 30 31	"#\$%&'() *+,/0	1	
	0000 1100 1101 = 1D: 205				2	0060 32	33 34 35 36 37 55 55	55 55		234567UU UU		
	Type: 1PV4 (0x0800)				-							
	Trailer: 5555555											
2	Internet Protocol Version 4, Src: 19	92.0.2.100, Dst:	198.51.100.100									
2	Internet Control Message Protocol											

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

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

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info		^
<b>_</b>	1 2022-08-07 21:21:01.607187	192.0.2.100	198.51.100.100	ICMP	106	0x411f (16671)	64 Echo (ping) request	id=0x0037, seq=1/256, ttl=64 (no res	
	2 2022-08-07 21:21:02.609418	192.0.2.100	198.51.100.100	ICMP	106	0x413a (16698)	64 Echo (ping) request	id=0x0037, seq=2/512, ttl=64 (no res	
	3 2022-08-07 21:21:03.610671	192.0.2.100	198.51.100.100	ICMP	106	0x421a (16922)	64 Echo (ping) request	id=0x0037, seq=3/768, ttl=64 (no res	
	4 2022-08-07 21:21:04.609160	192.0.2.100	198.51.100.100	ICMP	106	0x426c (17004)	64 Echo (ping) request	id=0x0037, seq=4/1024, ttl=64 (no re	
	5 2022-08-07 21:21:05.609409	192.0.2.100	198.51.100.100	ICMP	106	0x4310 (17168)	64 Echo (ping) request	id=0x0037, seq=5/1280, ttl=64 (no re	
	6 2022-08-07 21:21:06.611847	192.0.2.100	198.51.100.100	ICMP	106	0x43df (17375)	64 Echo (ping) request	id=0x0037, seq=6/1536, ttl=64 (no r€	
	7 2022-08-07 21:21:07.616688	192.0.2.100	198.51.100.100	ICMP	106	0x44d3 (17619)	64 Echo (ping) request	id=0x0037, seq=7/1792, ttl=64 (no r€	
	8 2022-08-07 21:21:08.618023	192.0.2.100	198.51.100.100	ICMP	106	0x4518 (17688)	64 Echo (ping) request	id=0x0037, seq=8/2048, ttl=64 (no re	
	9 2022-08-07 21:21:09.619326	192.0.2.100	198.51.100.100	ICMP	106	0x453d (17725)	64 Echo (ping) request	id=0x0037, seq=9/2304, ttl=64 (no r€	
	10 2022-08-07 21:21:10.616696	192.0.2.100	198.51.100.100	ICMP	106	0x462b (17963)	64 Echo (ping) request	id=0x0037, seq=10/2560, ttl=64 (no r	
	11 2022-08-07 21:21:11.621629	192.0.2.100	198.51.100.100	ICMP	106	0x4707 (18183)	64 Echo (ping) request	id=0x0037, seq=11/2816, ttl=64 (no r	
	12 2022-08-07 21:21:12.619309	192.0.2.100	198.51.100.100	ICMP	106	0x474b (18251)	64 Echo (ping) request	id=0x0037, seq=12/3072, ttl=64 (no r	
	13 2022-08-07 21:21:13.620168	192.0.2.100	198.51.100.100	ICMP	106	0x4781 (18305)	64 Echo (ping) request	id=0x0037, seq=13/3328, ttl=64 (no r	
	14 2022-08-07 21:21:14.623169	192.0.2.100	198.51.100.100	ICMP	106	0x4858 (18520)	64 Echo (ping) request	id=0x0037, seq=14/3584, ttl=64 (no r	
	15 2022-08-07 21:21:15.622497	192.0.2.100	198.51.100.100	ICMP	106	0x4909 (18697)	64 Echo (ping) request	id=0x0037, seq=15/3840, ttl=64 (no r	
	16 2022-08-07 21:21:16.626226	192.0.2.100	198.51.100.100	ICMP	106	0x490b (18699)	64 Echo (ping) request	id=0x0037, seq=16/4096, ttl=64 (no r	
	17 2022-08-07 21:21:17.629363	192.0.2.100	198.51.100.100	ICMP	106	0x4932 (18738)	64 Echo (ping) request	id=0x0037, seq=17/4352, ttl=64 (no r	
	18 2022-08-07 21:21:18.626651	192.0.2.100	198.51.100.100	ICMP	106	0x4a05 (18949)	64 Echo (ping) request	id=0x0037, seq=18/4608, ttl=64 (no r	×
<								>	
> En	ame 1: 106 bytes on wire (848 bits)	, 106 bytes capt	ured (848 bits)			0000 bc e7	12 34 9a 14 00 50 56 9d e8	be 81 00 00 cd 4 P V	
> Et	hernet II, Src: VMware_9d:e8:be (00	:50:56:9d:e8:be)	, Dst: Cisco_34:9a:	14 (bc:e7:12:	34:9a:14)	0010 08 00	45 00 00 54 41 1f 40 00 40	01 0c 8e c0 00 ··E··TA·@·@·····	
~ 80	2.1Q Virtual LAN, PRI: 0, DEI: 0, I	D: 205				0020 02 64	c6 33 64 64 08 00 06 67 00	37 00 01 b0 2c ·d·3dd·· ·g·7···,	
	000 Be: Priority: Be:	st Effort (defaul	lt) (0)			0030 f0 62	00 00 00 00 8e fe 03 00 00	00 00 00 10 11 ·b·····	
	0 = DEI: Ineligi	ble				0040 12 13	14 15 16 17 18 19 1a 1b 1c	1d 1e 1f 20 21	
	0000 1100 1101 = ID: 205				2	0050 22 23	24 25 26 27 28 29 28 20 20	20 20 27 30 31 #\$4& () -+,/01	
	Type: IPv4 (0x0800)				2	0000 32 33	34 33 30 37 33 33 33 33	23436700 00	
	Trailer: 55555555								
> In	Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100								
> In	ternet Control Message Protocol								
-									

Explication

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

Ce tableau récapitule la tâche :

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

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

# Capture de paquets sur des interfaces internes

Le pare-feu sécurisé 3100 dispose de 2 interfaces internes :

- in\_data\_uplink1 connecte l'application au commutateur interne.
- in\_mgmt\_uplink1 fournit un chemin de paquets dédié pour les connexions de gestion, telles

que SSH à l'interface de gestion, ou la connexion de gestion, également appelée sftunnel, entre le FMC et le FTD.

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

- in\_data\_uplink1 et in\_data\_uplink2 (4245 uniquement) : ces interfaces connectent l'application au commutateur interne. Dans le cas de la norme 4245, les paquets sont équilibrés en charge sur les deux interfaces de liaison ascendante.
- in\_mgmt\_uplink1 et in\_mgmt\_uplink2 ces interfaces fournissent un chemin de paquets dédié pour les connexions de gestion, telles que SSH vers l'interface de gestion, ou la connexion de gestion, également appelée sftunnel, entre le FMC et le FTD. Le pare-feu sécurisé 4200 prend en charge 2 interfaces de gestion.

# Tâche 1

Utilisez l'interface de ligne de commande FTD ou ASA pour configurer et vérifier une capture de paquets sur l'interface de liaison ascendante in\_data\_uplink1.

Topologie, flux de paquets et points de capture

Secure Firewall 3100 :



# Secure Firewall 4200 :



### Configuration

Procédez comme suit sur l'interface de ligne de commande ASA ou FTD pour configurer une capture de paquets sur l'interface in\_data\_uplink1 :

1. Créez une session de capture :

<#root>

>

```
capture capsw switch interface in_data_uplink1
```

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

### <#root>

```
> capture capsw switch interface in_data_uplink1 direction ?
```

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

> capture capsw switch interface in\_data\_uplink1 direction both

2.Activez la session de capture :

#### <#root>

> no capture capsw switch stop

### Vérification

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

<#root>

```
>
show capture capsw detail
```

Packet Capture info

Name: capsw Session: 1 Admin State: enabled Oper State: up Oper State Reason: Active Config Success: yes Config Fail Reason: Append Flag: overwrite Session Mem Usage: 256 Session Pcap Snap Len: 1518 Error Code: 0 Drop Count: 0 Total Physical ports involved in Packet Capture: 1 Physical port: Slot Id: 1 Port Id: 18 Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-data-uplink1.pcap Pcapsize: 7704 Filter: capsw-1-18 Packet Capture Filter Info Name: capsw-1-18 Protocol: 0 Ivlan: 0 Ovlan: 0 0.0.0.0 Src Ip: 0.0.0.0 Dest Ip: Src Ipv6: :: Dest Ipv6: :: 00:00:00:00:00:00 Src MAC: 00:00:00:00:00:00 Dest MAC: Src Port: 0 Dest Port: 0 0 Ethertype:

Total Physical breakout ports involved in Packet Capture: 0

66 packets captured on disk using switch capture

Reading of capture file from disk is not supported

Dans ce cas, une capture est créée sur l'interface avec un ID interne 18 qui est l'interface in\_data\_uplink1 sur le pare-feu sécurisé 3130. La commande show portmanager switch status dans l'interpréteur de commandes FXOS local-mgmt affiche les ID d'interface :

<#root>

>

...

connect fxos

firewall#

connect local-mgmt

firewall(local-mgmt)#

show portmanager switch status

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

0/36	n/a	Down	n/a	Full	N/A	Reset
,	,		,		,	

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

Collecter les fichiers de capture

Suivez les étapes de la section Collecter les fichiers de capture internes du commutateur du parefeu sécurisé.

### Capturer l'analyse des fichiers

Utilisez une application de lecture de fichiers de capture de paquets pour ouvrir les fichiers de capture pour l'interface in\_data\_uplink1. Dans cet exemple, les paquets capturés sur le pare-feu sécurisé 3100 sont analysés.

Vérifiez le point clé : dans ce cas, les paquets de requête et de réponse d'écho ICMP sont capturés. Il s'agit des paquets envoyés par l'application au commutateur interne.

No.	. Time 🚽	Source	Destination	Protocol	Length	IP ID	IP TTL Info	^
	1 2022-08-07 22:40:06.685606	192.0.2.100	198.51.100.100	ICMP	102	0x4d93 (19859)	64 Echo (ping) request	id=0x003a, seq=33/8448, ttl=64 (repl
4	2 2022-08-07 22:40:06.685615	198.51.100.100	192.0.2.100	ICMP	102	0x6cdc (27868)	64 Echo (ping) reply	id=0x003a, seq=33/8448, ttl=64 (requ
	3 2022-08-07 22:40:07.684219	192.0.2.100	198.51.100.100	1CMP	102	0x4de8 (19944)	64 Echo (ping) request	id=0x003a, seq=34/8704, ttl=64 (repl
	4 2022-08-07 22:40:07.689300	198.51.100.100	192.0.2.100	ICMP	102	0x6db2 (28082)	64 Echo (ping) reply	id=0x003a, seq=34/8704, ttl=64 (requ
	5 2022-08-07 22:40:08.685736	192.0.2.100	198.51.100.100	ICMP	102	0x4edc (20188)	64 Echo (ping) request	id=0x003a, seq=35/8960, ttl=64 (repl
	6 2022-08-07 22:40:08.690806	198.51.100.100	192.0.2.100	ICMP	102	0x6dbf (28095)	64 Echo (ping) reply	id=0x003a, seq=35/8960, ttl=64 (requ
	7 2022-08-07 22:40:09.690737	192.0.2.100	198.51.100.100	ICMP	102	0x4f2d (20269)	64 Echo (ping) request	id=0x003a, seq=36/9216, ttl=64 (repl
	8 2022-08-07 22:40:09.690744	198.51.100.100	192.0.2.100	ICMP	102	0x6e80 (28288)	64 Echo (ping) reply	id=0x003a, seq=36/9216, ttl=64 (requ
	9 2022-08-07 22:40:10.692266	192.0.2.100	198.51.100.100	ICMP	102	0x4fb1 (20401)	64 Echo (ping) request	id=0x003a, seq=37/9472, ttl=64 (repl
	10 2022-08-07 22:40:10.692272	198.51.100.100	192.0.2.100	ICMP	102	0x6ed5 (28373)	64 Echo (ping) reply	id=0x003a, seq=37/9472, ttl=64 (requ
	11 2022-08-07 22:40:11.691159	192.0.2.100	198.51.100.100	ICMP	102	0x5008 (20488)	64 Echo (ping) request	id=0x003a, seq=38/9728, ttl=64 (repl
	12 2022-08-07 22:40:11.691166	198.51.100.100	192.0.2.100	ICMP	102	0x6f3b (28475)	64 Echo (ping) reply	id=0x003a, seq=38/9728, ttl=64 (requ
	13 2022-08-07 22:40:12.692135	192.0.2.100	198.51.100.100	ICMP	102	0x50b8 (20664)	64 Echo (ping) request	id=0x003a, seq=39/9984, ttl=64 (repl
	14 2022-08-07 22:40:12.697209	198.51.100.100	192.0.2.100	ICMP	102	0x6fd7 (28631)	64 Echo (ping) reply	id=0x003a, seq=39/9984, ttl=64 (requ
	15 2022-08-07 22:40:13.697320	192.0.2.100	198.51.100.100	ICMP	102	0x5184 (20868)	64 Echo (ping) request	id=0x003a, seq=40/10240, ttl=64 (rep
	16 2022-08-07 22:40:13.697327	198.51.100.100	192.0.2.100	ICMP	102	0x703e (28734)	64 Echo (ping) reply	id=0x003a, seq=40/10240, ttl=64 (rec
	17 2022-08-07 22:40:14.698512	192.0.2.100	198.51.100.100	ICMP	102	0x51d8 (20952)	64 Echo (ping) request	id=0x003a, seq=41/10496, ttl=64 (rep
	18 2022-08-07 22:40:14.698518	198.51.100.100	192.0.2.100	ICMP	102	0x70dd (28893)	64 Echo (ping) reply	id=0x003a, seq=41/10496, ttl=64 (rec v
<								>
>	Frame 1: 102 bytes on wire (816 bits)	, 102 bytes capt	ured (816 bits)			0000 00 50 56	9d e7 50 bc e7 12 34 9a	15 08 00 45 00 ·PV··P·· ·4····E·
>	Ethernet II, Src: Cisco 34:9a:15 (bc:	e7:12:34:9a:15),	Dst: VMware 9d:e7:	50 (00:50:56:9	d:e7:50)	0010 00 54 4d	93 40 00 40 01 00 1a c0	00 02 64 c6 33 ·TM·@·@· ····d·3
>	Internet Protocol Version 4, Src: 192	.0.2.100, Dst: 19	98.51.100.100			0020 64 64 08	00 7f 15 00 3a 00 21 39	3f f0 62 00 00 dd
>	Internet Control Message Protocol					0030 00 00 8b	1a 05 00 00 00 00 00 10	11 12 13 14 15
						0040 16 17 18	3 19 1a 1b 1c 1d 1e 1f 20	21 22 23 24 25 !"#\$%
						0050 26 27 28	3 29 2a 2b 2c 2d 2e 2f 30	31 32 33 34 35 & ()*+,/012345
						0000 36 37 55		670000

### 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	in_data_uplink1	Aucune	Entrée uniquement*	Requêtes d'écho ICMP de l'hôte 192.0.2.100 vers l'hôte 198.51.100.100

ascendante in_data_uplink1		Réponses d'écho ICMP de l'hôte 198.51.100.100 à l'hôte 192.0.2.100
		I note 192.0.2.100

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

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 de connexions du plan de gestion sont capturés.

Topologie, flux de paquets et points de capture

Secure Firewall 3100 :



Secure Firewall 4200 :



# Configuration

Procédez comme suit sur l'interface de ligne de commande ASA ou FTD pour configurer une capture de paquets sur l'interface in\_mgmt\_uplink1 :

1. Créez une session de capture :

#### <#root>

>

capture capsw switch interface in\_mgmt\_uplink1

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

#### <#root>

```
> capture capsw switch interface in_mgmt_uplink1 direction ?
```

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

> capture capsw switch interface in\_mgmt\_uplink1 direction both

2. Activez la session de capture :

#### <#root>

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

# Vérification

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

### <#root>

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

Admin State: enabled

Oper State:	up
Oper State Reason:	Active
Config Success: Config Fail Reasor Append Flag: Session Mem Usage: Session Pcap Snap Error Code: Drop Count:	yes overwrite 256 Len: 1518 0 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: 1	37248
Filter:	capsw-1-19
Packet Capture Filte	r 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
Src Port:	0
Dest Port:	0
Ethertype:	0
Total Physical break	out ports involved in Packet Capture: 0
281 packets captured	on disk using switch capture

Reading of capture file from disk is not supported

Dans ce cas, une capture est créée sur l'interface avec un ID interne 19 qui est l'interface in\_mgmt\_uplink1 sur le pare-feu sécurisé 3130. La commande show portmanager switch status

dans l'interpréteur de commandes FXOS local-mgmt affiche les ID d'interface :

## <#root>

>

connect fxos

firewall#

connect local-mgmt

firewall(local-mgmt)#

show portmanager switch status

Dev/Port	Mode	Link 	Speed	Duplex	Loopback Mode	Port Manager
0/1	SGMII	Up	1G	Full	None	Link-Up
0/2	SGMII	Up	1G	Full	None	Link-Up
0/3	SGMII	Up	1G	Full	None	Link-Up
0/4	SGMII	Up	1G	Full	None	Link-Up
0/5	SGMII	Down	1G	Half	None	Mac-Link-Down
0/6	SGMII	Down	1G	Half	None	Mac-Link-Down
0/7	SGMII	Down	1G	Half	None	Mac-Link-Down
0/8	SGMII	Down	1G	Half	None	Mac-Link-Down
0/9	1000_BaseX	Down	1G	Full	None	Link-Down
0/10	1000_BaseX	Down	1G	Full	None	Link-Down
0/11	1000_BaseX	Down	1G	Full	None	Link-Down
0/12	1000_BaseX	Down	1G	Full	None	Link-Down
0/13	1000_BaseX	Down	1G	Full	None	Link-Down
0/14	1000_BaseX	Down	1G	Full	None	Link-Down
0/15	1000_BaseX	Down	1G	Full	None	Link-Down
0/16	1000_BaseX	Down	1G	Full	None	Link-Down
0/17	1000_BaseX	Up	1G	Full	None	Link-Up
0/18	KR2	Up	50G	Full	None	Link-Up
0/19	KR	Up	25G	Full	None	Link-Up
0/20	KR	lln	250	Fu]]	None	link-lln
0/20	KR4	Down	400	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	Ň/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 multicontexte, exécutez cette commande dans le contexte admin.

Collecter les fichiers de capture

Suivez les étapes de la section Collecter les fichiers de capture internes du commutateur du parefeu sécurisé .

# Capturer l'analyse des fichiers

Utilisez une application de lecture de fichiers de capture de paquets pour ouvrir les fichiers de capture pour l'interface in\_mgmt\_uplink1. Dans cet exemple, les paquets capturés sur le pare-feu sécurisé 3100 sont analysés.

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

No. Time	Source	Destination	Protocol	Length	IP ID		IP TTL Info	^
196 2022-08-07 23:21:45.133362	192.0.2.200	192.0.2.101	TCP	1518	0xb7d0	(47056)	64 39181 → 8305 [ACK] Seq=61372 Ack=875 Win=1384 Len=1448 TS	
197 2022-08-07 23:21:45.133385	192.0.2.200	192.0.2.101	TCP	1518	Øxb7d1	(47057)	64 39181 → 8305 [ACK] Seq=62820 Ack=875 Win=1384 Len=1448 TS	
198 2022-08-07 23:21:45.133388	192.0.2.200	192.0.2.101	TLSv1.2	990	Øxb7d2	(47058)	64 Application Data	
199 2022-08-07 23:21:45.928772	192.0.2.200	192.0.2.100	ICMP	78	Øxbd48	(48456)	64 Echo (ping) reply id=0x0001, seq=4539/47889, ttl=64	
200 2022-08-07 23:21:45.949024	192.0.2.200	192.0.2.101	TLSv1.2	128	0x4a97	(19095)	64 Application Data	
201 2022-08-07 23:21:45.949027	192.0.2.200	192.0.2.101	TCP	70	0x4a98	(19096)	64 8305 → 58885 [ACK] Seq=21997 Ack=26244 Win=4116 Len=0 TSv	
202 2022-08-07 23:21:46.019895	192.0.2.200	192.0.2.101	TLSv1.2	100	0x4a99	(19097)	64 Application Data	
203 2022-08-07 23:21:46.019899	192.0.2.200	192.0.2.101	TLSv1.2	96	0x4a9a	(19098)	64 Application Data	
204 2022-08-07 23:21:46.019903	192.0.2.200	192.0.2.101	TCP	70	0x4a9b	(19099)	64 8305 → 58885 [ACK] Seq=22053 Ack=26274 Win=4116 Len=0 TSv	
205 2022-08-07 23:21:46.019906	192.0.2.200	192.0.2.101	TCP	70	0x4a9c	(19100)	64 8305 → 58885 [ACK] Seq=22053 Ack=26300 Win=4116 Len=0 TSv	
206 2022-08-07 23:21:46.136415	192.0.2.200	192.0.2.101	TCP	70	Øxb7d3	(47059)	64 39181 → 8305 [ACK] Seq=65188 Ack=921 Win=1384 Len=0 TSval	
207 2022-08-07 23:21:46.958148	192.0.2.200	192.0.2.100	ICMP	78	Øxbd9e	(48542)	64 Echo (ping) reply id=0x0001, seq=4540/48145, ttl=64	
208 2022-08-07 23:21:47.980409	192.0.2.200	192.0.2.100	ICMP	78	Øxbdf2	(48626)	64 Echo (ping) reply id=0x0001, seq=4541/48401, ttl=64	
209 2022-08-07 23:21:48.406312	192.0.2.200	192.0.2.101	TCP	70	0x4a9d	(19101)	64 8305 → 58885 [ACK] Seq=22053 Ack=26366 Win=4116 Len=0 TSv	
210 2022-08-07 23:21:48.903236	192.0.2.200	192.0.2.101	TLSv1.2	747	0x4a9e	(19102)	64 Application Data	
211 2022-08-07 23:21:48.994386	192.0.2.200	192.0.2.100	ICMP	78	Øxbe48	(48712)	64 Echo (ping) reply id=0x0001, seq=4542/48657, ttl=64	
212 2022-08-07 23:21:50.008576	192.0.2.200	192.0.2.100	ICMP	78	Øxbea6	(48806)	64 Echo (ping) reply id=0x0001, seq=4543/48913, ttl=64	
213 2022-08-07 23:21:50.140167	192.0.2.200	192.0.2.101	TCP	1518	0xb7d4	(47060)	64 39181 → 8305 [ACK] Seq=65188 Ack=921 Win=1384 Len=1448 TS	
214 2022-08-07 23:21:50.140171	192.0.2.200	192.0.2.101	TCP	1518	Øxb7d5	(47061)	64 39181 → 8305 [ACK] Seq=66636 Ack=921 Win=1384 Len=1448 TS	
215 2022-08-07 23:21:50.140175	192.0.2.200	192.0.2.101	TLSv1.2	990	0xb7d6	(47062)	64 Application Data	
216 2022-08-07 23:21:51.015884	192.0.2.200	192.0.2.100	ICMP	78	Øxbec1	(48833)	64 Echo (ping) reply id=0x0001, seq=4544/49169, ttl=64	
217 2022-08-07 23:21:51.142842	192.0.2.200	192.0.2.101	TCP	70	0xb7d7	(47063)	64 39181 → 8305 [ACK] Seq=69004 Ack=967 Win=1384 Len=0 TSval	
218 2022-08-07 23:21:52.030118	192.0.2.200	192.0.2.100	ICMP	78	0xbf02	(48898)	64 Echo (ping) reply id=0x0001, seq=4545/49425, ttl=64	
219 2022-08-07 23:21:53.042744	192.0.2.200	192.0.2.100	ICMP	78	0xbf59	(48985)	64 Echo (ping) reply id=0x0001, seq=4546/49681, ttl=64	
220 2022-08-07 23:21:53.073144	192.0.2.200	192.0.2.100	SSH	170	0xad34	(44340)	64 Server: Encrypted packet (len=112)	
221 2022-08-07 23:21:53.194906	192.0.2.200	192.0.2.100	TCP	64	Øxad35	(44341)	64 22 → 53249 [ACK] Seq=1025 Ack=881 Win=946 Len=0	
222 2022-08-07 23:21:53.905480	192.0.2.200	192.0.2.101	TLSv1.2	747	0x4a9f	(19103)	64 Application Data	
223 2022-08-07 23:21:54.102899	192.0.2.200	192.0.2.100	ICMP	78	0xbf63	(48995)	64 Echo (ping) reply id=0x0001, seq=4547/49937, ttl=64	
224 2022-08-07 23:21:54.903675	192.0.2.200	192.0.2.101	TCP	70	0x4aa0	(19104)	64 8305 → 58885 [ACK] Seq=23407 Ack=26424 Win=4116 Len=0 TSv	١.
175 7077 00 07 72:71.55 126700	103 0 3 300	103 0 3 100	TCMD	70	Avhfc1	(10000)	Aleft+ CO103/0424-003 100000-14 vinon (0010) 43-64	
Ename 1: 747 bytes on wire (5976 bits	s). 747 bytes can	tured (5976 hi	ts)		0000	a4 53 0e	11 38 2a bc e7 12 34 9a 00 08 00 45 00 ·S··8*·· ·4····E·	-
> Ethernet II. Src: Cisco 34:9a:00 (hc)	e7:12:34:9a:00)	Dst: Cisco 11	:38:2a (a4:53:0e:11	·38:2a)	0010	02 d9 4a	a 3d 40 00 40 06 68 b4 c0 00 02 c8 c0 00 · J=@·@· h·····	Î
> Internet Protocol Version 4, Src: 192	2.0.2.200. Dst: 1	92.0.2.101	150120 (04155100111		0020	02 65 20	0 71 e6 05 67 1b 2a c5 db e3 6b d4 80 18 ·e q··g·*···k···	
> Transmission Control Protocol, Src Po	ort: 8305, Dst Po	rt: 58885, Sea	: 1. Ack: 1. Len: 6	77	0030	10 14 27	7 cc 00 00 01 01 08 0a 08 76 95 7f 91 02 ···································	
> Transport Laver Security			,		0040	3d 41 17	7 03 03 02 a0 22 6a 01 e0 ff cc 98 f9 af =A·····" j······	
, mansport cayer secondly					0050	07 40 75	5 19 a4 d5 df 64 d8 fe 66 8e 9b cc 8d 2f -@u····d ··f····/	
					0060	92 b2 1a	a 64 e7 20 36 03 8e 48 02 5a 7c 85 30 d4 ···d·6··H·Z 0·	
					0070	ta c0 a8	3 56 b8 ad a7 7e 19 3a c1 9c 4b 57 0e e0 ···V···~ ·:··KW··	
					0800	0e et 95	22 84 CI CI 90 97 24 78 04 15 1C 44 00 ································	
					0090	2f 86 73	8 8f b1 e1 b5 c6 57 e3 a8 46 9e cb 26 b7 / s W.E&	
					00b0	5b c7 e3	3 09 54 f3 c1 ff 26 d9 87 ea 51 3d 20 08 [T &O=	
					0000	16 fd cb	o f5 4f 91 98 5e 86 15 17 55 68 6f 5d 040^Uho].	
								Y

# 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	Direction	Trafic capturé
-------------------------------	-----------	----------------

		interne		
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 via le commutateur interne)	Réponses d'écho ICMP de l'adresse IP de gestion FTD 192.0.2.200 à l'hôte 192.0.2.100 Sftunnel de l'adresse IP de gestion FTD 192.0.2.200 à l'adresse IP FMC 192.0.2.101 SSH de l'adresse IP de gestion FTD 192.0.2.200 vers l'hôte 192.0.2.100

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

# Filtres de capture de paquets

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

# Configuration

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

1. Vérifiez le nom si :

### <#root>

```
>
```

```
show nameif
```

Interface	Name	Security
Ethernet1/1	inside	0
Ethernet1/2 Management1/1	outside diagnostic	0 0

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

### <#root>

```
>
```

capture capsw switch interface inside ethernet-type arp

#### <#root>

> capture capsw switch interface inside match icmp 198.51.100.100

### Vérification

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

<#root>

```
> show capture capsw detail
```

Packet Capture info

Name:

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		

capsw

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 O packet captured on disk using switch capture Reading of capture file from disk is not supported

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

#### <#root>

```
>
```

show capture capsw detail

Packet Capture info

Name:

capsw

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

Total Physical ports involved in Packet Capture: 1

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

Filter: capsw-1-1

Packet Capture Filter Info

Name:	capsw-1-1	
Protocol:	1	
Ivlan: Ovlan:	0 0	
Src Ip:	198.51.100.100	
Dest Ip: Src Ipv6: Dest Ipv6: Src MAC: Dest MAC: Src Port: Dest Port: Ethertype:	0.0.0.0 :: :: 00:00:00:00:00:00 00:00:00:00:00:00 0 0 0	
Total Physical bro	eakout ports involved in Packet Capture: O	
0 packets capture	d on disk using switch capture	

Reading of capture file from disk is not supported

Collecter les fichiers de capture internes du commutateur Secure Firewall

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

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

Dans le cas des interfaces port-channel, assurez-vous de collecter les fichiers de capture de paquets à partir de toutes les interfaces membres.

# ASA

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

1. Arrêtez la capture :

# <#root>

asa#

capture capsw switch stop

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

<#root>		
asa#		
show capture capsw	detail	
Packet Capture info		
Name:	capsw	
Session:	1	
Admin State:	disabled	
Oper State:	down	
Oper State Reason	: Session_Admin_Shut	
Config Success: Config Fail Reaso Append Flag: Session Mem Usage Session Pcap Snap Error Code: Drop Count:	yes n: overwrite : 256 Len: 1518 0 0	
Total Physical port	s involved in Packet Capture: 1	
Physical port: Slot Id: Port Id: Pcapfile:	1 1	
/mnt/disk0/packet-capture/		
sess-1-capsw-ethern	et-1-1-0.pcap	
Pcapsize: Filter:	139826 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	
Dest MAC:	00:00:00:00:00	
Src Port:	0	
Dest Port:	0	
Ethertype:	0	
Total Physical	breakout ports involved in Packet Capture:	0

886 packets captured on disk using switch capture Reading of capture file from disk is not supported

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

#### <#root>

#### asa#

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

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

#### asa#

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

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

139826 bytes copied in 0.532 secs

### FTD

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

l'interface de ligne de commande FTD et les copier sur des serveurs accessibles via des interfaces de données ou de diagnostic :

1. Accédez à la CLI de diagnostic :

```
<#root>
```

```
>
```

```
system support diagnostic-cli
```

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

firepower>

enable

Password:

<-- Enter

firepower#

2. Arrêtez la capture :

#### <#root>

firepower#

capture capi switch stop

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

### <#root>

firepower#

show capture capsw detail

Packet Capture info

Name: capsw

Session: 1

Admin State: disabled

Oper State 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 0.0.0.0 Src Ip: Dest Ip: 0.0.0.0 Src Ipv6: :: Dest Ipv6: :: 00:00:00:00:00:00 Src MAC: Dest MAC: 00:00:00:00:00:00 Src Port: 0 Dest Port: 0 Ethertype: 0 Total Physical breakout ports involved in Packet Capture: 0 886 packets captured on disk using switch capture Reading of capture file from disk is not supported

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

<#root>

firepower#

Oper State:

down

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

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

firepower#

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

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

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

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

1. Arrêtez la capture :

<#root>

>

capture capsw switch stop

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

### <#root>

Admin State:

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

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 0 Ethertype: Total Physical breakout ports involved in Packet Capture: 0 886 packets captured on disk using switch capture Reading of capture file from disk is not supported 3. Passez en mode expert et passez en mode racine :

<#root>

>

expert

admin@firepower:~\$

sudo su

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

#### <#root>

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

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



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

Firewall Management Center Devices / Troubleshoot / File Download	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	, Q	¢	¢	0	lab_domain \ admin \	cisco	SECURE
								Thr	eat De	fense (	СЦ	Packet Capture	Packe	t Tracer
		Device FPR3100-1 File	1	¥										
		sess-1-ca	psw-ethernet	-1-1-0.pcap										
		Back Download												

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

Lignes directrices et limites :

- Plusieurs sessions de configuration de capture de commutateur sont prises en charge, mais une seule session de capture de commutateur peut être active à la fois. Une tentative d'activation de 2 sessions de capture ou plus génère l'erreur « ERROR : Failed to enable session, as limit of maximum 1 active packet capture sessions reaché ».
- Impossible de supprimer une capture de commutateur active.
- Impossible de lire les captures de commutateur sur l'application. L'utilisateur doit exporter les fichiers.
- Certaines options de capture de plan de données, telles que dump, decode, packet-number, trace et autres, ne sont pas prises en charge pour les captures de commutateur.
- Dans le cas de l'ASA multicontexte, les captures du commutateur sur les interfaces de données sont configurées dans des contextes utilisateur. Les captures du commutateur sur les interfaces in\_data\_uplink1 et in\_mgmt\_uplink1 sont prises en charge uniquement dans le contexte admin.

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

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

# Informations connexes

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