Configurazione e verifica delle acquisizioni dello switch interno Secure Firewall e Firepower

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Premesse
Panoramica di alto livello dell'architettura del sistema
Panoramica generale delle operazioni dello switch interno
Flusso di pacchetti e punti di acquisizione
Configurazione e verifica su Firepower 4100/9300
Acquisizione dei pacchetti su un'interfaccia fisica o su un canale della porta
Acquisizioni di pacchetti su interfacce backplane
Acquisizione di pacchetti su porte applicazioni e porte applicazioni
Acquisizione di pacchetti su una sottointerfaccia di un'interfaccia fisica o di un canale della porta
Filtri di acquisizione pacchetti
Raccolta Dei File Di Acquisizione Dello Switch Interno Firepower 4100/9300
Linee guida, limitazioni e best practice per l'acquisizione di pacchetti di switch interni
Configurazione e verifica su Secure Firewall 3100/4200
Acquisizione dei pacchetti su un'interfaccia fisica o su un canale della porta
Acquisizione di pacchetti su una sottointerfaccia di un'interfaccia fisica o di un canale della porta
Acquisizione pacchetti su interfacce interne
Filtri di acquisizione pacchetti
Raccogli file di acquisizione switch interno Secure Firewall
Linee guida, limitazioni e best practice per l'acquisizione di pacchetti di switch interni
Informazioni correlate

Introduzione

In questo documento viene descritta la configurazione e la verifica di Firepower e delle acquisizioni dello switch interno Secure Firewall.

Prerequisiti

Requisiti

Conoscenze base dei prodotti, analisi delle acquisizioni.

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Secure Firewall 31xx, 42xx
- Firepower 41xx
- Firepower 93xx
- Cisco Secure eXtensible Operating System (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
- Adaptive Security Appliance (ASA) 9.18(1)x, 9.20(x)
- Wireshark 3.6.7 (<u>https://www.wireshark.org/download.html</u>)

Premesse

Panoramica di alto livello dell'architettura del sistema

Dal punto di vista del flusso dei pacchetti, l'architettura di Firepower 4100/9300 e Secure Firewall 3100/4200 può essere visualizzata come mostrato nella seguente figura:



Lo chassis comprende i seguenti componenti:

• Switch interno: inoltra il pacchetto dalla rete all'applicazione e viceversa. Lo switch interno è collegato alle interfacce anteriori che risiedono sul modulo di interfaccia incorporato o sui moduli di rete esterni e si connette a dispositivi esterni, ad esempio switch. Esempi di

interfacce anteriori sono Ethernet 1/1, Ethernet 2/4 e così via. Il "fronte" non è una definizione tecnica forte. In questo documento viene usato per distinguere le interfacce collegate a dispositivi esterni dal backplane o dalle interfacce uplink.

- Backplane o uplink: interfaccia interna che connette il modulo di sicurezza (SM) allo switch interno.
- Uplink di gestione: un'interfaccia interna esclusiva di Secure Firewall 3100/4200 che fornisce il percorso del traffico di gestione tra lo switch interno e l'applicazione.

Nella tabella seguente vengono mostrate le interfacce backplane su Firepower 4100/9300 e le interfacce uplink su Secure Firewall 3100/4200:

Piattaforma	Numero di moduli di sicurezza supportati	Interfacce backplane/uplink	Interfacce uplink di gestione	Interfacce applicazione mappate
Firepower 4100 (ad eccezione di Firepower 4110/4112)	1	SM1: Ethernet 1/9 Ethernet 1/10	N/D	Dati interni0/0 Dati interni0/1
Firepower 4110/4112	1	Ethernet 1/9	N/D	Dati interni0/0 Dati interni0/1
Firepower 9300	3	SM1: Ethernet 1/9 Ethernet 1/10 SM2: Ethernet 1/11 Ethernet 1/12 SM3 Ethernet 1/13 Ethernet 1/14	N/D	Dati interni0/0 Dati interni0/1 Dati interni0/0 Dati interni0/1 Dati interni0/1 Dati interni0/1
Secure Firewall 3100	1	SM1: in_data_uplink1	in_mgmt_uplink1	Dati interni0/1

				Gestione1/1
Secure Firewall 4200	1	SM1: in_data_uplink1 SM1: in_data_uplink2 (solo 4245)	in_mgmt_uplink1 in_mgmt_uplink2	Dati interni0/1 Dati interni0/2 (solo 4245) Gestione1/1 Gestione1/2

Nel caso in cui Firepower 4100/9300 con 2 interfacce backplane per modulo o Secure Firewall 4245 con 2 interfacce di uplink dati, lo switch interno e le applicazioni sui moduli eseguono il bilanciamento del carico del traffico sulle 2 interfacce.

- Modulo di sicurezza, motore di sicurezza o blade : il modulo in cui sono installate applicazioni quali FTD o ASA. Firepower 9300 supporta fino a 3 moduli di sicurezza.
- Mapped application interface: nomi delle interfacce backplane o uplink nelle applicazioni, ad esempio FTD o ASA.

Utilizzare il comando show interface detail per verificare le interfacce interne:

```
<#root>
>
show interface detail | grep Interface
Interface Internal-Control0/0 "ha_ctl_nlp_int_tap", is up, line protocol is up
 Control Point Interface States:
        Interface number is 6
        Interface config status is active
        Interface state is active
Interface Internal-Data0/0 "", is up, line protocol is up
 Control Point Interface States:
        Interface number is 2
        Interface config status is active
        Interface state is active
Interface Internal-Data0/1 "", is up, line protocol is up
 Control Point Interface States:
        Interface number is 3
        Interface config status is active
        Interface state is active
Interface Internal-Data0/2 "nlp_int_tap", is up, line protocol is up
 Control Point Interface States:
        Interface number is 4
        Interface config status is active
       Interface state is active
```

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

Panoramica generale delle operazioni dello switch interno

Firepower 4100/9300

Per prendere una decisione di inoltro, lo switch interno usa un tag interface VLAN, o tag port VLAN, e un tag virtual network (VN-tag).

Il tag port VLAN viene usato dallo switch interno per identificare un'interfaccia. Lo switch inserisce il tag VLAN della porta in ciascun pacchetto in entrata inviato sulle interfacce anteriori. Il tag VLAN viene configurato automaticamente dal sistema e non può essere modificato manualmente. Il valore del tag può essere controllato nella shell dei comandi 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

Il tag VN viene inoltre inserito dallo switch interno e utilizzato per inoltrare i pacchetti all'applicazione. Viene configurato automaticamente dal sistema e non può essere modificato manualmente.

Il tag VLAN della porta e il tag VN vengono condivisi con l'applicazione. L'applicazione inserisce i rispettivi tag VLAN dell'interfaccia in uscita e i tag VN in ciascun pacchetto. Quando uno switch interno riceve un pacchetto dall'applicazione sulle interfacce del backplane, lo switch legge il tag VLAN dell'interfaccia in uscita e il tag VN, identifica l'applicazione e l'interfaccia in uscita, rimuove il tag VLAN della porta e il tag VN, quindi inoltra il pacchetto alla rete.

Secure Firewall 3100/4200

Come in Firepower 4100/9300, il tag della porta VLAN viene usato dallo switch interno per identificare un'interfaccia.

Il tag della porta VLAN è condiviso con l'applicazione. L'applicazione inserisce i rispettivi tag VLAN dell'interfaccia in uscita in ciascun pacchetto. Quando uno switch interno riceve un pacchetto dall'applicazione sull'interfaccia uplink, lo switch legge il tag dell'interfaccia VLAN in uscita, identifica l'interfaccia in uscita, rimuove il tag della porta VLAN e inoltra il pacchetto alla rete.

Flusso di pacchetti e punti di acquisizione

Firepower 4100/9300 e Secure Firewall 3100

I firewall Firepower 4100/9300 e Secure Firewall 3100 supportano le acquisizioni di pacchetti sulle interfacce dello switch interno.

La figura mostra i punti di acquisizione del pacchetto lungo il percorso del pacchetto all'interno dello chassis e dell'applicazione:



I punti di acquisizione sono:

- 1. Punto di acquisizione in entrata interfaccia anteriore switch interno. Un'interfaccia anteriore è un'interfaccia connessa ai dispositivi peer, ad esempio gli switch.
- 2. Punto di acquisizione in entrata interfaccia piano dati
- 3. Punto di acquisizione snort
- 4. Punto di acquisizione uscita interfaccia piano dati
- 5. Punto di acquisizione in entrata uplink o backplane interno dello switch. Un'interfaccia di backplane o uplink collega lo switch interno all'applicazione.

Lo switch interno supporta solo le acquisizioni dell'interfaccia in entrata. In questo modo, è possibile acquisire solo i pacchetti ricevuti dalla rete o dall'applicazione ASA/FTD. Le acquisizioni di pacchetti in uscita non sono supportate.

Secure Firewall 4200

I firewall Secure Firewall 4200 supportano le acquisizioni di pacchetti sulle interfacce dello switch interno. La figura mostra i punti di acquisizione del pacchetto lungo il percorso del pacchetto all'interno dello chassis e dell'applicazione:



I punti di acquisizione sono:

- 1. Punto di acquisizione in entrata interfaccia anteriore switch interno. Un'interfaccia anteriore è un'interfaccia connessa ai dispositivi peer, ad esempio gli switch.
- 2. Punto di cattura dell'uscita dell'interfaccia del backplane dello switch interno.
- 3. Punto di acquisizione in entrata interfaccia piano dati
- 4. Punto di acquisizione snort
- 5. Punto di acquisizione uscita interfaccia piano dati
- 6. Punto di acquisizione in entrata uplink o backplane interno dello switch. Un'interfaccia di backplane o uplink collega lo switch interno all'applicazione.
- 7. Punto di acquisizione uscita interfaccia anteriore switch interno.

Lo switch interno supporta facoltativamente le acquisizioni bidirezionali in entrata e in uscita. Per impostazione predefinita, lo switch interno cattura i pacchetti in entrata.

Configurazione e verifica su Firepower 4100/9300

Le acquisizioni dello switch interno Firepower 4100/9300 possono essere configurate in Strumenti > Packet Capture su FCM o in Scope Packet Capture nella CLI di FXOS. Per la descrizione delle opzioni di acquisizione dei pacchetti, consultare la guida alla configurazione di Cisco Firepower 4100/9300 FXOS Chassis Manager o la guida alla configurazione della CLI di Cisco Firepower 4100/9300 FXOS, capitolo Risoluzione dei problemi, sezione Acquisizione pacchetti.

In questi scenari vengono illustrati i casi di utilizzo comuni delle acquisizioni dello switch interno Firepower 4100/9300.

Acquisizione dei pacchetti su un'interfaccia fisica o su un canale della porta

Usare FCM e CLI per configurare e verificare l'acquisizione di un pacchetto sull'interfaccia Ethernet1/2 o Portchannel1. Nel caso di un'interfaccia di canale della porta, assicurarsi di selezionare tutte le interfacce membro fisiche.

Topologia, flusso dei pacchetti e punti di acquisizione



Configurazione

FCM

Per configurare l'acquisizione di un pacchetto sulle interfacce Ethernet1/2 o Portchannel1, eseguire la procedura seguente su FCM:

1. Utilizzare Strumenti > Acquisizione pacchetti > Acquisisci sessione per creare una nuova sessione di acquisizione:

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

2. Selezionare l'interfaccia Ethernet1/2, fornire il nome della sessione e fare clic su Save and Run (Salva ed esegui) per attivare l'acquisizione:

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		
Ebeneti/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	r Capture All	
Ethernet1/5 (Portchannels)			
Ethernet1/4 (Portchannel3)			

3. Nel caso di un'interfaccia di canale della porta, selezionare tutte le interfacce fisiche, fornire il

nome della sessione e fare clic su Save and Run per attivare l'acquisizione:

Overview Interfaces Logical Devices Security Engine Platform Settings					System Tools Help admin
Select an instance: ftd1 💌			Save and Run	Save Can	cel
ftd1	Session Name* Selected Interfaces	Cap1 Ethernet1/5, Ethernet1/4			
Eberset1/2	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					
Ethernet1/4 (Portchannels)					

CLI FXOS

Attenersi alla seguente procedura dalla CLI di FXOS per configurare l'acquisizione di un pacchetto sulle interfacce Ethernet1/2 o Portchannel1:

1. Identificare il tipo di applicazione e l'identificatore:

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

2. Nel caso di un'interfaccia porta-canale, identificare le relative interfacce membro:

<#root>

firepower#

connect fxos

<output skipped>
firepower(fxos)#

show port-channel summary

Flags	: D - Down	I	P - Up in port-channel (members)								
	I - Indiv	/idual I	H - Hot-stan	dby (LACP on	ly)						
	s – Suspe	ended	r - Module-removed								
	S - Switc	hed I	R – Routed								
	U – Up (p	ort-chai	nnel)								
	M - Not i	in use. I	Min-links no	t met							
Group	Port- Channel	Туре	Protocol	Member Port	 S						
1	Pol(SU)	Eth	LACP	Eth1/4(P)	Eth1/5(P)						

3. Creare una sessione di acquisizione:

```
<#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 #

Per le interfacce port-channel, viene configurata un'acquisizione separata per ciascuna interfaccia membro:

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

firepower /packet-capture/session #

Verifica

FCM

Verificare il nome dell'interfaccia, verificare che lo stato operativo sia attivo e che le dimensioni del file (in byte) aumentino:

Overview	Interfaces	Logical Devices	Security Engine	Platform Settings					System	Tools	Help	admin
Capture Ses	sion Filter Li	st										
								C Refresh Capture	Session Delete Al	Sessions		
•	cap1	Drop Coun	t: 0	Operational State: up		Buffer Size: 256 MB		Snap Length: 1518	Bytes		4	
Interface Na	ame	Filter		File Size (in byte)	File Name	Device Name					
Ethernet1/2		None		28632		cap1-ethernet-1-2-0.pcap	ftd1		\pm			

Portchannel1 con interfacce membro Ethernet1/4 ed Ethernet1/5:

Overview Interfaces Le	ogical Devices Security Engine Platform	Settings				System Tools Help admin				
Capture Session Filter List	Capture Session Rer Lst									
					C Refresh Capture Session	Delete All Sessions				
ap1 cap1	Drop Count: 0	Operational State: up	Buffer	Size: 256 MB	Snap Length: 1518 Bytes					
Interface Name	Filter	File Size (in	bytes) File Name	Device Name						
Ethernet1/S	None	160	cap1-ethernet-1-5-0.	pcap ftd1	~] [(*					
Ethernet1/4	None	85000	cap1-ethernet-1-4-0.	pcap ftd1	⊻					

CLI FXOS

Verificare i dettagli di acquisizione nell'ambito 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 con interfacce membro Ethernet1/4 ed Ethernet1/5:

<#root>

firepower#

scope packet-capture

firepower /packet-capture #

show session cap1

Traffic Monitoring Session:

Packet Capture Session Name: cap1

Session: 1

Admin State: Enabled

Oper State: Up

```
Config Success: Yes
    Config Fail Reason:
   Append Flag: Overwrite
    Session Mem Usage: 256 MB
    Session Pcap Snap Len: 1518 Bytes
    Error Code: 0
   Drop Count: 0
Physical ports involved in Packet Capture:
Slot Id: 1
   Port Id: 4
   Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-4-0.pcap
   Pcapsize: 310276 bytes
    Filter:
    Sub Interface: 0
   Application Instance Identifier: ftd1
   Application Name: ftd
slot Id: 1
   Port Id: 5
   Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-5-0.pcap
   Pcapsize: 160 bytes
    Filter:
    Sub Interface: 0
   Application Instance Identifier: ftd1
   Application Name: ftd
```

Oper State Reason: Active

Raccogli file di acquisizione

Eseguire i passaggi descritti nella sezione Raccolta dei file di acquisizione degli switch interni Firepower 4100/9300.

Analisi dei file di acquisizione

Utilizzare un'applicazione per la lettura dei file di acquisizione dei pacchetti per aprire il file di acquisizione per Ethernet1/2. Selezionare il primo pacchetto e controllare i punti chiave:

- 1. Vengono acquisiti solo i pacchetti di richiesta echo ICMP. Ogni pacchetto viene acquisito e mostrato 2 volte.
- 2. L'intestazione del pacchetto originale è senza il tag VLAN.
- 3. Lo switch interno inserisce un tag VLAN 102 aggiuntivo che identifica l'interfaccia in entrata Ethernet 1/2.
- 4. Lo switch interno inserisce un tag VN aggiuntivo.

No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info		
E.	1 2022-07-13 06:23:58.285080930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (48428)	64 Echo (ping) requ	uest	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) requ	uest	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) req	uest	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) requ	uest	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) requ	uest	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) requ	uest	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) requ	uest	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) requ	uest	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) requ	uest	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) requ	uest	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) requ	uest	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) requ	uest	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) requ	uest	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) requ	uest	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) requ	uest	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) requ	uest	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) requ	uest	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) requ	uest	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) requ	uest	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) requ	uest	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) requ	uest	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) requ	uest	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) requ	uest	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) requ	uest	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) requ	uest	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) requ	uest	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) requ	uest	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) requ	uest	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) requ	uest	id=0x001a, seq=21/5376, ttl=64 (no response found!)
<									and the first of the state
5 E	name 1: 100 butes on wine (964 bit	c) 100 bytes (antured (064 bits)	on interface (anture u	a 1 id a			a 58 07 hd ha 77 as as 50 56 od as ha sa 26 89 as X D V &
11	rame 1: 108 bytes on wire (864 bit	s), 108 bytes o	aptured (864 bits)	on incertace o	apture_u	0_1, 10 0			10 00 00 21 00 00 66 00 00 45 00 00 54 94 er 40 00f. E.T. @
J.	N Tag	00:50:50:90:00	ide), Dst: Cisco D9:	77:00 (58:97:0	u:09:77:	e)		00	20 40 01 af c0 c0 00 02 64 c6 33 64 64 08 00 4e a2 @d .3ddN
Υ Υ	n-tag	- Dines	tion: Econ Doidao					00	30 00 1a 00 07 f4 64 ce 62 00 00 00 00 20 a2 07 00d.b
		- Doint	cion: From Bridge					00	40 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b
		- Point	er; vir_iu					00	50 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ···· !"# \$%&'()*+
		= Desti	di No					00	60 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,/0123 4567
		Doope	u. No	4					
		= Keser	ved: 0						
		= versi	011: 0						
		90 0000 = Sourc	e: 0						
	Type: 802.10 Virtual LAN (0x8100)								
1 8	02.10 Virtual LAN, PRI: 0, DEI: 0,	1D: 102	·						
	000 E Priority: E	sest Effort (de	fault) (0)	2					
	0 = DEI: Inelig	gible.		31					
	0000 0110 0110 = ID: 102			-					
	Type: IPv4 (0x0800)			_					
> 1	nternet Protocol Version 4, Src: 1	92.0.2.100, Dst	:: 198.51.100.100	2					
×I	nternet Control Message Protocol			2					

Selezionare il secondo pacchetto e controllare i punti chiave:

- 1. Vengono acquisiti solo i pacchetti di richiesta echo ICMP. Ogni pacchetto viene acquisito e mostrato 2 volte.
- 2. L'intestazione del pacchetto originale è senza il tag VLAN.
- 3. Lo switch interno inserisce un tag VLAN 102 aggiuntivo che identifica l'interfaccia in entrata Ethernet 1/2.

No. Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info	
1 2022-07-13 06:23:58.285080930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (48428)	64 Echo (ping) reques	t id=0x001a, seq=7/1792, ttl=64 (no response found!)
2 2022-07-13 06:23:58.285082858	192.0.2.100	198.51.100.100	ICMP	102	0x9dec (40428)	64 Echo (ping) reques	t id=0x001a, seq=7/1792, ttl=64 (no response found!)
3 2022-07-13 06:23:59.309048886	192.0.2.100	198.51.100.100	ICMP	108	0x9ed0 (40656)	64 Echo (ping) reques	t id=0x001a, seq=8/2048, ttl=64 (no response found!)
4 2022-07-13 06:23:59.309193731	192.0.2.100	198.51.100.100	ICMP	102	0x9ed0 (40656)	64 Echo (ping) reques	t id=0x001a, seq=8/2048, ttl=64 (no response found!)
5 2022-07-13 06:24:00.333054190	192.0.2.100	198.51.100.100	ICMP	108	0x9f20 (40736)	64 Echo (ping) reques	t id=0x001a, seq=9/2304, ttl=64 (no response found!)
6 2022-07-13 06:24:00.333056014	192.0.2.100	198.51.100.100	ICMP	102	0x9f20 (40736)	64 Echo (ping) reques	t id=0x001a, seq=9/2304, ttl=64 (no response found!)
7 2022-07-13 06:24:01.357173530	192.0.2.100	198.51.100.100	ICMP	108	0x9f2d (40749)	64 Echo (ping) reques	t id=0x001a, seq=10/2560, ttl=64 (no response found!)
8 2022-07-13 06:24:01.357174708	192.0.2.100	198.51.100.100	ICMP	102	0x9f2d (40749)	64 Echo (ping) reques	t id=0x001a, seq=10/2560, ttl=64 (no response found!)
9 2022-07-13 06:24:02.381073741	192.0.2.100	198.51.100.100	ICMP	108	0x9f88 (40840)	64 Echo (ping) reques	t id=0x001a, seq=11/2816, ttl=64 (no response found!)
10 2022-07-13 06:24:02.381074999	192.0.2.100	198.51.100.100	ICMP	102	0x9f88 (40840)	64 Echo (ping) reques	t id=0x001a, seq=11/2816, ttl=64 (no response found!)
11 2022-07-13 06:24:03.405199041	192.0.2.100	198.51.100.100	ICMP	108	0xa077 (41079)	64 Echo (ping) reques	t id=0x001a, seq=12/3072, ttl=64 (no response found!)
12 2022-07-13 06:24:03.405200261	192.0.2.100	198.51.100.100	ICMP	102	0xa077 (41079)	64 Echo (ping) reques	t id=0x001a, seq=12/3072, ttl=64 (no response found!)
13 2022-07-13 06:24:04.429155683	192.0.2.100	198.51.100.100	ICMP	108	0xa10f (41231)	64 Echo (ping) reques	t id=0x001a, seq=13/3328, ttl=64 (no response found!)
14 2022-07-13 06:24:04.429156831	192.0.2.100	198.51.100.100	ICMP	102	0xa10f (41231)	64 Echo (ping) reques	t id=0x001a, seq=13/3328, ttl=64 (no response found!)
15 2022-07-13 06:24:05.453156612	192.0.2.100	198.51.100.100	ICMP	108	0xa16a (41322)	64 Echo (ping) reques	t id=0x001a, seq=14/3584, ttl=64 (no response found!)
16 2022-07-13 06:24:05.453158052	192.0.2.100	198.51.100.100	ICMP	102	0xa16a (41322)	64 Echo (ping) reques	t id=0x001a, seq=14/3584, ttl=64 (no response found!)
17 2022-07-13 06:24:06.477127687	192.0.2.100	198.51.100.100	ICMP	108	0xa1e9 (41449)	64 Echo (ping) reques	t id=0x001a, seq=15/3840, ttl=64 (no response found!)
18 2022-07-13 06:24:06.477129899	192.0.2.100	198.51.100.100	ICMP	102	0xa1e9 (41449)	64 Echo (ping) reques	t id=0x001a, seq=15/3840, ttl=64 (no response found!)
19 2022-07-13 06:24:07.501291314	192.0.2.100	198.51.100.100	ICMP	108	0xa1f6 (41462)	64 Echo (ping) reques	t id=0x001a, seq=16/4096, ttl=64 (no response found!)
20 2022-07-13 06:24:07.501293041	192.0.2.100	198.51.100.100	ICMP	102	0xa1f6 (41462)	64 Echo (ping) reques	t id=0x001a, seq=16/4096, ttl=64 (no response found!)
21 2022-07-13 06:24:08.525089956	192.0.2.100	198.51.100.100	ICMP	108	0xa257 (41559)	64 Echo (ping) reques	t id=0x001a, seq=17/4352, ttl=64 (no response found!)
22 2022-07-13 06:24:08.525092088	192.0.2.100	198.51.100.100	ICMP	102	0xa257 (41559)	64 Echo (ping) reques	t id=0x001a, seq=17/4352, ttl=64 (no response found!)
23 2022-07-13 06:24:09.549236500	192.0.2.100	198.51.100.100	ICMP	108	0xa2a9 (41641)	64 Echo (ping) reques	t id=0x001a, seq=18/4608, ttl=64 (no response found!)
24 2022-07-13 06:24:09.549238564	192.0.2.100	198.51.100.100	ICMP	102	0xa2a9 (41641)	64 Echo (ping) reques	t id=0x001a, seq=18/4608, ttl=64 (no response found!)
25 2022-07-13 06:24:10.573110146	192.0.2.100	198.51.100.100	ICMP	108	0xa345 (41797)	64 Echo (ping) reques	t id=0x001a, seq=19/4864, ttl=64 (no response found!)
26 2022-07-13 06:24:10.573112504	192.0.2.100	198.51.100.100	ICMP	102	0xa345 (41797)	64 Echo (ping) reques	t id=0x001a, seq=19/4864, ttl=64 (no response found!)
27 2022-07-13 06:24:11.597086027	192.0.2.100	198.51.100.100	ICMP	108	0xa349 (41801)	64 Echo (ping) reques	t id=0x001a, seq=20/5120, ttl=64 (no response found!)
28 2022-07-13 06:24:11.597088170	192.0.2.100	198.51.100.100	ICMP	102	0xa349 (41801)	64 Echo (ping) reques	t id=0x001a, seq=20/5120, ttl=64 (no response found!)
29 2022-07-13 06:24:12.621061022	192.0.2.100	198.51.100.100	ICMP	108	0xa3dc (41948)	64 Echo (ping) reques	t id=0x001a, seq=21/5376, ttl=64 (no response found!)
< C							
> Frame 2: 182 bytes on wire (816 bit	s) 102 bytes (cantured (816 hits)	on interface	canture u	e 1. id e		0000 58 97 bd b9 77 8e 80 50 56 9d e8 be 81 80 80 66 X W P V f
> Ethernet II. Src: VMware 9d:e8the (00:50:56:9d:e8	the). Dst: Cisco h9:	77:00 (58:97:	hd:b9:77:	0e)		0010 08 00 45 00 00 54 9d ec 40 00 40 01 af c0 c0 00 ··E··T·· @·@····
802 10 Victual LAN DRT: 0 DET: 0	ID: 102	locy) oser erses os	(50151)				0020 02 64 c6 33 64 64 08 00 4e a2 00 1a 00 07 f4 64 ·d·3dd·· N·····d
000 = Priority: 1	Rest Effort (de	fault) (0)					0030 ce 62 00 00 00 20 a2 07 00 00 00 00 10 11 .b
DET: Inelia	sible		2				0040 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21
0000 0110 0110 = ID: 102	Broke		J				0050 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 "#\$%&"() *+,/01
Type: TPv4 (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			21				
Contract Contract Ressage Fractores			-				

Aprire i file di acquisizione per le interfacce membro di Portchannel1. Selezionare il primo pacchetto e controllare i punti chiave:

- 1. Vengono acquisiti solo i pacchetti di richiesta echo ICMP. Ogni pacchetto viene acquisito e mostrato 2 volte.
- 2. L'intestazione del pacchetto originale è senza il tag VLAN.
- 3. Lo switch interno inserisce un tag VLAN 1001 aggiuntivo che identifica l'interfaccia in entrata Portchannel1.
- 4. Lo switch interno inserisce un tag VN aggiuntivo.

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 ((nc	
	2 2022-08-05 23:07:31.865875131	192.0.2.100	198.51.100.100	ICMP	102	Øx322e ((12846)	64 Echo (ping)	request	id=0x002d,	seq=245/62720,	ttl=64 ((nc	
	3 2022-08-05 23:07:32.867144598	192.0.2.100	198.51.100.100	ICMP	108	0x32b9 ((12985)	64 Echo (ping	request	id=0x002d,	seq=246/62976,	ttl=64 ((nc	
	4 2022-08-05 23:07:32.867145852	192.0.2.100	198.51.100.100	ICMP	102	0x32b9 ((12985)	64 Echo (ping)	request	id=0x002d,	seq=246/62976,	ttl=64 ((nc	
	5 2022-08-05 23:07:33.881902485	192.0.2.100	198.51.100.100	ICMP	108	0x32d8 ((13016)	64 Echo (ping)	request	id=0x002d,	seq=247/63232,	ttl=64 ((nc	
	6 2022-08-05 23:07:33.881904191	192.0.2.100	198.51.100.100	ICMP	102	0x32d8 ((13016)	64 Echo (ping)	request	id=0x002d,	seq=247/63232,	ttl=64 ((nc	
	7 2022-08-05 23:07:34.883049425	192.0.2.100	198.51.100.100	ICMP	108	Øx3373 ((13171)	64 Echo (ping)	request	id=0x002d,	seq=248/63488,	ttl=64 ((nc	
	8 2022-08-05 23:07:34.883051649	192.0.2.100	198.51.100.100	ICMP	102	Øx3373 ((13171)	64 Echo (ping)	request	id=0x002d,	seq=248/63488,	ttl=64 ((nc	
	9 2022-08-05 23:07:35.883478016	192.0.2.100	198.51.100.100	ICMP	108	0x3427 ((13351)	64 Echo (ping)	request	id=0x002d,	seq=249/63744,	ttl=64 ((nc	
	10 2022-08-05 23:07:35.883479190	192.0.2.100	198.51.100.100	ICMP	102	0x3427 ((13351)	64 Echo (ping)	request	id=0x002d,	seq=249/63744,	ttl=64 ((nc	
	11 2022-08-05 23:07:36.889741625	192.0.2.100	198.51.100.100	ICMP	108	Øx34de ((13534)	64 Echo (ping)	request	id=0x002d,	seq=250/64000,	ttl=64 ((nc	
	12 2022-08-05 23:07:36.889742853	192.0.2.100	198.51.100.100	ICMP	102	Øx34de ((13534)	64 Echo (ping)	request	id=0x002d,	seq=250/64000,	ttl=64 ((nc	
	13 2022-08-05 23:07:37.913770117	192.0.2.100	198.51.100.100	ICMP	108	0x354c ((13644)	64 Echo (ping)	request	id=0x002d,	seq=251/64256,	ttl=64 ((nc	
	14 2022-08-05 23:07:37.913772219	192.0.2.100	198.51.100.100	ICMP	102	0x354c ((13644)	64 Echo (ping)	request	id=0x002d,	seq=251/64256,	ttl=64 ((nc	
	15 2022-08-05 23:07:38.937829879	192.0.2.100	198.51.100.100	ICMP	108	0x3602 ((13826)	64 Echo (ping)	request	id=0x002d,	seq=252/64512,	ttl=64 ((nc	
	16 2022-08-05 23:07:38.937831215	192.0.2.100	198.51.100.100	ICMP	102	0x3602 ((13826)	64 Echo (ping)	request	id=0x002d,	seq=252/64512,	ttl=64 ((nc	
	17 2022-08-05 23:07:39.961786128	192.0.2.100	198.51.100.100	ICMP	108	Øx36ed ((14061)	64 Echo (ping)	request	id=0x002d,	seq=253/64768,	ttl=64 ((nc	
	18 2022-08-05 23:07:39.961787284	192.0.2.100	198.51.100.100	ICMP	102	Øx36ed ((14061)	64 Echo (ping)	request	id=0x002d,	seq=253/64768,	ttl=64 ((nc	
	19 2022-08-05 23:07:40.985773090	192.0.2.100	198.51.100.100	ICMP	108	0x37d5 ((14293)	64 Echo (ping)	request	id=0x002d,	seq=254/65024,	ttl=64 ((nc	~
<													>	
>	Frame 1: 108 bytes on wire (864 bits)), 108 bytes cap	otured (864 bits) on	interfac∉	e capture_u0_3,	i 0000	a2 76	f2 00 00 25 00 50	56 9d e8	be 89 26 80	54 · v · · · % · P	V · · · · & · т		
>	Ethernet II, Src: VMware_9d:e8:be (00	ð:50:56:9d:e8:be	e), Dst: a2:76:f2:00	:00:25 (a2	2:76:f2:00:00:2	5) 0010	00 00	81 00 03 e9 08 00	45 00 00	54 32 2e 40	00	ET2.@-		
Ι.	VN-Tag					0020	40 01	1b 7f c0 00 02 64	c6 33 64	64 08 00 1e	d6 @·····d	· 3dd · · · ·		
	1	= Directi	on: From Bridge			0030	00 2d	00 15 a6 a2 ed 62	00 00 00	00 7a 2f 0b	00 ·-···b	····z/··		
ш	.0	= Pointer	: vif_id			0040	00 00	00 00 10 11 12 13	14 15 16	17 18 19 1a	10 ·····	e%0.1/1*.		
ш	00 0000 0101 0100	= Destina	tion: 84			0050	20.20	20 2f 20 21 22 23	24 25 20	27 20 29 28	- /0123	\$/00 () + 4567		
ш	···· ···· ···· ···· 0 ····	···· = Looped:	No 4			0000	20 20	26 21 30 31 32 33	54 55 50	57	,/0125	4307		
ш	0	= Reserve	d: 0											
ш	00	= Version	: 0											
ш	0000 0000	0000 = Source:	0											
IL	Type: 802.10 Virtual LAN (0x8100)													
	802.1Q Virtual LAN, PRI: 0, DEI: 0, 1	ID: 1001												
	000 Be	st Effort (defa	ult) (0)											
ш	0 = DEI: Ineligi	ble	2											
ш	0011 1110 1001 = ID: 1001		5											
11	Type: IPv4 (0x0800)													
L D	Internet Protocol Version 4, Src: 192	2.0.2.100, Dst:	198.51.100.100											
н	Internet Control Message Protocol		2											
6														

Selezionare il secondo pacchetto e controllare i punti chiave:

- 1. Vengono acquisiti solo i pacchetti di richiesta echo ICMP. Ogni pacchetto viene acquisito e mostrato 2 volte.
- 2. L'intestazione del pacchetto originale è senza il tag VLAN.
- 3. Lo switch interno inserisce un tag VLAN 1001 aggiuntivo che identifica l'interfaccia in entrata Portchannel1.

																	_
No.	Time	Source	Destination	Protocol	Length	IP ID		IP TT	'L Info								^
F	1 2022-08-05 23:07:31.865872877	192.0.2.100	198.51.100.100	ICMP	108	Øx322e (12846)	6	4 Echo	(ping)	request	id=0x002d,	seq=24	5/62720,	ttl=64	(nc	
	2 2022-08-05 23:07:31.865875131	192.0.2.100	198.51.100.100	ICMP	102	Øx322e (12846)	6	4 Echo	(ping)	request	id=0x002d,	seq=24	5/62720,	ttl=64	(nc	
	3 2022-08-05 23:07:32.867144598	192.0.2.100	198.51.100.100	ICMP	108	0x32b9 (12985)	6	4 Echo	(ping)	request	id=0x002d,	seq=24	6/62976,	ttl=64	(nc	
	4 2022-08-05 23:07:32.867145852	192.0.2.100	198.51.100.100	ICMP	102	0x32b9 (12985)	6	4 Echo	(ping)	request	id=0x002d,	seq=24	6/62976,	ttl=64	(nc	
	5 2022-08-05 23:07:33.881902485	192.0.2.100	198.51.100.100	ICMP	108	0x32d8 (13016)	6	4 Echo	(ping)	request	id=0x002d,	seq=24	7/63232,	ttl=64	(nc	
	6 2022-08-05 23:07:33.881904191	192.0.2.100	198.51.100.100	ICMP	102	0x32d8 (13016)	6	4 Echo	(ping)	request	id=0x002d,	seq=24	7/63232,	ttl=64	(nc	
	7 2022-08-05 23:07:34.883049425	192.0.2.100	198.51.100.100	ICMP	108	0x3373 (13171)	6	4 Echo	(ping)	request	id=0x002d,	seq=24	8/63488,	ttl=64	(nc	
	8 2022-08-05 23:07:34.883051649	192.0.2.100	198.51.100.100	ICMP	102	0x3373 (13171)	6	4 Echo	(ping)	request	id=0x002d,	seq=24	8/63488,	ttl=64	(nc	
	9 2022-08-05 23:07:35.883478016	192.0.2.100	198.51.100.100	ICMP	108	0x3427 (13351)	6	4 Echo	(ping)	request	id=0x002d,	seq=24	9/63744,	ttl=64	(nc	
	10 2022-08-05 23:07:35.883479190	192.0.2.100	198.51.100.100	ICMP	102	0x3427 (13351)	6	4 Echo	(ping)	request	id=0x002d,	seq=24	9/63744,	ttl=64	(nc	
	11 2022-08-05 23:07:36.889741625	192.0.2.100	198.51.100.100	ICMP	108	0x34de (13534)	6	4 Echo	(ping)	request	id=0x002d,	seq=25	0/64000,	ttl=64	(nc	
	12 2022-08-05 23:07:36.889742853	192.0.2.100	198.51.100.100	ICMP	102	0x34de (13534)	6	4 Echo	(ping)	request	id=0x002d,	seq=25	0/64000,	ttl=64	(nc	
	13 2022-08-05 23:07:37.913770117	192.0.2.100	198.51.100.100	ICMP	108	0x354c (13644)	6	4 Echo	(ping)	request	id=0x002d,	seq=25	1/64256,	ttl=64	(nc	
	14 2022-08-05 23:07:37.913772219	192.0.2.100	198.51.100.100	ICMP	102	0x354c (13644)	6	4 Echo	(ping)	request	id=0x002d,	seq=25	1/64256,	ttl=64	(nc	
	15 2022-08-05 23:07:38.937829879	192.0.2.100	198.51.100.100	ICMP	108	0x3602 (13826)	6	4 Echo	(ping)	request	id=0x002d,	seq=25	2/64512,	ttl=64	(nc	
	16 2022-08-05 23:07:38.937831215	192.0.2.100	198.51.100.100	ICMP	102	0x3602 (13826)	6	4 Echo	(ping)	request	id=0x002d,	seq=25	2/64512,	ttl=64	(nc	
	17 2022-08-05 23:07:39.961786128	192.0.2.100	198.51.100.100	ICMP	108	Øx36ed (14061)	6	4 Echo	(ping)	request	id=0x002d,	seq=25	3/64768,	ttl=64	(nc	
	18 2022-08-05 23:07:39.961787284	192.0.2.100	198.51.100.100	ICMP	102	0x36ed (14061)	6	4 Echo	(ping)	request	id=0x002d,	seq=25	3/64768,	ttl=64	(nc	
	19 2022-08-05 23:07:40.985773090	192.0.2.100	198.51.100.100	ICMP	108	0x37d5 (14293)	6	4 Echo	(ping)	request	id=0x002d,	seq=25	4/65024,	ttl=64	(nc	~
<																>	
> Ena	me 2: 102 bytes on wire (816 bits)	, 102 bytes capt	ured (816 bits) on	interface cap	ture u0 3,	i 0000	a2 76	f2 00	00 25 (90 50	56 9d e8	be 81 00 03	e9	·v···%·P	v		
> Eth	ernet II, Src: VMware 9d:e8:be (00	:50:56:9d:e8:be)	. Dst: a2:76:f2:00	:00:25 (a2:76:	f2:00:00:2	(5) 0010	08 00	45 00	00 54 3	32 2e	40 00 40	01 1b 7f ce	00	··E··T2.	0.0		
802	2.10 Virtual LAN, PRI: 0, DEI: 0, I	D: 1001	,			0020	02 64	c6 33	64 64 6	98 99	1e d6 00	2d 00 f5 a6	a2	d · 3dd · ·			
	000 Bes	st Effort (defaul	lt) (0)			0030	ed 62	00 00	00 00 7	7a 2f	0b 00 00	00 00 00 10	11	·b····z/	• • • • • • • •		
	0 = DEI: Ineligit	ole	3			0040	12 13	14 15	16 17 1	18 19	1a 1b 1c	1d 1e 1f 20	21			1	
	0011 1110 1001 = ID: 1001					0050	22 23	24 25	26 27 2	28 29	2a 2b 2c	2d 2e 2f 30	31	"#\$%&'()	*+,/0	1	
	Type: IPv4 (0x0800)					0060	32 33	34 35	36 37				-	234567			
Int	ernet Protocol Version 4, Src: 192	.0.2.100, Dst: 1	98,51,100,100														
Int	ernet Control Message Protocol	,	2														

Spiegazione

Quando si configura la cattura di un pacchetto su un'interfaccia anteriore, lo switch acquisisce simultaneamente ciascun pacchetto due volte:

- Dopo l'inserimento del tag VLAN della porta.
- Dopo l'inserimento del tag VN.

Nell'ordine delle operazioni, il tag VN viene inserito in una fase successiva all'inserimento del tag VLAN della porta. Tuttavia, nel file di acquisizione, il pacchetto con il tag VN viene visualizzato prima del pacchetto con il tag port VLAN.

Nella tabella seguente viene riepilogata l'attività:

Attività	Punto di acquisizione	VLAN della porta interna nei pacchetti acquisiti	Direzione	Traffico acquisito
Configurazione e verifica dell'acquisizione di un pacchetto sull'interfaccia Ethernet1/2	Ethernet 1/2	102	Solo in ingresso	Richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.100

Configurazione e verifica dell'acquisizione di un pacchetto sull'interfaccia Portchannel1 con le interfacce membro Ethernet1/4 ed Ethernet1/5	Ethernet1/4 Ethernet1/5	1001	Solo in ingresso	Richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.100
---	----------------------------	------	---------------------	---

Acquisizioni di pacchetti su interfacce backplane

Usare FCM e CLI per configurare e verificare l'acquisizione di un pacchetto sulle interfacce backplane.

Topologia, flusso dei pacchetti e punti di acquisizione



Configurazione

FCM

Per configurare le acquisizioni dei pacchetti sulle interfacce backplane, eseguire la procedura seguente su FCM:

1. Utilizzare Strumenti > Acquisizione pacchetti > Acquisisci sessione per creare una nuova sessione di acquisizione:

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

2. Per acquisire i pacchetti su tutte le interfacce backplane, selezionare l'applicazione, quindi Tutte le porte backplane dall'elenco a discesa Acquisisci su. In alternativa, scegliete l'interfaccia del backplane specifica. In questo caso, sono disponibili interfacce backplane Ethernet1/9 ed Ethernet1/10. Specificare il Nome sessione e fare clic su Salva ed esegui per attivare l'acquisizione:

Overview Interfaces Logical Devices Security Engine Platform Settings	System Tools Help admin
Select an instance: td1	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	EthernetI/10 Al Backplane Ports
Ethernet1/1	

CLI FXOS

Eseguire questi passaggi sulla CLI di FXOS per configurare le acquisizioni dei pacchetti sulle interfacce backplane:

1. Identificare il tipo di applicazione e l'identificatore:

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

2. Creare una sessione di acquisizione:

```
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 #
```

Verifica

FCM

Verificare il nome dell'interfaccia, verificare che lo stato operativo sia attivo e che le dimensioni del

file (in byte) aumentino:

Overview	Interfaces	Logical Devices Security	Engine Platfo	orm Settings				System	Tools H	elp admin
Capture Ses	sion Filter L	ist								
							Capture Session	Delete All S	iessions	
•	cap1	Drop Count: 0	Oper	rational State: up	Buffer Size: 256 MB		Snap Length: 1518 Bytes			
Interface Na	me	Filter		File Size (in bytes)	File Name	Device Name				
Ethernet1/10		None		194352	cap1-ethernet-1-10-0.pcap	ftd1	⊻			
Ethernet1/9		None		286368	cap1-ethernet-1-9-0.pcap	ftd1	*			

CLI FXOS

Verificare i dettagli di acquisizione nell'ambito 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
```

```
Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-10-0.pcap
Pcapsize: 1017424 bytes
Filter:
Sub Interface: 0
Application Instance Identifier: ftd1
Application Name: ftd
Slot Id: 1
Port Id: 9
Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-9-0.pcap
Pcapsize: 1557432 bytes
Filter:
Sub Interface: 0
Application Instance Identifier: ftd1
Application Name: ftd
```

Raccogli file di acquisizione

Port Id: 10

Eseguire i passaggi descritti nella sezione Raccolta dei file di acquisizione degli switch interni Firepower 4100/9300.

Analisi dei file di acquisizione

Utilizzare un'applicazione per la lettura dei file di acquisizione dei pacchetti per aprire i file di acquisizione. In caso di più interfacce backplane, assicurarsi di aprire tutti i file di acquisizione per ciascuna interfaccia backplane. In questo caso, i pacchetti vengono acquisiti sull'interfaccia Ethernet1/9 del backplane.

Selezionare il primo e il secondo pacchetto e verificare i punti principali:

- 1. Ogni pacchetto di richiesta echo ICMP viene acquisito e visualizzato 2 volte.
- 2. L'intestazione del pacchetto originale è senza il tag VLAN.
- 3. Lo switch interno inserisce un tag VLAN 103 aggiuntivo che identifica l'interfaccia Ethernet1/3 in uscita.
- 4. Lo switch interno inserisce un tag VN aggiuntivo.

_						_									
No.	Time	Source	Destination	Protocol	Length	IP ID		IP TTL Info							
-	1 2022-07-14 20:20:36.513854256	192.0.2.100	198.51.100.100	ICMP	108	0x5990	(22928)	64 Echo	(ping)	request	1d=0x0001,	seq=15/3840,	tt1=64	(no response found!)	
	2 2022-07-14 20:20:36.513857289	192.0.2.100	198.51.100.100	ICMP	108	0x5990	(22928)	64 Echo	(ping)	request	id=0x0001,	seq=15/3840,	tt1=64	(reply in 3)	
	3 2022-07-14 20:20:36.514117394	198.51.100.100	9 192.0.2.100	ICMP	108	0xcc2c	(52268)	64 Echo	(ping)	reply	id=0x0001,	seq=15/3840,	ttl=64	(request in 2)	
	4 2022-07-14 20:20:36.514119312	198.51.100.100	0 192.0.2.100	ICMP	108	0xcc2c	(52268)	64 Echo	(ping)	reply	id=0x0001,	seq=15/3840,	ttl=64		
	5 2022-07-14 20:20:37.537723822	192.0.2.100	198.51.100.100	ICMP	108	0x5a00	(23840)	64 Echo	(ping)	request	id=0x0001,	seq=16/4096,	ttl=64	(no response found!)	
	6 2022-07-14 20:20:37.537726588	192.0.2.100	198.51.100.100	ICMP	108	0x5a00	(23040)	64 Echo	(ping)	request	id=0x0001,	seq=16/4096,	ttl=64	(reply in 7)	
	7 2022-07-14 20:20:37.538046165	198.51.100.100	9 192.0.2.100	ICMP	108	Øxcc9b	(52379)	64 Echo	(ping)	reply	id=0x0001,	seq=16/4096,	ttl=64	(request in 6)	
	8 2022-07-14 20:20:37.538048311	198.51.100.100	0 192.0.2.100	ICMP	108	Øxcc9b	(52379)	64 Echo	(ping)	reply	id=0x0001,	seq=16/4096,	ttl=64		
	9 2022-07-14 20:20:38.561776064	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7	(23223)	64 Echo	(ping)	request	id=0x0001,	seq=17/4352,	ttl=64	(no response found!)	
	10 2022-07-14 20:20:38.561778310	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7	(23223)	64 Echo	(ping)	request	id=0x0001,	seq=17/4352,	ttl=64	(reply in 11)	
	11 2022-07-14 20:20:38.562048288	198.51.100.100	9 192.0.2.100	ICMP	108	0xccc4	(52420)	64 Echo	(ping)	reply	id=0x0001,	seq=17/4352,	ttl=64	(request in 10)	
	12 2022-07-14 20:20:38.562050333	198.51.100.100	9 192.0.2.100	ICMP	108	0xccc4	(52420)	64 Echo	(ping)	reply	id=0x0001	seq=17/4352,	ttl=64		
	13 2022-07-14 20:20:39.585677043	192.0.2.100	198.51.100.100	ICMP	108	0x5b46	(23366)	64 Echo	(ping)	request	id=0x0001,	seq=18/4608,	ttl=64	(no response found!)	
	14 2022-07-14 20:20:39.585678455	192.0.2.100	198.51.100.100	ICMP	108	0x5b46	(23366)	64 Echo	(ping)	request	id=0x0001,	seq=18/4608,	ttl=64	(reply in 15)	
	15 2022-07-14 20:20:39.585936554	198.51.100.100	9 192.0.2.100	ICMP	108	0xcd8d	(52621)	64 Echo	(ping)	reply	id=0x0001,	seq=18/4608,	ttl=64	(request in 14)	
	16 2022-07-14 20:20:39.585937900	198.51.100.100	9 192.0.2.100	ICMP	108	0xcd8d	(52621)	64 Echo	(ping)	reply	id=0x0001,	seq=18/4608,	tt1=64		
	17 2022-07-14 20:20:40.609804804	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b	(23419)	64 Echo	(ping)	request	id=0x0001,	seg=19/4864,	ttl=64	(no response found!)	
	18 2022-07-14 20:20:40.609807618	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b	(23419)	64 Echo	(ping)	request	id-0x0001.	seg=19/4864,	ttl=64	(reply in 19)	
	19 2022-07-14 20:20:40.610179685	198.51.100.100	9 192.0.2.100	ICMP	108	Øxcd8f	(52623)	64 Echo	(ping)	reply	id-0x0001	seg=19/4864,	ttl=64	(request in 18)	
	20 2022-07-14 20:20:40.610181944	198.51.100.100	9 192.0.2.100	ICMP	108	0xcd8f	(52623)	64 Echo	(ping)	reply	id-0x0001	seg=19/4864,	ttl=64		
	21 2022-07-14 20:20:41.633805153	192.0.2.100	198,51,100,100	ICMP	108	0x5b7e	(23422)	64 Echo	(ping)	request	id-0x0001	seg=20/5120,	tt1=64	(no response found!)	
	22 2022-07-14 20:20:41.633806997	192.0.2.100	198,51,100,100	ICMP	108	0x5b7e	(23422)	64 Echo	(ping)	request	id=0x0001	seg=20/5120,	tt1=64	(reply in 23)	
	23 2022-07-14 20:20:41.634084102	198.51.100.100	9 192.0.2.100	ICMP	108	0xce36	(52790)	64 Echo	(ping)	reply	id=0x0001	seq=20/5120.	tt1=64	(request in 22)	
	24 2022-07-14 20:20:41.634085368	198.51.100.100	192.0.2.100	TCMP	108	0xce36	(52798)	64 Echo	(ning)	reply	id=0x0001	seg=28/5128.	tt1=64	(
	25 2022-07-14 20:20:42.657709898	192.0.2.100	198, 51, 100, 100	TCMP	108	ex5hfe	(23536)	64 Echo	(ning)	request	id=exeen1	seq=21/5376.	tt1=64	(no response found!)	
	26 2022-07-14 20:20:42 657711660	192.0.2.100	198.51.100.100	TCMP	108	exshfe	(23536)	64 Echo	(ning)	request	id=exeent	seq=21/5376	tt1=64	(renly in 27)	
	27 2022-07-14 20:20:42:0577110000	198.51.100.100	192.0.2.100	TCMP	108	Oxcod9	(52809)	64 Echo	(ping)	request	id=0x0001	500=21/5376	++1=64	(request in 26)	
	20 2022-07-14 20:20:42:057900075	100 51 100 100	102 0 2 100	TCMP	100	Oxcod9	(52000)	64 Echo	(ping)	coply	id=0x0001	seq=21/5376	++1-64	(request in 20)	
	20 2022-07-14 20:20:42:057501571	192.0.2.100	198 51 100 100	TCMP	108	Oxcesp OxSc52	(23634)	64 Echo	(ping)	request	id=0x0001	seq=22/5632	tt1=64	(no response found!)	
÷.,	29 2022-07-14 20:20:43:001730037	152.0.2.100	190.91.100.100	Acre	100	UNJEJE	(25054)	ou ceno	(brue)	request		seq-zz/ Josz ;		(no response roundr)	
<															
>	Frame 1: 108 bytes on wire (864 bit	s), 108 bytes o	captured (864 bits)	on interface	capture_u	⊎0_8, id 0				0	000 00 50	56 9d e7 50 5	8 97 b	d b9 77 2d 89 26 00 00	•PV • PX • • • • • • •
>	Ethernet II, Src: Cisco_b9:77:2d (5	8:97:bd:b9:77:2	2d), Dst: VMware_9d	:e7:50 (00:50	:56:9d:e7:	:50)				6	010 00 0a	81 00 00 67 0	8 00 4	5 00 00 54 59 90 40 00	·····g·· E··TY·@·
1	VN-Tag									6	020 40 01	f4 1c c0 00 0	2 64 c	6 33 64 64 08 00 22 68	@·····d ·3dd··*h
	0	= Direc	tion: To Bridge							6	030 00 01	00 0f 89 7a d	0 62 0	0 00 00 00 b3 d7 09 00	·····z·b ·····
	.0	= Point	er: vif_id							6	040 00 00	00 00 10 11 1	2 13 14	4 15 16 17 18 19 1a 1b	194 4901/28.
	0000 0000 0000	= Desti	nation: 0								050 1c 1d	10 17 20 21 2	2 23 2	4 25 26 27 28 29 28 20	(0100 4557
	0	= Loope	d: No	A							20 20 20	20 21 30 31 3	2 33 34	4 35 36 37	,/0123 450/
		= Reser	ved: 0	71											
		= Versi	on: 0												
	0000 000	00 1010 = Sourc	e: 10												
	Type: 802.10 Virtual LAN (0x8100))													
	802.10 Virtual LAN, PRI: 0. DEI: 0.	ID: 103													
I I	000 Priority: P	Best Effort (de	fault) (0)												
11		zible		2											
11	0000 0110 0111 = ID: 103			5											
11	Type: IPv4 (0x0800)														
	Internet Protocol Version A. Spc: 1	92.8.2.108. Det	: 198.51.100.100	-											
5	Internet Control Message Protocol			2											
Ľ	the second se			-											
-															

Selezionare il terzo e il quarto pacchetto, quindi verificare i punti chiave:

- 1. Ogni risposta echo ICMP viene acquisita e visualizzata 2 volte.
- 2. L'intestazione del pacchetto originale è senza il tag VLAN.
- 3. Lo switch interno inserisce un tag VLAN 102 aggiuntivo che identifica l'interfaccia di uscita Ethernet1/2.
- 4. Lo switch interno inserisce un tag VN aggiuntivo.

- 1 2022-07-14 2020:36.513854256 192.0.2.100 198.51.100.100 TUMP 108 0x590 (2228) 64 Echo (ping) request id-0x0001, seq=15/3840, ttl=64 (no response found)) + 2 022-07-14 2020:36.51385728 192.0.2.100 109.100 107P 108 + 2 022-07-14 2020:36.51385728 192.0.2.100 107P 108 0x5200 (2228) 64 Echo (ping) reply id-0x0001, seq=15/3840, ttl=64 (reply in 3) 4 2022-07-14 2020:36.514117394 198.51.100.100 192.0.2.100 107P 108 0x5200 (22268) 64 Echo (ping) reply id-0x0001, seq=15/3840, ttl=64 (reply in 3) 5 2022-07-14 2020:37.53772382 192.0.2.100 108 108.51.100.100 107P 108 0x5200 (22040) 64 Echo (ping) reply id-0x0001, seq=15/3840, ttl=64 (reply in 3) 7 2022-07-14 2020:37.53772382 192.0.2.100 108.51.100.100 107P 108 0x5200 (22040) 64 Echo (ping) reply id-0x0001, seq=15/3840, ttl=64 (reply in 7) 7 2022-07-14 2020:37.53723846 198.51.100.100 107P 108 0x5200 (22327) 64 Echo (ping) reply id-0x0001, seq=16/4096, ttl=64 (reply in 7) 8 2022-07-14 2020:37.53846656 198.51.100.100 107P 108 0x5206 (52379) 64 Echo (ping) rep	
+ 2 2022-07-14 20:20:36.51187289 192.0.2.100 198.51.100.100 ICMP 108 + 3 2022-07-14 20:20:36.514117394 198.51.100.100 120.P2 104	
s 2 022-07-14 202:07-14	
4 2022-07-14 20:20:36.514119312 198.51.100.100 192.0.2.100 1CMP 108 0xc2c (52268) 64 Echo (ping) reply id=0x0001, seq=15/3840, tt]=64 5 2022-07-14 20:20:37.537223822 192.0.2.100 198.51.100.100 1CMP 108 0x5a00 (23040) 64 Echo (ping) reply id=0x0001, seq=16/3056, ttl=64 (reply in 7) 7 2022-07-14 20:20:37.53846165 198.51.100.100 1CMP 108 0xc300 (23040) 64 Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (reply in 7) 7 2022-07-14 20:20:37.53846165 198.51.100.100 120.42.100 120.42.100 1CMP 108 0xc206 (52379) 64 Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (reply in 7) 7 2022-07-14 20:20:37.53846311 198.51.100.100 120.42.100 109.42.100 102.42.100 1CMP 108 0xc206 (52379) 64 Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (reply in 7) 9 2022-07-14 20:20:38.561776646 198.51.100.100 1CMP 108 0xc206 (52379) 64 Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (reply in 7) 10 202-07-14 20:20:38.561776816 198.51.100.100 1CMP 108 0xc206 (52379) 64 Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (reply in 16) 100.20.20.100 108.20.20.100 0	
5 2022-07-14 20:20:37.53723622 192.0.2.100 198.51.100.100 ICMP 108 0x5a00 (23040) 64 Echo (ping) request id=xx0001, seq=16/4096, ttl=64 (no response found!) 6 2022-07-14 20:20:37.5372658 192.0.2.100 198.51.100.100 ICMP 108 0x5a00 (23040) 64 Echo (ping) request id=xx0001, seq=16/4096, ttl=64 (request in 6) 7 2022-07-14 20:20:37.538046165 198.51.100.100 12.0.0 ICMP 108 0xc:00 (52379) 64 Echo (ping) reply id=xx0001, seq=16/4096, ttl=64 (request in 6) 8 2022-07-14 20:20:37.538046165 198.51.100.100 120.0.2.100 ICMP 108 0xc:00 (52379) 64 Echo (ping) reply id=xx0001, seq=16/4096, ttl=64 (request in 6) 9 2022-07-14 20:20:38.561776664 192.0.2.100 ICMP 108 0xc:09 (52379) 64 Echo (ping) reply id=xx0001, seq=16/4096, ttl=64 (no response found!) 9 2022-07-14 20:20:38.56177664 192.0.2.100 198.51.100.100 ICMP 108 0xc:09 (52379) 64 Echo (ping) request id=xx0001, seq=16/4096, ttl=64 (no response found!) 10 2022-07-14 20:20:38.561776810 192.0.2.100 198.51.100.100 ICMP 108 0xc:07 (2323) 64 Echo (ping) request id=xx0001, seq=16/4096, ttl=64	
6 2022-07-14 20:20:37.537726588 192.0.2.100 198.51.100.100 ICMP 108 0x5a00 (23040) 64 Echo (ping) request id-0x0001, seq=16/4096, ttl=64 (reply in 7) 7 2022-07-14 20:20:37.538048115 198.51.100.100 120.2.100 ICMP 108 0xcc0b (52379) 64 Echo (ping) reply id-0x0001, seq=16/4096, ttl=64 8 2022-07-14 20:20:37.538048115 198.51.100.100 120.2.100 ICMP 108 0xcc0b (52379) 64 Echo (ping) reply id-0x0001, seq=16/4096, ttl=64 9 2022-07-14 20:20:38.561776064 192.0.2.100 198.51.100.100 ICMP 108 0x5ab7 (23223) 64 Echo (ping) request id-0x0001, seq=17/4352, ttl=64 (no response found!) 10 2022-07-14 20:20:38.561778310 192.0.2.100 198.51.100.100 ICMP 108 0x5ab7 (23223) 64 Echo (ping) request id-0x0001, seq=17/4352, ttl=64 (no response found!) 10 2022-07-14 20:20:38.561778310 192.0.2.100 198.51.100.100 ICMP 108 0x5ab7 (23223) 64 Echo (ping) request id-0x0001, seq=17/4352, ttl=64 (no response found!) 10 2022-07-14 20:20:38.561778310 192.0.2.100 198.51.100.100 ICMP 108 0x5ab7 (23223) 64 Echo (ping) request id-0x0001, seq=17/4352, ttl=64 (no reply in 11) 10 2022-07-14 20:20:38.561778310 192.51.100.100	
7 2022-07-14 20:20:37.5380463165 198.51.100.100 192.0.2.100 ICMP 108 0xcc9b (52379) 64 Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 9 2022-07-14 20:20:37.538048311 198.51.100.100 192.0.2.100 ICMP 108 0xcc9b (52379) 64 Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 9 2022-07-14 20:20:38.561776646 192.0.2.100 198.51.100.100 ICMP 108 0xcc9b (52379) 64 Echo (ping) reputy id=0x0001, seq=16/4096, ttl=64 10 2022-07-14 20:20:38.561776846 192.0.2.100 198.51.100.100 ICMP 108 0x5ab7 (23223) 64 Echo (ping) reputst id=0x0001, seq=16/4352, ttl=64 (no response found) 10 2022-07-14 20:20:38.561778310 192.0.2.100 198.51.100.100 ICMP 108 0x5ab7 (23223) 64 Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (no response found) 10 2022-07-14 20:20:38.56178310 192.51.100.100 ICMP 108 0x5ab7 (23223) 64 Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (no response found) 11 2012-07.14 20:20:38.56178310 192.51.100.100 ICMP 108 0x5ab7 (23223) 64 Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (no reputst in 10)	
8 2022-07-14 20:20:37.538048311 198.51.100.100 192.0.2.100 ICMP 108 0xcc9b (52279) 64 Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 9 2022-07-14 20:20:38.561778316 192.0.2.100 198.51.100.100 ICMP 108 0x5ab7 (23223) 64 Echo (ping) request id=0x0001, seq=17/452, ttl=64 (no response found!) 10 2022-07-14 20:20:38.561778316 192.0.2.100 198.51.100.100 ICMP 108 0x5ab7 (23223) 64 Echo (ping) request id=0x0001, seq=17/452, ttl=64 (no response found!) 11 2022-07-14 20:20:38.561778316 192.0.2.100 198.51.100.100 ICMP 108 0x5ab7 (23223) 64 Echo (ping) request id=0x0001, seq=17/452, ttl=64 (reply in 11) 12 2022-07-14 20:20:38.56178316 192.0.2.100 198.51.100.100 ICMP 108 0x5ab7 (23223) 64 Echo (ping) request id=0x0001, seq=17/452, ttl=64 (reply in 11)	
9 2022-07-14 20:20:38.561776064 192.0.2.100 198.51.100.100 ICMP 108 0x5ab7 (23223) 64 Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (no response found1) 10 2022-07-14 20:20:38.561778310 192.0.2.100 198.51.100.100 ICMP 108 0x5ab7 (23223) 64 Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (reply in 11) 11 2022-07-14 20:20:38.56178310 192.0.2.100 198.51.100.100 ICMP 108 0x5ab7 (23223) 64 Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (reply in 11)	
10 2022-07-14 20:20:8.56172810 102.0.2.100 108.51.100.100 ICMP 108 0X5a07 (23223) 64 Echo (ping) request id-ox0001, seq=17/4552, ttl=64 (reply in 11) 11 2012-07.14 20:20:20 Echo(2018 Echo(2018 Control 10, 10, 10, 10, 10, 10, 10, 10, 10, 10,	
11 2022-07-14 20:20:38 562048288 108 51 100 102 0 2 100 TCND 108 0xccc4 (52420) 64 Echo (ning) renly id=0x0001 con=17/4352 tt]=64 (request in 10)	
11 2022-07-14 20-20-30-302040200 130-31-100-100 132-0-2-100 100 100 132-0-2-100 100 100 100 100 100 100 100 100 100	
12 2022-07-14 20:20:38.562050333 198.51.100.100 192.0.2.100 ICNP 108 0xccc4 (52420) 64 Echo (ping) reply id=0x0001, seq=17/4352, ttl=64	
13 2022-07-14 20:20:39.585677043 192.0.2.100 198.51.100.100 ICMP 108 0x5b46 (23366) 64 Echo (ping) request id=0x0001, seg=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 0x5046 (23366) 64 Echo (ping) request id=0x0001, seg=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) reply id=0x0001, seg=18/4608, ttl=64 (request in 14)	
16 2022-07-14 20:20:39,585937900 198,51,100,100 192,0,2,100 ICMP 108 0xcd8d (52621) 64 Echo (ping) reply id=0x0001, seg=18/4608, ttl=64	
17 2022-07-14 20:20:40.609804804 192.0.2.100 198.51.100.100 ICMP 108 0x5b7b (23419) 64 Echo (ping) request id=0x0001. seq=19/4864. tt]=64 (no response found])	
18 2027-07-14 20:20:40.609087618 192.0.2.100 198.51.100.100 TCMP 108 0x5h7b (2341) 64 Feho (nino) request id=0x0001, seq=10/4864, tt]=64 (rent) in 19	
19 2022-07-14 20:20:40.610129685 198.51.100.100 192.0.2.100 TCMP 108 0xcd8f (52621) 64 Echo (ninp) reply id=0x0001, seq.10/4864, ttl=64 (request in 18)	
20 2027-07-14 20:20:40.610181944 198.51.100.100 192.0.2.100 TCNP 108 0xcd8f (52623) 64 Erbo (nino) renty (dayaoa), sea-10/4864, tt1=64	
21 2022-07-14 20:20:41.633805153 192.0.2.100 198.51.100.100 TONP 108 0x5h7e (23422) (4 Echo (ning) reput) tid_s0x0001.sequ20/5120.ttl=64 (no response found))	
222227.7.142612641633986907 192 196 51 196 51 196 197 198 51 196 199 198 51 196 198 51 196 199 198 51 196 199 198 51 196 199 198 51 196 199 198 51 196 199 198 51 196 199 198 51 196 199 198 51 196 199 198 51 196 199 198 51 196 199 198 51 196 199 198 51 196 199 198 51 196 199 198 51 196 199 198 51 196 199 198 51 196 199 198 51 196 199 198 51 19	
23 2022 07.41 20120-41 524045102 198 110 100 102 0.2 100 TKND 108 60000 (2012) 04 Cin (parg) request to downood, seq-20/5120, tt] = 64 (request in 27)	
2A 2012 01.44 EXECUTE AND ALL EXECUTES AND ALL EXECUTE	
25 2022-07-14 60720144.0557060306 102 0.2 104 105 51 104 104 101 104 0 0 0 0 0 0 0 0 0 0 0	
26 2020 27.4 2010 12.0 12.0 12.0 10.0	
272027-97-42 2010 12:001 22:001 22:001 12:001 100 100 100 100 100 100 100 100 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	
27 2022-07-14 201001421037300073 130:5111001100 132:02:100 1107 100 0XC042 (32007) 04 ECHO (PANg) (EPV 100-0X001) 60-21/576 (ELIOA (EQUESC AT 20)	
$20.2022^{-0/-4}$ 20.20^{-4} 20.20^{-4} $20.50^{-5/2}$ $50^{-5/2}$ $10^{-5/2}$ 10^{-	
29 2022-07-14 20:20:43.00173097 192.0.2.100 190.31.100.100 100 100 100 00302 (2004) 04 cuto (pang) request 10-000001, seq-22/3022, cu-04 (no response round)	
> Frame 3: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0 000 00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00 PV · X · · · w	e&
> Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: Whware 9d:e8:be (00:50:56:9d:e8:be) 001 00 0a 81 00 00 66 08 00 45 00 00 54 cc 2c 00 00f. E	т.,
VW-Tag 0020 40 01 c1 80 c6 33 64 64 c0 00 02 64 00 00 2a 68 g 3dd	d*h
0 Direction: To Bridge	
.0	
	x ()~+
Type: 802.1Q Virtual LAN (0x8100)	
✓ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102	
000 = Priority: Best Effort (default) (0)	
0000 0110 0110 = ID: 102	
Type: IPv4 (0x0000)	
> Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100	
Internet Control Message Protocol	

Spiegazione

Quando si configura un pacchetto da acquisire su un'interfaccia backplane, lo switch acquisisce simultaneamente ciascun pacchetto due volte. In questo caso, lo switch interno riceve i pacchetti che sono già stati contrassegnati dall'applicazione sul modulo di sicurezza con il tag port VLAN e il tag VN. Il tag VLAN identifica l'interfaccia in uscita usata dallo chassis interno per inoltrare i pacchetti alla rete. Il tag VLAN 103 nei pacchetti di richiesta echo ICMP identifica Ethernet 1/3 come interfaccia di uscita, mentre il tag VLAN 102 nei pacchetti di risposta echo ICMP identifica Ethernet 1/2 come interfaccia di uscita. Lo switch interno rimuove il tag VN e il tag VLAN dell'interfaccia interna prima che i pacchetti vengano inoltrati alla rete.

Nella tabella seguente viene riepilogata l'attività:

Attività	Punto di acquisizione	VLAN della porta interna nei pacchetti acquisiti	Direzione	Traffico acquisito
Configurazione e verifica delle acquisizioni dei pacchetti sulle interfacce backplane	Interfacce backplane	102 103	Solo in ingresso	Richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.100 ICMP echo risponde dall'host 198.51.100.100 all'host

		192.0.2.100

Acquisizione di pacchetti su porte applicazioni e porte applicazioni

Le acquisizioni di pacchetti di porte applicative o applicazioni vengono sempre configurate sulle interfacce backplane e sulle interfacce anteriori se l'utente specifica la direzione di acquisizione dell'applicazione.

Esistono principalmente 2 casi di utilizzo:

- Configurare le acquisizioni dei pacchetti sulle interfacce backplane per i pacchetti che lasciano un'interfaccia anteriore specifica. Ad esempio, configurare le acquisizioni dei pacchetti sull'interfaccia Ethernet1/9 del backplane per i pacchetti che lasciano l'interfaccia Ethernet1/2.
- Configurare le acquisizioni simultanee dei pacchetti su un'interfaccia anteriore specifica e sulle interfacce del backplane. Ad esempio, configurare l'acquisizione simultanea dei pacchetti sull'interfaccia Ethernet1/2 e sull'interfaccia backplane Ethernet1/9 per i pacchetti che lasciano l'interfaccia Ethernet1/2.

In questa sezione vengono illustrati entrambi i casi di utilizzo.

Attività 1

Usare FCM e CLI per configurare e verificare l'acquisizione di un pacchetto sull'interfaccia del backplane. Vengono acquisiti i pacchetti per i quali la porta dell'applicazione Ethernet1/2 è identificata come interfaccia in uscita. In questo caso, vengono acquisite le risposte ICMP.

Topologia, flusso dei pacchetti e punti di acquisizione



Configurazione

FCM

Per configurare l'acquisizione di un pacchetto sull'applicazione FTD e sulla porta Ethernet1/2

dell'applicazione, eseguire la procedura seguente su FCM:

1. Utilizzare Strumenti > Acquisizione pacchetti > Acquisisci sessione per creare una nuova sessione di acquisizione:

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

2. Selezionare l'applicazione Ethernet1/2 nell'elenco a discesa Porta applicazione e selezionare Pacchetto in uscita in Direzione di acquisizione applicazione. Specificare il Nome sessione e fare clic su Salva ed esegui per attivare l'acquisizione:

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

CLI FXOS

Eseguire questi passaggi sulla CLI di FXOS per configurare le acquisizioni dei pacchetti sulle interfacce backplane:

1. Identificare il tipo di applicazione e l'identificatore:

ftd	ftd1						
1		Enabled	Online	7.2.0.82	7.2.0.82	Native	No

```
2. Creare una sessione di acquisizione:
```

```
<#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 #
```

Verifica

FCM

Verificare il nome dell'interfaccia, verificare che lo stato operativo sia attivo e che le dimensioni del file (in byte) aumentino:

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		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		土				

CLI FXOS

Verificare i dettagli di acquisizione nell'ambito 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:

Raccogli file di acquisizione

Eseguire i passaggi descritti nella sezione Raccolta dei file di acquisizione degli switch interni Firepower 4100/9300.

Analisi dei file di acquisizione

Utilizzare un'applicazione per la lettura dei file di acquisizione dei pacchetti per aprire i file di acquisizione. Nel caso di più interfacce backplane, assicurarsi di aprire tutti i file di acquisizione per ciascuna interfaccia backplane. In questo caso, i pacchetti vengono acquisiti sull'interfaccia Ethernet1/9 del backplane.

Selezionare il primo e il secondo pacchetto e verificare i punti principali:

- 1. Ogni risposta echo ICMP viene acquisita e visualizzata 2 volte.
- 2. L'intestazione del pacchetto originale è senza il tag VLAN.
- 3. Lo switch interno inserisce un tag VLAN 102 aggiuntivo che identifica l'interfaccia di uscita Ethernet1/2.
- 4. Lo switch interno inserisce un tag VN aggiuntivo.

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 (DINR) 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, seq=9/2304, ttl=64
19 2022-08-01 10:03:31.402772217	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18842)	64 Echo (ping) reply	id=0x0012, seq=10/2560, ttl=64
20 2022-08-01 10:03:31.402774775	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18842)	64 Echo (ping) reply	id=0x0012, seq=10/2560, ttl=64
21 2022-08-01 10:03:32.426693254	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64 Echo (ping) reply	id=0x0012, 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
C							
> Frame 1: 108 bytes on wire (864 bit: > Ethernet II, Src: Cisco b9:77:00 (Si VN-Tag 0	<pre>s), 108 bytes ca 8:97:bd:b9:77:0e</pre>	ptured (864 bits) o), Dst: VMware 9d: ion: To Bridge r: vif_id iNO d: 0 1: 0 2: 10 sult) (0) st: 192.0.2.100	n interface ca 82:be (00:50:50 4	apture_u@_ 5:9d:e8:be	8, id 0)		30000 00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00

Spiegazione

In questo caso, Ethernet 1/2 con tag VLAN 102 è l'interfaccia di uscita per i pacchetti di risposta echo ICMP.

Quando la direzione di acquisizione dell'applicazione è impostata su Egress nelle opzioni di acquisizione, i pacchetti con il tag VLAN della porta 102 nell'intestazione Ethernet vengono catturati sulle interfacce del backplane nella direzione in entrata.

Nella tabella seguente viene riepilogata l'attività:

Attività	Punto di acquisizione	VLAN della porta interna nei pacchetti acquisiti	Direzione	Traffico acquisito
Configurazione e verifica delle acquisizioni sulla porta dell'applicazione e sulla porta Ethernet1/2	Interfacce backplane	102	Solo in ingresso	ICMP echo risponde dall'host 198.51.100.100 all'host 192.0.2.100

Attività 2

Usare FCM e CLI per configurare e verificare l'acquisizione di un pacchetto sull'interfaccia backplane e sull'interfaccia anteriore Ethernet1/2.

Le acquisizioni simultanee dei pacchetti sono configurate su:

- Front interface (interfaccia anteriore) cattura i pacchetti con la porta VLAN 102 sull'interfaccia Ethernet 1/2. I pacchetti acquisiti sono richieste echo ICMP.
- Interfacce backplane: pacchetti per cui Ethernet1/2 è identificata come interfaccia in uscita o pacchetti con la porta VLAN 102 vengono acquisiti. I pacchetti acquisiti sono risposte echo ICMP.

Topologia, flusso dei pacchetti e punti di acquisizione



Configurazione

FCM

Per configurare l'acquisizione di un pacchetto sull'applicazione FTD e sulla porta Ethernet1/2 dell'applicazione, eseguire la procedura seguente su FCM:

1. Utilizzare Strumenti > Acquisizione pacchetti > Acquisisci sessione per creare una nuova sessione di acquisizione:

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

2. Selezionare l'applicazione FTD Ethernet1/2 nell'elenco a discesa Porta applicazione e selezionare All Packets in Application Capture Direction. Specificare il Nome sessione e fare clic su Salva ed esegui per attivare l'acquisizione:

Overview I	nterfaces Logical Devices Security Engine	Natform Settings				Sy	rstem Tools Help admin
Select an instar	rce: 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	1		
		Ethernet1/9, Ethernet1/10	Application Capture Direction	All Packets Egress Packet			
			Capture Filter	Apply Filter Capture All	Г		
Ethernet1/1							

CLI FXOS

Eseguire questi passaggi sulla CLI di FXOS per configurare le acquisizioni dei pacchetti sulle interfacce backplane:

1. Identificare il tipo di applicazione e l'identificatore:

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

2. Creare una sessione di acquisizione:

```
<#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
```

Verifica

FCM

Verificare il nome dell'interfaccia, verificare che lo stato operativo sia attivo e che le dimensioni del file (in byte) aumentino:

Overview Interfaces L	ogical Devices Security Engine Plat	form Settings				System To	ools Help a	idmin
Capture Session Filter List								
					6	C Refresh	Capture Session	Del
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	None	95040	cap1-ethernet-1-2-0.pcap	ftd1	±			
Ethernet1/2 - Ethernet1/10	None	368	cap1-vethernet-1175.pcap	ftd1	4			
Ethernet1/2 - Ethernet1/9	None	13040	cap1-vethernet-1036.pcap	ftd1	2			

CLI FXOS

Verificare i dettagli di acquisizione nell'ambito 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

```
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:
```

Raccogli file di acquisizione

Eq Port Id: 10

Eseguire i passaggi descritti nella sezione Raccolta dei file di acquisizione degli switch interni Firepower 4100/9300.

Analisi dei file di acquisizione

Utilizzare un'applicazione per la lettura dei file di acquisizione dei pacchetti per aprire i file di acquisizione. Nel caso di più interfacce backplane, assicurarsi di aprire tutti i file di acquisizione per ciascuna interfaccia backplane. In questo caso, i pacchetti vengono acquisiti sull'interfaccia Ethernet1/9 del backplane.

Aprire il file di acquisizione per l'interfaccia Ethernet1/2, selezionare il primo pacchetto e controllare i punti chiave:

- 1. Vengono acquisiti solo pacchetti di richieste echo ICMP. Ogni pacchetto viene acquisito e mostrato 2 volte.
- 2. L'intestazione del pacchetto originale è senza il tag VLAN.
- 3. Lo switch interno inserisce un tag VLAN 102 aggiuntivo che identifica l'interfaccia in entrata Ethernet 1/2.
- 4. Lo switch interno inserisce un tag VN aggiuntivo.

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 (4	9161) 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 (4	9161) 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	8XC889 (4	9161) 64 ECNO	(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	8xc889 (4	9161) 64 Echo	(ping)	request	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	BxcBae (4	9326) 64 Echo	(ping)	request	id=0x0013, seq=2/512, ttl=64 (no response foundl)
	6 2022-00-01 11-22-20 072020200	192 8 2 188	109 51 100 100	TCMP	102	BycBao (4	0326) 64 Echo	(ping)	request	id=0x0013 seq=3/512 ttl=64 (no response foundl)
	7 2022 00 01 11:33:20:072030399	102.0.2.100	100 51 100 100	TCHD	102	0xc00e (4	(520) 04 ECh	(ping)	request	id-0x0013, seq-2/322, ttl-64 (no response found)
	/ 2022-08-01 11:33:21.0/3200030	192.0.2.100	198.51.100.100	ICHP	108	0XC107 (4	(9511) 64 ECHC	(ping) i	request	id=0x0015, seq=3/768, ttl=04 (no response round)
	8 2022-08-01 11:33:21.0/320832/	192.0.2.100	198.51.100.100	ICHP	102	0xc167 (4	9511) 64 ECRG	(ping) i	request	1d=0x0013, seq=3/768, tt1=04 (no response round)
	9 2022-08-01 11:33:22.074576640	192.0.2.100	198.51.100.100	ICMP	108	0xc175 (4	(9525) 64 Echo	(ping) r	request	1d=0x0013, seq=4/1024, tt1=64 (no response found!)
	10 2022-08-01 11:33:22.074578010	192.0.2.100	198.51.100.100	ICMP	102	0xc175 (4	9525) 64 Echo) (ping) r	request	id=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 (4	.9672) 64 Echo) (ping) r	request	id=0x0013, seq=5/1280, ttl=64 (no response found!)
	12 2022-08-01 11:33:23.075781513	192.0.2.100	198.51.100.100	ICMP	102	0xc208 (4	9672) 64 Echo) (ping) r	request	id=0x0013, seq=5/1280, ttl=64 (no response found!)
	13 2022-08-01 11:33:24.081839490	192.0.2.100	198.51.100.100	ICMP	108	0xc211 (4	9681) 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 (4	9681) 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	Øxc2e2 (4	9890) 64 Echo	(ping) r	request	id=0x0013, seg=7/1792, ttl=64 (no response found!)
	16 2022-08-01 11:33:25.105807895	192.0.2.100	198,51,100,100	ICMP	102	Øxc2e2 (4	9890) 64 Echo	(ping)	request	id=0x0013, seg=7/1792, ttl=64 (no response found!)
	17 2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	TCMP	108	exc3h4 (5	(0100) 64 Echo	(ning)	request	id=0x0013, seq=8/2048, ttl=64 (no response found))
	10 2022 00 01 11:33:26 120030114	102 0 2 100	100 51 100 100	TCMD	100	Oxeah4 (5	0100) 64 Eche	(ping)	request	(d-0x0013, seq-0/2040, ttl-64 (no response found))
	10 2022-00-01 11.55.20.125050114	192.0.2.100	190.51.100.100	TCHP	102	0xc304 (5	0100) 04 ECIN	(ping)	request	id-0x0013, seq=0/2040, ttl=64 (no response found!)
	19 2022-08-01 11.33.27.133828033	192.0.2.100	198.51.100.100	ICHP	108	0AC470 (5	0294) 04 ECIIC	(ping) i	equest	id exects, 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	0xc4/6 (5	(0294) 64 ECho	(ping) r	request	1d=0x0013, seq=9/2304, tt1=64 (no response round!)
	21 2022-08-01 11:33:28.177847175	192.0.2.100	198.51.100.100	ICMP	108	0xc516 (5	(8454) 64 Echo	(ping) r	request	1d=0x0013, seq=10/2560, tt1=64 (no response found!)
	22 2022-08-01 11:33:28.177849075	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (5	0454) 64 Echo	o (ping) r	request	id=0x0013, seq=10/2560, ttl=64 (no response found!)
	23 2022-08-01 11:33:29.201804760	192.0.2.100	198.51.100.100	ICMP	108	0xc578 (5	0552) 64 Echo	o (ping) n	request	id=0x0013, seq=11/2816, ttl=64 (no response found!)
	24 2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	102	0xc578 (5	0552) 64 Echo	o (ping) n	request	id=0x0013, seq=11/2816, ttl=64 (no response found!)
	25 2022-08-01 11:33:30.225834765	192.0.2.100	198.51.100.100	ICMP	108	0xc585 (5	0565) 64 Echo	(ping) r	request	id=0x0013, seq=12/3072, ttl=64 (no response found!)
	26 2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (5	0565) 64 Echo	(ping)	request	id=0x0013, seq=12/3072, ttl=64 (no response found!)
	27 2022-08-01 11:33:31.249828955	192.0.2.100	198.51.100.100	ICMP	108	0xc618 (5	0712) 64 Echo	(ping) r	request	id=0x0013, seq=13/3328, ttl=64 (no response found!)
	28 2022-08-01 11:33:31.249831121	192.0.2.100	198.51.100.100	ICMP	102	0xc618 (5	(0712) 64 Echo	(ping)	request	id=0x0013, seg=13/3328, ttl=64 (no response found!)
	29 2822-88-81 11:33:32.273867968	192.0.2.100	198.51.100.100	TCMP	108	0xc64f (5	0767) 64 Echo	(ping)	request	id=0x0013, seg=14/3584, ttl=64 (no response found!)
<				2011				(bru0) .	edacae	re-onorry sequences (no response round)
	and 1, 100 butes on view (064 bit	 top butter en 	stuned (BEA bits) a	. intenfere co	eture un	1 14 0				0 50 07 bd b0 77 00 00 50 56 0d o0 bo 00 26 00 00 V
2 11	ame 1: 108 bytes on wire (864 bit	s), 108 bytes ca	ptured (864 Dits) o	i interrace ca	pture_uo_	1, 10 0			000	0 36 97 00 09 77 00 00 50 50 90 08 00 89 20 80 08 A W P V A
	thernet 11, SFC: VMware 90:08:De (00:50:56:90:68:00	e), DST: C15C0 D9:/	(28:97:00	:09:77:0e)			002	
∽ vi	I-Tag								002	a a 13 aa a1 f2 ha a7 62 aa aa aa aa aa ch 7f a6 aa
	1	= Directi	on: From Bridge						003	0 00 13 00 01 12 05 07 02 00 00 00 00 00 00 00 00 00 00 00 00
	.0	= Pointer	: vif_id						005	1 c 1d 1a 1f 20 21 22 23 24 25 26 27 28 29 28 2b ["# \$\$\$\$'()*+
		= Destina	tion: 10							a 2c 2d 2e 2f 3a 31 32 33 34 35 36 37
	···· ··· ··· ··· ··· 0 ····	= Looped:	NO							, to be set to be
	0	= Reserve	d: 0	·						
		= Version	: 0							
	0000 000	00 0000 = Source:	0							
	Type: 802.10 Virtual LAN (0x8100)									
V 80	2.10 Virtual LAN, PRI: 0, DET: 0.	ID: 102								
	000 = Priority	Rest Effort (defa	ult) (0)							
	- DET: Toolic	vible								
	= DEI: Inellg	linie.								
	0000 0110 0110 = 1D: 102									
	Type: 1PV4 (0x0800)			_						
> It	iternet Protocol Version 4, Src: 1	92.0.2.100, Dst:	198.51.100.100							
> It	nternet Control Message Protocol		6							

Selezionare il secondo pacchetto e controllare i punti chiave:

- 1. Vengono acquisiti solo pacchetti di richieste echo ICMP. Ogni pacchetto viene acquisito e mostrato 2 volte.
- 2. L'intestazione del pacchetto originale è senza il tag VLAN.
- 3. Lo switch interno inserisce un tag VLAN 102 aggiuntivo che identifica l'interfaccia in entrata Ethernet 1/2.

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									

Aprire il file di acquisizione per l'interfaccia Ethernet1/9, selezionare il primo e il secondo pacchetto e controllare i punti chiave:

- 1. Ogni risposta echo ICMP viene acquisita e visualizzata 2 volte.
- 2. L'intestazione del pacchetto originale è senza il tag VLAN.
- 3. Lo switch interno inserisce un tag VLAN 102 aggiuntivo che identifica l'interfaccia di uscita Ethernet1/2.
- 4. Lo switch interno inserisce un tag VN aggiuntivo.

						-		
No. Time	Source	Destination	Protocol	Length	PD	PTTL Info	11	
1 2022-08-01 11:33:19.0/1512098	198.51.100.100	192.0.2.100	ICHP	108	0x4127 (20263)	64 Echo (ping) reply	10=0x0013, Seq=1/250, tt1=04	
2 2022-08-01 11:33:19.0/1514882	198.51.100.100	192.0.2.100	ICMP	108	0x4127 (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)	of Ecuo (brug) Lebi	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, seq=12/3072, ttl=64	
25 2022-08-01 11:33:31.250387808	198.51.100.100	192.0.2.100	ICMP	108	0x55f2 (22002)	64 Echo (ping) reply	id=0x0013, 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	
¢						or come (hang) , cha	an outside and and and outside	
Ename 1: 108 bytes on wire (864 bit	s). 108 bytes ca	ntured (864 hits)	n interface c	anture uB	8. id 0		0000 00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00 PVX	
Ethernet II. Src: Cisco b9:77:0e (5	9 • 97 • hd • h9 • 77 • 00) Det: Whene 9d:	R he (00.50.5)	6 • 9d • e8 • be	a)		0010 00 0a 81 00 00 66 08 00 45 00 00 54 4f 27 00 00f. E. TO'	
VN-Tag	0137100103177100	7, oser windre san	0100 (0015015	0150100100	-/		0020 40 01 3e 86 c6 33 64 64 c0 00 02 64 00 00 95 7c @->3ddd	1
0	- Directi	ion: To Bridge	_				0030 00 13 00 01 f2 b9 e7 62 00 00 00 cb 7f 06 00bb	
A	= Pointer	wif id					0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b	
00 0000 0000 0000	- Docting	tion: 0					0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ···· !"# \$%&'()*e	+
	- Looped	No.					0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,/0123 4567	
		d: 0	4					
	- Version							
		. 10						
Turner 002 to Mintural Lth (overlage	00 1010 = 2001.ce:	10						
Type: 802.10 VIrtual LAN (0x8100	70: 400		_					
002.10 VIPTUAL LAN, PKI: 0, DEI: 0,	10: 102 Dest Effect (def	with) (0)						
000 = Priority:	est Effort (defa	JUIL) (0)						
	giore		5					
0000 0110 0110 = ID: 102								
Type: IPv4 (0x0800)	00 54 400 405 5	-+- +00 0 0 400	_					
Internet Protocol Version 4, Src: 1	198.51.100.100, D	st: 192.0.2.100	2					
Internet Control Message Protocol			6					

Spiegazione

Se si seleziona l'opzione All Packets in the Application Capture Direction, vengono configurate due acquisizioni simultanee di pacchetti relative alla porta dell'applicazione selezionata Ethernet1/2: un'acquisizione sull'interfaccia anteriore Ethernet1/2 e un'acquisizione sulle interfacce del backplane selezionate.

Quando si configura la cattura di un pacchetto su un'interfaccia anteriore, lo switch acquisisce simultaneamente ciascun pacchetto due volte:

- Dopo l'inserimento del tag VLAN della porta.
- Dopo l'inserimento del tag VN.

Nell'ordine delle operazioni, il tag VN viene inserito in una fase successiva all'inserimento del tag VLAN della porta. Tuttavia, nel file di acquisizione, il pacchetto con il tag VN viene visualizzato prima del pacchetto con il tag port VLAN. Nell'esempio, il tag VLAN 102 nei pacchetti di richiesta echo ICMP identifica Ethernet 1/2 come interfaccia in entrata.

Quando si configura un pacchetto da acquisire su un'interfaccia backplane, lo switch acquisisce simultaneamente ciascun pacchetto due volte. Lo switch interno riceve i pacchetti che sono già stati contrassegnati dall'applicazione sul modulo di sicurezza con il tag della porta VLAN e il tag VN. Il tag port VLAN identifica l'interfaccia in uscita usata dallo chassis interno per inoltrare i

pacchetti alla rete. Nell'esempio, il tag VLAN 102 nei pacchetti di risposta echo ICMP identifica Ethernet1/2 come interfaccia di uscita.

Lo switch interno rimuove il tag VN e il tag VLAN dell'interfaccia interna prima che i pacchetti vengano inoltrati alla rete.

Nella tabella seguente viene riepilogata l'attività:

Attività	Punto di acquisizione	VLAN della porta interna nei pacchetti acquisiti	Direzione	Traffico acquisito
Configurazione e verifica delle acquisizioni sulla porta dell'applicazione e sulla porta Ethernet1/2	Interfacce backplane	102	Solo in ingresso	ICMP echo risponde dall'host 198.51.100.100 all'host 192.0.2.100
	Interfaccia Ethernet1/2	102	Solo in ingresso	Richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.100

Acquisizione di pacchetti su una sottointerfaccia di un'interfaccia fisica o di un canale della porta

Usare FCM e CLI per configurare e verificare l'acquisizione di un pacchetto sull'interfaccia secondaria Ethernet1/2.205 o Portchannel1.207. Le sottointerfacce e le acquisizioni sulle sottointerfacce sono supportate solo per l'applicazione FTD in modalità contenitore. In questo caso, viene configurata l'acquisizione di un pacchetto su Ethernet1/2.205 e Portchannel1.207.

Topologia, flusso dei pacchetti e punti di acquisizione



Configurazione

FCM

Per configurare l'acquisizione di un pacchetto sull'applicazione FTD e sulla porta Ethernet1/2 dell'applicazione, eseguire la procedura seguente su FCM:

1. Utilizzare Strumenti > Acquisizione pacchetti > Acquisisci sessione per creare una nuova sessione di acquisizione:

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. Selezionare l'istanza specifica dell'applicazione ftd1, la sottointerfaccia Ethernet1/2.205, fornire il nome della sessione e fare clic su Salva ed esegui per attivare l'acquisizione:

Overview Interfaces Logical Devices Security Engine Platform Settings	System Tools Help admin
Select an instance: ftd1 🗸	Save and Run Save Cancel
Subinterface selection ftd1 [themet1/2.205 [themet1/2.206	Session Name" [ap1] Selected Interfaces Ethernet1/2.205
Subinterfaces(2) Ethernet1/2	Buffer Size 256 MB Sinap length: 1518 Bytes Store Packets Overwrite Append
Etheret/10	Capture Filter Apply Filter Cepture All
Ethernet1/1	

3. Nel caso di una sottointerfaccia port-channel, a causa dell'ID bug Cisco <u>CSCvq3119</u> le sottointerfacce non sono visibili in FCM. Usare la CLI di FXOS per configurare le acquisizioni sulle sottointerfacce del canale della porta.

CLI FXOS

Attenersi alla seguente procedura dalla CLI di FXOS per configurare l'acquisizione di un pacchetto sulle sottointerfacce Ethernet1/2.205 e Portchannel1.207:

1. Identificare il tipo di applicazione e l'identificatore:

<#I	°OC	ot>

firepower#

scope ssa

firepower /ssa #

show	app-inst	tance
	-F.F	

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. Nel caso di un'interfaccia porta-canale, identificare le relative interfacce membro:

<#roo	t>				
firepo	ower#				
connec	et fxos				
<outpu firepo 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	rt-channel (n dby (LACP on] emoved t met	nembers) y)	
Group	Port- Type Channel	Protocol	Member Ports	 5 	
1	Pol(SU) Eth	LACP	Eth1/3(P)	Eth1/3(P)	

3. Creare una sessione di acquisizione:

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

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

firepower /packet-capture/session #

Per le sottointerfacce del canale della porta, creare un'acquisizione di pacchetto per ogni interfaccia membro del canale della porta:

```
<#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 #

Verifica

FCM

Verificare il nome dell'interfaccia, verificare che lo stato operativo sia attivo e che le dimensioni del

file (in byte) aumentino:

Overview Interfaces Logic	al Devices Security Engine Platform	n Settings			s	iystem Tools Help admin
Capture Session Filter Lat					(# talach) Casture Service	Public Al Environm
(D) (D)			n - 6		C Anneal Colour Annou	
Capr	brop Coant. o	Operational state: up	Builer Size, 230 HB		anap cengue. 1510 bytes	A 3 2
Interface Name	Filter	File Size (in bytes)	File Name	Device Name		
Ethernet1/2.205	None	233992	cap1-ethernet-1-2-0.pcap	ftd1	2	

Le acquisizioni della sottointerfaccia del canale della porta configurate nella CLI di FXOS sono visibili anche in FCM; tuttavia, non possono essere modificate:

Overview Interfaces Log	gical Devices Security Engine Platform Se	ttings				System Tools Help admin
Capture Session Fiter List						
					Capture Session	Delete Al Sessions
cap1	Drop Count: 0	Operational State: up	Buffer Size: 256 HB		Snap Length: 1518 Bytes	A.8.0
Interface Name	Filter	File Size (in bytes)	File Name	Device Name		
Ethernet1/4.207	None	624160	cap1-ethemet-1-4-0.pcap	Not available	*	
Ethernet1/3.207	None	160	cap1-ethernet-1-3-0.pcap	Not available	土	

CLI FXOS

Verificare i dettagli di acquisizione nell'ambito 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 con interfacce membro Ethernet1/3 e 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

Raccogli file di acquisizione

Eseguire i passaggi descritti nella sezione Raccolta dei file di acquisizione degli switch interni Firepower 4100/9300.

Analisi dei file di acquisizione

Utilizzare un'applicazione per la lettura dei file di acquisizione dei pacchetti per aprire il file di acquisizione. Selezionare il primo pacchetto e controllare i punti chiave:

- 1. Vengono acquisiti solo pacchetti di richieste echo ICMP. Ogni pacchetto viene acquisito e mostrato 2 volte.
- 2. L'intestazione del pacchetto originale ha il tag VLAN 205.
- 3. Lo switch interno inserisce un tag VLAN 102 aggiuntivo che identifica l'interfaccia in entrata Ethernet 1/2.
- 4. Lo switch interno inserisce un tag VN aggiuntivo.

No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info		
F	1 2022-08-04 07:21:56.993302102	192.0.2.100	198.51.100.100	ICMP	112	0x9574 (38260)	64 Echo (ping) requ	Jest	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) requ	Jest	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) requ	Jest	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) requ	Jest	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) requ	est	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) requ	est	id=0x0022, seq=11/2816, ttl=64 (no response found!)
	7 2022-08-04 07:22:08.229938577	192.0.2.100	198.51.100.100	ICMP	112	0x9b33 (39731)	64 Echo (ping) requ	iest	id=0x0022, seq=12/3072, ttl=64 (no response found!)
	8 2022-08-04 07:22:08.229940829	192.0.2.100	198.51.100.100	ICMP	102	0x9b33 (39731)	64 Echo (ping) requ	est	<pre>id=0x0022, seq=12/3072, ttl=64 (no response found!)</pre>
	9 2022-08-04 07:22:09.253944601	192.0.2.100	198.51.100.100	ICMP	112	0x9c0e (39950)	64 Echo (ping) requ	iest	<pre>id=0x0022, seq=13/3328, ttl=64 (no response found!)</pre>
	10 2022-08-04 07:22:09.253946899	192.0.2.100	198.51.100.100	ICMP	102	0x9c0e (39950)	64 Echo (ping) requ	iest	id=0x0022, seq=13/3328, ttl=64 (no response found!)
	11 2022-08-04 07:22:10.277953070	192.0.2.100	198.51.100.100	ICMP	112	0x9ccb (40139)	64 Echo (ping) requ	iest	id=0x0022, seq=14/3584, ttl=64 (no response found!)
	12 2022-08-04 07:22:10.277954736	192.0.2.100	198.51.100.100	ICMP	102	0x9ccb (40139)	64 Echo (ping) requ	est	<pre>id=0x0022, seq=14/3584, ttl=64 (no response found!)</pre>
	13 2022-08-04 07:22:11.301931282	192.0.2.100	198.51.100.100	ICMP	112	0x9d84 (40324)	64 Echo (ping) requ	est	1d=0x0022, seq=15/3840, ttl=64 (no response found!)
	14 2022-08-04 07:22:11.301933600	192.0.2.100	198.51.100.100	ICMP	102	0x9d84 (40324)	64 Echo (ping) requ	est	1d=0x0022, seq=15/3840, tt1=64 (no response found!)
	15 2022-08-04 07:22:12.325936521	192.0.2.100	198.51.100.100	ICMP	112	0x9da2 (40354)	64 Echo (ping) requ	est	1d=0x0022, seq=16/4096, ttl=64 (no response found!)
	16 2022-08-04 07:22:12.325937895	192.0.2.100	198.51.100.100	ICMP	102	0x9da2 (40354)	64 Echo (ping) requ	lest	1d=0x0022, seq=16/4096, tt1=64 (no response tound!)
	17 2022-08-04 07:22:13.326988040	192.0.2.100	198.51.100.100	ICMP	112	0x9e07 (48455)	64 Echo (ping) requ	lest	1d=0x0022, seq=17/4352, ttl=64 (no response found!)
	18 2022-08-04 07:22:13.326990258	192.0.2.100	198.51.100.100	ICMP	102	0x9e07 (48455)	64 Echo (ping) requ	lest	1d=0x0022, seq=1//4352, ttl=64 (no response found!)
	19 2022-08-04 07:22:14.341944773	192.0.2.100	198.51.100.100	TCMP	112	0x9e6a (40554)	64 Echo (ping) requ	lest	id=0x0022, seq=18/4608, ttl=64 (no response found!)
	20 2022-08-04 07:22:14.341946249	192.0.2.100	198.51.100.100	ICMP	102	0x9e6a (40554)	64 Echo (ping) requ	lest	1d=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	TCMP	112	0x9010 (40699)	64 Echo (ping) requ	lest	id=0x0022, seq=19/4864, ttl=64 (no response found!)
	22 2022-00-04 07:22:15.303942300	192.0.2.100	198.51.100.100	ICMP	102	0x9610 (40099)	64 Echo (ping) requ	lost	id=0x0022, seq=19/4804, ttl=04 (no response found))
	23 2022-00-04 07:22:10.309973043	192.0.2.100	198.51.100.100	TCMP	102	0x9fe8 (40936)	64 Echo (ping) requ	lost .	id=0x0022, seq=20/5120, tt1=04 (no response found1)
	24 2022-00-04 07:22:10.309975129	192.0.2.100	198.51.100.100	ICMP	112	0X9108 (40950)	64 Echo (ping) requ	iost .	id=0x0022, seq=20/5120, ((1=04 (no response found))
	25 2022-08-04 07:22:17.413930452	192.0.2.100	198.51.100.100	TCMP	102	0x3079 (41081) 0x3070 (41081)	64 Echo (ping) requ	lost	id=0x0022, seq=21/5376, ttl=64 (no response found1)
	20 2022-00-04 07:22.17.413930090	102.0.2.100	100 51 100 100	TCMD	112	0x3079 (41001)	64 Echo (ping) requ	nest .	id=0x0022, seq=21/55/0, (cl=04 (no response foundl)
ι.	27 2022-00-04 07.22.10.437354333	19210121100	190.91.100.100	ICIP	***	0x0116 (41240)	or cono (pring) requ	icse .	in response foundly
5									
2	Frame 1: 112 bytes on wire (896 bit	ts), 112 bytes ca	ptured (896 bits) o	n interface ca	pture_u0_	1, id 0		0000	a2 76 f2 00 00 1b 00 50 56 9d e8 be 89 26 80 54 · · · · · · · · · · · · · · · · · ·
2	Ethernet II, Src: VMware 9d:e8:be	(00:50:56:9d:e8:b	e), Dst: a2:76:f2:0	0:00:1b (a2:76	5:f2:00:00	:1b)		0010	00 00 81 00 00 00 81 00 00 cd 08 00 45 00 00 54
M	VN-Tag							0020	95 74 40 00 40 01 08 38 C0 00 02 64 C0 33 64 64
	1	= Direct:	ion: From Bridge					0040	d9 9d 00 00 00 00 00 00 10 11 12 13 14 15 16 17
	.0	= Pointer	r: v1t_1d					0050	18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 !"#\$38"
		= Destina	ation: 84	4				0060	28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ()*+,/ 01234567
	0	= Looped	NO	+					
		= Reserve	20:0						
		= Version	1: 0						
		00 0000 = Source:	: 0						
Ŀ	Type: 802.10 Virtual LAN (0X8100	10: 102		_					
1	202. IQ VIFTUAI LAN, PKI: 0, DEI: 0	, ID; 102 Post Effort (dof:	w1+) (0)						
	ooo Priority:	sest errort (dera	surc) (0)						
		Rinis							
	0000 0110 0110 = 10: 102								
L	Type: 802.10 VIPCual LAN (0X8100	10: 205		_					
1	802.10 VIFtual LAN, PKI: 0, DEI: 0	, 10: 205 Bost Effort (dof:	w1+) (0)						
11	000 = Priority:	est errort (defa	urc) (0)						
11	DEI: Ineli	R1016							
П	0000 1100 1101 = ID: 205			21					
IJ	Type: IPV4 (0x0800)	03 0 3 100 0.4.	100 51 100 100	-					
11	Internet Protocol Version 4, Src: 1	192.0.2.100, Dst:	198.51.100.100						
1	incernet control Message Protocol								
•									
-									

Selezionare il secondo pacchetto e controllare i punti chiave:

- 1. Vengono acquisiti solo pacchetti di richieste echo ICMP. Ogni pacchetto viene acquisito e mostrato 2 volte.
- 2. L'intestazione del pacchetto originale ha il tag VLAN 205.

1 2022-08-04 07:21:56.993302102 192.0.2.100 198.51.100.100 ICMP 112 0x9574 (38260) 64 Echo (ping) request id-0x0022, seq=1/256, ttl=64 (no response found!) 2 2022-08-04 07:21:56.993305597 192.0.2.100 198.51.100.100 ICMP 102 0x9574 (38260) 64 Echo (ping) request id-0x0022, seq=1/256, ttl=64 (no response found])
2 2022-08-04 07:21:56-993103597 192.0.2.100 198.51.100.100 10/ 10/ 102 000574 (38260) 64 Echo (ping) request [d=0x0022, sq=1/256, t11=64 (no response found]) 000101 (100100 10010 10010 10010 10010 10010 10010 1000000
2 2022-09-04 07-22 06 214264777 102 0 2 100 100 51 100 100 1/WP 112 0/00-021 (20552) 64 5/b0 (ning) nonunet id-0/0022 con=10/2560 tt]=64 (no reconce found)
2 YOYY-00-04 CLEAROALLY TAYOUTTOD TOLD THE TAY ON AND TOLD TOLD TOLD TOLD TOLD TOLD TOLD TOL
4 2022-08-04 07:22:06.214267373 192.0.2.100 198.51.100.100 ICMP 102 0x9a81 (39553) 64 Echo (ping) request id=0x0022, seq=10/2560, ttl=64 (no response found)
5 2022-08-04 07:22:07.215113393 192.0.2.100 198.51.100.100 ICMP 112 0x9ac3 (39619) 64 Echo (ping) request id=0x0022, seq=11/2816, ttl=64 (no response found!)
6 2022-08-04 07:22:07.215115445 192.0.2.100 198.51.100.100 ICMP 102 0x9ac3 (39619) 64 Echo (ping) request id=0x0022, seq=11/2816, ttl=64 (no response found1)
7 2022-08-04 07:22:08.229938577 192.0.2.100 198.51.100.100 ICMP 112 0x9b33 (39731) 64 Echo (ping) request id=0x0022, seq=12/3072, ttl=64 (no response found1)
8 2022-08-04 07:22:08.229940829 192.0.2.100 198.51.100.100 ICMP 102 0x9b33 (39731) 64 Echo (ping) request id=0x0022, seq=12/3072, ttl=64 (no response found1)
9 2022-08-04 07:22:09.253944601 192.0.2.100 198.51.100.100 ICMP 112 0x9c0e (39950) 64 Echo (ping) request id=0x0022, seq=13/3328, ttl=64 (no response found1)
10 2022-08-04 07:22:09.253946899 192.0.2.100 198.51.100.100 ICMP 102 0x9c0e (39950) 64 Echo (ping) request id=0x0022, seq=13/3328, ttl=64 (no response found))
11 2022-08-04 07:22:10.277953070 192.0.2.100 198.51.100.100 ICMP 112 0x9ccb (40139) 64 Echo (ping) request id=0x0022, seq=14/3584, ttl=64 (no response found))
12 2022-08-04 07:22:10.277954736 192.0.2.100 198.51.100.100 ICMP 102 0x9ccb (40139) 64 Echo (ping) request id=0x0022, seq=14/3584, ttl=64 (no response found))
13 2022-08-04 07:22:11.301931282 192.0.2.100 198.51.100.100 ICMP 112 0x9d84 (40324) 64 Echo (ping) request id=0x0022, seq=15/3840, ttl=64 (no response foundl)
14 2022-08-04 07:22:11.301933600 192.0.2.100 198.51.100.100 ICMP 102 0x9d84 (40324) 64 Echo (ping) request id=0x0022, seq=15/3840, tt]=64 (no response found])
15 2022-08-04 07:22:12.325936521 192.0.2.100 198.51.100.100 ICMP 112 0x9da2 (40354) 64 Echo (ping) request id=0x0022, seq=16/4096, ttl=64 (no response found)
16 2022-08-04 07:22:12.325937895 192.0.2.100 198.51.100.100 ICMP 102 0x9da2 (40354) 64 Echo (ping) request id=0x0022, seq=16/4096, ttl=64 (no response found1)
17 2022-08-04 07:22:13.326988040 192.0.2.100 198.51.100.100 ICMP 112 0x9e07 (40455) 64 Echo (ping) request id=0x0022, seq=17/4352, ttl=64 (no response found)
18 2022-08-04 07:22:13.326990258 192.0.2.100 198.51.100.100 ICMP 102 0x9e07 (40455) 64 Echo (ping) request id=0x0022, seq=17/4352, ttl=64 (no response found))
19 2022-08-04 07:22:14.341944773 192.0.2.100 198.51.100.100 ICMP 112 0x9e6a (40554) 64 Echo (ping) request id=0x0022, seq=18/4608, ttl=64 (no response found!)
20 2022-08-04 07:22:14.341946249 192.0.2.100 198.51.100.100 ICMP 102 0x9e6a (40554) 64 Echo (ping) request id=0x0022, seq=18/4608, ttl=64 (no response found1)
21 2022-08-04 07:22:15.365941588 192.0.2.100 198.51.100.100 ICMP 112 0x9efb (40699) 64 Echo (ping) request id=0x0022, seq=19/4864, ttl=64 (no response found!)
22 2022-08-04 07:22:15.365942566 192.0.2.100 198.51.100.100 ICMP 102 0x9efb (40699) 64 Echo (ping) request id=0x0022, seq=19/4864, ttl=64 (no response found1)
23 2022-08-04 07:22:16.389973843 192.0.2.100 198.51.100.100 ICMP 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 ICMP 102 0x9fe8 (40936) 64 Echo (ping) request id=0x0022, seq=20/5120, ttl=64 (no response found1)
25 2022-08-04 07:22:17.413936452 192.0.2.100 198.51.100.100 ICMP 112 0xa079 (41081) 64 Echo (ping) request id=0x0022, seq=21/5376, ttl=64 (no response found1)
26 2022-08-04 07:22:17.413938090 192.0.2.100 198.51.100.100 ICMP 102 0xa079 (41081) 64 Echo (ping) request id=0x0022, seq=21/5376, ttl=64 (no response found1)
27 2022-08-04 07:22:18.437954335 192.0.2.100 198.51.100.100 ICMP 112 0xa11e (41246) 64 Echo (ping) request id=0x0022, seg=22/5632, ttl=64 (no response found))
5) Frame 21 102 09/tes on wire (sio bits) on intervace capture (sio bits) on intervace capt
2 Externet 11, SrC: Weare Succesce (06:56:56:56:56:56:56:56:56:56:56:56:56:56
9 392/10 VIPCUal Law, PKI 9, DEI: 0, 10: 205
000 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21
0050 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 "#\$X&'() *+,-,/01
Time Unit 0 110 110 110 21 0060 32 33 34 35 36 37 234567
1 Jpc: 1 PV4 (0x0000)
Internet Protocol Version 4, 57C 124.04.000, USC: 126.51.100.100
and the control pessage Frotocol

Aprire i file di acquisizione per Portchannel1.207. Selezionare il primo pacchetto e controllare i punti chiave

- 1. Vengono acquisiti solo pacchetti di richieste echo ICMP. Ogni pacchetto viene acquisito e mostrato 2 volte.
- 2. L'intestazione del pacchetto originale ha il tag VLAN 207.
- 3. Lo switch interno inserisce un tag VLAN 1001 aggiuntivo che identifica l'interfaccia in entrata Portchannel1.
- 4. Lo switch interno inserisce un tag VN aggiuntivo.

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) re	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) re	equest	id=0x007b, seq=1/256, ttl=255 (no response found!)
5 2022-08-04 08:18:24.573794751	192.168.247.100	192.168.247.102	ICMP	128	0x60a0 (24736)	255 Echo (ping) re	equest	id=0x007b, seq=2/512, ttl=255 (no response found!)
6 2022-08-04 08:18:24.573795748	192.168.247.100	192.168.247.102	ICMP	118	0x60a0 (24736)	255 Echo (ping) re	equest	id=0x007b, seq=2/512, ttl=255 (no response found!)
7 2022-08-04 08:18:24.574368638	192.168.247.100	192.168.247.102	ICMP	128	0x60a1 (24737)	255 Echo (ping) re	equest	id=0x007b, seq=3/768, ttl=255 (no response found!)
8 2022-08-04 08:18:24.574369574	192.168.247.100	192.168.247.102	ICMP	118	0x60a1 (24737)	255 Echo (ping) re	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	ICMP	128	0x60a2 (24738)	255 Echo (ping) re	equest	id=0x007b, seq=4/1024, ttl=255 (no response found!)
10 2022-08-04 08:18:24.574915415	192.168.247.100	192.168.247.102	ICMP	118	0x60a2 (24738)	255 Echo (ping) re	equest	id=0x007b, seq=4/1024, ttl=255 (no response found!)
11 2022-08-04 08:18:24.575442569	192.168.247.100	192.168.247.102	ICMP	128	0x60a3 (24739)	255 Echo (ping) re	equest	id=0x007b, seq=5/1280, ttl=255 (no response found!)
12 2022-08-04 08:18:24.575443601	192.168.247.100	192.168.247.102	ICMP	118	0x60a3 (24739)	255 Echo (ping) re	equest	id=0x007b, seq=5/1280, ttl=255 (no response found!)
13 2022-08-04 08:18:24.575918119	192.168.247.100	192.168.247.102	ICMP	128	0x60a4 (24740)	255 Echo (ping) re	equest	id=0x007b, seq=6/1536, ttl=255 (no response found!)
14 2022-08-04 08:18:24.575919057	192.168.247.100	192.168.247.102	ICMP	118	0x60a4 (24740)	255 Echo (ping) re	equest	id=0x007b, seq=6/1536, ttl=255 (no response found!)
15 2022-08-04 08:18:24.576407671	192.168.247.100	192.168.247.102	ICMP	128	0x60a5 (24741)	255 Echo (ping) re	equest	id=0x007b, seq=7/1792, ttl=255 (no response found!)
16 2022-08-04 08:18:24.576408585	192.168.247.100	192.168.247.102	ICMP	118	0x60a5 (24741)	255 Echo (ping) re	equest	id=0x007b, seq=7/1792, ttl=255 (no response found!)
17 2022-08-04 08:18:24.576885643	192.168.247.100	192.168.247.102	ICMP	128	0x60a6 (24742)	255 Echo (ping) re	equest	id=0x007b, seq=8/2048, ttl=255 (no response found!)
18 2022-08-04 08:18:24.576886561	192.168.247.100	192.168.247.102	ICMP	118	0x60a6 (24742)	255 Echo (ping) re	equest	id=0x007b, seq=8/2048, ttl=255 (no response found!)
19 2022-08-04 08:18:24.577394328	192.168.247.100	192.168.247.102	ICMP	128	0x60a7 (24743)	255 Echo (ping) re	equest	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) re	equest	id=0x007b, seq=9/2304, ttl=255 (no response found!)
21 2022-08-04 08:18:24.577987632	192.168.247.100	192.168.247.102	ICMP	128	0x60a8 (24744)	255 Echo (ping) re	equest	id=0x007b, seq=10/2560, ttl=255 (no response found!)
22 2022-08-04 08:18:24.577989290	192.168.247.100	192.168.247.102	ICMP	118	0x60a8 (24744)	255 Echo (ping) re	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) re	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) re	equest	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) re	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) re	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) re	equest	id=0x007b, seq=13/3328, ttl=255 (no response found!)
ć								
> Frame 1: 128 bytes on wire (1024 bits)). 128 bytes cant	ured (1024 bits) or	interface ca	nture 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 (00:1	17:df:d6:ec:00).	Dst: a2:76:f2:00:0	a:1c (a2:76:f2	: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	: From Bridge					0030	08 00 e5 c8 00 7b 00 00 00 00 00 02 4d 8c 4a 78 ·····{···M·Jx
.0	= Pointer:	vif id					0040	ab cd
	= Destinati	on: 61					0050	ab cd
	= Looped: N	0	41				0060	ab cd
	= Reserved:	0					0070	ab cd
	= Version:	0						
0000 0000	0000 = Source: 0							
Type: 802.10 Virtual LAN (0x8100)								
802.10 Virtual LAN, PRI: 0, DEI: 0, II	D: 1001							
000 Bes	t Effort (defaul	t) (0)	-					
0 = DEI: Ineligib	le		31					
0011 1110 1001 = ID: 1001			-					
Type: 802.10 Virtual LAN (0x8100)								
802.10 Virtual LAN, PRI: 0, DEI: 0, II	D: 207							
000 = Priority: Bes	t Effort (defaul	t) (0)						
0 = DEI: Ineligib	le							
0000 1100 1111 = ID: 207			2					
Type: IPv4 (0x0800)			4					
Internet Protocol Version 4, Src: 192.	.168.247.100, Dst	: 192.168.247.102						
> Internet Control Message Protocol								
							1	

Selezionare il secondo pacchetto e controllare i punti chiave:

- 1. Vengono acquisiti solo pacchetti di richieste echo ICMP. Ogni pacchetto viene acquisito e mostrato 2 volte.
- 2. L'intestazione del pacchetto originale ha il tag VLAN 207.

No.	Time	Source	Destination	Protocol	Length	2° 20	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) requ	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) requ	uest	id=0x007b, seg=0/0, ttl=255 (no response found1)
	3 2022-08-04 08:18:24.573286630	192.168.247.100	192.168.247.102	ICMP	128	0x609f (24735)	255 Echo (ping) requ	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) requ	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) requ	uest	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) requ	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) requ	uest	id=0x007b, seq=3/768, ttl=255 (no response found!)
	8 2022-08-04 08:18:24.574369574	192.168.247.100	192.168.247.102	ICMP	118	0x60a1 (24737)	255 Echo (ping) requ	uest	id=0x007b, seq=3/768, ttl=255 (no response found!)
	9 2022-08-04 08:18:24.574914512	192.168.247.100	192.168.247.102	ICMP	128	0x60a2 (24738)	255 Echo (ping) requ	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) requ	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) requ	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) requ	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) requ	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) requ	uest	id=0x007b, seg=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) requ	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) requ	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) requ	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) requ	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) requ	uest	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) requ	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) requ	uest	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) requ	uest	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) requ	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) requ	uest	id=0x007b, seg=11/2816, ttl=255 (no response found!)
	25 2022-08-04 08:18:24.578900043	192.168.247.100	192.168.247.102	ICMP	128	0x60aa (24746)	255 Echo (ping) requ	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) requ	uest	id=0x007b, seg=12/3072, ttl=255 (no response found!)
	27 2022-08-04 08:18:24.579426962	192.168.247.100	192.168.247.102	ICMP	128	0x60ab (24747)	255 Echo (ping) requ	uest	id=0x007b, seq=13/3328, ttl=255 (no response found!)
4									
			and down hits a second			11.0			
> Fra	me 2: 118 bytes on wire (944 bits)	, 118 bytes capt	ured (944 bits) on :	interface capt	ure_u0_3,	, 1d 0		0000	a2 76 f2 00 00 1c 00 17 df d6 ec 00 81 00 00 cf
> Eth	ernet II, Src: Cisco d6:ec:00 (00:	17:df:d6:ec:00),	Dst: a2:76:12:00:0	a:1c (a2:76:12	:00:00:10	:)		0010	f7 64 c9 a8 f7 66 98 99 a5 c8 99 7h 99 99 99 a
× 802	1.10 Virtual LAN, PRI: 0, DEI: 0, I	D: 207						0020	00 02 4d 8c 4a 78 ah cd ah cd ah cd ah cd ah cd ah cd
	000 Priority: Bes	st Effort (defaul	t) (0)					0040	ab cd
	= DEI: Ineligit	01e		2				0050	ab cd
	0000 1100 1111 = ID: 207			21				0060	ab cd
	Type: IPv4 (0x0800)			_				0070	ab cd ab cd ab cd
Int	ernet Protocol version 4, Src: 192	.168.247.100, DS	: 192.168.247.102						
Int	ternet control Message Protocol								

Spiegazione

Quando si configura la cattura di un pacchetto su un'interfaccia anteriore, lo switch acquisisce simultaneamente ciascun pacchetto due volte:

- Dopo l'inserimento del tag VLAN della porta.
- Dopo l'inserimento del tag VN.

Nell'ordine delle operazioni, il tag VN viene inserito in una fase successiva all'inserimento del tag VLAN della porta. Tuttavia, nel file di acquisizione, il pacchetto con il tag VN viene visualizzato prima del pacchetto con il tag port VLAN. Inoltre, nel caso delle sottointerfacce, nei file di acquisizione, il pacchetto ogni secondo non contiene il tag port VLAN.

Nella tabella seguente viene riepilogata l'attività:

Attività	Punto di acquisizione	VLAN della porta interna nei pacchetti acquisiti	Direzione	Traffico acquisito
Configurazione e verifica dell'acquisizione di un pacchetto sull'interfaccia Ethernet1/2.205	Ethernet 1/2.205	102	Solo in ingresso	Richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.100

Configurazione e verifica dell'acquisizione di un pacchetto sull'interfaccia secondaria di Portchannel1 con le interfacce membro Ethernet1/3 ed Ethernet1/4	Ethernet 1/3 Ethernet 1/4	1001	Solo in ingresso	Richieste echo ICMP da 192.168.207.100 all'host 192.168.207.102
--	------------------------------	------	---------------------	---

Filtri di acquisizione pacchetti

Usare FCM e CLI per configurare e verificare un'acquisizione pacchetto sull'interfaccia Ethernet1/2 con un filtro.

Topologia, flusso dei pacchetti e punti di acquisizione



Configurazione

FCM

Eseguire la procedura seguente su FCM per configurare un filtro di acquisizione per i pacchetti di richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.100 e applicarlo all'acquisizione dei pacchetti sull'interfaccia Ethernet1/2:

- 1. Utilizzare Strumenti > Acquisizione pacchetti > Elenco filtri > Aggiungi filtro per creare un filtro di acquisizione.
- 2. Specificare il nome del filtro, il protocollo, l'IPv4 di origine e quello di destinazione, quindi fare clic su Salva:

Overview Inter	faces Logical Devices Se	curity Engine Platf	form Settings									System Tools	Help admin
Capture Session	Filter List												_
Filter List												Ad	d Filter
Editors Name		From				То			Destand	Teneradan	Ordenudan	FilmsTown	-
Filter Name	MAC	IPv4	IPv6	Port	MAC	IPv4	IPv6	Port	Protocol	Inner vian	Outer vian	conertype	
filter_icmp	00:00:00:00:00:00	192.0.2.100		0	00:00:00:00:00:00	192.0.2.100	п	0	1	0	0	0	/8
				Edit Declar									
				Edit Packet	Filter			0.8					
				Filter Name*	filter_icmp								
				Protocol	ICMP_IPv4 ¥								
				EtherType	Any 👻								
				Inner vlan	0	Outer vian	0						
				Source		Destination							
				IPv4	192.0.2.100	IPv4	198.51.100.100						
				1Pv6	=	IPv6	=						
				Port	0	Port	0						
				MAC	00:00:00:00:00	MAC	00:00:00:00:00:00						
							Save	Cancel					

3. Utilizzare Strumenti > Acquisizione pacchetti > Acquisisci sessione per creare una nuova sessione di acquisizione:

Overview Interfaces Logical Devices Security Engine Platform Settings	Syste	m Tools Help admin
	Packet Capture	Troubleshooting Logs
Capture Session Filter List		
c	fresh Capture Session D	elete All Sessions
No Session available		

4. Selezionare Ethernet1/2, fornire il Nome sessione, applicare il filtro di acquisizione e fare clic su Salva ed esegui per attivare l'acquisizione:

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
Ethernet1/2	Selected Interfaces External Append
Ethernet1/1	Apply fitter_cmp V To Ethemet1/2 V

CLI FXOS

Eseguire questi passaggi sulla CLI di FXOS per configurare le acquisizioni dei pacchetti sulle interfacce backplane:

1. Identificare il tipo di applicazione e l'identificatore:

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

2. Identificare il numero del protocollo IP in <u>https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml</u>. In questo caso, il numero di protocollo ICMP è 1.

3. Creare una sessione di acquisizione:

```
<#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 #
```

Verifica

FCM

Verificare il nome dell'interfaccia, verificare che lo stato operativo sia attivo e che le dimensioni del file (in byte) aumentino:



Verificare il nome dell'interfaccia, il filtro, accertarsi che lo stato operativo sia attivo e che le dimensioni del file (in byte) aumentino in Strumenti > Acquisizione pacchetti > Sessione di acquisizione:

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	
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

Verificare i dettagli di acquisizione nell'ambito 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 Raccogli file di acquisizione Eseguire i passaggi descritti nella sezione Raccolta dei file di acquisizione degli switch interni Firepower 4100/9300.

Analisi dei file di acquisizione

Utilizzare un'applicazione per la lettura dei file di acquisizione dei pacchetti per aprire il file di acquisizione. Selezionare il primo pacchetto e controllare i punti chiave

1. Vengono acquisiti solo pacchetti di richieste echo ICMP. Ogni pacchetto viene acquisito e

mostrato 2 volte.

- 2. L'intestazione del pacchetto originale è senza il tag VLAN.
- 3. Lo switch interno inserisce un tag VLAN 102 aggiuntivo che identifica l'interfaccia in entrata Ethernet 1/2.
- 4. Lo switch interno inserisce un tag VN aggiuntivo.

÷														_
1	No. Time	Source	Destination	Protocol	Length	IP ID	₽ TT	L Info					_	^
	1 2022-08-02 15:46:55.603277760	192.0.2.100	198.51.100.100	ICMP	108 -	0x0012 (18) 6	4 Echo (ping)	request	id=0x0018,	seq=349/23809,	ttl=64 (no r	
L	2 2022-08-02 15:46:55.603279688	192.0.2.100	198.51.100.100	ICMP	102	0x0012 (18) 6	4 Echo (ping)	request	id=0x0018,	seq=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) 6	4 Echo (ping)	request	id=0x0018,	seq=350/24065,	ttl=64 (no r	
н	4 2022-08-02 15:46:56.627140919	192.0.2.100	198.51.100.100	ICMP	102	0x00db (219) 6	4 Echo (ping)	request	id=0x0018,	seq=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) 6	4 Echo (ping)	request	id=0x0018,	seq=351/24321,	ttl=64 (no r	
L	6 2022-08-02 15:46:57.651186787	192.0.2.100	198.51.100.100	ICMP	102	0x01cb (459) 6	4 Echo (ping)	request	id=0x0018,	seq=351/24321,	ttl=64 (no r	
L	7 2022-08-02 15:46:58.675153317	192.0.2.100	198.51.100.100	ICMP	108	0x01d6 (470) 6	4 Echo (ping)	request	id=0x0018,	seq=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) 6	4 Echo (ping)	request	id=0x0018,	seq=352/24577,	ttl=64 (no r	
L	9 2022-08-02 15:46:59.699152639	192.0.2.100	198.51.100.100	ICMP	108	0x01f4 (500) 6	4 Echo (ping)	request	id=0x0018,	seq=353/24833,	ttl=64 (no r	
L	10 2022-08-02 15:46:59.699153835	192.0.2.100	198.51.100.100	ICMP	102	0x01f4 (500) 6	4 Echo (ping)	request	id=0x0018,	seq=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) 6	4 Echo (ping)	request	id=0x0018,	seq=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) 6	4 Echo (ping)	request	id=0x0018,	seq=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) 6	4 Echo (ping)	request	id=0x0018,	seq=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) 6	4 Echo (ping)	request	id=0x0018,	seq=355/25345,	ttl=64 (no r	
E	15 2022-08-02 15:47:02.771209952	192.0.2.100	198.51.100.100	ICMP	108	0x02bc (700) 6	4 Echo (ping)	request	id=0x0018,	seq=356/25601,	ttl=64 (no r	
E	16 2022-08-02 15:47:02.771211062	192.0.2.100	198.51.100.100	ICMP	102	0x02bc (700) 6	4 Echo (ping)	request	id=0x0018,	seq=356/25601,	ttl=64 (no r	
E	17 2022-08-02 15:47:03.772258550	192.0.2.100	198.51.100.100	ICMP	108	0x032f (815) 6	4 Echo (ping)	request	id=0x0018,	seq=357/25857,	ttl=64 (no r	
E	18 2022-08-02 15:47:03.772259724	192.0.2.100	198.51.100.100	ICMP	102	0x032f (815) 6	4 Echo (ping)	request	id=0x0018,	seq=357/25857,	ttl=64 (no r	
E	19 2022-08-02 15:47:04.791118519	192.0.2.100	198.51.100.100	ICMP	108	0x040f (1039) 6	4 Echo (ping)	request	id=0x0018,	seq=358/26113,	ttl=64 (no r	
E	20 2022-08-02 15:47:04.791119721	192.0.2.100	198.51.100.100	ICMP	102	0x040f (1039) 6	4 Echo (ping)	request	id=0x0018,	seq=358/26113,	ttl=64 (no r	~
	< Comparison of the second sec						,	(1 - 0)			, , , , , , , , , , , , , , , , , , , ,		>	
F	Ename 1: 100 bytes on wire (064 bi	te) 100 hutes c	antured (964 hits)	on interfac	e canture ue :	1 1 000	a 58 97 hd h	9 77 00 00 50	56 9d e	8 he 89 26 1	RA A3 X W	P. V		
Т	Ethernet II. Src: Wware 0d:e8:he	(00:50:56:0d:00:	a) Det: Cisco ba:	77.00 (59.0	7.hd.h0.77.00	001	0 00 00 81 0	0 00 66 08 00	45 00 0	0 54 00 12	40 00 ·····f·	· E · · T · · /	a.	
Ι.	VN_Tag	(00.50.50.50.60.0	<i>iej</i> , <i>bsc. cisco bs</i> .	77.00 (58.5	7.00.05.77.0e	002	0 40 01 4d 9	b c0 00 02 64	c6 33 6	4 64 08 00 9	9e 67 @·M····	d · 3dd · ·	· e	
Г	1	- Direct	ion: From Bridge	_		003	0 00 18 01 5	d e2 46 e9 62	00 00 0	00 00 c1 a6 0	0c 00 ···]·F·	b		
Т	A	- Pointe	n wif id			004	0 00 00 00 0	0 10 11 12 13	14 15 1	6 17 18 19 1	1a 1b			
Т	00 0000 0000 1010	- Doctin	ation: 10			005	0 1c 1d 1e 1	f 20 21 22 23	24 25 2	6 27 28 29 2	2a 2b ···· !"	# \$%&'()'	*+	
Т		- Looped	I No			006	2c 2d 2e 2	f 30 31 32 33	34 35 3	36 37	,/012	3 4567		
Т		- Rocory	odu A	• •										
Т		- Vencio	eu. 0											
Т		000 0000 - Sourco												
Т	Tupo: 902 10 Vintual LAN (0x910)	000 0000 = Source	. 0											
Ι.	Page 10 Victual LAN DBI: 0 DEI: 0	TD: 102		_										
Г	- Boionitus	, IU: 102 Post Effort (dof	ault) (0)											
Т	000 = Priority:	dest errort (der	aurc) (0)	2										
Т		rgrore		' I										
Т	0000 0110 0110 = 1D: 102													
L	Type: IPV4 (0x0800)	100 0 0 100 0-1-	100 51 100 100	_										
L	> Internet Protocol Version 4, Src:	192.0.2.100, Dst:	198.51.100.100											
Т	Internet control Message Protocol													
Т														
Т														
Ľ						1								

Selezionare il secondo pacchetto e controllare i punti chiave:

- 1. Vengono acquisiti solo pacchetti di richieste echo ICMP. Ogni pacchetto viene acquisito e mostrato 2 volte.
- 2. L'intestazione del pacchetto originale è senza il tag VLAN.
- 3. Lo switch interno inserisce un tag VLAN 102 aggiuntivo che identifica l'interfaccia in entrata Ethernet 1/2.

No	o. Time	Source	Destination	Protocol	Length	IP ID		IP TTL Ir	fo						^
C	- 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	opture u0 1	, i. 000	0 58 9	7 bd b9 7	7 0e 00 !	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	1:b9:77:0e)	001	0 08 00	45 00 0	0 54 00	2 40 00	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	Ø 9e 67 0	00 18 01 5d	e2 46 ·d·3dd·	····g····]	٠F	
	000 = Priority:	Best Effort (defa	ault) (0)			003	0 e9 62	2 00 00 0	0 00 c1 a	6 0c 00	00 00 00 00	10 11 ·b·····			
	0 = DEI: Ineli	gible	3			004	0 12 1	3 14 15 1	6 17 18	9 1a 1b	lc 1d 1e 1f	20 21		1	
	0000 0110 0110 = ID: 102	0	~			005	0 22 2	3 24 25 2	6 27 28	9 2a 2b 3	2c 2d 2e 2f	30 31 "#\$%&'() *+,/	01	
	Type: IPv4 (0x0800)					006	0 32 3	3 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												

Spiegazione

Quando si configura la cattura di un pacchetto su un'interfaccia anteriore, lo switch acquisisce simultaneamente ciascun pacchetto due volte:

- Dopo l'inserimento del tag VLAN della porta.
- Dopo l'inserimento del tag VN.

Nell'ordine delle operazioni, il tag VN viene inserito in una fase successiva all'inserimento del tag VLAN della porta. Tuttavia, nel file di acquisizione, il pacchetto con il tag VN viene visualizzato prima del pacchetto con il tag port VLAN.

Quando si applica un filtro di acquisizione, vengono acquisiti solo i pacchetti che corrispondono al filtro nella direzione in entrata.

Nella tabella seguente viene riepilogata l'attività:

Attività	Punto di acquisizione	VLAN della porta interna nei pacchetti acquisiti	Direzione	Filtro utente	Traffico acquisito
Configurare e verificare l'acquisizione di un pacchetto con un filtro sull'interfaccia anteriore Ethernet1/2	Ethernet 1/2	102	Solo in ingresso	Protocollo: ICMP Fonte:192.0.2.100 Destinazione: 198.51.100.100	Richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.100

Raccolta Dei File Di Acquisizione Dello Switch Interno Firepower 4100/9300

FCM

Per raccogliere i file di acquisizione dello switch interno, eseguire la procedura seguente in FCM:

1. Fare clic sul pulsante Disabilita sessione per interrompere l'acquisizione attiva:

oois neip aumin
assions

2. Verificare che lo stato operativo sia 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 All Session	5
	cap1	Drop Count: 0	Operational State: DOWN - Session	Admin_Shut Buffer Size: 256	мв	Snap Length: 1518 Bytes		a 🛛
Interface Na	ame	Filter	File Size (in bytes)	File Name	Device Name	e		
Ethernet1/2		None	218828	cap1-ethemet-1-2-0.pcap	ftd1	土		

3. Fare clic su Download per scaricare il file di acquisizione:

Overview	Interfaces	Logical Devices	Security Engine	Platform Settings			Syste	m Tools I	Help admin
Capture Ses	sion Filter Lis	t							
							C Refresh Capture Session Dele	te All Sessions	
	cap1	Drop Count	: 0	Operational State: DOWN - Session_Admin_St	nut Buffer Size: 256 MB		Snap Length: 1518 Bytes		/88
Interface Na	me	Filter		File Size (in bytes)	File Name	Device Name			
Ethernet1/2		None		218828	cap1-ethemet-1-2-0.pcap	ftd1	土		

Nel caso di interfacce porta-canale, ripetere questo passaggio per ciascuna interfaccia membro.

CLI FXOS

Per raccogliere i file di acquisizione, attenersi alla seguente procedura dalla CLI di FXOS:

1. Arrestare l'acquisizione attiva:

<#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. Caricare il file di acquisizione dall'ambito del comando 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:

Nel caso delle interfacce port-channel, copiare il file di acquisizione per ciascuna interfaccia membro.

Linee guida, limitazioni e best practice per l'acquisizione di pacchetti di switch interni

Per le linee guida e i limiti relativi all'acquisizione degli switch interni Firepower 4100/9300, fare riferimento alla guida alla configurazione di Cisco Firepower 4100/9300 FXOS Chassis Manager o alla guida alla configurazione della CLI di Cisco Firepower 4100/9300 FXOS, capitolo Risoluzione dei problemi, sezione Packet Capture.

Questo è l'elenco delle best practice basate sull'uso della cattura di pacchetti nei casi TAC:

- · Stai attento alle linee guida e ai limiti.
- Acquisire pacchetti su tutte le interfacce membro del canale della porta e analizzare tutti i file di acquisizione.
- Utilizzare i filtri di acquisizione.
- Considerare l'impatto di NAT sugli indirizzi IP dei pacchetti quando viene configurato un filtro di acquisizione.
- Aumentate o diminuite la Lunghezza snap che specifica le dimensioni del fotogramma nel caso in cui differisca dal valore predefinito di 1518 byte. Dimensioni inferiori determinano un numero maggiore di pacchetti acquisiti e viceversa.
- Regolare le dimensioni del buffer in base alle esigenze.
- Tenere presente il conteggio di perdita sulla CLI di FCM o FXOS. Una volta raggiunto il limite delle dimensioni del buffer, il contatore di rilascio aumenta.
- Usare il filtro !vntag su Wireshark per visualizzare solo i pacchetti senza tag VN. Questa

opzione permette di nascondere i pacchetti con tag VN nei file di acquisizione dei pacchetti dell'interfaccia anteriore.

- Utilizzare il filtro frame.number&1 su Wireshark per visualizzare solo i fotogrammi dispari. Ciò è utile per nascondere i pacchetti duplicati nei file di acquisizione dei pacchetti dell'interfaccia del backplane.
- Nel caso di protocolli come TCP, Wireshark applica per impostazione predefinita regole di colorizzazione che visualizzano pacchetti con condizioni specifiche in colori diversi. Nel caso di acquisizioni interne dello switch causate da pacchetti duplicati nei file di acquisizione, il pacchetto può essere colorato e contrassegnato in modo falso-positivo. Se si analizzano i file di acquisizione dei pacchetti e si applica un filtro, esportare i pacchetti visualizzati in un nuovo file e aprire il nuovo file.

Configurazione e verifica su Secure Firewall 3100/4200

A differenza di Firepower 4100/9300, le acquisizioni dello switch interno sugli switch Secure Firewall 3100/4200 vengono configurate sull'interfaccia della riga di comando dell'applicazione tramite il comando capture <name> switch, dove l'opzione switch specifica che le acquisizioni sono configurate sullo switch interno.

Questo è il comando capture con l'opzione 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>	

Di seguito sono riportati i passi generali per la configurazione dell'acquisizione dei pacchetti:

1. Specificare un'interfaccia in entrata:

La configurazione di acquisizione dello switch accetta il nome dell'interfaccia in entrata, se presente. L'utente può specificare i nomi delle interfacce dati, l'uplink interno o le interfacce di gestione:

<#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

Secure Firewall 4200 supporta le acquisizioni bidirezionali. Se non specificato diversamente, il valore predefinito è in entrata:

<#root>

>

capture capi switch interface inside direction

bothTo capture switch bi-directional trafficegressTo capture switch egressing trafficingressTo capture switch ingressing traffic

Inoltre, Secure Firewall 4245 è dotato di 2 interfacce dati interne e 2 interfacce uplink di gestione:

<#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. Specificare EtherType del frame Ethernet. Il valore predefinito di EtherType è IP. I valori dell'opzione ethernet-type specificano EtherType:

<#root>

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

3. Specificare le condizioni di corrispondenza. L'opzione di acquisizione corrispondenza specifica i criteri di corrispondenza:

<#root>

>

capture capsw switch interface inside match ?
 <0-255> Enter protocol number (0 - 255)
 ah
 eigrp
 esp
 gre
 icmp6
 igmp
 igrp
 ip
 ipinip

ipsec mac Mac-address filter nos ospf pcp pim pptp sctp snp spi SPI value tcp udp <cr>

- 4. Specificare altri parametri facoltativi, ad esempio le dimensioni del buffer, la lunghezza del pacchetto e così via.
- 5. Abilitare l'acquisizione. Il comando no capture <name> switch stop attiva l'acquisizione:

```
capture capsw switch interface inside match ip
```

>

>

no capture capsw switch stop

- 6. Verificare i dettagli di acquisizione:
- Lo stato amministrativo è abilitato e lo stato operativo è attivo e attivo.
- Le dimensioni del file di acquisizione del pacchetto aumentano.
- Il numero di pacchetti acquisiti nell'output del comando show capture <cap_name> è diverso da zero.
- Percorso di acquisizione Pcapfile. I pacchetti catturati vengono salvati automaticamente nella cartella /mnt/disk0/packet-capture/.
- Condizioni di acquisizione. Il software crea automaticamente i filtri di acquisizione in base alle condizioni di acquisizione.

```
<#root>
```

```
>
show capture capsw
27 packet captured on disk using switch capture
Reading of capture file from disk is not supported
>
show capture capsw detail
Packet Capture info
 Name:
                     capsw
 Session:
                     1
                     enabled
 Admin State:
 Oper State:
                     up
Oper State Reason: Active
 Config Success:
                    yes
 Config Fail Reason:
 Append Flag: overwrite
```

Session Mem Usage: Session Pcap Snap Error Code:	256 Len: 1518 0				
Drop Count:	0				
Total Physical ports Physical port:	involved in Packet Capture: 1				
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 Filte	Packet Capture Filter Info				
Name:	capsw-1-1				
Protocol:	0				
Ivlan:	0				
Ovlan: 2	05				
Src Ip:	0.0.0.0				
Dest Ip:	0.0.0.0				
Src Ipv6:					
Dest Ipvo:	::				
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				
o packet captured or	o packet captured on disk using switch capture				

Reading of capture file from disk is not supported

7. Arrestare le clip quando necessario:

<#root>

>

capture capsw switch stop

>

show capture capsw detail

Packet Capture info Name: capsw Session: 1 Admin State: disabled Oper State: down Oper State Reason: Session_Admin_Shut Config Success: yes Config Fail Reason: Append Flag: overwrite Session Mem Usage: 256 Session Pcap Snap Len: 1518 Error Code: 0 0 Drop Count: Total Physical ports involved in Packet Capture: 1 Physical port: Slot Id: 1 Port Id: 1 Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap Pcapsize: 24 Filter: capsw-1-1 Packet Capture Filter Info Name: capsw-1-1 Protocol: 0 Ivlan: 0 205 Ovlan: 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 0 Dest Port: 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. Raccogliere i file di acquisizione. Eseguire la procedura descritta nella sezione Raccolta dei file di acquisizione di switch interni Secure Firewall.

Nel software Secure Firewall versione 7.4, la configurazione di acquisizione dello switch interno non è supportata in FMC o FDM. Nel caso del software ASA versione 9.18(1) e successive, le acquisizioni dello switch interno possono essere configurate in ASDM versione 7.18.1.x e

successive.

In questi scenari vengono illustrati i casi di utilizzo comuni di acquisizioni di switch interni Secure Firewall 3100/4200.

Acquisizione dei pacchetti su un'interfaccia fisica o su un canale della porta

Usare FTD o ASA CLI per configurare e verificare un'acquisizione pacchetto sull'interfaccia Ethernet1/1 o Portchannel1. Entrambe le interfacce hanno il nome if inside.

Topologia, flusso dei pacchetti e punti di acquisizione

Secure Firewall 3100:



Secure Firewall 4200 con acquisizioni bidirezionali:



Configurazione

Attenersi alla seguente procedura sull'appliance ASA o sulla CLI FTD per configurare l'acquisizione di un pacchetto sull'interfaccia Ethernet1/1 o Port-channel1:

1. Verificare il nome se:

<#root>

>

show nameif

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

<#root>

>

show nameif

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

2. Creare una sessione di acquisizione

<#root>

>

capture capsw switch interface inside

Secure Firewall 4200 supporta la direzionalità di acquisizione:

<#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. Abilitare la sessione di acquisizione:

<#root>

> no capture capsw switch stop

Verifica

Verificare il nome della sessione di acquisizione, lo stato amministrativo e operativo, lo slot di interfaccia e l'identificatore. Verificare che il valore Pcapsize in byte aumenti e che il numero di pacchetti acquisiti sia diverso da zero:

<#root>	
>	
show capture capsw de	tail
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 L Error Code: Drop Count:	yes overwrite 256 .en: 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:	12653
Filter:	capsw-1-1

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

Total Physical breakout ports involved in Packet Capture: 0

79 packets captured on disk using switch capture

Reading of capture file from disk is not supported

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:	DOTH
Drop:	disable
Filter:	capsw-1-1
Packet Capture Fi	ilter 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 br	eakout ports involved in Packet Capture: 0
33 packet capture	ed on disk using switch capture

Reading of capture file from disk is not supported

Nel caso di Port-channel1, l'acquisizione viene configurata su tutte le interfacce membro:

<#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 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: 2
Physical port:	
Slot Id:	1
Port Id:	4
Pcapfile:	/mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-4-0.pcap
Pcapsize:	28824
Filter:	capsw-1-4
Packet Capture Filte Name: Protocol: Ivlan: Ovlan: Src Ip: Dest Ip: Src Ipv6: Dest Ipv6: Src MAC: Dest MAC: Src Port: Dest Port: Ethertype:	r Info capsw-1-4 0 0 0 0.0.0.0 0.0.0.0 :: :: :: 00:00:00:00:00:00 00:00:00:00
Slot Id:	1
Port Id:	3
Pcapfile:	/mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-3-0.pcap
Pcapsize:	18399
Filter:	capsw-1-3
Packet Capture Filte	r Info
Name: Protocol:	capsw-1-3 0
Ivlan:	0
Ovlan:	0

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

Total Physical breakout ports involved in Packet Capture: 0

56 packet captured on disk using switch capture

Reading of capture file from disk is not supported

Le interfacce membro port-channel possono essere verificate nella shell dei comandi FXOS localmgmt tramite il comando show portchannel summary:

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

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

Per accedere a FXOS sull'appliance ASA, eseguire il comando connect fxos admin. In caso di contesto multiplo, eseguire il comando nel contesto admin.

Raccogli file di acquisizione

Eseguire la procedura descritta nella sezione Raccolta dei file di acquisizione di switch interni Secure Firewall.

Analisi dei file di acquisizione

Utilizzare un'applicazione per la lettura dei file di acquisizione dei pacchetti per aprire i file di acquisizione per Ethernet1/1. Nell'esempio vengono analizzati i pacchetti acquisiti con Secure Firewall 3100. Selezionare il primo pacchetto e controllare i punti chiave:

- 1. Vengono acquisiti solo pacchetti di richieste echo ICMP.
- 2. L'intestazione del pacchetto originale è senza il tag VLAN.

No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info		^
Γ.	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 re	ś
	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 re	5
	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 re	5
	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	ē 👘
	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	é 👘
	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	e
	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	e
	8 2022-08-07 19:50:13.934155	192.0.2.100	198.51.100.100	ICMP	102	0x9b8b (39819)	64 Echo (ping) request	id=0x0034, seq=8/2048, ttl=64 (no re	e
	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 r	e
	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	é
	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	¢
	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	¢
	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	¢
	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	¢
	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	é
	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	¢
	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 🗸
<								>	
	rame 1: 102 bytes on wire (816 bit	s), 102 bytes car	tured (816 bits)			0000 bc e7 12	2 34 9a 14 00 50 56 9d e8	be 08 00 45 00 ····4····P V·····E·	
> E	thernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco 34:9a	a:14 (bc:e7:	12:34:9a:14)	0010 00 54 9a	10 40 00 40 01 b3 9c c0	00 02 64 c6 33 ·T··@·@· ····d·3	
> 1	Internet Protocol Version 4. Src: 1	92.0.2.100. Dst:	198,51,100,100		2	0020 64 64 08	3 00 c6 91 00 34 00 01 61	17 f0 62 00 00 dd ····· 4 ··a··b··	
> 1	Internet Control Message Protocol	,			2	0030 00 00 18	3 ec 08 00 00 00 00 00 10	11 12 13 14 15	
Ľ	0					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	
						0060 36 37 55	5 55 55 55	670000	

Aprire i file di acquisizione per le interfacce membro di Portchannel1. Selezionare il primo pacchetto e controllare i punti chiave:

- 1. Vengono acquisiti solo pacchetti di richieste echo ICMP.
- 2. L'intestazione del pacchetto originale è senza il tag VLAN.

No.	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 (3	7526)	64 Echo (ping) request	id=0x0035, seq=1/	256, ttl=64 (no res	
	2 2022-08-07 20:40:59.658611	192.0.2.100	198.51.100.100	ICMP	102	0x9370 (3	7744)	64 Echo (ping) request	id=0x0035, seq=2/	512, ttl=64 (no res	
	3 2022-08-07 20:41:00.655662	192.0.2.100	198.51.100.100	ICMP	102	0x93f0 (3	7872)	64 Echo (ping) request	id=0x0035, seq=3/	768, ttl=64 (no res	
	4 2022-08-07 20:41:01.659749	192.0.2.100	198.51.100.100	ICMP	102	0x946f (3	7999)	64 Echo (ping) request	id=0x0035, seq=4/	1024, ttl=64 (no re	
	5 2022-08-07 20:41:02.660624	192.0.2.100	198.51.100.100	ICMP	102	0x94a4 (3	8052)	64 Echo (ping) request	id=0x0035, seq=5/	1280, ttl=64 (no re	
	6 2022-08-07 20:41:03.663226	192.0.2.100	198.51.100.100	ICMP	102	0x952d (3	8189)	64 Echo (ping) request	id=0x0035, seq=6/	1536, ttl=64 (no re	
	7 2022-08-07 20:41:04.661262	192.0.2.100	198.51.100.100	ICMP	102	0x958d (3	8285)	64 Echo (ping) request	id=0x0035, seq=7/	1792, ttl=64 (no r€	
	8 2022-08-07 20:41:05.665955	192.0.2.100	198.51.100.100	ICMP	102	0x95d8 (3	8360)	64 Echo (ping) request	id=0x0035, seq=8/	2048, ttl=64 (no re	
	9 2022-08-07 20:41:06.666538	192.0.2.100	198.51.100.100	ICMP	102	0x964b (3	8475)	64 Echo (ping) request	id=0x0035, seq=9/	2304, ttl=64 (no r€	
	10 2022-08-07 20:41:07.667298	192.0.2.100	198.51.100.100	ICMP	102	0x972b (3	8699)	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 (3	8922)	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 (3	8961)	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 (3	9074)	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 (3	9159)	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 (3	9396)	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 (3	9556)	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 (3	9667)	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 (3	9822)	64 Echo (ping) request	id=0x0035, seq=18	/4608, ttl=64 (no r	~
<										>	
>	Frame 1: 102 bytes on wire (816 bits	s), 102 bytes ca	otured (816 bits)			0000	bc e7 12	34 9a 2c 00 50 56 9d e	3 be 08 00 45 00	···4·, ·P V····E·	
>	Ethernet II, Src: VMware 9d:e8:be (6	00:50:56:9d:e8:b	e), Dst: Cisco 34:9a	:2c (bc:e7	:12:34:9a:2c)	0010	00 54 92	96 40 00 40 01 bb 16 c	0 00 02 64 c6 33	T@.@d.3	
>	Internet Protocol Version 4, Src: 19	92.0.2.100, Dst:	198.51.100.100		-	0020	64 64 08	00 58 a8 00 35 00 01 4	1 23 f0 62 00 00	ld∙·X··5 ··M#·b··	
>	Internet Control Message Protocol				2	0030	00 00 9e	c8 04 00 00 00 00 00 1	0 11 12 13 14 15		
	÷					0040	16 17 18	19 1a 1b 1c 1d 1e 1f 2	0 21 22 23 24 25		
						0050	26 27 28	29 2a 2b 2c 2d 2e 2f 3	31 32 33 34 35	()"+,/012345	
						0060	30 37 55	22 22 22		1/0000	

Spiegazione

Le clip dello switch sono configurate sulle interfacce Ethernet1/1 o Portchannel1.

Nella tabella seguente viene riepilogata l'attività:

Attività	Punto di acquisizione	Filtro interno	Direzione	Traffico acquisito
Configurazione e verifica dell'acquisizione di un pacchetto sull'interfaccia Ethernet1/1	Ethernet 1/1	Nessuna	Solo in ingresso*	Richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.100
Configurazione e verifica dell'acquisizione di un pacchetto sull'interfaccia Portchannel1 con le interfacce membro Ethernet1/3 ed Ethernet1/4	Ethernet 1/3 Ethernet 1/4	Nessuna	Solo in ingresso*	Richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.100

* A differenza della serie 3100, Secure Firewall 4200 supporta le acquisizioni bidirezionali (in entrata e in uscita).

Acquisizione di pacchetti su una sottointerfaccia di un'interfaccia fisica o di un canale della porta

Usare FTD o ASA CLI per configurare e verificare l'acquisizione di un pacchetto sulle sottointerfacce Ethernet1/1.205 o Portchannel1.205. Entrambe le sottointerfacce hanno il nome if inside.

Topologia, flusso dei pacchetti e punti di acquisizione

Secure Firewall 3100:



Secure Firewall 4200:

		Cha	ssis	
	Internal Switch		Security Module	
	E III		FTD/ASA	
192.0.2.100 ICMP echo-request	Eth1/2	Uplink	inside	
ICMP echo-reply 198.51.100.100			outside	

Configurazione

Attenersi alla seguente procedura sull'appliance ASA o sulla CLI FTD per configurare l'acquisizione di un pacchetto sull'interfaccia Ethernet1/1 o Port-channel1:

1. Verificare il nome se:

<#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. Creare una sessione di acquisizione:

<#root>

>

capture capsw switch interface inside

Secure Firewall 4200 supporta la direzionalità di acquisizione:

<#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. Abilitare la sessione di acquisizione:

<#root>

> no capture capsw switch stop

Verifica

Verificare il nome della sessione di acquisizione, lo stato amministrativo e operativo, lo slot di interfaccia e l'identificatore. Verificare che il valore Pcapsize in byte aumenti e che il numero di pacchetti acquisiti sia diverso da zero:

<#root>	
>	
show capture capsw de	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 I Error Code: Drop Count:	yes : overwrite 256 Len: 1518 O O
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:	0 0
Ovlan:	205

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

Total Physical breakout ports involved in Packet Capture: 0

46 packets captured on disk using switch capture

Reading of capture file from disk is not supported

In questo caso, viene creato un filtro con VLAN Ovlan=205 esterna che viene applicato all'interfaccia.

Nel caso di Port-channel1, l'acquisizione con un filtro Ovlan=205 viene configurata su tutte le interfacce membro:

<#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 0 Drop Count:

Total Physical ports involved in Packet Capture: 2

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

Packet Capture Fil	ter Info
Name:	capsw-1-4
Protocol:	0
Ivlan:	0
Ovlan:	205
Src In:	
Dest In:	
Src Inv6:	
Dest Inv6:	
Src MAC:	00:00:00:00:00
Dest MAC:	00:00:00:00:00:00
Src Port:	0
Dest Port:	0
Ethertype:	0
Physical port:	
Slot Id:	1
Port Id:	3
Pcapfile:	/mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-3-0.pcap
Pcapsize:	5600
Filter:	capsw-1-3
Packet Capture Fil	ter Info
Name:	capsw-1-3
Protocol:	0
Ivlan:	0
Ovlan:	205
Src Ip:	0.0.0.0
Dest Ip:	0.0.0.0
Src Ipv6:	::
Dest Ipv6:	::
Src MAC:	00:00:00:00:00:00

 Dest MAC:
 00:00:00:00:00:00

 Src Port:
 0

 Dest Port:
 0

 Ethertype:
 0

Total Physical breakout ports involved in Packet Capture: 0

49 packet captured on disk using switch capture

Reading of capture file from disk is not supported

Le interfacce membro port-channel possono essere verificate nella shell dei comandi FXOS localmgmt tramite il comando show portchannel summary:

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

Per accedere a FXOS sull'appliance ASA, eseguire il comando connect fxos admin. In caso di contesto multiplo, eseguire questo comando nel contesto admin.

Raccogli file di acquisizione

Eseguire la procedura descritta nella sezione Raccolta dei file di acquisizione di switch interni Secure Firewall.

Analisi dei file di acquisizione

Utilizzare un'applicazione per la lettura dei file di acquisizione dei pacchetti per aprire i file di acquisizione per Ethernet 1/1.205. Nell'esempio vengono analizzati i pacchetti acquisiti con Secure Firewall 3100. Selezionare il primo pacchetto e controllare i punti chiave:

- 1. Vengono acquisiti solo pacchetti di richieste echo ICMP.
- 2. L'intestazione del pacchetto originale ha il tag VLAN 205.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info		^
C.	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 re	5
	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 re	s
	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 re	s
	4 2022-08-07 21:21:04.609160	192.0.2.100	198.51.100.100	ICMP	106	0x426c (17004)	64 Echo (ping) request	id=0x0037, seq=4/1024, ttl=64 (no r	e
	5 2022-08-07 21:21:05.609409	192.0.2.100	198.51.100.100	ICMP	106	0x4310 (17168)	64 Echo (ping) request	id=0x0037, seq=5/1280, ttl=64 (no r	e
	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	e
	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	e
	8 2022-08-07 21:21:08.618023	192.0.2.100	198.51.100.100	ICMP	106	0x4518 (17688)	64 Echo (ping) request	id=0x0037, seq=8/2048, ttl=64 (no r	e
	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	e
	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 v
<								>	
>	Frame 1: 106 bytes on wire (848 bits	s), 106 bytes car	otured (848 bits)			0000 bc e7	12 34 9a 14 00 50 56 9d e8	be 81 00 00 cd ···4···P V·····	
>	Ethernet II, Src: VMware_9d:e8:be (6	00:50:56:9d:e8:be	2), Dst: Cisco_34:9a	a: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·@·@·····	
\sim	802.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 205				0020 02 64	c6 33 64 64 08 00 06 67 00	37 00 01 b0 2c ·d·3dd·· ·g·7···,	
	000 Briority: B	est Effort (defa	ult) (0)			0030 f0 62	00 00 00 00 8e fe 03 00 00	00 00 00 10 11 ·b·····	
	0 = DEI: Inelig	ible				0040 12 13	14 15 16 17 18 19 1a 1b 1c	1d 1e 1f 20 21	
	0000 1100 1101 = ID: 205				-	0050 22 23	24 25 26 27 28 29 2a 2b 2c	2d 2e 2f 30 31 #\$%& () *+,/01	
	Type: IPv4 (0x0800)				2	0000 32 33	34 35 36 37 55 55 55 55	23456700 00	
	Trailer: 5555555								
>	Internet Protocol Version 4, Src: 19	92.0.2.100, Dst:	198.51.100.100						
>	Internet Control Message Protocol								
•									

Aprire i file di acquisizione per le interfacce membro di Portchannel1. Selezionare il primo pacchetto e controllare i punti chiave:

- 1. Vengono acquisiti solo pacchetti di richieste echo ICMP.
- 2. L'intestazione del pacchetto originale ha il tag VLAN 205.

No. Time		Source	Destination	Protocol	Length	IP ID	Ib.	TTL Info						^
1 2022-08-07 21	1:21:01.607187	192.0.2.100	198.51.100.100	ICMP	106	0x411f (1	.6671)	64 Echo (ping)	request	id=0x0037,	seq=1/256, t	ttl=64 (no	res	
2 2022-08-07 21	1:21:02.609418	192.0.2.100	198.51.100.100	ICMP	106	0x413a (1	.6698)	64 Echo (ping)	request	id=0x0037,	seq=2/512, t	ttl=64 (no	res	
3 2022-08-07 21	1:21:03.610671	192.0.2.100	198.51.100.100	ICMP	106	0x421a (1	.6922)	64 Echo (ping)	request	id=0x0037,	seq=3/768, t	ttl=64 (no	res	
4 2022-08-07 21	1:21:04.609160	192.0.2.100	198.51.100.100	ICMP	106	0x426c (1	7004)	64 Echo (ping)	request	id=0x0037,	seq=4/1024,	ttl=64 (m	io re	
5 2022-08-07 21	1:21:05.609409	192.0.2.100	198.51.100.100	ICMP	106	0x4310 (1	7168)	64 Echo (ping)	request	id=0x0037,	seq=5/1280,	ttl=64 (m	io re	
6 2022-08-07 21	1:21:06.611847	192.0.2.100	198.51.100.100	ICMP	106	0x43df (1	7375)	64 Echo (ping)	request	id=0x0037,	seq=6/1536,	ttl=64 (n	io re	
7 2022-08-07 21	1:21:07.616688	192.0.2.100	198.51.100.100	ICMP	106	0x44d3 (1	7619)	64 Echo (ping)	request	id=0x0037,	seq=7/1792,	ttl=64 (n	io ne	
8 2022-08-07 21	1:21:08.618023	192.0.2.100	198.51.100.100	ICMP	106	0x4518 (1	7688)	64 Echo (ping)	request	id=0x0037,	seq=8/2048,	ttl=64 (m	io re	
9 2022-08-07 21	1:21:09.619326	192.0.2.100	198.51.100.100	ICMP	106	0x453d (1	7725)	64 Echo (ping)	request	id=0x0037,	seq=9/2304,	ttl=64 (m	io re	
10 2022-08-07 21	1:21:10.616696	192.0.2.100	198.51.100.100	ICMP	106	0x462b (1	7963)	64 Echo (ping)	request	id=0x0037,	seq=10/2560,	, ttl=64 (no r	
11 2022-08-07 21	1:21:11.621629	192.0.2.100	198.51.100.100	ICMP	106	0x4707 (1	8183)	64 Echo (ping)	request	id=0x0037,	seq=11/2816,	, ttl=64 (no r	
12 2022-08-07 21	1:21:12.619309	192.0.2.100	198.51.100.100	ICMP	106	0x474b (1	8251)	64 Echo (ping)	request	id=0x0037,	seq=12/3072,	, ttl=64 (no r	
13 2022-08-07 21	1:21:13.620168	192.0.2.100	198.51.100.100	ICMP	106	0x4781 (1	.8305)	64 Echo (ping)	request	id=0x0037,	seq=13/3328,	, ttl=64 (no r	
14 2022-08-07 21	1:21:14.623169	192.0.2.100	198.51.100.100	ICMP	106	0x4858 (1	.8520)	64 Echo (ping)	request	id=0x0037,	seq=14/3584,	, ttl=64 (no r	
15 2022-08-07 21	1:21:15.622497	192.0.2.100	198.51.100.100	ICMP	106	0x4909 (1	.8697)	64 Echo (ping)	request	id=0x0037,	seq=15/3840,	, ttl=64 (no r	
16 2022-08-07 21	1:21:16.626226	192.0.2.100	198.51.100.100	ICMP	106	0x490b (1	.8699)	64 Echo (ping)	request	id=0x0037,	seq=16/4096,	, ttl=64 (no r	
17 2022-08-07 21	1:21:17.629363	192.0.2.100	198.51.100.100	ICMP	106	0x4932 (1	.8738)	64 Echo (ping)	request	id=0x0037,	seq=17/4352,	, ttl=64 (no r	
18 2022-08-07 21	1:21:18.626651	192.0.2.100	198.51.100.100	ICMP	106	0x4a05 (1	.8949)	64 Echo (ping)	request	id=0x0037,	seq=18/4608,	ttl=64 (no r	~
<													>	
> Frame 1: 106 bytes	on wire (848 bits)), 106 bytes cap	tured (848 bits)			0000	bc e7 12 34	4 9a 14 00 50	56 9d e8	be 81 00 00	cd4	· p v · · · · ·		
> Ethernet II, Src: V	Mware_9d:e8:be (00	0:50:56:9d:e8:be), Dst: Cisco_34:9a	:14 (bc:e7:	12:34:9a:14)	0010	08 00 45 00	0 00 54 41 1f	40 00 40	01 0c 8e c0	00 ··E··T/	A- @-@		
✓ 802.1Q Virtual LAN,	PRI: 0, DEI: 0, 1	ID: 205				0020	02 64 c6 33	3 64 64 08 00	06 67 00	37 00 01 b0	2c ·d·3dd	··· ·g·7···		
000	= Priority: Be	st Effort (defau	ult) (0)			0030	f0 62 00 00	0 00 00 8e fe	03 00 00	00 00 00 10	11 ·b····			
	= DEI: Ineligi	ble				0040	12 13 14 19	5 16 17 18 19	1a 1b 1c	1d 1e 1f 20	21 """"""""""""""""""""""""""""""""""""	/>	!	
0000 1100 11	101 = ID: 205				2	0050	22 23 24 2	5 26 27 28 29	2a 20 2C	2d 2e 2t 30	31 #\$%&	() ~+,/0	31	
Type: IPv4 (0x080	00)				2	0000	52 55 54 5.	5 50 57 55 55	33 33		2545070	00 00		
Trailer: 55555555	5													
> Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100														
Internet Control Me	ssage Protocol													

Spiegazione

Le acquisizioni dello switch vengono configurate sulle sottointerfacce Ethernet1/1.205 o Portchannel1.205 con un filtro che corrisponde alla VLAN 205 esterna.

Nella tabella seguente viene riepilogata l'attività:

Attività	Punto di acquisizione	Filtro interno	Direzione	Traffico acquisito
Configurazione e verifica dell'acquisizione di un pacchetto sull'interfaccia Ethernet1/1.205	Ethernet 1/1	VLAN esterna 2005	Solo in ingresso*	Richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.100
Configurare e verificare l'acquisizione di un pacchetto sull'interfaccia secondaria Portchannel1.205 con le interfacce membro Ethernet1/3 ed Ethernet1/4	Ethernet 1/3 Ethernet 1/4	VLAN esterna 2005	Solo in ingresso*	Richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.100

* A differenza della serie 3100, Secure Firewall 4200 supporta le acquisizioni bidirezionali (in entrata e in uscita).

Acquisizione pacchetti su interfacce interne

Secure Firewall 3100 ha 2 interfacce interne:

• in_data_uplink1: connette l'applicazione allo switch interno.

 in_mgmt_uplink1: fornisce un percorso di pacchetto dedicato per le connessioni di gestione, ad esempio SSH all'interfaccia di gestione o la connessione di gestione, nota anche come sftunnel, tra FMC e FTD.

Secure Firewall 4200 dispone di un massimo di 4 interfacce interne:

- in_data_uplink1 e in_data_uplink2 (solo 4245) : queste interfacce collegano l'applicazione allo switch interno. Nel caso di 4245, i pacchetti vengono bilanciati del carico sulle 2 interfacce uplink.
- in_mgmt_uplink1 e in_mgmt_uplink2 queste interfacce forniscono un percorso di pacchetto dedicato per le connessioni di gestione, ad esempio SSH all'interfaccia di gestione o alla connessione di gestione, nota anche come sftunnel, tra FMC e FTD. Secure Firewall 4200 supporta 2 interfacce di gestione.

Attività 1

Usare la CLI FTD o ASA per configurare e verificare l'acquisizione di un pacchetto sull'interfaccia uplink in_data_uplink1.

Topologia, flusso dei pacchetti e punti di acquisizione

Secure Firewall 3100:



Secure Firewall 4200:

			Cha	ssis	
		Internal Switch		Securit	y Module
	Eth1/			FT	D/ASA
192.0.2.100 ICMP echo	-request		in_data_uplink1		
198.51.100.100	-reply				

Configurazione

Per configurare l'acquisizione di un pacchetto sull'interfaccia in_data_uplink1, eseguire la procedura seguente sull'appliance ASA o sulla CLI di FTD:

1. Creare una sessione di acquisizione:

<#root>

> capture capsw switch interface in_data_uplink1

Secure Firewall 4200 supporta la direzionalità di acquisizione:

<#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. Abilitare la sessione di acquisizione:

<#root>

> no capture capsw switch stop

Verifica

Verificare il nome della sessione di acquisizione, lo stato amministrativo e operativo, lo slot di interfaccia e l'identificatore. Verificare che il valore Pcapsize in byte aumenti e che il numero di pacchetti acquisiti sia diverso da zero:

<#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 O O
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 Filte Name: Protocol: Ivlan: Ovlan: Src Ip:	r Info capsw-1-18 0 0 0 0.0.0.0

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

66 packets captured on disk using switch capture

Reading of capture file from disk is not supported

In questo caso, viene creata un'acquisizione sull'interfaccia con ID interno 18 che è l'interfaccia in_data_uplink1 sul Secure Firewall 3130. Il comando show portmanager switch status nella shell dei comandi FXOS local-mgmt mostra gli ID dell'interfaccia:

```
<#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

Per accedere a FXOS sull'appliance ASA, eseguire il comando connect fxos admin. In caso di contesto multiplo, eseguire questo comando nel contesto admin.

Raccogli file di acquisizione

Eseguire la procedura descritta nella sezione Raccolta dei file di acquisizione di switch interni Secure Firewall.

Analisi dei file di acquisizione

Utilizzare un'applicazione packet capture file reader per aprire i file di acquisizione per l'interfaccia in_data_uplink1. Nell'esempio vengono analizzati i pacchetti acquisiti con Secure Firewall 3100.

Controllare il punto chiave - in questo caso, i pacchetti di richiesta echo ICMP e di risposta echo vengono acquisiti. Questi sono i pacchetti inviati dall'applicazione allo switch interno.

No	Time	Source	Destination	Protocol	Length	1P 1D	IP TTL Info		A
	1 2022-08-07 22:40:05 685606	192.0.2.100	198.51.100.100	TCMP	102	0y4d93 (10859)	64 Echo (ning) request	id=0x003a, sen=33/844	8. ttl=64 (ren]
	2 2022-08-07 22:40:06 685615	198 51 100 100	192 9 2 109	TCMP	102	0x6cdc (27868)	64 Echo (ping) reply	id=0x003a, seq=33/844	8 ttl=64 (reg
1	3 2022-08-07 22:40:07 684210	102 0 2 100	198 51 100 100	TCMP	102	0x0cac (27000)	64 kcho (ping) repuy	id=0x003a, seq=34/870	A ttl=64 (requ
	4 2022-08-07 22:40:07 680300	108 51 100 100	102 0 2 100	TCMP	102	av6db2 (28082)	64 Echo (ping) reply	id=0x0032 son=34/870	A ttl=64 (regu
	5 2022-08-07 22:40:08-685736	192.0.2.100	198.51.100.100	TCMP	102	0x4edc (20188)	64 Echo (ping) request	id=0x003a, seq=35/896	0. ttl=64 (ren]
	6 2022-08-07 22:40:08 600806	198.51.100.100	192.0.2.100	TCMP	102	0x6dbf (28005)	64 Echo (ping) reply	id=0x003a, seq=35/896	0, ttl=64 (reg
	7 2022-08-07 22:40:00 600737	192 0 2 100	198.51.100.100	TCMP	102	0x4f2d (20259)	64 Echo (ping) request	id=0x003a, seq=36/031	6. ttl=64 (reql
	9 2022-08-07 22:40:09 690737	100 51 100 100	102 0 2 100	TCMP	102	0x4120 (20209)	64 Echo (ping) request	id=0x003a, seq=36/921	6 ttl=64 (repi
	0 2022-08-07 22:40:09:090744	102 0 2 100	100 51 100 100	TCMP	102	0x4fb1 (20200)	64 Echo (ping) repry	id=0x003a, seq=30/921	2, ttl=64 (requ
	10 2022-08-07 22:40:10:092200	100 51 100 100	102 0 2 100	TCMP	102	0x4101 (20401)	64 Echo (ping) request	id=0x003a, seq=37/947	2, ttl=64 (repi
	10 2022-08-07 22:40:10:092272	102 0 2 100	100 51 100 100	TCMP	102	0x0203 (20373)	64 Echo (ping) repry	id=0x003a, seq=37/947	2, ttl=64 (requ
	11 2022-08-07 22:40:11.091159	192.0.2.100	198.51.100.100	TCMP	102	0x3008 (20488)	64 Echo (ping) request	id_0u003a, seq=38/972	s, ttl=64 (repi
	12 2022-08-07 22:40:11.091100	198.51.100.100	192.0.2.100	TCMP	102	0X0T30 (28475)	64 Echo (ping) reply	1d=0x003a, Seq=38/9/2	s, ttl=64 (requ
	13 2022-08-07 22:40:12.692135	192.0.2.100	198.51.100.100	ICMP	102	0X5008 (20664)	64 Echo (ping) request	1d=0x003a, seq=39/998	1, ttl=64 (repl
	14 2022-08-07 22:40:12.697209	198.51.100.100	192.0.2.100	ICMP	102	0x6td7 (28631)	64 Echo (ping) reply	1d=0x003a, seq=39/998	4, 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	1d=0x003a, seq=40/102	40, 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=40/102	40, 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=41/104	96, ttl=64 (rep
н.	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=41/104	96, 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: 1	98.51.100.100			0020 64 64 0	08 00 7f 15 00 3a 00 21 39	3f f0 62 00 00 dd	· · · · !9? · b · ·
>	Internet Control Message Protocol					0030 00 00 1	3b 1a 05 00 00 00 00 00 10	11 12 13 14 15	
	0					0040 16 17	18 19 1a 1b 1c 1d 1e 1f 20	21 22 23 24 25	!"#\$%
						0050 26 27 3	28 29 2a 2b 2c 2d 2e 2f 30	31 32 33 34 35 &'()*	+,/012345
						0060 36 37	55 55 55 55	67000	U

Quando si configura l'acquisizione di uno switch sull'interfaccia uplink, vengono acquisiti solo i pacchetti inviati dall'applicazione allo switch interno. I pacchetti inviati all'applicazione non vengono acquisiti.

Nella tabella seguente viene riepilogata l'attività:

Attività	Punto di acquisizione	Filtro interno	Direzione	Traffico acquisito
Configurare e verificare l'acquisizione di un pacchetto sull'interfaccia uplink in_data_uplink1	in_data_uplink1	Nessuna	Solo in ingresso*	Richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.100 ICMP echo risponde dall'host 198.51.100.100 all'host 192.0.2.100

* A differenza della serie 3100, Secure Firewall 4200 supporta le acquisizioni bidirezionali (in entrata e in uscita).

Attività 2

Usare la CLI FTD o ASA per configurare e verificare l'acquisizione di un pacchetto sull'interfaccia uplink in_mgmt_uplink1. Vengono acquisiti solo i pacchetti delle connessioni del piano di gestione.

Topologia, flusso dei pacchetti e punti di acquisizione

Secure Firewall 3100:



Secure Firewall 4200:



Configurazione

Per configurare l'acquisizione di un pacchetto sull'interfaccia in_mgmt_uplink1, eseguire la procedura seguente sull'appliance ASA o sulla CLI di FTD:

1. Creare una sessione di acquisizione:

<#root>

> capture capsw switch interface in_mgmt_uplink1

Secure Firewall 4200 supporta la direzionalità di acquisizione:

<#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. Abilitare la sessione di acquisizione:

<#root>

> no capture capsw switch stop

Verifica

Verificare il nome della sessione di acquisizione, lo stato amministrativo e operativo, lo slot di interfaccia e l'identificatore. Verificare che il valore Pcapsize in byte aumenti e che il numero di pacchetti acquisiti sia diverso da zero:

<#root>	
> show capture capsw	7 detail
Packet Capture info	
Name: c	apsw
Session:	1
Admin State: e	enabled
Oper State:	up
Oper State Reason:	Active
Config Success: Config Fail Reasor Append Flag: Session Mem Usage: Session Pcap Snap	yes overwrite 256 Len: 1518
Error Code: Drop Count:	0 0
Total Physical ports	s 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 Name: Protocol: Ivlan: Ovlan:	er Info capsw-1-19 0 0 0

Src Ip:	0.0.0.0
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

281 packets captured on disk using switch capture

Reading of capture file from disk is not supported

In questo caso, viene creata un'acquisizione sull'interfaccia con ID interno 19, che è l'interfaccia in_mgmt_uplink1 sul Secure Firewall 3130. Il comando show portmanager switch status nella shell dei comandi FXOS local-mgmt visualizza gli ID dell'interfaccia:

<#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	SGMTT	 Up	 1G	 Full	None	link-Up
0/2	SGMII	qu 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	KD	lla	250	F	None	
0/20	KK	Up	256		None	Link-Up
0/21	KR4	Down	40G	FUII	None	L1nk-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

Per accedere a FXOS sull'appliance ASA, eseguire il comando connect fxos admin. In caso di contesto multiplo, eseguire questo comando nel contesto admin.

Raccogli file di acquisizione

Eseguire la procedura descritta nella sezione Raccolta dei file di acquisizione degli switch interni del firewall protetto.

Analisi dei file di acquisizione

Utilizzare un'applicazione packet capture file reader per aprire i file di acquisizione per l'interfaccia in_mgmt_uplink1. Nell'esempio vengono analizzati i pacchetti acquisiti con Secure Firewall 3100.

Controllare il punto chiave: in questo caso vengono visualizzati solo i pacchetti dell'indirizzo IP di gestione 192.0.2.200. Ad esempio, i pacchetti di risposta echo SSH, Sftunnel o ICMP. Si tratta dei pacchetti inviati dall'interfaccia di gestione delle applicazioni alla rete tramite lo switch interno.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info
	196 2022-08-07 23:21:45.133362	192.0.2.200	192.0.2.101	TCP	1518	0xb7d0 (47056)	64 39181 → 8305 [ACK] Seq=61372 Ack=875 Win=1384 Len=1448 TS
	197 2022-08-07 23:21:45.133385	192.0.2.200	192.0.2.101	TCP	1518	0xb7d1 (47057)	64 39181 → 8305 [ACK] Seq=62820 Ack=875 Win=1384 Len=1448 TS
	198 2022-08-07 23:21:45.133388	192.0.2.200	192.0.2.101	TLSv1.2	990	0xb7d2 (47058)	64 Application Data
	199 2022-08-07 23:21:45.928772	192.0.2.200	192.0.2.100	ICMP	78	0xbd48 (48456)	64 Echo (ping) reply id=0x0001, seq=4539/47889, ttl=64
	200 2022-08-07 23:21:45.949024	192.0.2.200	192.0.2.101	TLSv1.2	128	0x4a97 (19095)	64 Application Data
	201 2022-08-07 23:21:45.949027	192.0.2.200	192.0.2.101	TCP	70	0x4a98 (19096)	64 8305 → 58885 [ACK] Seq=21997 Ack=26244 Win=4116 Len=0 TSv
	202 2022-08-07 23:21:46.019895	192.0.2.200	192.0.2.101	TLSv1.2	100	0x4a99 (19097)	64 Application Data
	203 2022-08-07 23:21:46.019899	192.0.2.200	192.0.2.101	TLSv1.2	96	0x4a9a (19098)	64 Application Data
	204 2022-08-07 23:21:46.019903	192.0.2.200	192.0.2.101	TCP	70	0x4a9b (19099)	64 8305 → 58885 [ACK] Seq=22053 Ack=26274 Win=4116 Len=0 TSv
	205 2022-08-07 23:21:46.019906	192.0.2.200	192.0.2.101	TCP	70	0x4a9c (19100)	64 8305 → 58885 [ACK] Seq=22053 Ack=26300 Win=4116 Len=0 TSv
	206 2022-08-07 23:21:46.136415	192.0.2.200	192.0.2.101	TCP	70	0xb7d3 (47059)	64 39181 → 8305 [ACK] Seq=65188 Ack=921 Win=1384 Len=0 TSval
	207 2022-08-07 23:21:46.958148	192.0.2.200	192.0.2.100	ICMP	78	Øxbd9e (48542)	64 Echo (ping) reply id=0x0001, seq=4540/48145, ttl=64
	208 2022-08-07 23:21:47.980409	192.0.2.200	192.0.2.100	ICMP	78	Øxbdf2 (48626)	64 Echo (ping) reply id=0x0001, seq=4541/48401, ttl=64
	209 2022-08-07 23:21:48.406312	192.0.2.200	192.0.2.101	TCP	70	0x4a9d (19101)	64 8305 → 58885 [ACK] Seq=22053 Ack=26366 Win=4116 Len=0 TSv
	210 2022-08-07 23:21:48.903236	192.0.2.200	192.0.2.101	TLSv1.2	747	0x4a9e (19102)	64 Application Data
	211 2022-08-07 23:21:48.994386	192.0.2.200	192.0.2.100	ICMP	78	Øxbe48 (48712)	64 Echo (ping) reply id=0x0001, seq=4542/48657, ttl=64
	212 2022-08-07 23:21:50.008576	192.0.2.200	192.0.2.100	ICMP	78	Øxbea6 (48806)	64 Echo (ping) reply id=0x0001, seq=4543/48913, ttl=64
	213 2022-08-07 23:21:50.140167	192.0.2.200	192.0.2.101	TCP	1518	0xb7d4 (47060)	64 39181 → 8305 [ACK] Seq=65188 Ack=921 Win=1384 Len=1448 TS
	214 2022-08-07 23:21:50.140171	192.0.2.200	192.0.2.101	TCP	1518	0xb7d5 (47061)	64 39181 → 8305 [ACK] Seq=66636 Ack=921 Win=1384 Len=1448 TS
	215 2022-08-07 23:21:50.140175	192.0.2.200	192.0.2.101	TLSv1.2	990	0xb7d6 (47062)	64 Application Data
	216 2022-08-07 23:21:51.015884	192.0.2.200	192.0.2.100	ICMP	78	Øxbec1 (48833)	64 Echo (ping) reply id=0x0001, 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	Øxbf59 (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
<	115 1011 00 07 12·11·55 126700	103 0 3 300	103 0 3 100	TCMD	70	avhfr1 (10000)	64 Echo (ning) nonly id-avagat con-4540/50102 ++1-64
. En	and 1, 747 butes on wine (5076 bits	> 747 butos cor	turned (E076 bi	te)		0000 04 53 00	11 20 20 hc o7 12 24 00 00 00 45 00
2 FD	ame 1: 747 bytes on wire (5976 bits	s), 747 Dytes cap	Detu Cieco 11	(5) (20,22 (24,52,02,1)	1.20.22)	0000 a4 53 00 0010 a2 do 4a	11 38 28 00 67 12 34 98 00 08 00 45 00 55 8 ··· 4 ··· E·
/ EU	ternet II, Src: CISCO_34:94:00 (DC:	e/:12:34:98:00),	DSU: UISCO_II	:38:2d (d4:53:00:1	1:38:24)	0020 02 65 20	71 e6 05 67 1b 2a c5 db e3 6b d4 80 18 e g.g. *···k···
2 10	cernet Protocol Version 4, Src: 192		192.0.2.101		(77	0030 10 14 27	cc 00 00 01 01 08 0a 08 76 95 7f 91 02
2 In	ansmission Control Protocol, Src Po	ort: 8305, Ust Po	ort: 58885, Seq	: 1, ACK: 1, Len: 0	6//	0040 3d 41 17	03 03 02 a0 22 6a 01 e0 ff cc 98 f9 af =A" j
2 10	ansport Layer Security					0050 07 40 75	19 a4 d5 df 64 d8 fe 66 8e 9b cc 8d 2f -@u····d ··f····/
						0060 92 b2 1a	64 e7 20 36 03 8e 48 02 5a 7c 85 30 d4 ····d· 6· ·H·Z ·0·
						0070 fa c0 a8	56 b8 ad a7 7e 19 3a c1 9c 4b 57 0e e0 ····V···~ ·:··KW··
						0080 be ef 95	22 84 c1 c1 9d 9f 24 78 b4 15 1c 44 0e ··· "···· ·\$x···D·
						0090 ea cb 43	9e 1f fd a7 70 75 e5 6b a4 f8 2b ee 47 ···· p u·k··+·G
						00a0 2f 86 73	8t b1 e1 b5 c6 57 e3 a8 46 0e cb 26 b7 / s · · · · W · F · &
						0000 5b c7 e3	09 54 t3 c1 tt 26 d9 87 ea 51 3d 20 08 [T&Q= .
						0000 16 fd CD	12 41 31 38 26 80 12 1/ 22 08 01 20 840.0.

Spiegazione

Quando si configura l'acquisizione di uno switch sull'interfaccia uplink di gestione, vengono acquisiti solo i pacchetti in entrata inviati dall'interfaccia di gestione dell'applicazione. I pacchetti destinati all'interfaccia di gestione delle applicazioni non vengono acquisiti.

Nella tabella seguente viene riepilogata l'attività:

Attività	Punto di acquisizione	Filtro interno	Direzione	Traffico acquisito
Configurazione e verifica dell'acquisizione di un pacchetto sull'interfaccia uplink di gestione	in_mgmt_uplink1	Nessuna	Solo in ingresso* (dall'interfaccia di gestione alla rete tramite lo switch interno)	Risposte echo ICMP da gestione FTD indirizzo IP 192.0.2.200 all'host 192.0.2.100 Sftunnel dall'indirizzo IP di gestione FTD 192.0.2.200 all'indirizzo IP FMC 192.0.2.101 SSH da FTD management IP address 192.0.2.200 all'host 192.0.2.100

* A differenza della serie 3100, Secure Firewall 4200 supporta le acquisizioni bidirezionali (in entrata e in uscita).

Filtri di acquisizione pacchetti

I filtri di acquisizione dei pacchetti dello switch interno sono configurati allo stesso modo delle acquisizioni del piano dati. Utilizzare le opzioni ethernet-type e match per configurare i filtri.

Configurazione

Eseguire la procedura seguente sull'appliance ASA o sulla CLI del protocollo FTD per configurare l'acquisizione di un pacchetto con un filtro che corrisponda ai frame ARP o ai pacchetti ICMP dell'host 198.51.100.100 sull'interfaccia Ethernet1/1:

1. Verificare il nome se:

<#root>

```
>
```

```
show nameif
```

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

2. Creare una sessione di acquisizione per ARP o ICMP:

<#root>

>

capture capsw switch interface inside ethernet-type arp

<#root>

> capture capsw switch interface inside match icmp 198.51.100.100

Verifica

Verificare il nome della sessione di acquisizione e il filtro. Il valore di Ethertype è 2054 in decimale e 0x0806 in esadecimale:

<#root>

> show capture capsw detail Packet Capture info Name: capsw Session: 1 Admin State: disabled Oper State: down Oper State Reason: Session_Admin_Shut Config Success: yes Config Fail Reason: Append Flag: overwrite Session Mem Usage: 256 Session Pcap Snap Len: 1518 Error Code: 0 Drop Count: 0 Total Physical ports involved in Packet Capture: 1 Physical port: Slot Id: 1 Port Id: 1 Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap Pcapsize: 0 Filter: capsw-1-1 Packet Capture Filter Info Name: capsw-1-1 Protocol: 0 Ivlan: 0 Ovlan: 0 0.0.0.0 Src Ip: Dest Ip: 0.0.0.0 Src Ipv6: :: Dest Ipv6: :: Src MAC: 00:00:00:00:00:00 00:00:00:00:00:00 Dest MAC: Src Port: 0 Dest Port: 0 2054 Ethertype:

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

Questa è la verifica del filtro per ICMP. Il protocollo IP 1 è l'ICMP:

<#root>

>

show capture capsw detail

Packet Capture info

Name:

capsw

Session:1Admin State:disabledOper State:downOper State Reason:Session_Admin_ShutConfig Success:yesConfig Fail Reason:Append Flag:Append Flag:overwriteSession Mem Usage:256Session Pcap Snap Len:1518Error Code:0Drop 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:	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 break	out ports involved in Packet Capture: 0
0 packets captured or	n disk using switch capture
Reading of capture fi	le from disk is not supported

Raccogli file di acquisizione switch interno Secure Firewall

Usare ASA o FTD CLI per raccogliere i file di acquisizione dello switch interno. Su FTD, il file di acquisizione può anche essere esportato tramite il comando copy della CLI verso destinazioni raggiungibili tramite le interfacce di dati o di diagnostica.

In alternativa, il file può essere copiato in /ngfw/var/common in modalità Expert e scaricato da FMC tramite l'opzione File Download.

Nel caso delle interfacce port-channel, assicurarsi di raccogliere i file di acquisizione dei pacchetti da tutte le interfacce membro.

ASA

Per raccogliere i file di acquisizione degli switch interni sulla CLI dell'ASA, attenersi alla seguente procedura:

1. Interrompere l'acquisizione:

<#root>

asa#

capture capsw switch stop

2. Verificare che la sessione di acquisizione sia stata arrestata e annotare il nome del file di acquisizione.

<#root>

asa#

show capture capsw detail

Packet Capture info

Name: capsw Session: 1 Admin State: disabled Oper State: down Oper State Reason: Session_Admin_Shut Config Success: yes Config Fail Reason: Append Flag: overwrite Session Mem Usage: 256 Session Pcap Snap Len: 1518 Error Code: 0 0 Drop Count: Total Physical ports involved in Packet Capture: 1 Physical port: Slot Id: 1 Port Id: 1 Pcapfile: /mnt/disk0/packet-capture/ sess-1-capsw-ethernet-1-1-0.pcap Pcapsize: 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 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. Utilizzare il comando copy della CLI per esportare il file in destinazioni remote:

<#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
               Copy to smb: file system
 smb:
 startup-config Copy to startup configuration
                Copy to system: file system
 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

Eseguire questi passaggi per raccogliere i file di acquisizione dello switch interno sulla CLI FTD e copiarli sui server raggiungibili tramite interfacce di dati o di diagnostica:

1. Andare alla CLI di diagnostica:

<#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. Interrompere l'acquisizione:

<#root>

firepower#

```
capture capi switch stop
```

3. Verificare che la sessione di acquisizione sia stata arrestata e annotare il nome del file di acquisizione:

<#root> firepower# show capture capsw detail Packet Capture info Name: capsw Session: 1 Admin State: disabled Oper State: down Oper State Reason: Session_Admin_Shut Config Success: yes Config Fail Reason: Append Flag: overwrite Session Mem Usage: 256 Session Pcap Snap Len: 1518 Error Code: 0 Drop Count: 0 Total Physical ports involved in Packet Capture: 1 Physical port: Slot Id: 1 Port Id: 1 Pcapfile: /mnt/disk0/packet-capture/

Pcap	osize:	139	9826					
Filt	ter:	cap	osw-1-1	L				
Packet	Capture	Filter Tu	nfo					
Name		car		l				
Prot		0		-				
Tvla	an:	0						
0v1a	an:	0						
Src	Ip:	0.0	0.0.0					
Dest	ID:	0.0	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						
Ethe	ertype:	0						
Total	Dhysical	brookout	nonta	involved	in	Dacket	Conturo	0
Total	Physical	preakout	ports	involved	in	racket	capture:	0

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

4. Usare il comando copy della CLI per esportare il file in destinazioni remote.

<#root>

firepower#

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

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

firepower#

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

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

139826 bytes copied in 0.532 secs

Per raccogliere i file di acquisizione da FMC tramite l'opzione Download file, eseguire la procedura seguente:

1. Interrompere l'acquisizione:

```
<#root>
```

>

```
capture capsw switch stop
```

2. Verificare che la sessione di acquisizione sia stata arrestata e prendere nota del nome del file e del percorso completo del file di acquisizione:

<#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 Reaso	n:
Append Flag:	overwrite
Session Mem Usage	: 250 Long 1518
Frror Code:	0
Drop Count:	0
Total Physical port	s involved in Packet Capture: 1
Physical port:	
Slot Id:	1
Port Id:	1
Pcapfile:	/mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize:	139826
·	

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

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

3. Andare alla modalità Expert e passare alla modalità root:

<#root>

>

expert

admin@firepower:~\$

sudo su

root@firepower:/home/admin

4. Copiare il file di acquisizione in /ngfw/var/common/:

<#root>

root@KSEC-FPR3100-1:/home/admin

cp /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap /ngfw/var/common/

root@KSEC-FPR3100-1:/home/admin

ls -l /ngfw/var/common/sess*

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

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

5. In FMC scegliere Dispositivi > Download file:

Firewall Management Center Overview / Dashboards / Dashboard	Overview	Analysis Policies	Devices Objects	Integration	Deploy Q 🧐 🌣 🖉 lab_domain \ admir	train secure		
Summary Dashboard (swetch dashboard) Provides a summary of activity on the appliance Network × Threats Intrusion Events	location QoS	Device Management Device Upgrade NAT QoS Platform Settings FlexConfig Certificates	VPN Site To Site Remote Acc Dynamic Ac Troubleshoo Site to Site	Troubleshoot File Download Cess Threat Defense CLI Cess Policy Packet Tracer Oting Packet Capture Monitoring	Reporting II Add Widgets			
Unique Applications over Time	-×	Top Web Applica	tions occu	- ^	F TOP Client Applications Seen	- ×		
25 20 15 10 05 00 15:25 15:35 15:45 15:55 Last updated less than a minute ago	16.05	Last updated less than	No Data a minute ago		No Data Last updated less than a minute ago			
Traffic by Application Risk	- ×	h Ton Senier Appli	antione Coop		 Top Operating Systems Seen 			
Risk Total Madum	Bytes (KB) 52.83	 Top Server Appli 	No Data	- ×	No Data	- ×		

6. Scegliere l'FTD, fornire il nome del file di acquisizione e fare clic su Download:

Firewall Management Center Overview	Analysis	Policies	Devices	Objects	Integration	Deplo	y Q	. 🧬	۵	0	lab_domain \ ad	min 🔻	cisco SE	CURE
							Th	reat De	fense	СЦ	Packet Captu	ire	Packet Tra	acer
	Device FPR3100-1 File		*											
	sess-1-caps	w-ethernet-	1-1-0.pcap											
		l	Back	Download										

Linee guida, limitazioni e best practice per l'acquisizione di pacchetti di switch interni

Linee guida e limitazioni:

- Sono supportate più sessioni di configurazione dell'acquisizione degli switch, ma può essere attiva solo una sessione di acquisizione alla volta. Un tentativo di abilitare 2 o più sessioni di acquisizione genera l'errore "ERRORE: impossibile abilitare la sessione, è stato raggiunto il limite massimo di 1 sessione di acquisizione pacchetti attiva".
- · Impossibile eliminare un'acquisizione switch attiva.
- Impossibile leggere le acquisizioni di switch nell'applicazione. L'utente deve esportare i file.
- Alcune opzioni di acquisizione del piano dati, quali dump, decode, packet-number, trace e altre, non sono supportate per le acquisizioni dello switch.

• Nel caso di un'ASA multi-contesto, le acquisizioni dello switch sulle interfacce dati vengono configurate nei contesti utente. Le acquisizioni dello switch sulle interfacce in_data_uplink1 e in_mgmt_uplink1 sono supportate solo nel contesto admin.

Questo è l'elenco delle best practice basate sull'uso della cattura di pacchetti nei casi TAC:

- Stai attento alle linee guida e ai limiti.
- Utilizzare i filtri di acquisizione.
- Considerare l'impatto di NAT sugli indirizzi IP dei pacchetti quando viene configurato un filtro di acquisizione.
- Aumenta o diminuisce la lunghezza del pacchetto che specifica le dimensioni del frame, nel caso differisca dal valore predefinito di 1518 byte. Dimensioni inferiori determinano un numero maggiore di pacchetti acquisiti e viceversa.
- Regolare le dimensioni del buffer in base alle esigenze.
- Prendere nota del valore Drop Count nell'output del comando show cap<cap_name>detail. Una volta raggiunto il limite delle dimensioni del buffer, il contatore di rilascio aumenta.

Informazioni correlate

- Guide alla configurazione di Firepower 4100/9300 Chassis Manager e FXOS CLI
- Guida introduttiva a Cisco Secure Firewall 3100
- Guida di riferimento ai comandi di Cisco Firepower 4100/9300 FXOS

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).