Uso di Firepower Threat Defense Capture e Packet Tracer

Sommario

Introduzione

In questo documento viene descritto come usare le acquisizioni Firepower Threat Defense (FTD) e le utility Packet Tracer.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

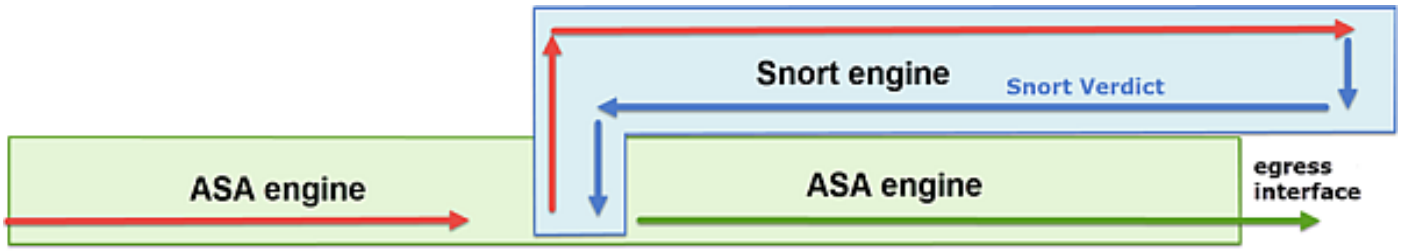
- ASA 5515-X con software FTD 6.1.0
- FPR4110 con software FTD 6.2.2
- FS4000 con software Firepower Management Center (FMC) 6.2.2

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.

Premesse

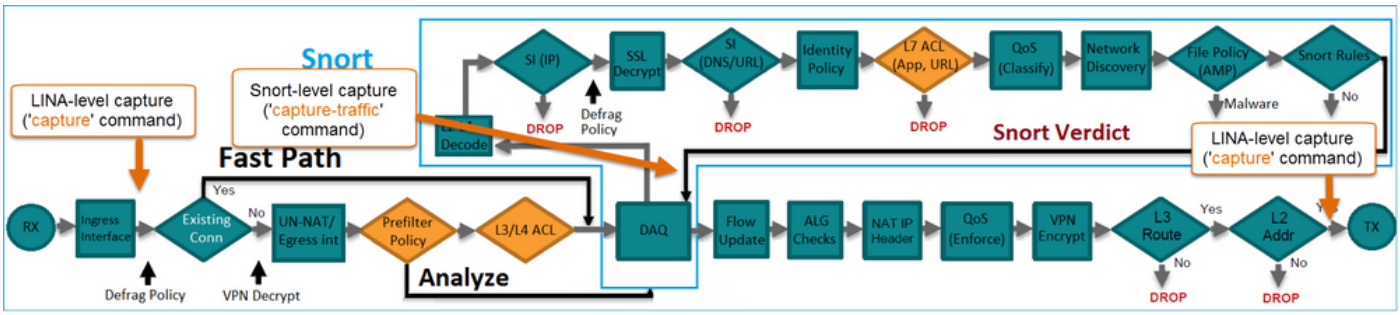
Elaborazione pacchetti FTD

L'elaborazione del pacchetto FTD viene visualizzata come segue:



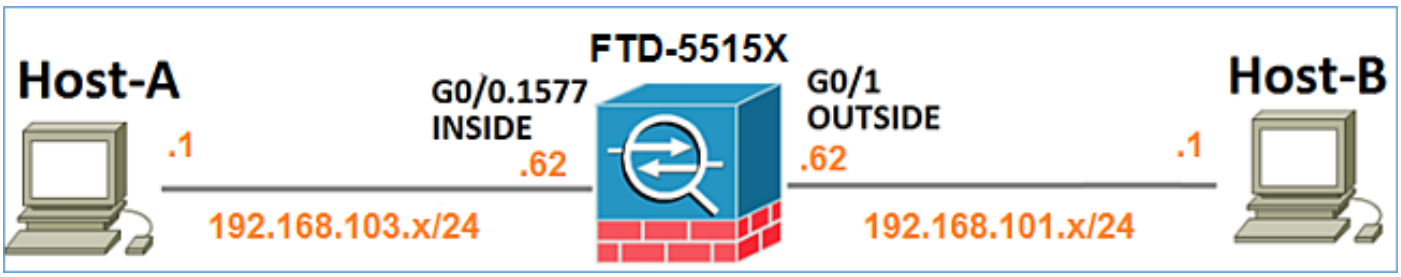
1. Un pacchetto entra nell'interfaccia in entrata e viene gestito dal motore LINA.
2. Se il criterio richiede che il pacchetto venga ispezionato dal motore Snort.
3. Il motore Snort restituisce un verdetto per il pacchetto.
4. In base a questo verdetto, il motore LINA elimina il pacchetto o lo inoltra.

In base all'architettura, le acquisizioni FTD possono essere effettuate nei seguenti luoghi:



Configurazione

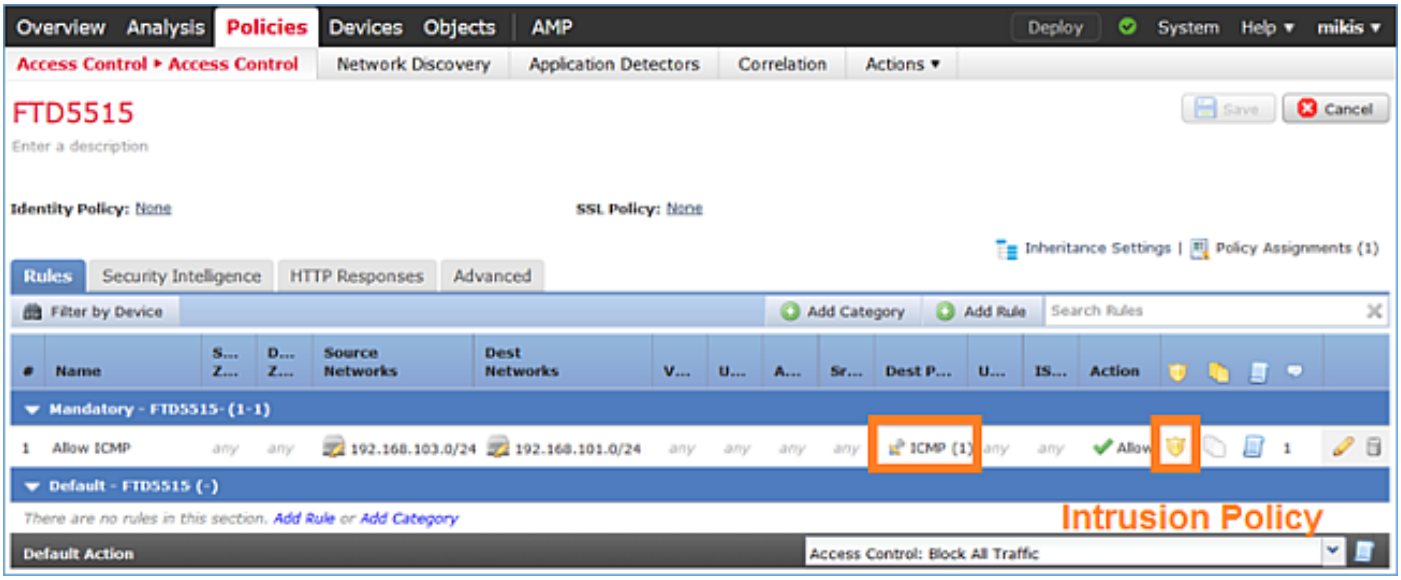
Esempio di rete



Operazioni con le acquisizioni motore di snort

Prerequisiti

All'FTD è applicata una policy di controllo dell'accesso (ACP) che consente il passaggio del traffico ICMP (Internet Control Message Protocol). La politica prevede anche l'applicazione di una politica sulle intrusioni:



Requisiti

1. Abilita l'acquisizione in modalità FTD CLISH senza un filtro.
2. Eseguire il ping attraverso l'FTD e controllare l'output acquisito.

Soluzione

Passaggio 1. Accedere alla console FTD o SSH all'interfaccia br1 e abilitare l'acquisizione in modalità FTD CLISH senza un filtro.

<#root>

```
>

capture-traffic


Please choose domain to capture traffic from:
  0 - br1
  1 - Router

Selection?

1


Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
```

Su FTD 6.0.x il comando è:

<#root>

```
>

system support

capture-traffic
```

Passaggio 2. Eseguire il ping tra FTD e controllare l'output acquisito.

<#root>

```
>

capture-traffic


Please choose domain to capture traffic from:
  0 - br1
  1 - Router

Selection?
```

```
1


Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:

12:52:34.749945 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 1, le
12:52:34.749945 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq 1, leng
12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 2, le
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq 2, leng
12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 3, le
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq 3, leng
12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 4, le
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq 4, leng
^C    <- to exit press CTRL + C
```

Operazioni con le acquisizioni motore di snort

Requisiti

1. Abilitare l'acquisizione in modalità FTD CLISH con l'uso di un filtro per IP 192.168.101.1.
2. Eseguire il ping tra FTD e controllare l'output acquisito.

Soluzione

Passaggio 1. Abilitare l'acquisizione in modalità FTD CLISH con l'uso di un filtro per IP 192.168.101.1.

```
<#root>

>

capture-traffic


Please choose domain to capture traffic from:
  0 - br1
  1 - Router

Selection?

1


Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:

host 192.168.101.1
```

Passaggio 2. Eseguire il ping attraverso l'FTD e controllare l'output acquisito:

```
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 0, len
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 1, len
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 2, len
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 3, len
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 4, len
```

È possibile utilizzare l'opzione -n per visualizzare gli host e i numeri di porta in formato numerico. Ad esempio, l'acquisizione precedente viene mostrata come:

<#root>

```
>

capture-traffic


Please choose domain to capture traffic from:
  0 - br1
  1 - Router

Selection?

1


Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:

-n host 192.168.101.1

13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 0, length 80
13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 1, length 80
13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 2, length 80
13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 3, length 80
13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 4, length 80
```

Esempi Di Filtro Tcpdump

Esempio 1:

Per acquisire Src IP o Dst IP = 192.168.101.1 e Src port o Dst port = TCP/UDP 23, immettere questo comando:

<#root>

```
Options:

-n host 192.168.101.1 and port 23
```

Esempio 2:

Per acquisire Src IP = 192.168.101.1 e Src port = TCP/UDP 23, immettere questo comando:

<#root>

Options:

-n src 192.168.101.1 and src port 23

Esempio 3:

Per acquisire Src IP = 192.168.101.1 e Src port = TCP 23, immettere questo comando:

<#root>

Options:

-n src 192.168.101.1 and tcp and src port 23

Esempio 4:

Per acquisire Src IP = 192.168.101.1 e vedere l'indirizzo MAC dei pacchetti, aggiungere l'opzione 'e' e immettere questo comando:

<#root>

Options:

-ne

src 192.168.101.1

17:57:48.709954

6c:41:6a:a1:2b:f6 > a8:9d:21:93:22:90,

ethertype IPv4 (0x0800), length 58: 192.168.101.1.23 > 192.168.103.1.25420:
Flags [S.], seq 3694888749, ack 1562083610, win 8192, options [mss 1380], length 0

Esempio 5:

Per uscire dopo aver acquisito 10 pacchetti, immettere questo comando:

<#root>

Options:

```
-n -c 10 src 192.168.101.1

18:03:12.749945 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 3758037348, win 32768, length
18:03:12.749945 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 1, win 32768, length 2
18:03:12.949932 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 1, win 32768, length 10
18:03:13.249971 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 3, win 32768, length 0
18:03:13.249971 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 3, win 32768, length 2
18:03:13.279969 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 5, win 32768, length 0
18:03:13.279969 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 5, win 32768, length 10
18:03:13.309966 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 7, win 32768, length 0
18:03:13.309966 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 7, win 32768, length 12
18:03:13.349972 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 9, win 32768, length 0
```

Esempio 6:

Per scrivere un'acquisizione in un file denominato capture.pcap e copiarla su un server remoto tramite FTP, immettere questo comando:

```
<#root>

Options:

-w capture.pcap host 192.168.101.1
CTRL + C <- to stop the capture
> file copy 10.229.22.136 ftp / capture.pcap

Enter password for ftp@10.229.22.136:
Copying capture.pcap

Copy successful.


>
```

Operazioni con le acquisizioni del motore LINA FTD

Requisiti

1. Abilitare due acquisizioni su FTD con l'uso di questi filtri:

IP di origine	192.168.103.1
IP di destinazione	192.168.101.1
Protocollo	ICMP

Interfaccia	INTERNO
IP di origine	192.168.103.1
IP di destinazione	192.168.101.1
Protocollo	ICMP
Interfaccia	ESTERNO

2. Eseguire il ping tra l'host A (192.168.103.1) e l'host B (192.168.101.1) e controllare le acquisizioni.

Soluzione

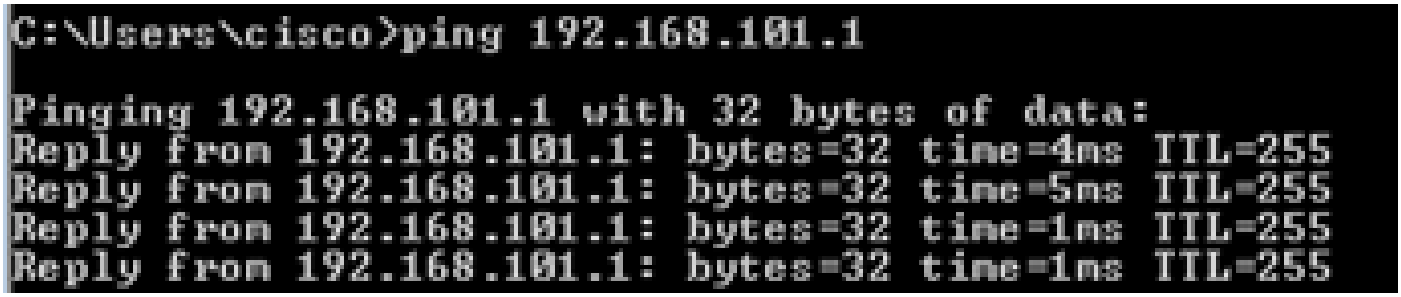
Passaggio 1. Abilitare le clip:

<#root>

```
> capture CAPI interface INSIDE match icmp host 192.168.103.1 host 192.168.101.1
> capture CAPO interface OUTSIDE match icmp host 192.168.101.1 host 192.168.103.1
```

Passaggio 2. controllare le clip nella CLI.

Eseguire il ping tra l'host A e l'host B:



<#root>

```
> show capture

capture CAPI type raw-data interface INSIDE [Capturing

- 752 bytes

]
```

```
  match icmp host 192.168.103.1 host 192.168.101.1
capture CAPO type raw-data interface OUTSIDE [Capturing
- 720 bytes
]
  match icmp host 192.168.101.1 host 192.168.103.1
```

Le due clip hanno dimensioni diverse a causa dell'intestazione Dot1Q sull'interfaccia INSIDE, come mostrato nell'esempio di output:

<#root>

```
> show capture CAPI

8 packets captured
   1: 17:24:09.122338
802.1Q vlan#1577
 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   2: 17:24:09.123071 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
   3: 17:24:10.121392 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   4: 17:24:10.122018 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
   5: 17:24:11.119714 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   6: 17:24:11.120324 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
   7: 17:24:12.133660 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   8: 17:24:12.134239 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
8 packets shown
```

<#root>

```
> show capture CAPO

8 packets captured
   1: 17:24:09.122765  192.168.103.1 > 192.168.101.1: icmp: echo request
   2: 17:24:09.122994  192.168.101.1 > 192.168.103.1: icmp: echo reply
   3: 17:24:10.121728  192.168.103.1 > 192.168.101.1: icmp: echo request
   4: 17:24:10.121957  192.168.101.1 > 192.168.103.1: icmp: echo reply
   5: 17:24:11.120034  192.168.103.1 > 192.168.101.1: icmp: echo request
   6: 17:24:11.120263  192.168.101.1 > 192.168.103.1: icmp: echo reply
   7: 17:24:12.133980  192.168.103.1 > 192.168.101.1: icmp: echo request
   8: 17:24:12.134194  192.168.101.1 > 192.168.103.1: icmp: echo reply
8 packets shown
```

Operazioni con le acquisizioni del motore LINA FTD - Esportazione di un'acquisizione tramite HTTP

Requisiti

Esporta le clip acquisite nello scenario precedente con un browser.

Soluzione

Per esportare le clip con un browser, è necessario:

1. Abilita il server HTTPS
2. Consenti accesso HTTPS

Per impostazione predefinita, il server HTTPS è disabilitato e non è consentito alcun accesso:

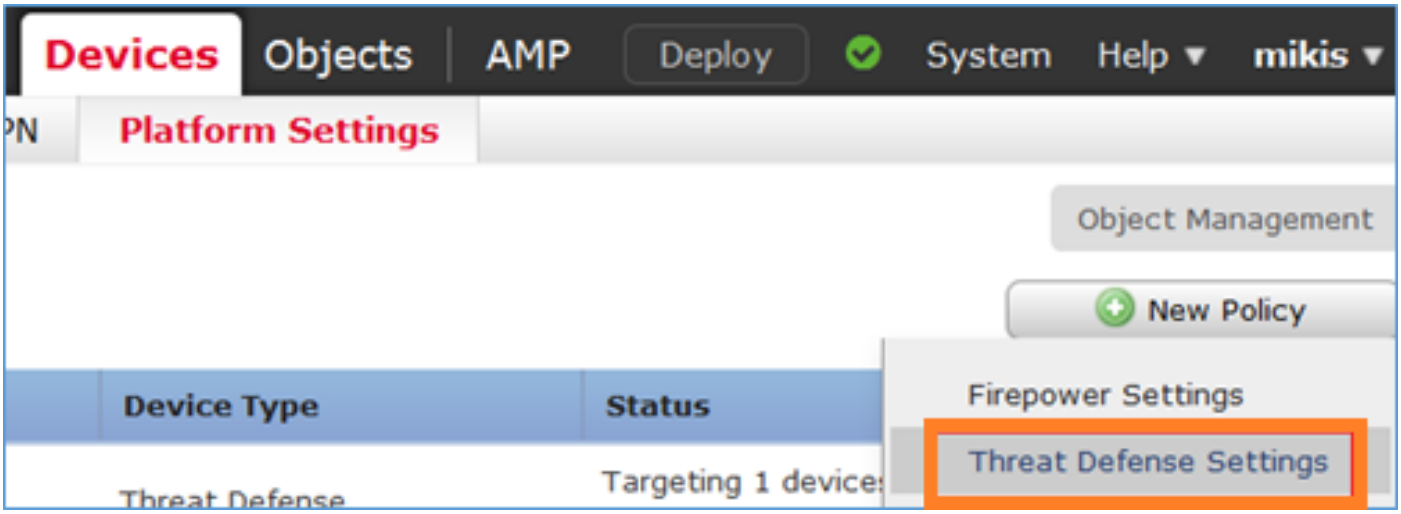
<#root>

>

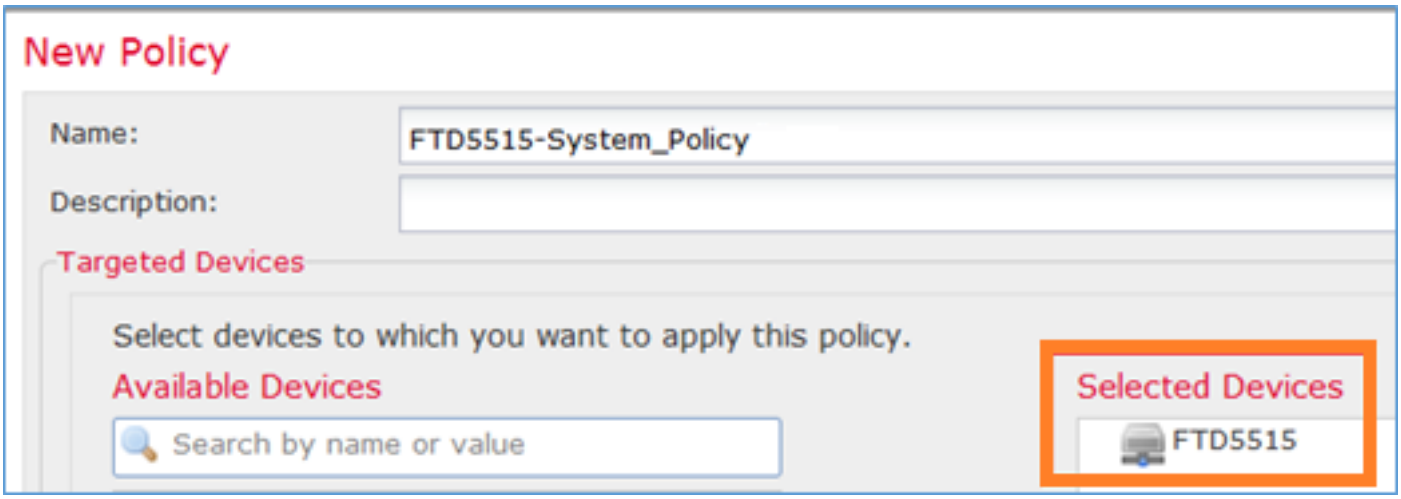
show running-config http

>

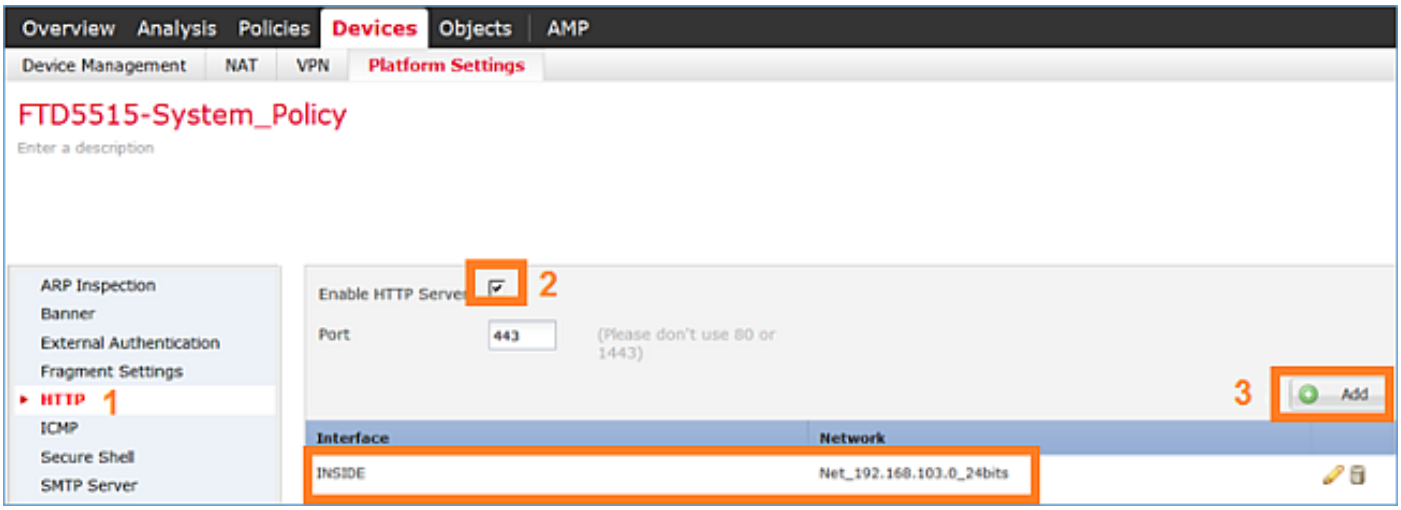
Passaggio 1. Passare a Dispositivi > Impostazioni piattaforma, fare clic su Nuovo criterio e scegliere Impostazioni di difesa dalle minacce:



Specificare il nome del criterio e la destinazione del dispositivo:



Passaggio 2. Abilitare il server HTTPS e aggiungere la rete a cui si desidera consentire l'accesso al dispositivo FTD tramite HTTPS:



Salvataggio e distribuzione.

Al momento della distribuzione dei criteri, è possibile abilitare il comando debug http per visualizzare l'avvio del servizio HTTP:

<#root>

```
> debug http 255

debug http enabled at level 255.

http_enable: Enabling HTTP server
HTTP server starting.
```

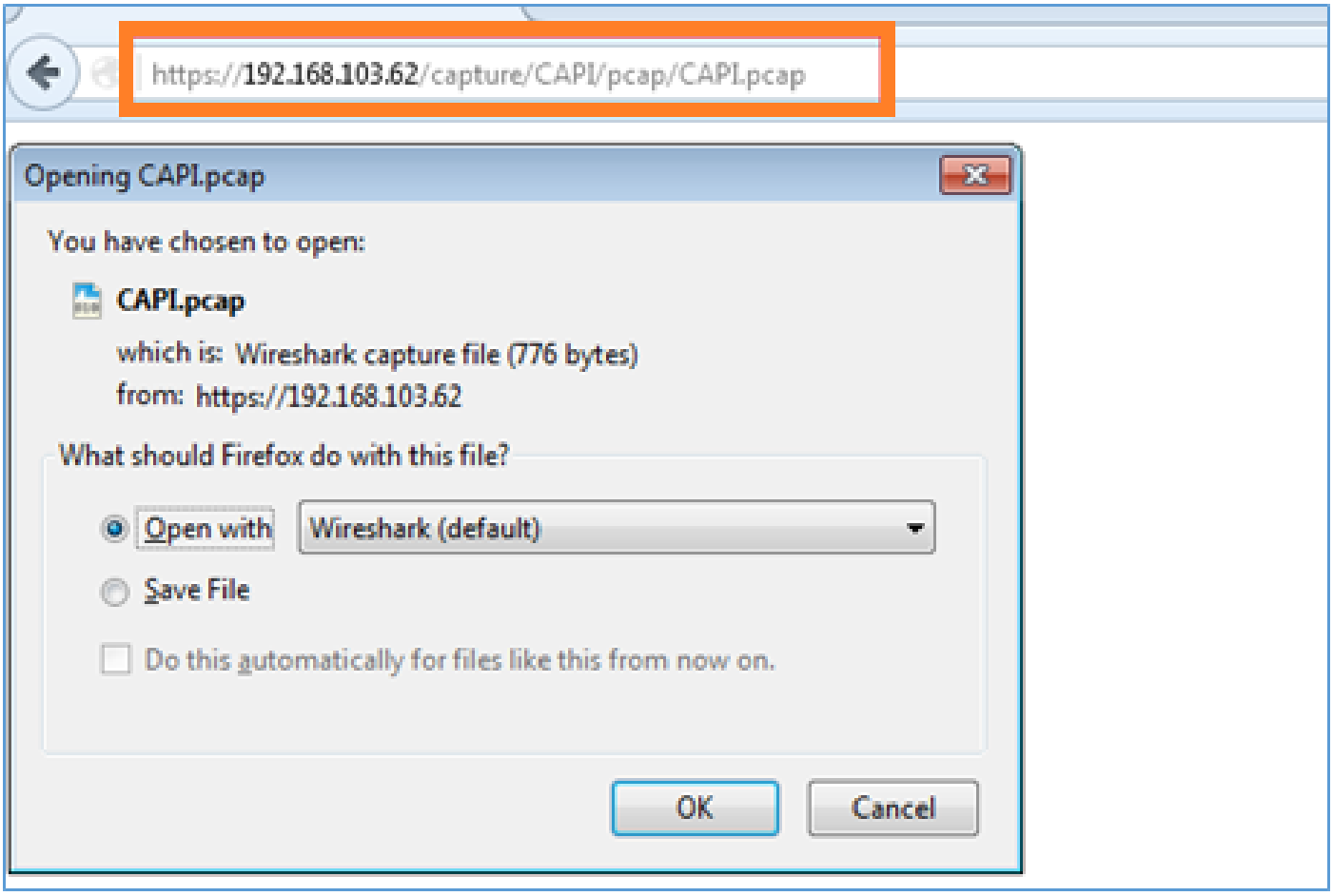
Il risultato sulla CLI FTD è:

<#root>

```
> unebug all
```

```
> show run http
http server enable
http 192.168.103.0 255.255.255.0 INSIDE
```

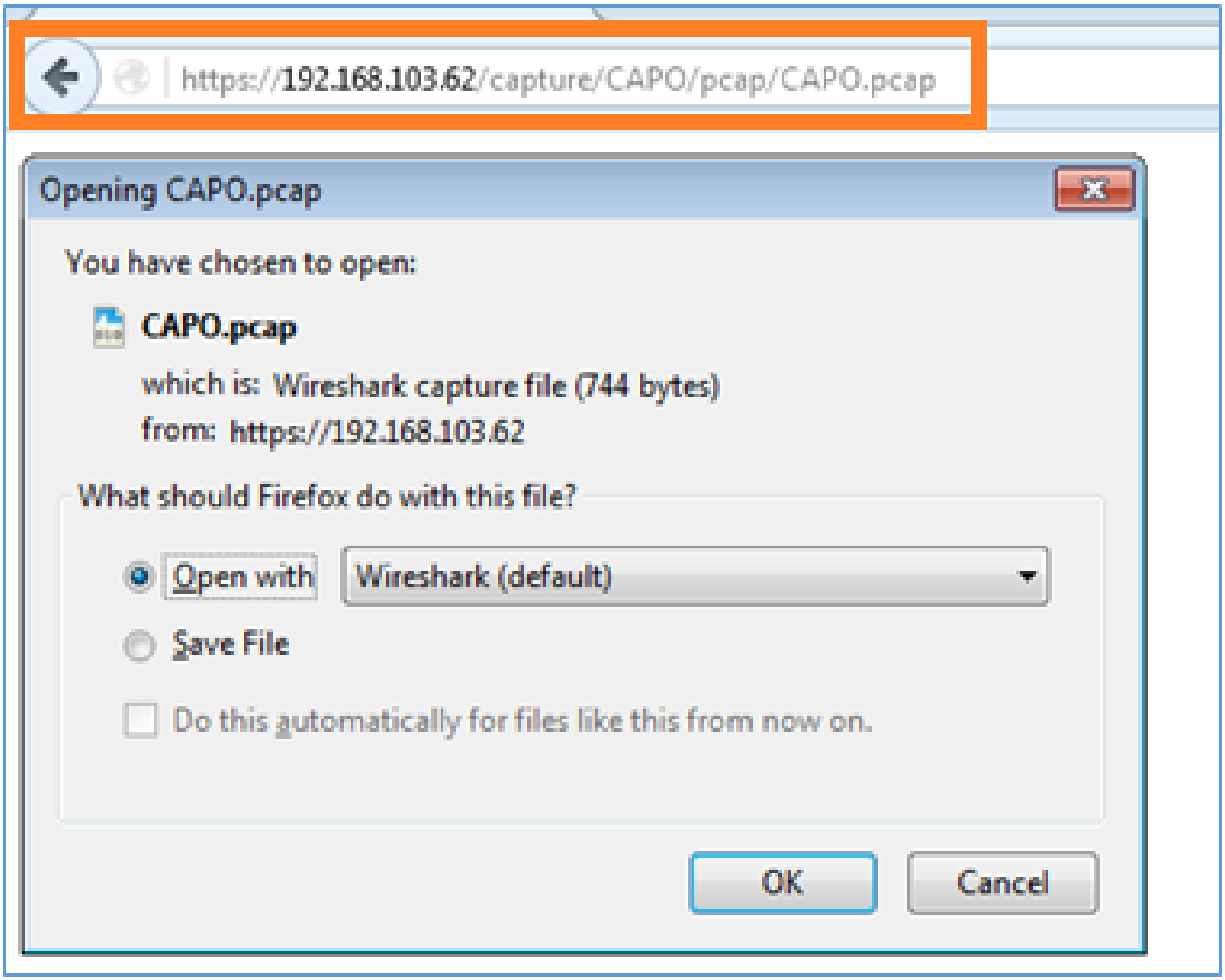
Aprire un browser sull'host A (192.168.103.1) e usare questo URL per scaricare la prima clip: https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap.



Per riferimento:

https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	IP dell'interfaccia dati FTD in cui è abilitato il server HTTP
https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	Nome dell'acquisizione FTD
https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	Nome del file scaricato

Per la seconda acquisizione, utilizzare https://192.168.103.62/capture/CAPO/pcap/CAPO.pcap.



Operazioni con le acquisizioni del motore LINA FTD - Esportazione di un'acquisizione tramite FTP/TFTP/SCP

Requisiti

Esportare le clip acquisite negli scenari precedenti con i protocolli FTP/TFTP/SCP.

Soluzione

Esportare un'acquisizione su un server FTP:

<#root>

```
firepower

# copy /pcap capture:CAPI ftp://ftp_username:ftp_password@192.168.78.73/CAPI.pcap

Source capture name [CAPI]?

Address or name of remote host [192.168.78.73]?
```

```
Destination username [ftp_username]?

Destination password [ftp_password]?

Destination filename [CAPI.pcap]?
!!!!!!
```

114 packets copied in 0.170 secs

```
firepower#
```

Esportare un'acquisizione su un server TFTP:

<#root>

```
firepower

# copy /pcap capture:CAPI tftp://192.168.78.73


Source capture name [CAPI]?

Address or name of remote host [192.168.78.73]?

Destination filename [CAPI]?
!!!!!!!!!!!!!!!
```

346 packets copied in 0.90 secs

```
firepower#
```

Esportare un'acquisizione su un server SCP:

<#root>

```
firepower#

copy /pcap capture:CAPI scp://scp_username:scp_password@192.168.78.55


Source capture name [CAPI]?

Address or name of remote host [192.168.78.55]?

Destination username [scp_username]?

Destination filename [CAPI]?
The authenticity of host '192.168.78.55 (192.168.78.55)' can't be established.
RSA key fingerprint is <cb:ca:9f:e9:3c:ef:e2:4f:20:f5:60:21:81:0a:85:f9:02:0d:0e:98:d0:9b:6c:dc:f9:af:4
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.78.55' (SHA256) to the list of known hosts.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
454 packets copied in 3.950 secs (151 packets/sec)
```

```
firepower#
```

Offload di acquisizioni da FTD. Al momento, quando è necessario scaricare le acquisizioni da FTD, il metodo più semplice è eseguire i seguenti passaggi:

1. Da Lina - copy /pcap capture:<nome_cap> disco0:

2. Dalla radice FPR - mv /ngfw/mnt/disk0/<nome_cap> /ngfw/var/common/

3. Dall'interfaccia utente di FMC - Sistema > Integrità > Monitor > Dispositivo > Risoluzione avanzata dei problemi e immettere il <cap_name> nel campo e scaricare.

Operazioni con le acquisizioni del motore LINA FTD - Traccia un pacchetto di traffico reale

Requisiti

Abilitare un'acquisizione su FTD con questi filtri:

IP di origine	192.168.103.1
IP di destinazione	192.168.101.1
Protocollo	ICMP
Interfaccia	INTERNO
Traccia pacchetti	sì
Numero di pacchetti di traccia	100

Eseguire il ping tra l'host A (192.168.103.1) e l'host B (192.168.101.1) e controllare le clip.

Soluzione

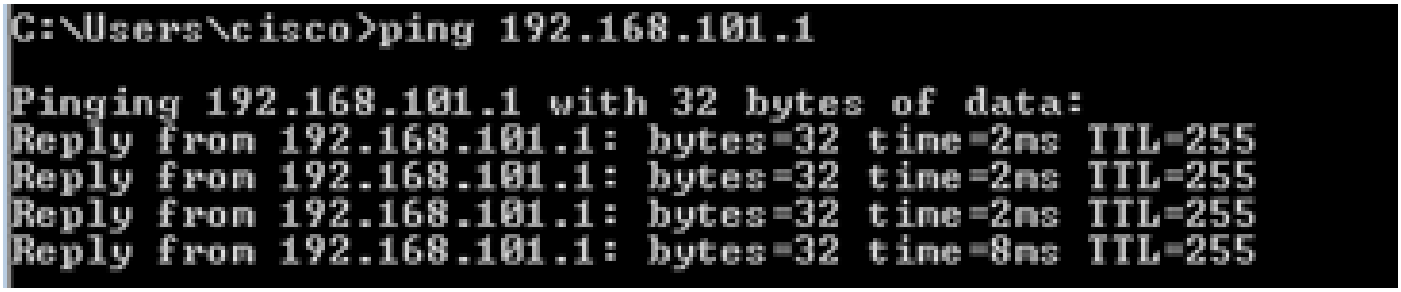
Tracciare un pacchetto reale è molto utile per risolvere i problemi di connettività. Permette di vedere tutti i controlli interni attraverso cui deve passare un pacchetto. Aggiungere le parole chiave trace detail e specificare il numero di pacchetti di cui si desidera eseguire la traccia. Per impostazione predefinita, l'FTD traccia i primi 50 pacchetti in entrata.

In questo caso, abilitare l'acquisizione con i dettagli di traccia per i primi 100 pacchetti ricevuti da FTD sull'interfaccia INSIDE:

<#root>

```
> capture CAPI2 interface INSIDE trace detail trace-count 100 match icmp host 192.168.103.1 host 192.168
```

Eseguire il ping tra l'host A e l'host B e verificare il risultato:



I pacchetti acquisiti sono:

<#root>

```
> show capture CAPI2

8 packets captured
   1: 18:08:04.232989  802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   2: 18:08:04.234622  802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
   3: 18:08:05.223941  802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   4: 18:08:05.224872  802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
   5: 18:08:06.222309  802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   6: 18:08:06.223148  802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
   7: 18:08:07.220752  802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   8: 18:08:07.221561  802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
8 packets shown
```

Questo output mostra una traccia del primo pacchetto. Le parti di interesse:

- La fase 12 è quella in cui si osserva il "flusso in avanti". Questo è l'array di invio del motore LINA (in pratica l'ordine interno delle operazioni).
- La fase 13 è la fase in cui il FTD invia il pacchetto all'istanza Snort.
- La fase 14 è quella in cui si parla del Verdetto Snort.

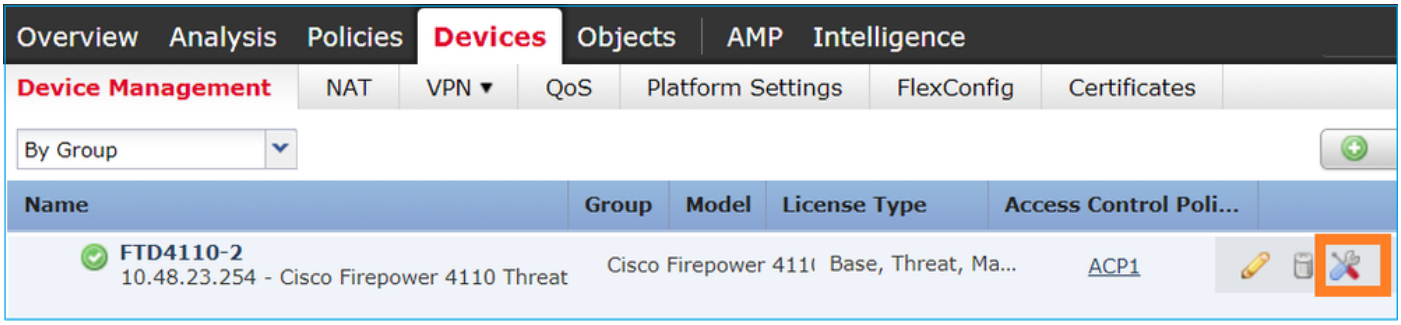
<#root>

```
> show capture CAPI2 packet-number 1 trace detail

8 packets captured
   1: 18:08:04.232989 000c.2998.3fec a89d.2193.2293 0x8100 Length: 78
      802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request (ttl 128, id 3346)
Phase: 1
```

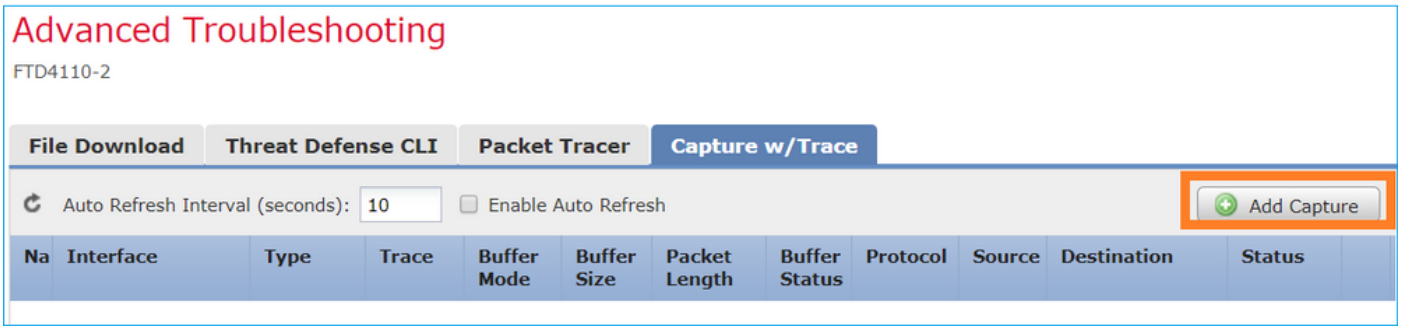
```
Type: CAPTURE
... output omitted ...

Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 195, packet dispatched to next module
Module information for forward flow ...

snp_fp_inspect_ip_options
snp_fp_snort
snp_fp_inspect_icmp
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat


Module information for reverse flow ...

snp_fp_inspect_ip_options
snp_fp_inspect_icmp
snp_fp_snort
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat



Phase: 13
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 14
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet


... output omitted ...

Result:
input-interface: OUTSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow

1 packet shown
>
```

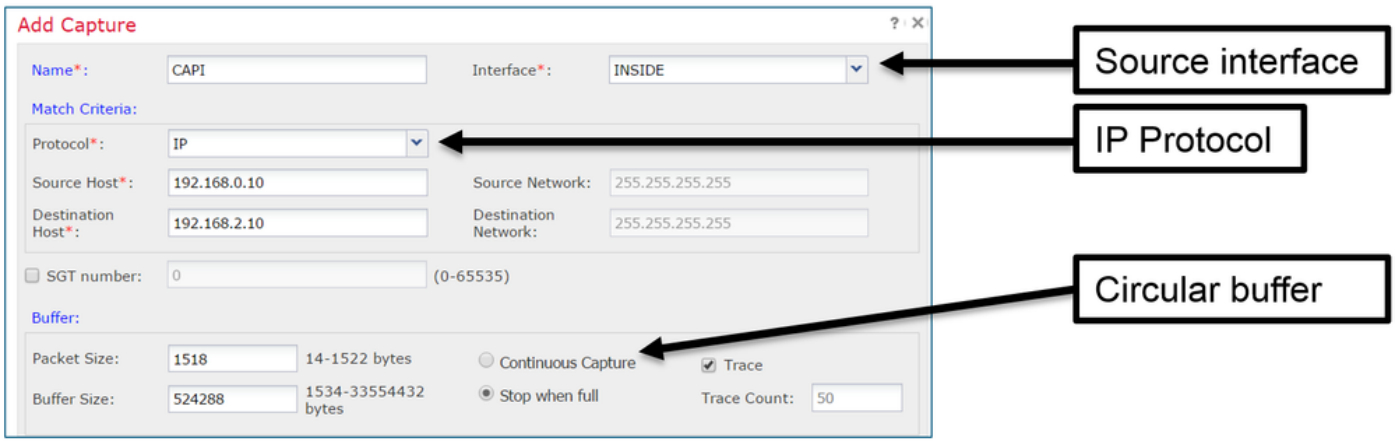
Strumento di acquisizione nelle versioni software FMC successive alla 6.2

In FMC versione 6.2.x è stata introdotta una nuova procedura guidata di acquisizione dei pacchetti. Passare a Dispositivi > Gestione dispositivi e fare clic sull'icona Risoluzione dei problemi. Quindi scegliere Advanced Troubleshooting e infine Capture w/Trace.



Scegliere Aggiungi acquisizione per creare un'acquisizione FTD:



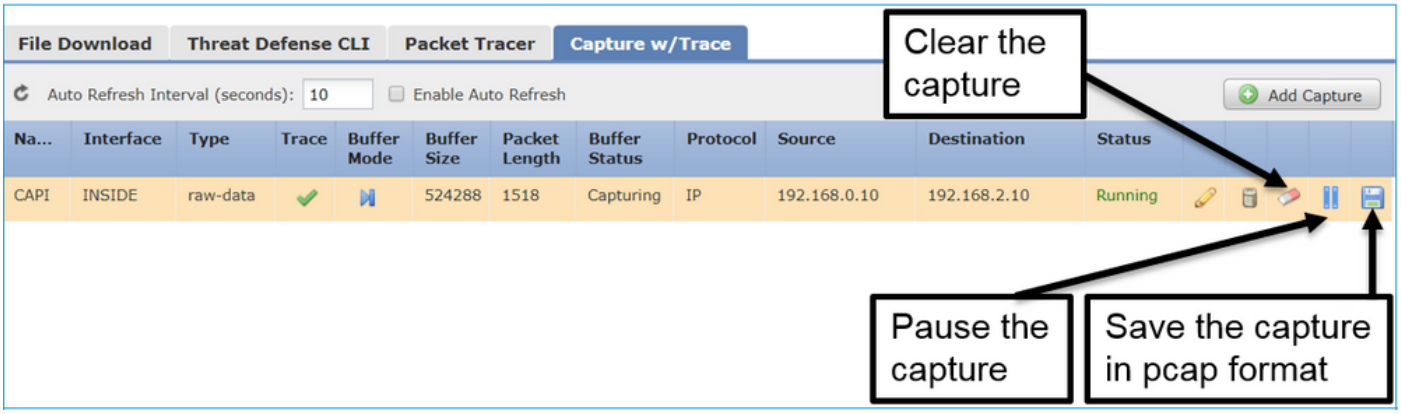


Le limitazioni correnti dell'interfaccia utente del FMC sono:

- Impossibile specificare le porte Src e Dst
- Corrispondenza consentita solo per i protocolli IP di base
- Impossibile abilitare l'acquisizione per le interruzioni ASP del motore LINA

Soluzione. Usare la CLI FTD

Quando si applica un'acquisizione dall'interfaccia utente di FMC, l'acquisizione viene eseguita:

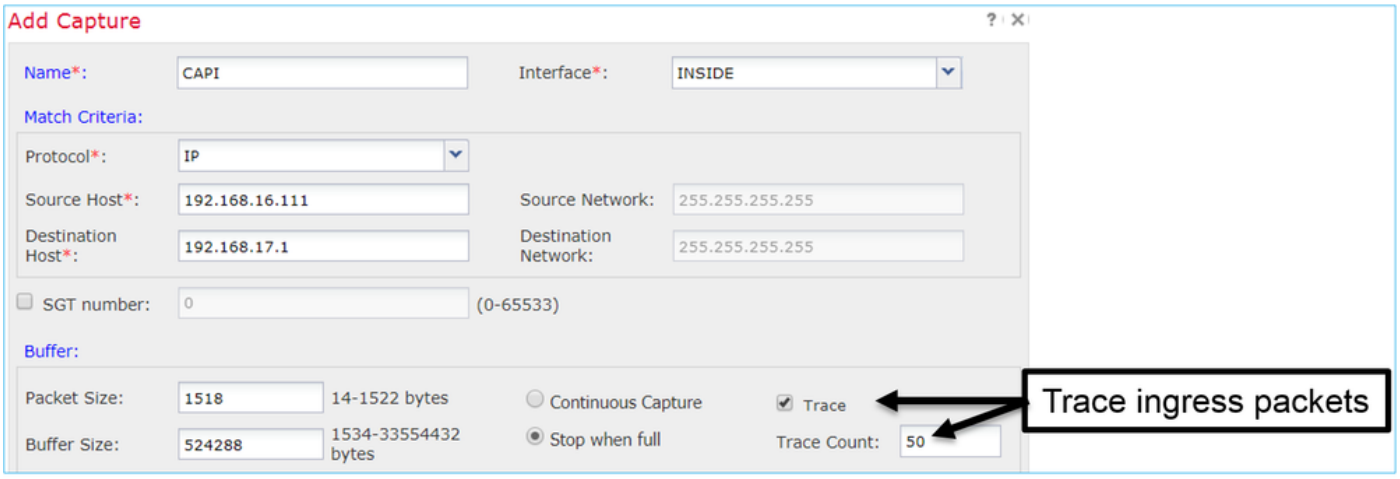


Acquisizione nella CLI FTD:

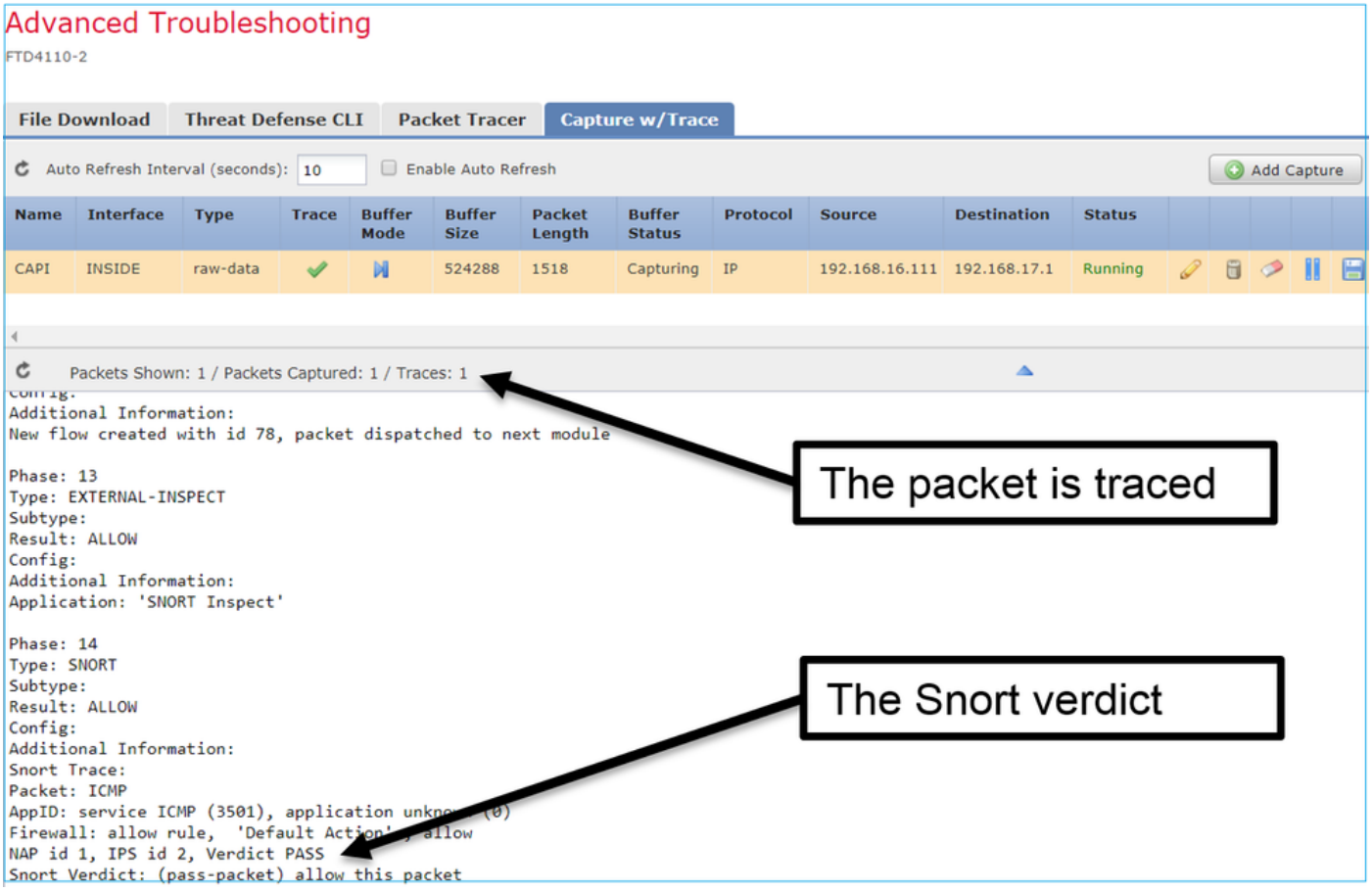
```
<#root>

> show capture

capture CAPI%intf=INSIDE% type raw-data trace interface INSIDE [Capturing - 0 bytes]
  match ip host 192.168.0.10 host 192.168.2.10
>
```

Traccia di un vero pacchetto su FMC post-6.2

In FMC 6.2.x, la procedura guidata Acquisizione con traccia consente di acquisire e tracciare pacchetti reali su FTD:



È possibile controllare il pacchetto tracciato nell'interfaccia utente di FMC:



Utility Packet Tracer FTD

Requisiti

Utilizzare l'utility Packet Tracer per questo flusso e verificare come il pacchetto viene gestito internamente:

Interfaccia in ingresso	INTERNO
Protocollo	Richiesta echo ICMP
IP di origine	192.168.103.1
IP di destinazione	192.168.101.1

Soluzione

Packet Tracer genera un pacchetto virtuale. Come mostrato nell'esempio, il pacchetto è soggetto a ispezione Snort. Un'acquisizione presa contemporaneamente a livello di script (capture-traffic) mostra la richiesta echo ICMP:

<#root>

> packet-tracer input INSIDE icmp 192.168.103.1 8 0 192.168.101.1

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.101.1 using egress ifc OUTSIDE

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip 192.168.103.0 255.255.255.0 192.168.101.0 255.255.255.0 rule
access-list CSM_FW_ACL_ remark rule-id 268436482: ACCESS POLICY: FTD5515 - Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 268436482: L4 RULE: Allow ICMP

Additional Information:
This packet is sent to snort for additional processing where a verdict is reached

... output omitted ...

Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 203, packet dispatched to next module

Phase: 13
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: ICMP

```
AppID: service ICMP (3501), application unknown (0)
Firewall: allow rule, id 268440225, allow
NAP id 2, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet


Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow

>
```

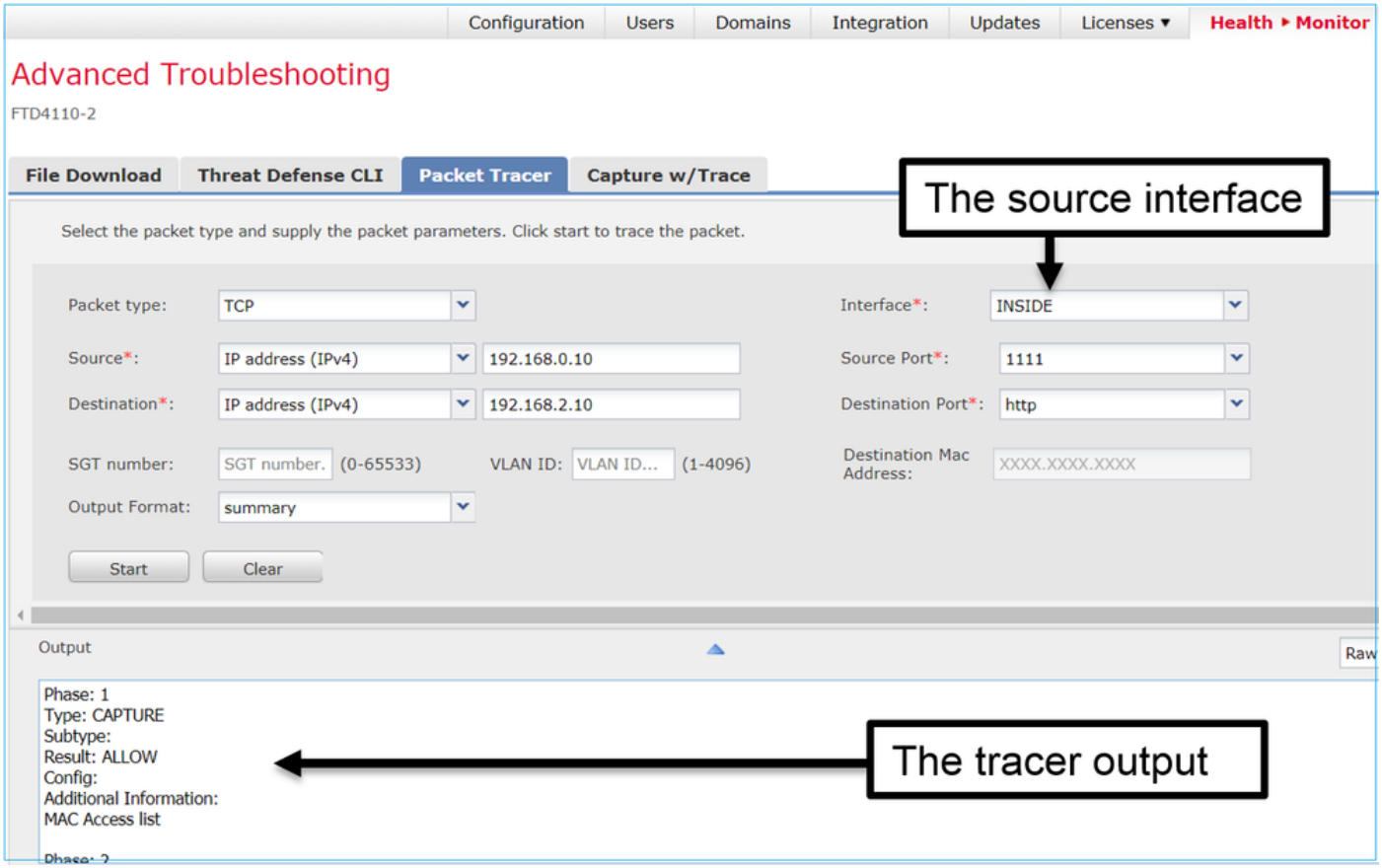
L'acquisizione a livello di script al momento del test packet-tracer mostra il pacchetto virtuale:

<#root>

```
>

capture-traffic


Please choose domain to capture traffic from:
  0 - management0
  1 - Router

Selection? 1

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:

-n
13:27:11.939755 IP 192.168.103.1 > 192.168.101.1: ICMP echo request, id 0, seq 0, length 8
```

Strumento di interfaccia utente di Packet Tracer nelle versioni software FMC successive alla 6.2

In FMC versione 6.2.x è stato introdotto lo strumento Packet Tracer UI. Lo strumento è accessibile allo stesso modo dello strumento di acquisizione e consente di eseguire Packet Tracer su FTD dall'interfaccia utente di FMC:



Informazioni correlate

- Guida di riferimento ai comandi di Firepower Threat Defense
- Note sulla versione di Firepower System, versione 6.1.0
- Guida alla configurazione di Cisco Firepower Threat Defense per Firepower Device Manager, versione 6.1
- Documentazione e supporto tecnico – Cisco Systems

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).