使用Firepower威脅防禦捕獲和Packet Tracer

目錄

簡介

本文說明如何使用Firepower威脅防禦(FTD)捕獲和Packet Tracer實用程式。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據以下軟體版本：

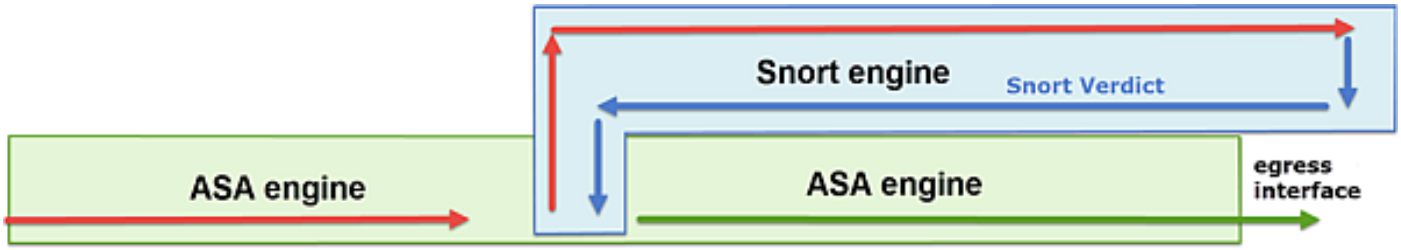
- 執行FTD軟體6.1.0的ASA5515-X
- 執行FTD軟體6.2.2的FPR4110
- 執行Firepower管理中心(FMC)軟體6.2.2的FS4000

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

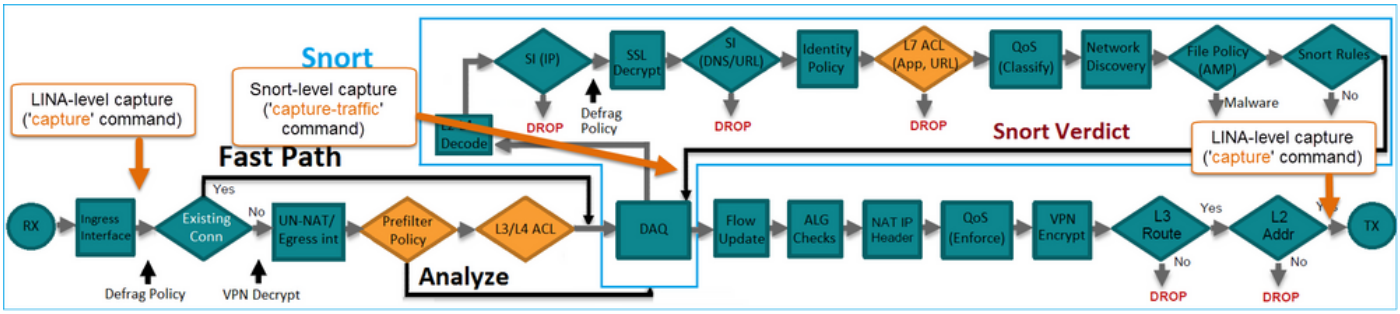
FTD封包處理

FTD封包處理視覺化，如下所示：



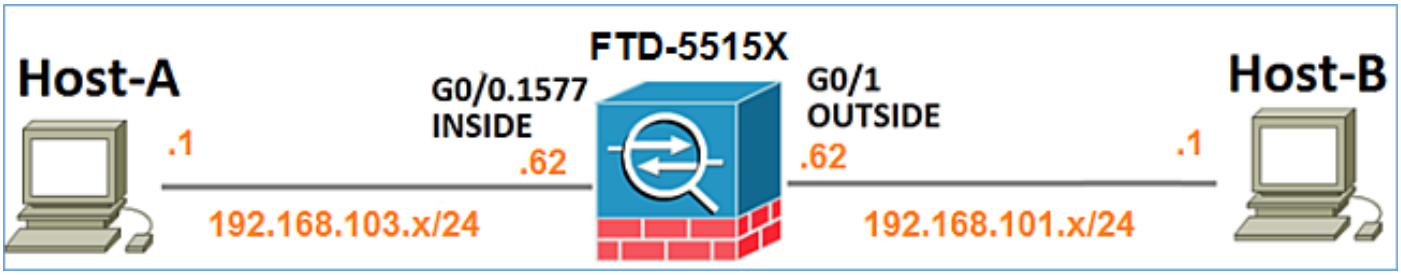
1. 封包進入輸入介面，並由LINA引擎處理。
2. 如果策略要求Snort引擎檢查資料包，
3. Snort引擎傳回封包的判定結果。
4. LINA 引擎根據 Snort 的判定結果捨棄或轉送封包.

根據架構，FTD擷取可位於以下位置：



設定

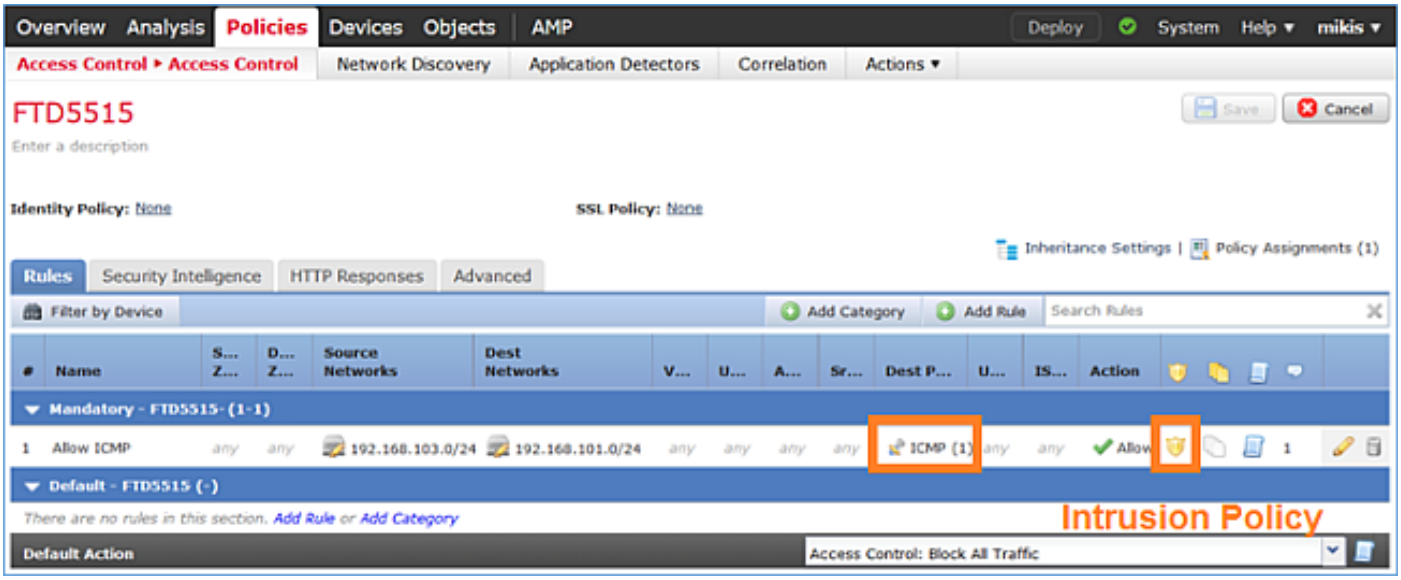
網路圖表



使用Snort引擎擷取

必要條件

FTD上應用了存取控制原則(ACP)，允許網際網路控制訊息通訊協定(ICMP)流量通過。該策略還應用了入侵策略：



需求

1. 在FTD CLISH模式下啟用擷取，而無需使用篩選條件。
2. 通過FTD Ping並檢查擷取的輸出。

解決方案

步驟 1.登入FTD主控台或SSH到br1介面，並在FTD CLISH模式下啟用擷取，而無需使用篩選條件。

<#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:
```

在FTD 6.0.x上，命令如下：

```
<#root>

>

system support

capture-traffic
```

步驟 2.透過FTD Ping並檢查擷取的輸出。

```
<#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
```

使用Snort引擎擷取

需求

1. 在FTD CLISH模式下使用IP 192.168.101.1的篩選條件啟用擷取。
2. 透過FTD Ping並檢查擷取的輸出。

解決方案

步驟 1.在FTD CLISH模式下使用IP 192.168.101.1的篩選條件啟用擷取。

```
<#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
```

步驟 2.透過FTD Ping並檢查擷取的輸出：

```
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
```

您可以使用-n選項以數字格式檢視主機和埠號。例如，較早的捕獲顯示為：

```
<#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
```

Tcpdump過濾器示例

範例 1：

若要擷取Src IP或Dst IP = 192.168.101.1和Src port或Dst port = TCP/UDP 23，請輸入以下命令：

```
<#root>

Options:

-n host 192.168.101.1 and port 23
```

範例 2：

若要擷取Src IP = 192.168.101.1和Src port = TCP/UDP 23，請輸入以下命令：

```
<#root>

Options:

-n src 192.168.101.1 and src port 23
```

範例 3:

若要擷取Src IP = 192.168.101.1和Src port = TCP 23，請輸入以下命令：

```
<#root>
```

```
Options:
-n src 192.168.101.1 and tcp and src port 23
```

範例 4:

若要擷取Src IP = 192.168.101.1並檢視封包的MAC位址，請新增「e」選項，然後輸入以下命令：

```
<#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
```

範例 5：

若要在擷取10個封包後退出，請輸入以下命令：

```
<#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
```

範例 6：

若要將擷取寫入名稱為capture.pcap的檔案，並透過FTP將其複製到遠端伺服器，請輸入以下命令：

```
<#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.


>
```

使用FTD LINA引擎擷取

需求

1.使用以下過濾器在FTD上啟用兩個擷取：

來源 IP	192.168.103.1
目的地 IP	192.168.101.1
通訊協定	ICMP
介面	INSIDE
來源 IP	192.168.103.1
目的地 IP	192.168.101.1
通訊協定	ICMP
介面	OUTSIDE

2.從主機A(192.168.103.1)對主機B(192.168.101.1)執行Ping並檢查捕獲。

解決方案

步驟 1.啟用捕獲：

<#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
```

步驟 2.在CLI中檢查捕獲。

從主機A ping主機B:

```
C:\Users\cisco>ping 192.168.101.1

Pinging 192.168.101.1 with 32 bytes of data:
Reply from 192.168.101.1: bytes=32 time=4ms TTL=255
Reply from 192.168.101.1: bytes=32 time=5ms TTL=255
Reply from 192.168.101.1: bytes=32 time=1ms TTL=255
Reply from 192.168.101.1: bytes=32 time=1ms TTL=255
```

<#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
```

由於INSIDE介面上的Dot1Q報頭，兩個捕獲具有不同的大小，如以下輸出示例所示：

<#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
```

使用FTD LINA引擎擷取 — 透過HTTP匯出擷取

需求

使用瀏覽器匯出先前場景中獲取的捕獲。

解決方案

若要使用瀏覽器匯出擷取，您需要：

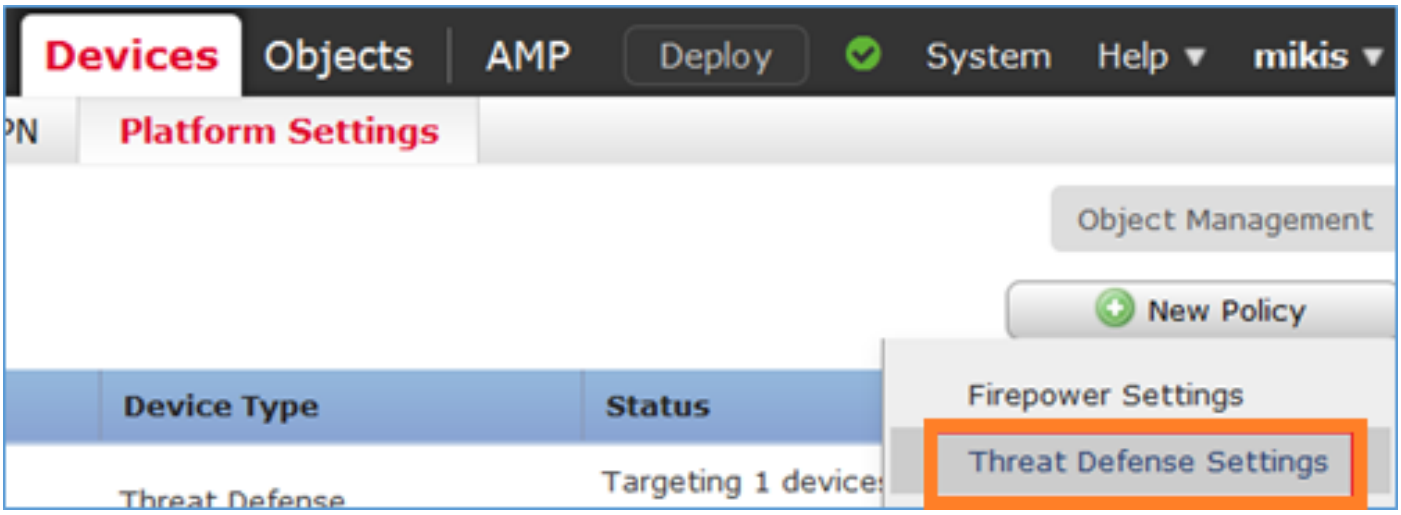
1. 啟用HTTPS伺服器
2. 允許HTTPS訪問

預設情況下，HTTPS伺服器會停用，且不允許存取：

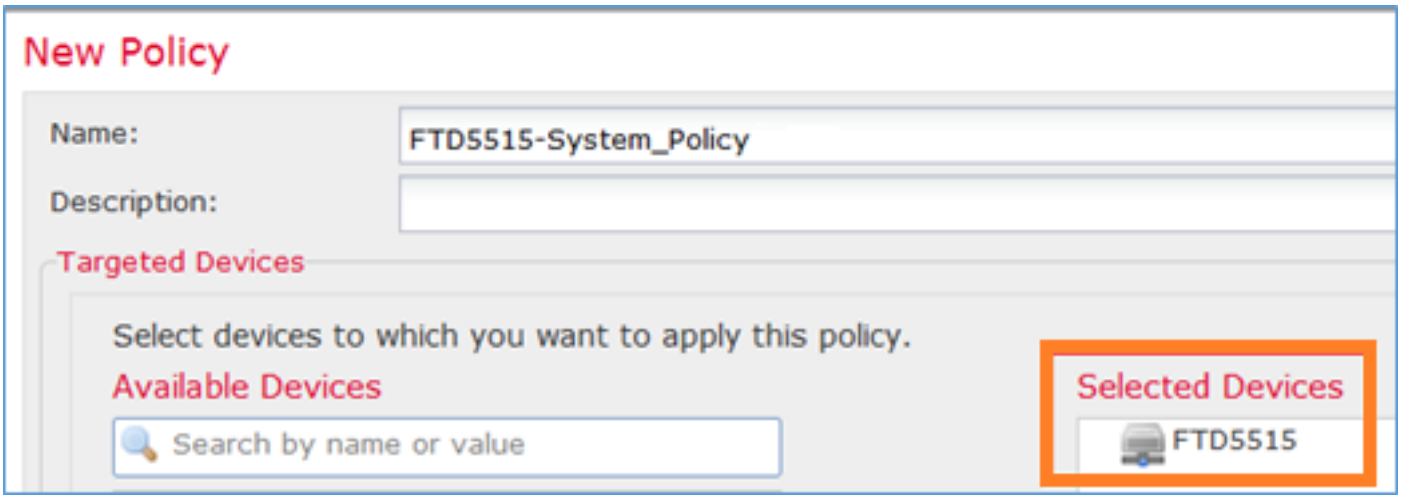
<#root>

```
>

show running-config http


>
```

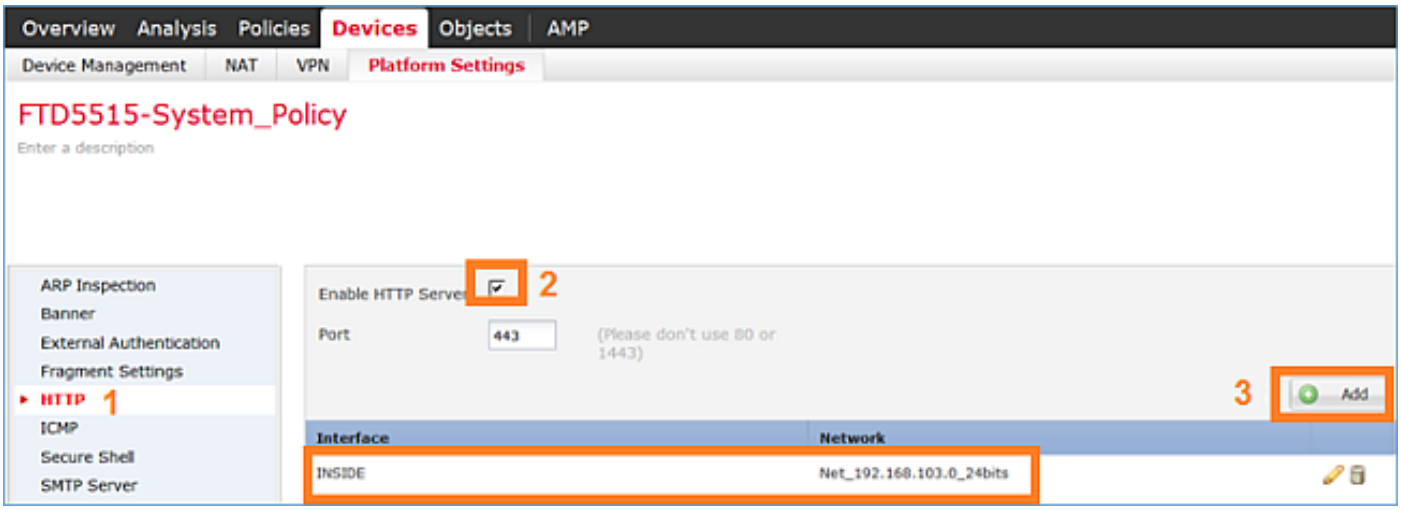
步驟 1.導覽至Devices > Platform Settings，按一下New Policy，然後選擇Threat Defense Settings:



指定策略名稱和裝置目標：



步驟 2.啟用HTTPS伺服器並新增要允許透過HTTPS存取FTD裝置的網路：



儲存和部署。

在策略部署時，可以啟用debug http以檢視HTTP服務的啟動：

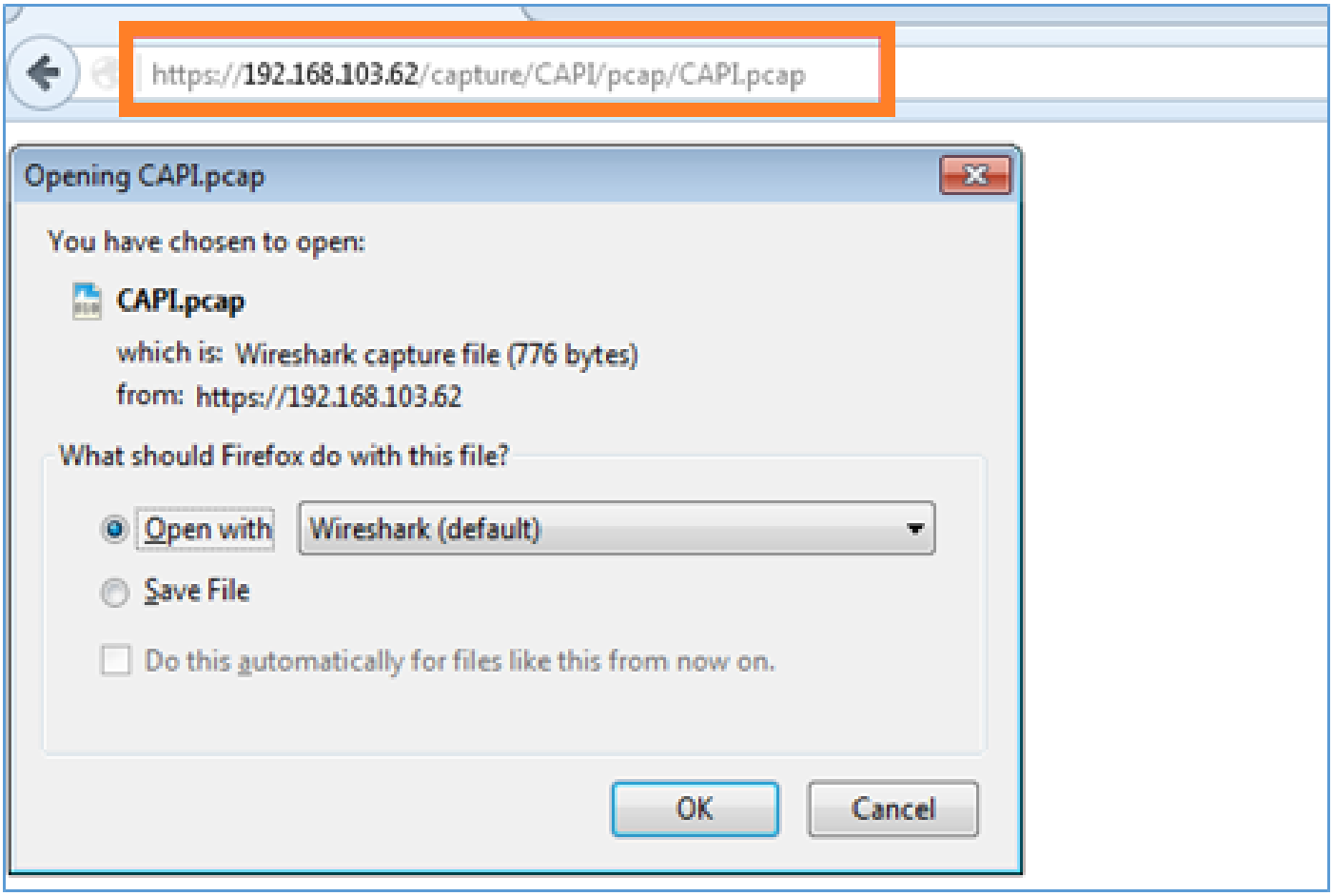
<#root>

```
> debug http 255

debug http enabled at level 255.

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

FTD CLI上的結果為：

```
<#root>

> unebug all

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

在主機A(192.168.103.1)上開啟瀏覽器並使用此URL下載第一個擷取：https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap。

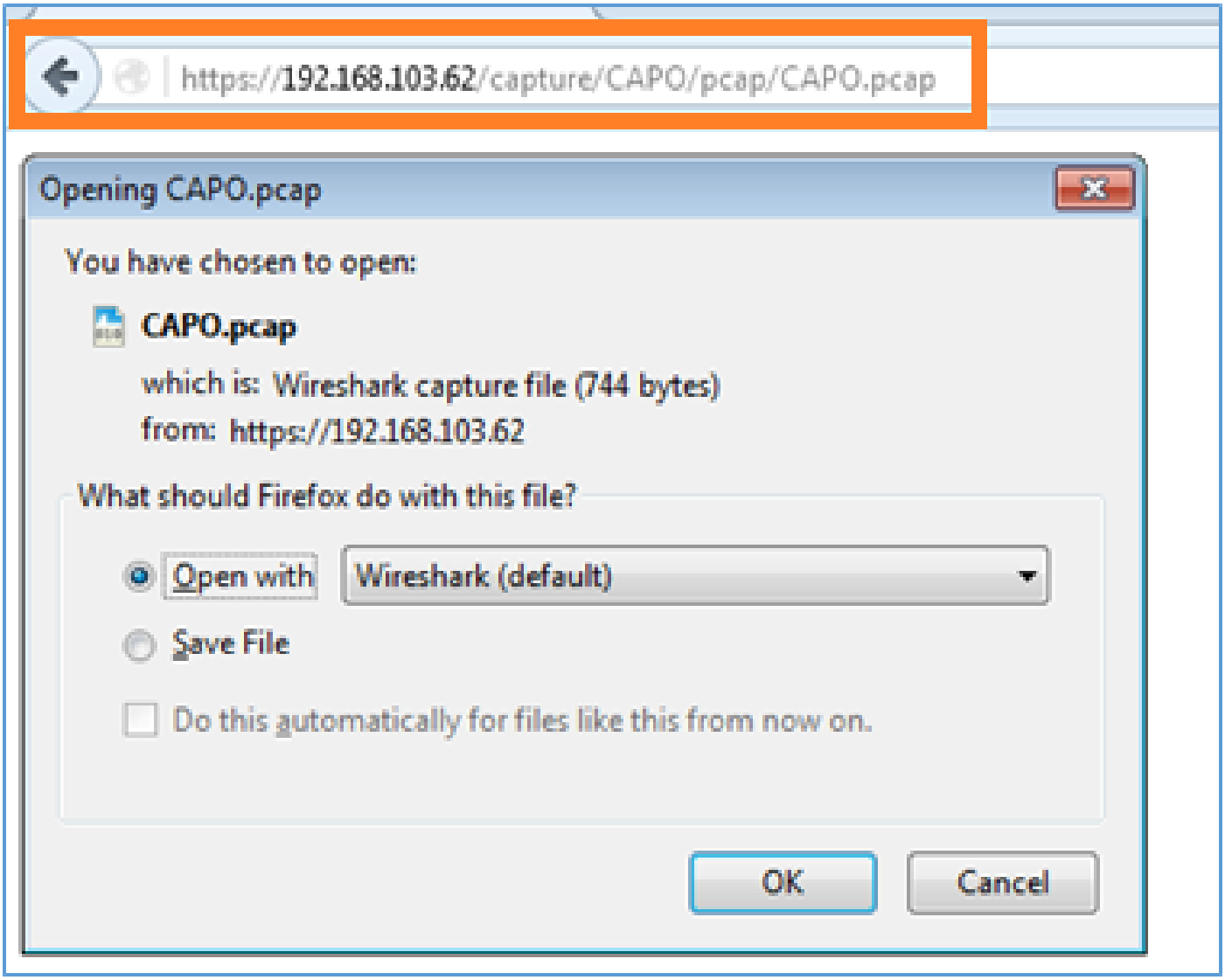


供參考：

https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	已啟用HTTP伺服器的FTD資料介面

	的IP
https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	FTD擷取的名稱
https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	下載的檔案的名稱

對於第二次捕獲，請使用https://192.168.103.62/capture/CAPO/pcap/CAPO.pcap。



使用FTD LINA引擎擷取 — 透過FTP/TFTP/SCP匯出擷取

需求

使用FTP/TFTP/SCP協定匯出先前場景中獲取的捕獲。

解決方案

將擷取匯出至FTP伺服器：

<#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#

將擷取匯出至TFTP伺服器：

<#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#

將捕獲匯出到SCP伺服器：

<#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#
```

從FTD中解除安裝擷取。 目前，當您需要從FTD解除安裝擷取時，最簡單的方法是執行以下步驟：

1.在Lina中 — copy /pcap capture:<cap_name> disk0:

2.從FPR root - mv /ngfw/mnt/disk0/<cap_name> /ngfw/var/common/

3.在FMC UI - System > Health > Monitor > Device > Advanced Troubleshooting中，輸入<cap_name>欄位並下載。

使用FTD LINA引擎擷取 — 追蹤實際流量封包

需求

使用以下過濾器在FTD上啟用擷取：

來源 IP	192.168.103.1
目的地 IP	192.168.101.1
通訊協定	ICMP
介面	INSIDE
封包追蹤	是
跟蹤資料包數	100

從主機A(192.168.103.1)主機B(192.168.101.1)執行Ping並檢查捕獲。

解決方案

跟蹤實際資料包對於排除連線問題非常有用。它允許您檢視資料包經過的所有內部檢查。新增trace detail關鍵字並指定要跟蹤的資料包數。預設情況下，FTD會追蹤前50個輸入封包。

在這種情況下，為FTD在INSIDE介面上接收的前100個封包啟用含有追蹤詳細資訊的擷取：

<#root>

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

從主機A ping主機B，並檢查結果：

```
C:\Users\cisco>ping 192.168.101.1

Pinging 192.168.101.1 with 32 bytes of data:
Reply from 192.168.101.1: bytes=32 time=2ms TTL=255
Reply from 192.168.101.1: bytes=32 time=2ms TTL=255
Reply from 192.168.101.1: bytes=32 time=2ms TTL=255
Reply from 192.168.101.1: bytes=32 time=8ms TTL=255
```

捕獲的資料包為：

<#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
```

此輸出顯示第一個封包的追蹤軌跡。感興趣的部分：

- 在第12階段，可以看到「正向流」。這是LINA引擎派遣陣列（實際上為內部操作順序）。
- 第13階段是FTD將封包傳送到Snort執行個體的地方。
- 第14階段是看到Snort裁決的地方。

<#root>

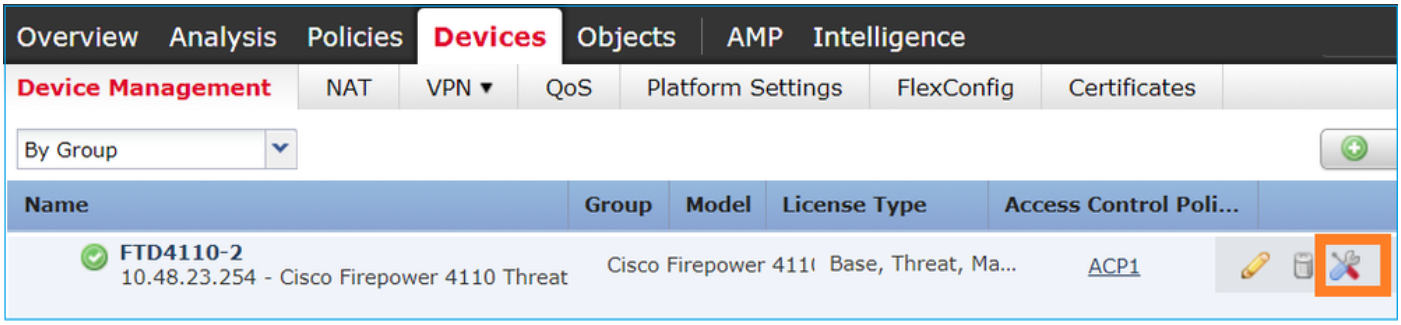
```
> show capture CAPI2 packet-number 1 trace detail
```

```
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
```

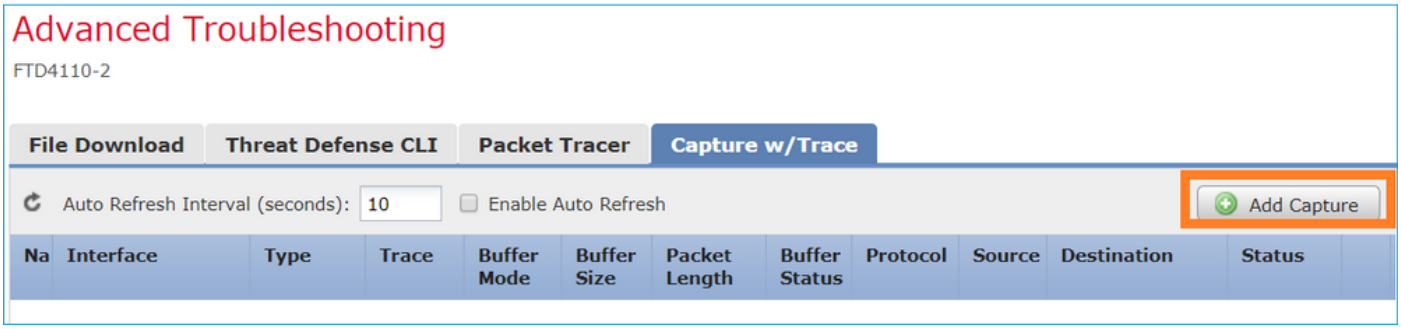
>

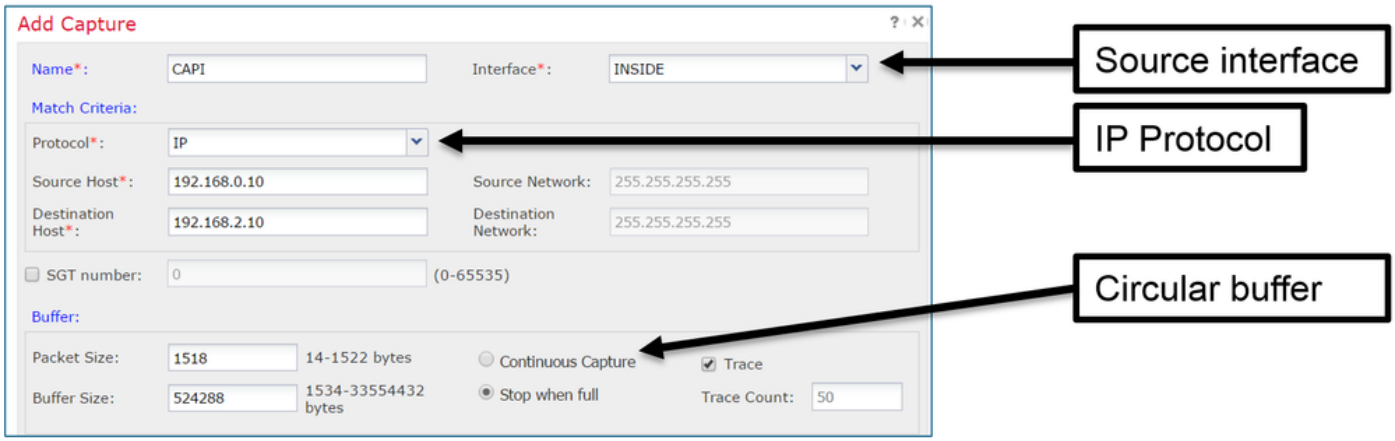
6.2後FMC軟體版本中的捕獲工具

在FMC 6.2.x版中，引入了新的資料包捕獲嚮導。導覽至Devices > Device Management，然後點選Troubleshoot圖示。然後選擇Advanced Troubleshooting，最後選擇Capture w/Trace。



選擇Add Capture以建立FTD捕獲：



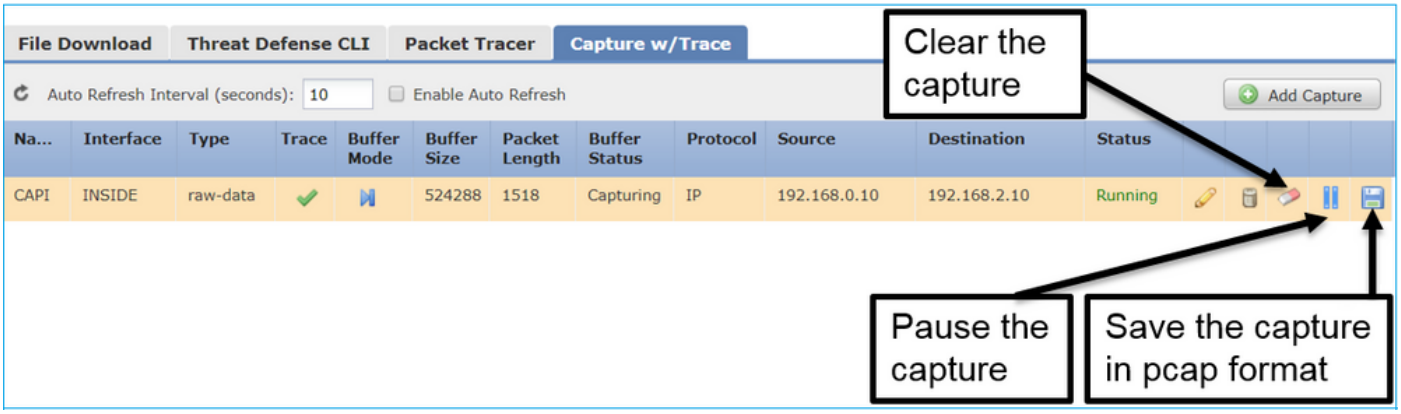


當前FMC UI限制如下：

- 無法指定Src和Dst埠
- 只能匹配基本IP協定
- 無法為LINA引擎ASP丟棄啟用捕獲

因應措施 — 使用FTD CLI

從FMC UI應用捕獲後，捕獲會運行：



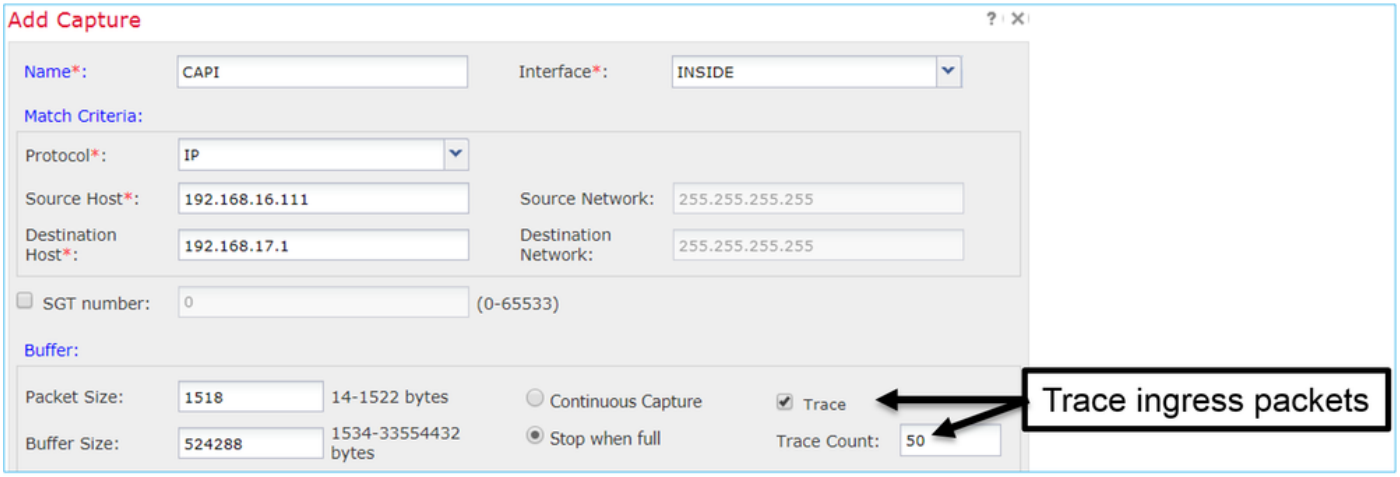
FTD CLI上的擷取：

<#root>

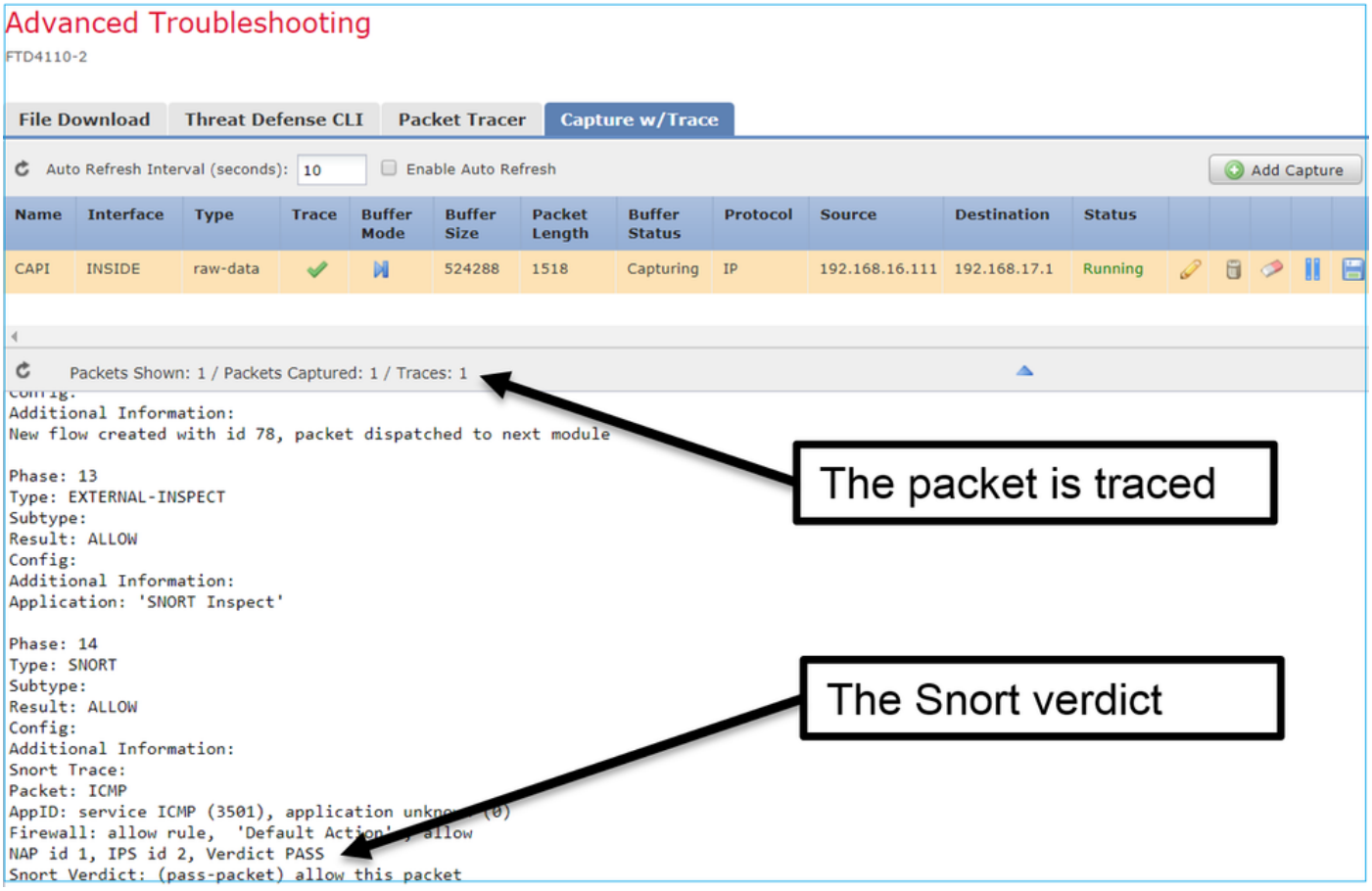
```
> show capture

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
>
```

在6.2之後FMC上跟蹤實際資料包

在FMC 6.2.x上，Capture w/Trace嚮導允許您在FTD上捕獲和跟蹤實際資料包：



您可以在FMC UI中檢查跟蹤的資料包：



FTD Packet Tracer實用程式

需求

使用Packet Tracer實用程式處理此流，並檢查資料包的內部處理方式：

輸入介面	INSIDE
通訊協定	ICMP回應請求
來源 IP	192.168.103.1
目的地 IP	192.168.101.1

解決方案

Packet Tracer生成虛擬資料包。如本例所示，資料包接受Snort檢測。在Snort層級同時進行的擷取(capture-traffic)顯示ICMP回應要求：

<#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
```

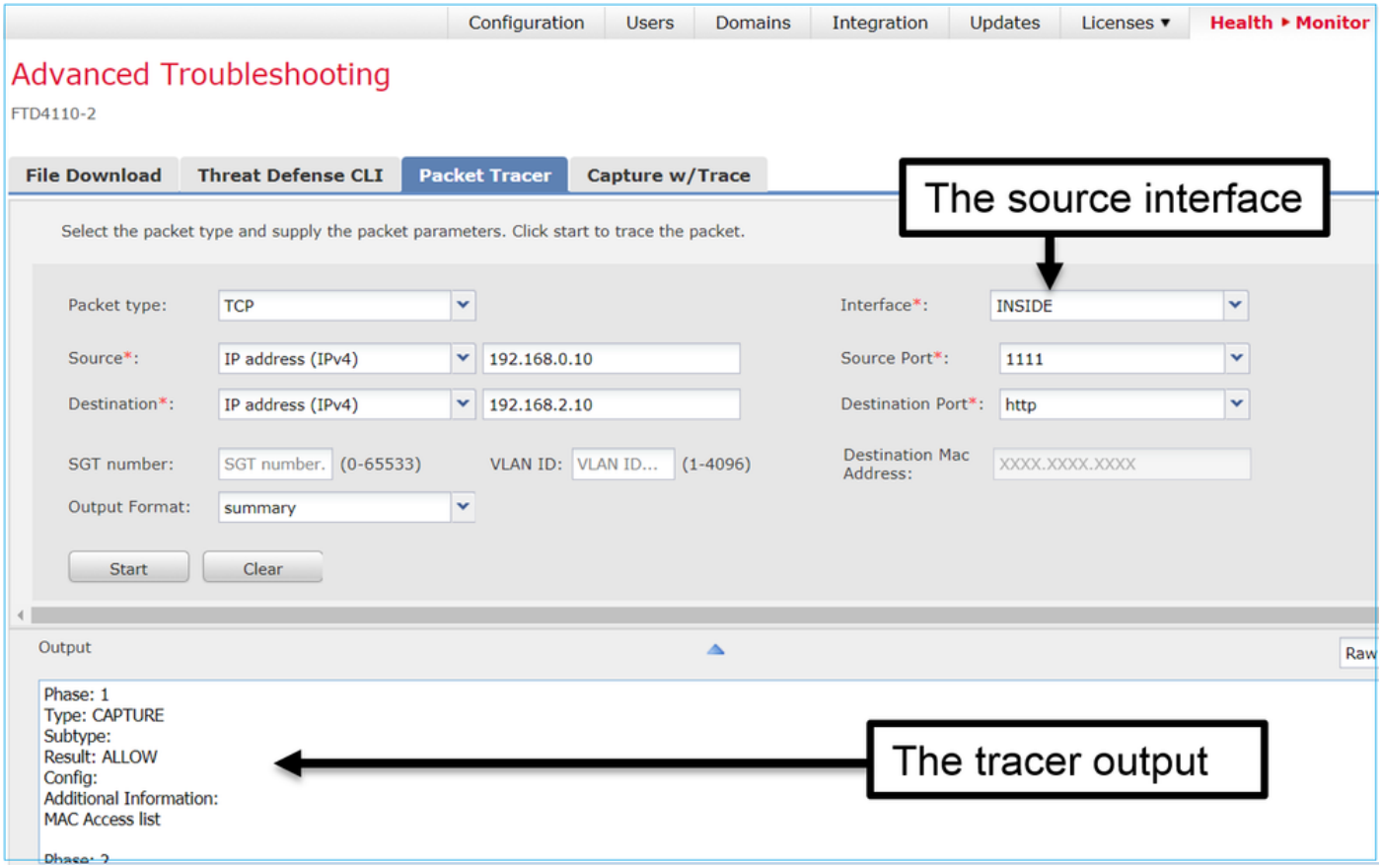
```
Snort Verdict: (pass-packet) allow this packet


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

>
```

Packet Tracer測試時的Snort級捕獲顯示虛擬資料包：

```
<#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
```

6.2後FMC軟體版本中的Packet Tracer UI工具

在FMC 6.2.x版中引入了Packet Tracer UI工具。該工具與擷取工具可相同方式存取，並允許您在FTD上從FMC UI執行Packet Tracer:



相關資訊

- [Firepower威脅防禦命令參考指南]
- [Firepower 系統版本資訊，6.1.0 版本]
- [適用於 Firepower 裝置管理員 6.1 版的 Cisco Firepower 威脅防禦設定指南]
- [技術支援與文件 - Cisco Systems]

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。