إستخدام التقاط الدفاع عن تهديد FirePOWER وتتبع الحزم

المحتويات

المقدمة

يوضح هذا المستند كيفية إستخدام لقطات "الدفاع عن تهديد FirePOWER (FTD)" والأدوات المساعدة لتتبع الحزم.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

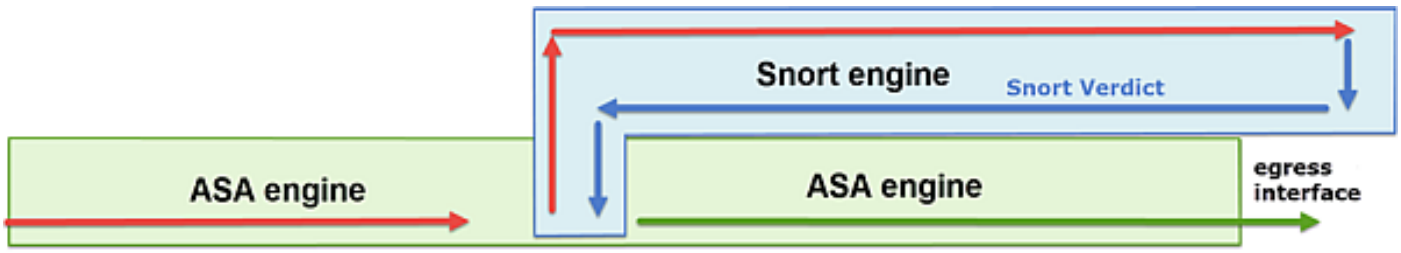
- ASA5515-X الذي يعمل ببرنامج FTD 6.1.0
- FPR4110 الذي يشغل برنامج FTD 6.2.2
- FS4000 التي تعمل ببرنامج مركز إدارة FirePOWER (FMC) 6.2.2

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

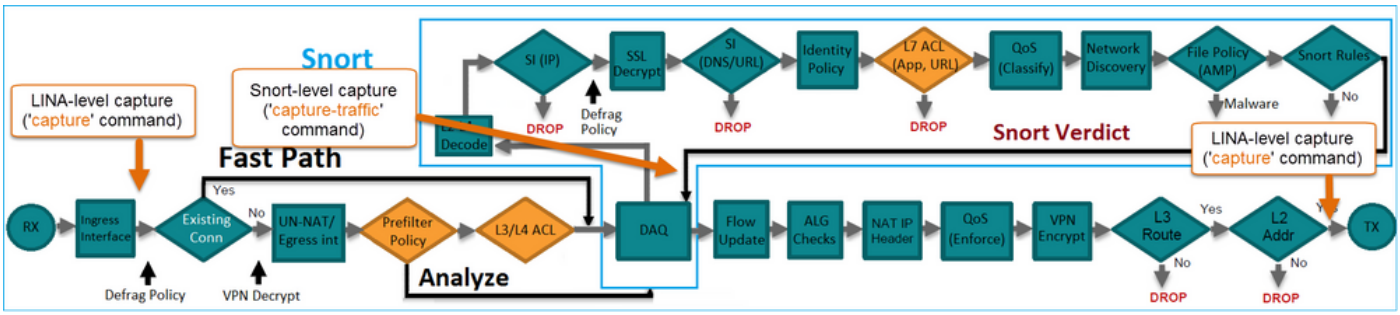
معالجة حزمة FTD

يتم عرض معالجة حزمة FTD كما يلي:



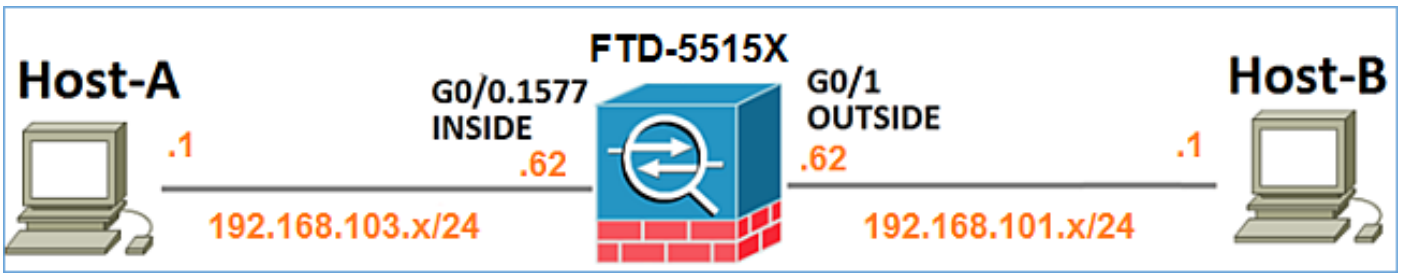
1. يدخل ربط المدخل قارن، ويعالج ب ال LINA محرك.
2. إذا كان النهج يتطلب فحص الحزمة بواسطة محرك الشخير.
3. يرجع محرك الشخير حكما للحزمة.
4. يقوم محرك LINA بإسقاط الحزمة أو إعادة توجيهها بناءً على قرار Snort.

استنادا إلى البنية المعمارية، يمكن التقاط FTD في هذه الأماكن:



التكوين

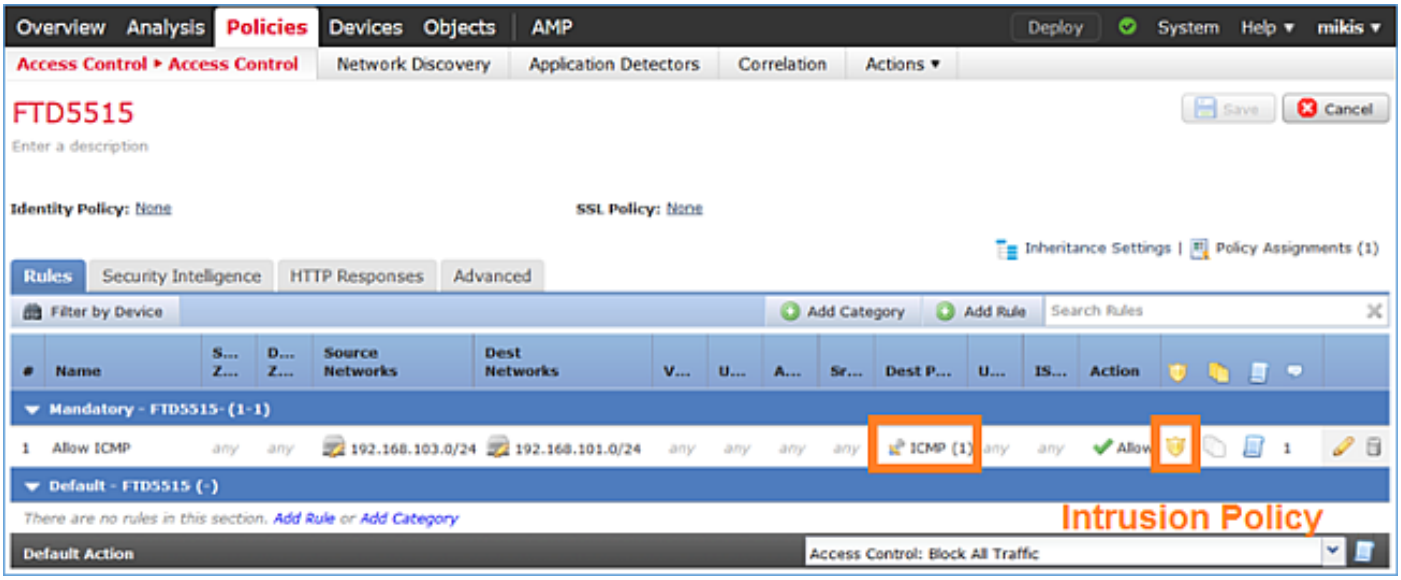
الرسم التخطيطي للشبكة



العمل باستخدام التقاط محرك الشخير

المتطلبات الأساسية

هناك سياسة التحكم في الوصول (ACP) مطبقة على FTD التي تسمح لحركة مرور بروتوكول رسائل التحكم في الإنترنت (ICMP) بالمرور. ويتم تطبيق هذه السياسة أيضا على نهج التطفل:



المتطلبات

1. تمكين الالتقاط على وضع CLISH ل FTD بدون عامل تصفية.
2. إختبار الاتصال من خلال FTD والتحقق من المخرجات الملتقطة.

الحل

الخطوة 1. قم بتسجيل الدخول إلى وحدة تحكم FTD أو SSH إلى واجهة BR1 وتمكين الالتقاط على وضع CLISH ل FTD بدون عامل تصفية.

```
<#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:
```

في FTD 6.0.x الأمر:

```
<#root>

>

system support

capture-traffic
```

الخطوة 2. إختبار الاتصال من خلال FTD والتحقق من الإخراج الملتقط.

```
<#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
```

العمل باستخدام التقاط محرك الشخير

المتطلبات

1. قم بتمكين التقاط على وضع CLISH ل FTD باستخدام عامل تصفية ل IP 192.168.101.1.
2. إختبار الاتصال من خلال FTD والتحقق من الإخراج الملتقط.

الحل

الخطوة 1. قم بتمكين التقاط على وضع CLISH ل FTD باستخدام عامل تصفية ل 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
```

الخطوة 2. إختبار الاتصال من خلال FTD والتحقق من المخرجات الملتقطة:

```
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
```

يمكنك إستخدام خيار N لرؤية المضيف وأرقام المنافذ بتنسيق رقمي. على سبيل المثال، يتم عرض الالتقاط السابق على النحو التالي:

```
<#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
```

أمثلة عامل تصفية TCPDUMP

مثال 1:

دخلت in order to عل قبض src ip أو dst ip = 192.168.101.1 و src عنوان أو dst عنوان = TCP/UDP و port = 23، هذا أمر:

```
<#root>

Options:

-n host 192.168.101.1 and port 23
```

مثال 2:

دخلت in order to على قبض src ip = 192.168.101.1 ومنفذ src = TCP/UDP 23، هذه أمر:

<#root>

Options:

-n src 192.168.101.1 and src port 23

المثال 3:

دخلت in order to على قبض src ip = 192.168.101.1 ومنفذ src = TCP 23، هذه أمر:

<#root>

Options:

-n src 192.168.101.1 and tcp and src port 23

مثال 4:

أضفت in order to على قبض src ip = 192.168.101.1 وراجع ال MAC عنوان من الربط الخيار 'e'، وأدخل هذه أمر:

<#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
```

مثال 5:

دخلت in order to خرجت بعد أن على قبض أنت 10 ربط، هذه أمر:

<#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
```

مثال 6:

دخلت in order to كتبت التقاط إلى مبرد مع الإسم capture.pcap ونسخه من خلال FTP إلى لدان بعيد، هذه أمر:

```
<#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.


>
```

العمل باستخدام التقاط محرك FTD LINA

المتطلبات

1. تمكين إلتقطين على FTD باستخدام عوامل التصفية التالية:

IP المصدر	192.168.103.1
IP الوجهة	192.168.101.1
البروتوكول	ICMP
الواجهة	دخل

IP المصدر	192.168.103.1
IP الوجهة	192.168.101.1
البروتوكول	ICMP
الواجهة	خارج

2. إختبار الاتصال من المضيف-A (192.168.103.1) إلى المضيف-B (192.168.101.1) والتحقق من إلتقاطات.

الحل

الخطوة 1. تمكين الالتقاط:

<#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
```

الخطوة 2. تحقق من التقاط واجهة سطر الأوامر (CLI).

إختبار الاتصال من المضيف-A إلى المضيف-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
```

يحتوي التقطيفان على أحجام مختلفة بسبب رأس Dot1Q على الواجهة الداخلية، كما هو موضح في مثال الإخراج هذا:

```
<#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
```

العمل باستخدام التقاط محرك FTD LINA - تصدير التقاط عبر HTTP

المتطلبات

تصدير االلتقاطات التي تم التقاطها في السيناريو السابق باستخدام مستعرض.

الحل

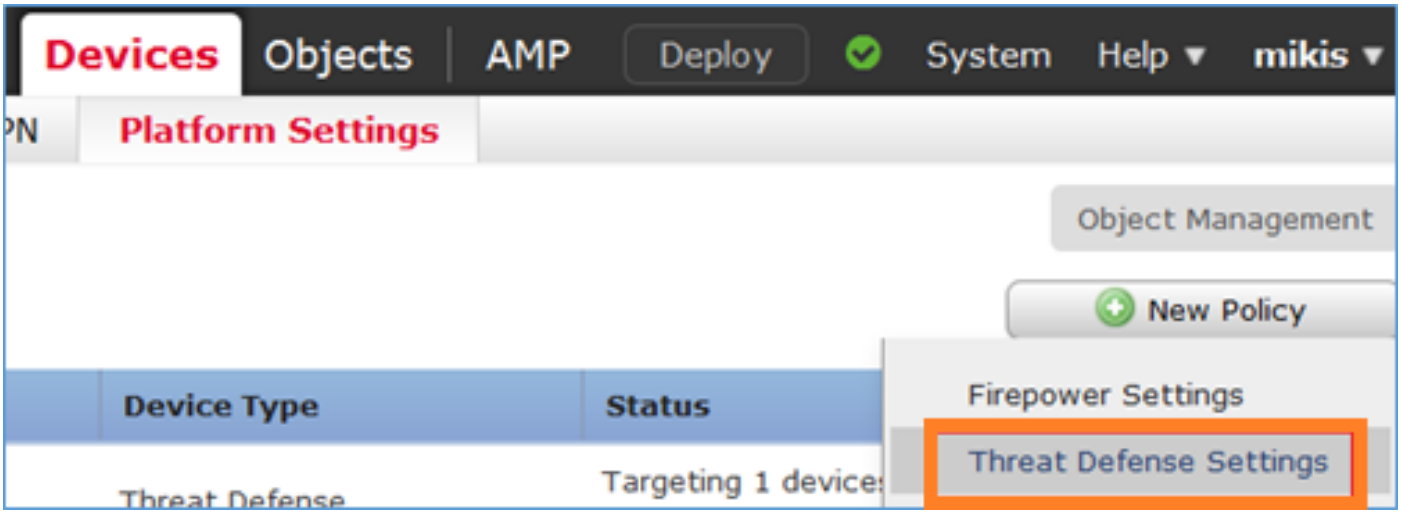
لتصدير االلتقاط باستخدام متصفح، تحتاج إلى:

1. تمكين خادم HTTPS
2. السماح بالوصول إلى HTTPS

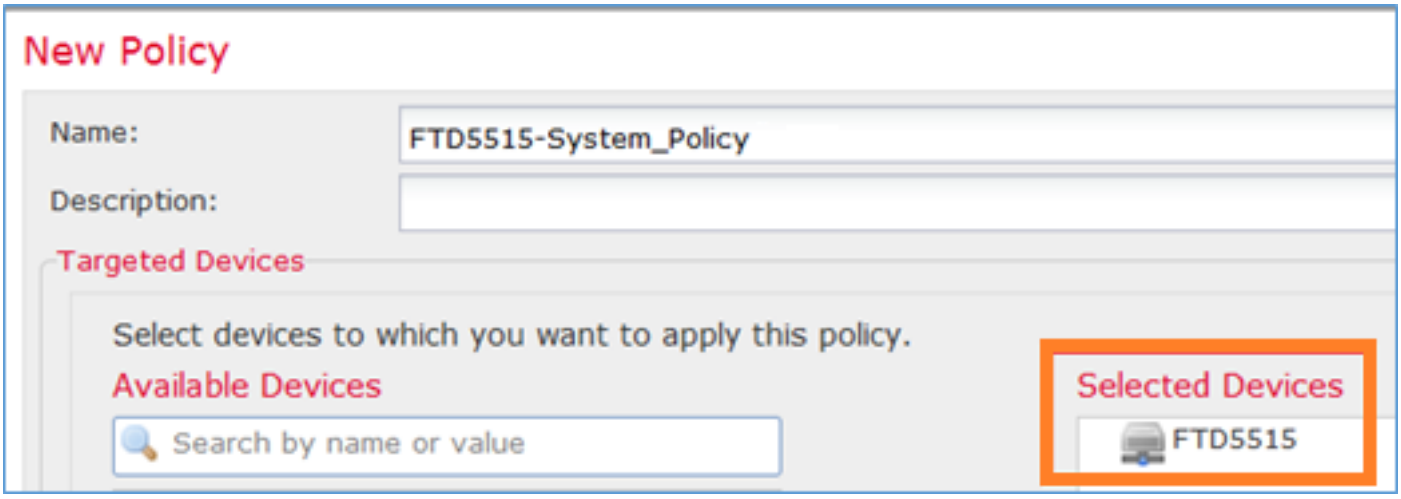
بشكل افتراضي، يتم تعطيل خادم HTTPS، ولا يتم السماح بالوصول:

```
<#root>

>

show running-config http


>
```

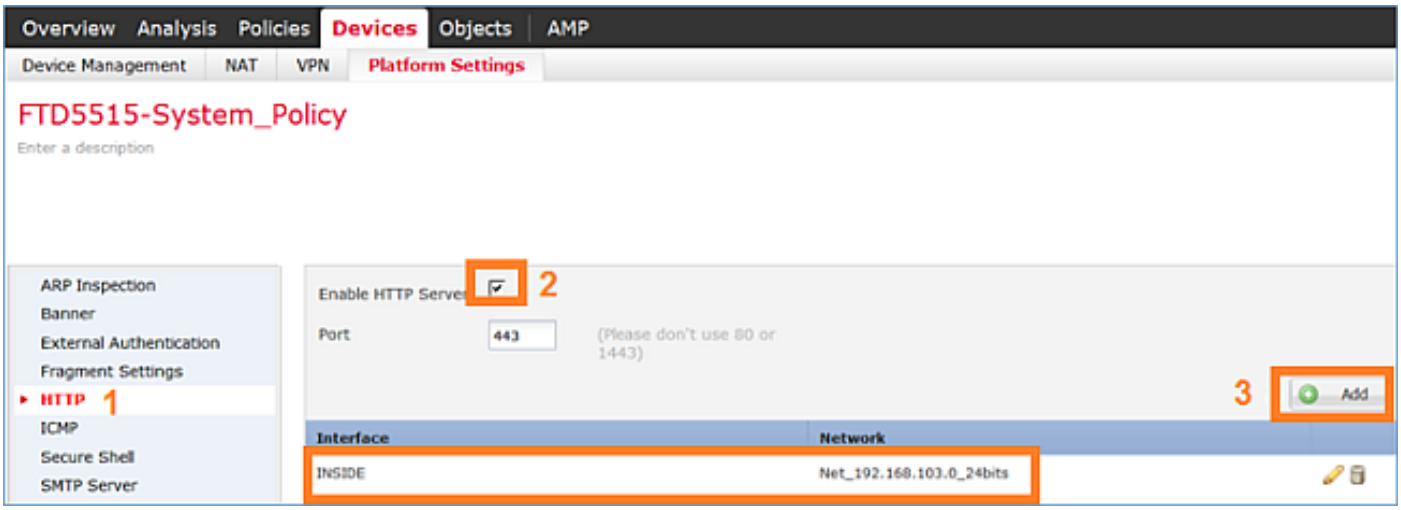
الخطوة 1. انتقل إلى الأجهزة > إعدادات النظام الأساسي، وانقر نهج جديد، واختر إعدادات الدفاع عن التهديد:



حدد اسم النهج وهدف الجهاز:



الخطوة 2. قم بتمكين خادم HTTPS وأضف الشبكة التي تريد السماح لك بالوصول إلى جهاز FTD عبر HTTPS:



حفظ ونشر.

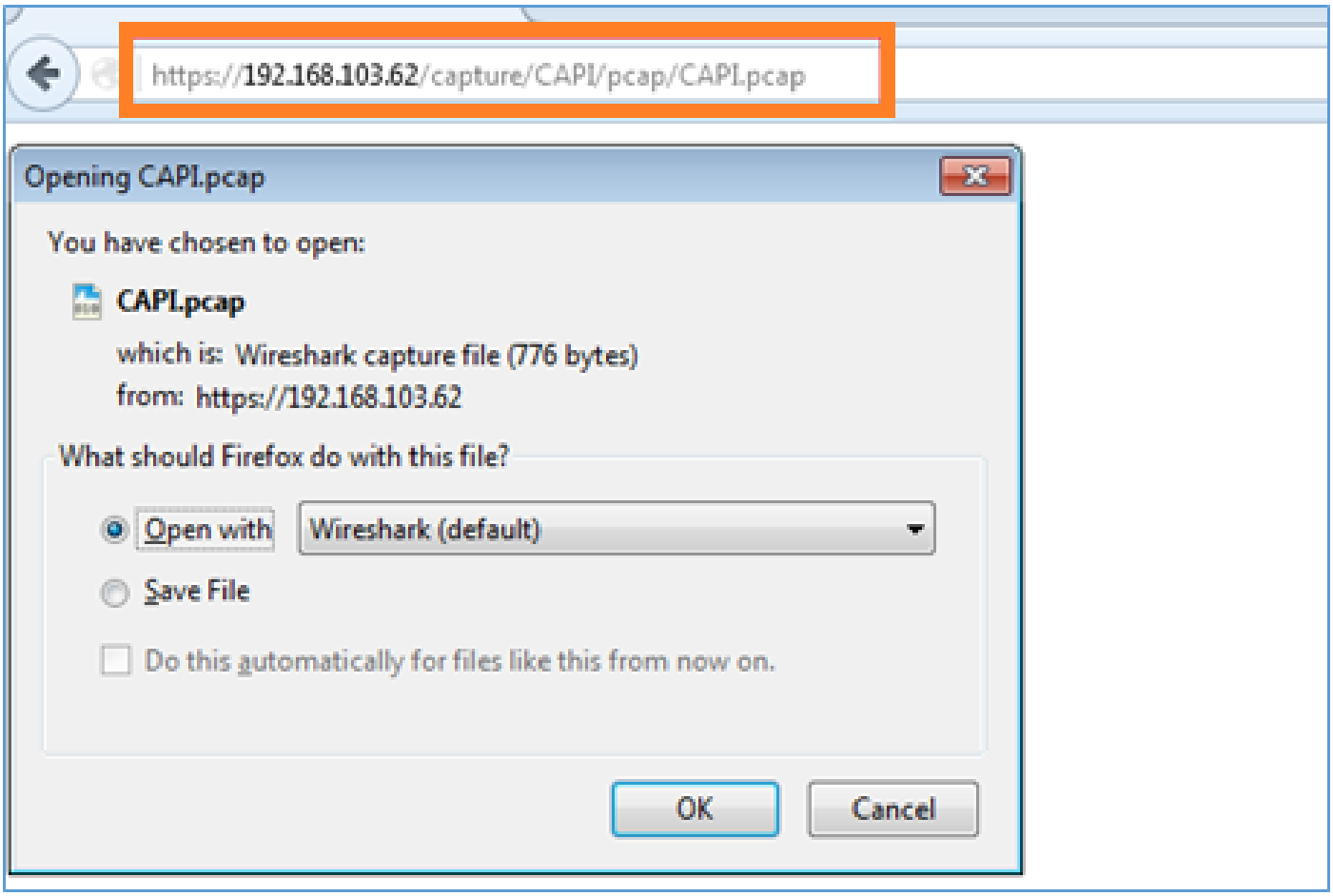
في وقت نشر النهج، يمكنك تمكين debug http لعرض بداية خدمة HTTP:

```
<#root>

> debug http 255

debug http enabled at level 255.

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

النتيجة على واجهة سطر الأوامر (CLI) ل FTD هي:

```
<#root>

> unebug all

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

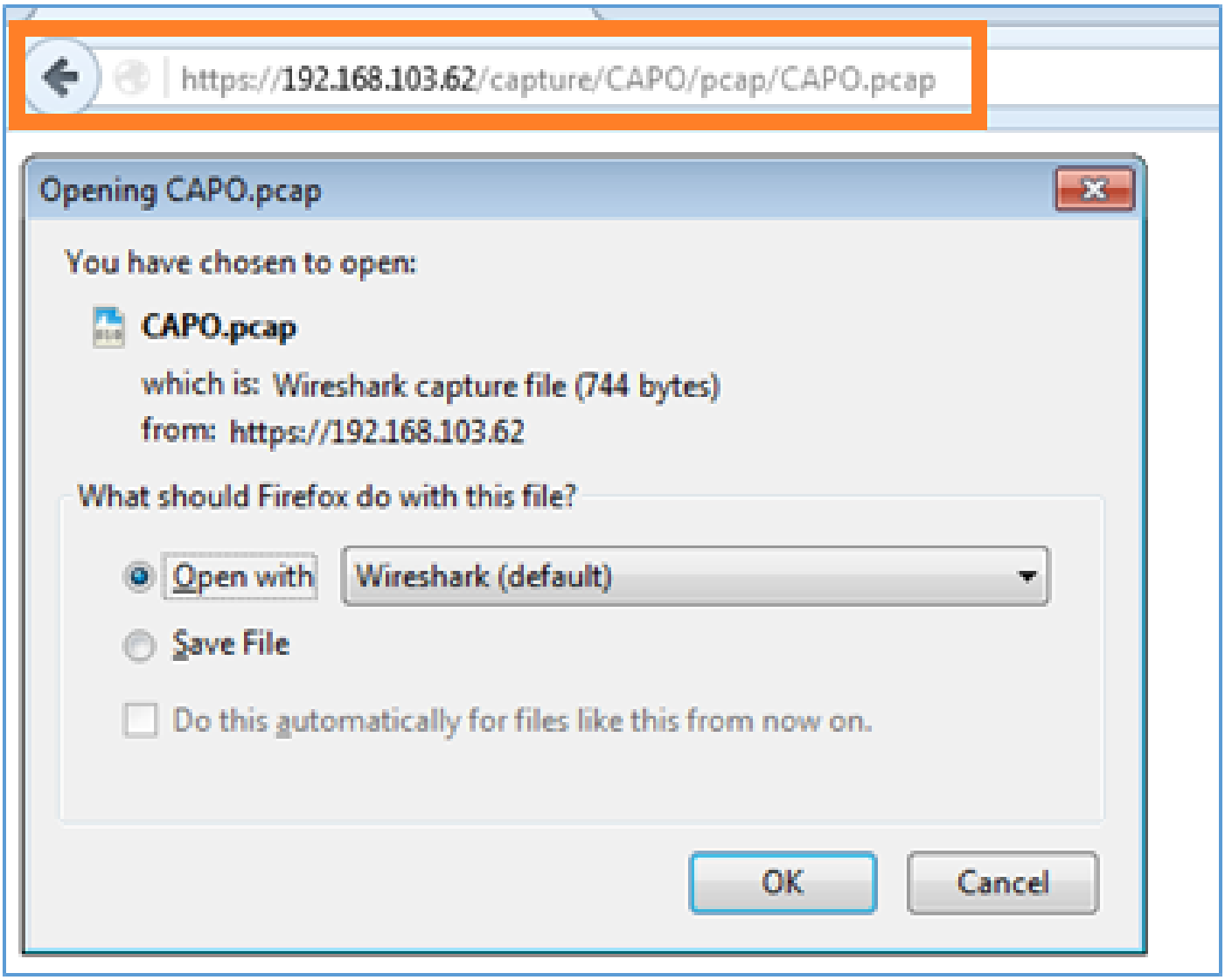
افتح مستعرض على host-A (192.168.103.1) واستخدم عنوان URL هذا لتنزيل الالتقاط الأول: https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap.



للرجوع إليه:

https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	IP الخاص بواجهة بيانات FTD حيث يتم تمكين خادم HTTP
https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	اسم التقاط FTD
https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	اسم الملف الذي تم تنزيله

الالتقاط الثاني، أستخدم https://192.168.103.62/capture/CAPO/pcap/CAPO.pcap.



العمل باستخدام التقاط محرك FTD LINA - تصدير التقاط عبر FTP/TFTP/SCP

المتطلبات

تصدير االلتقاط المأخوذة في السيناريوهات السابقة باستخدام بروتوكوالت FTP/TFTP/SCP.

الحل

تصدير التقاط إلى خادم 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#
```

تصدير التقاط إلى خادم 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#
```

تصدير التقاط إلى خادم 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#
```

التقاط إلغاء التحميل من FTD. حاليا، عندما تحتاج إلى إلغاء تحميل التقاط من FTD، فإن أسهل طريقة هي تنفيذ هذه الخطوات:

1. من Lina - copy /pcap capture:<cap_name> disk0:

2. من جذر FPR - mv /ngfw/mnt/disk0/<cap_name> /ngfw/var/common/

3. من واجهة مستخدم FMC - مراقبة > تحليل > شاشة > جمع أستكشاف الأخطاء وإصلاحها > التقاط لملف وتنزيل في الحقل <cap_name> أدخل المتقدم.

العمل باستخدام التقاط محرك FTD LINA - تعقب حزمة حركة مرور حقيقية

المتطلبات

تمكين التقاط على FTD باستخدام عوامل التصفية التالية:

IP المصدر	192.168.103.1
IP الوجهة	192.168.101.1
البروتوكول	ICMP
الواجهة	داخل
تتبع الحزمة	نعم
عدد حزم التتبع	100

يتم إختبار الاتصال من المضيف-A (192.168.103.1) المضيف-B (192.168.101.1) والتحقق من عمليات الالتقاط.

الحل

يعد تتبع حزمة حقيقية مفيدا جدا لاستكشاف أخطاء الاتصال وإصلاحها. وهو يسمح لك بتصفية التحقق الداخلية التي تمر بها الحزمة. قم بإضافة كلمات بحث تفصيلية لكل واجهة تحقق التي تريد تتبعها. بشكل افتراضي، يتتبع FTD أول 50 حزمة دخلت.

في هذه الحالة، قم بتمكين الالتقاط باستخدام تفاصيل التتبع للحزم 100 الأولى التي

يتلقاها FTD على الواجهة الداخلية:

<#root>

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

إختبار الاتصال من المضيف-A إلى المضيف-B وفحص النتيجة:

```
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
```

الحزم الملتقطة هي:

<#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
```

يعرض هذا الإخراج تتبع الحزمة الأولى. الاجزاء التي تهمنا:

- المرحلة 12 هي المكان الذي يتم فيه رؤية "التدفق الأمامي". هذا هو "صفيف إرسال محركات LINA" (فعليا هو ترتيب العمليات الداخلي).
- المرحلة 13 هي المكان الذي يرسل فيه FTD الحزمة إلى مثيل snort.
- المرحلة 14 هي التي ينظر فيها في حكم الشخير.

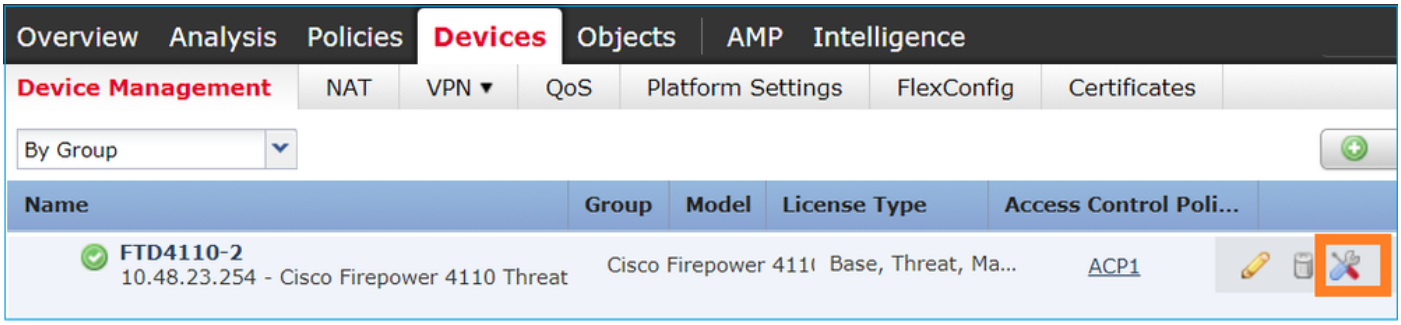
<#root>

```
> 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
```

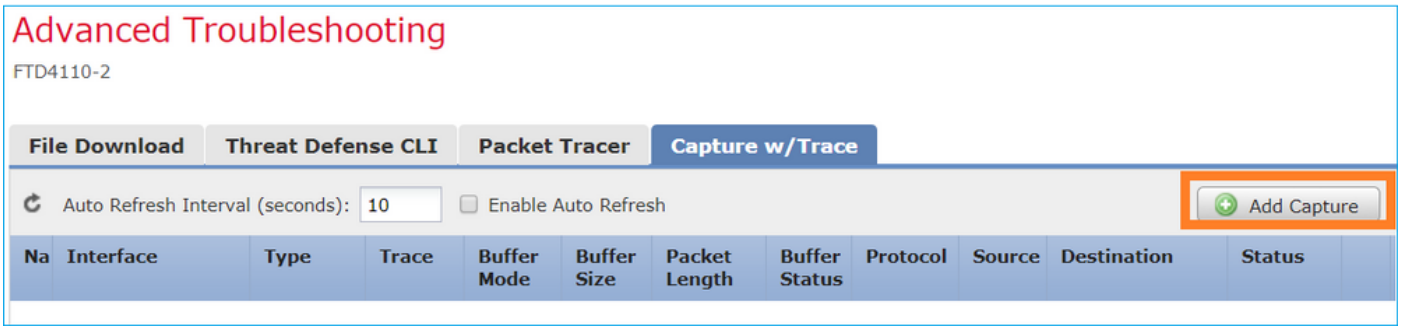
```
... output omitted ...

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
>
```

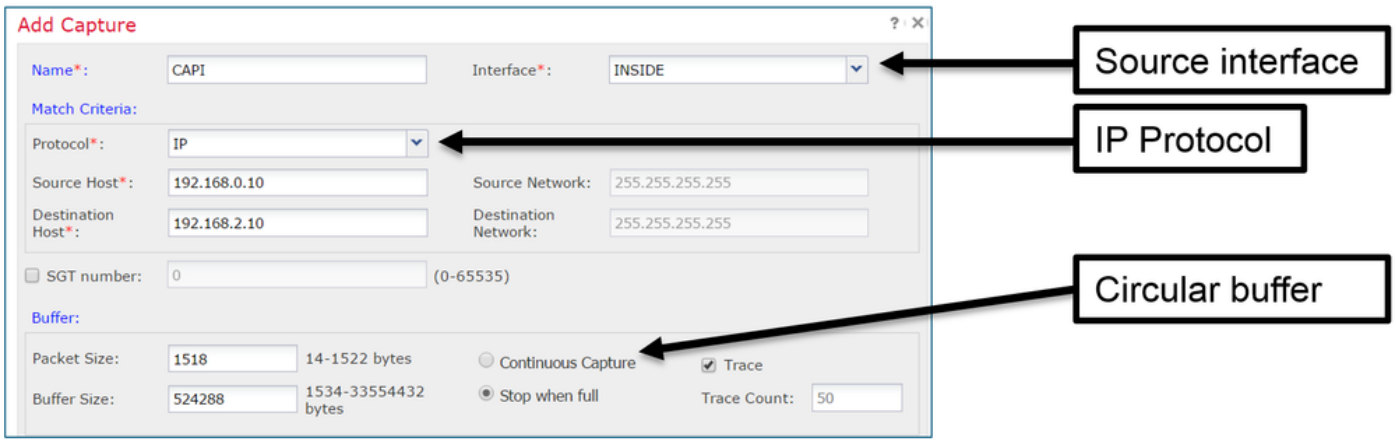
أداة الالتقاط في إصدارات برامج FMC بعد 6.2

في الإصدار 6.2.x من FMC، تم تقديم معالج التقاط حزم جديد. انتقل إلى الأجهزة > إدارة الأجهزة وانقر فوق أيقونة أستكشاف الأخطاء وإصلاحها. ثم أختر أستكشاف الأخطاء وإصلاحها المتقدم وأخيرا الالتقاط w/Trace.



أختر إضافة التقاط لإنشاء التقاط FTD:



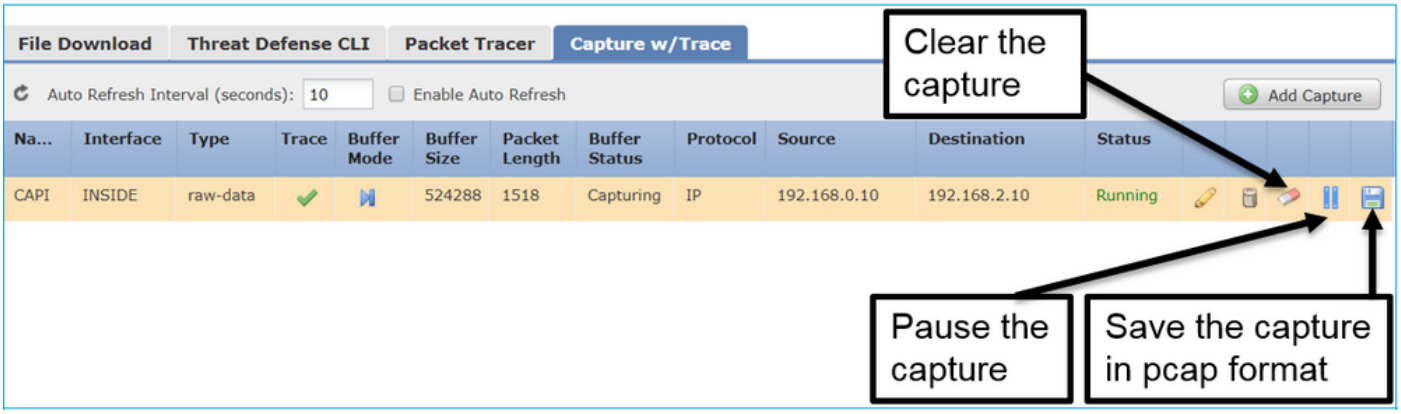


قيود واجهة مستخدم FMC الحالية هي:

- لا يمكن تحديد منافذ SRC و DST
- يمكن مطابقة بروتوكولات IP الأساسية فقط
- لا يمكن تمكين الالتقاط لعمليات إسقاط ASP لمحرك LINA

الحل البديل - إستخدام واجهة سطر الأوامر (CLI) الخاصة ب FTD

بمجرد تطبيق التقاط من واجهة مستخدم FMC، يتم تشغيل الالتقاط:

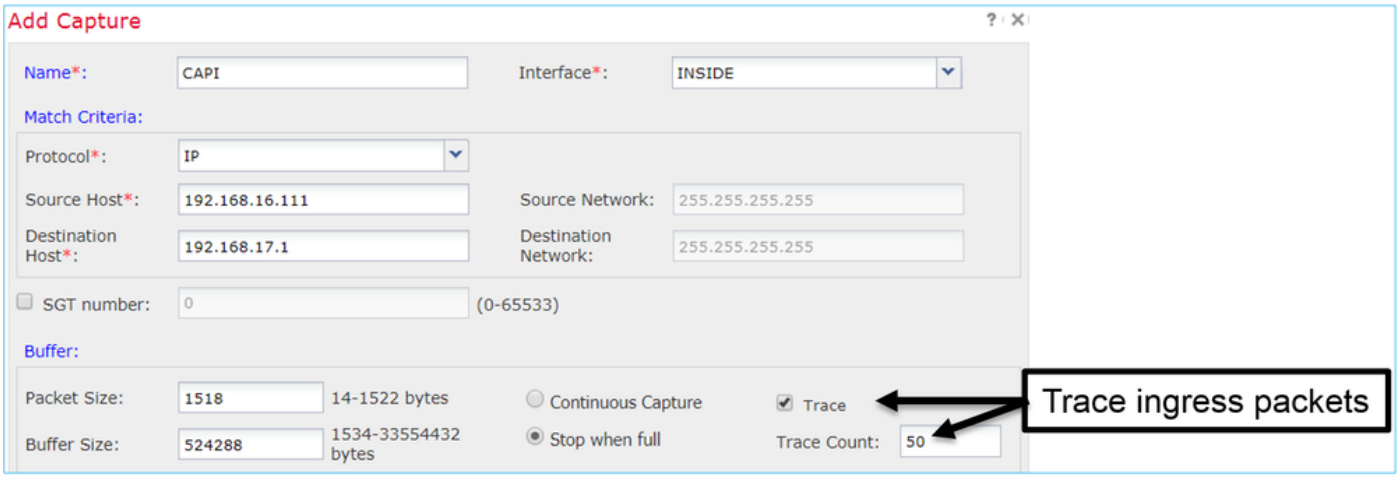


الالتقاط على CLI ل FTD:

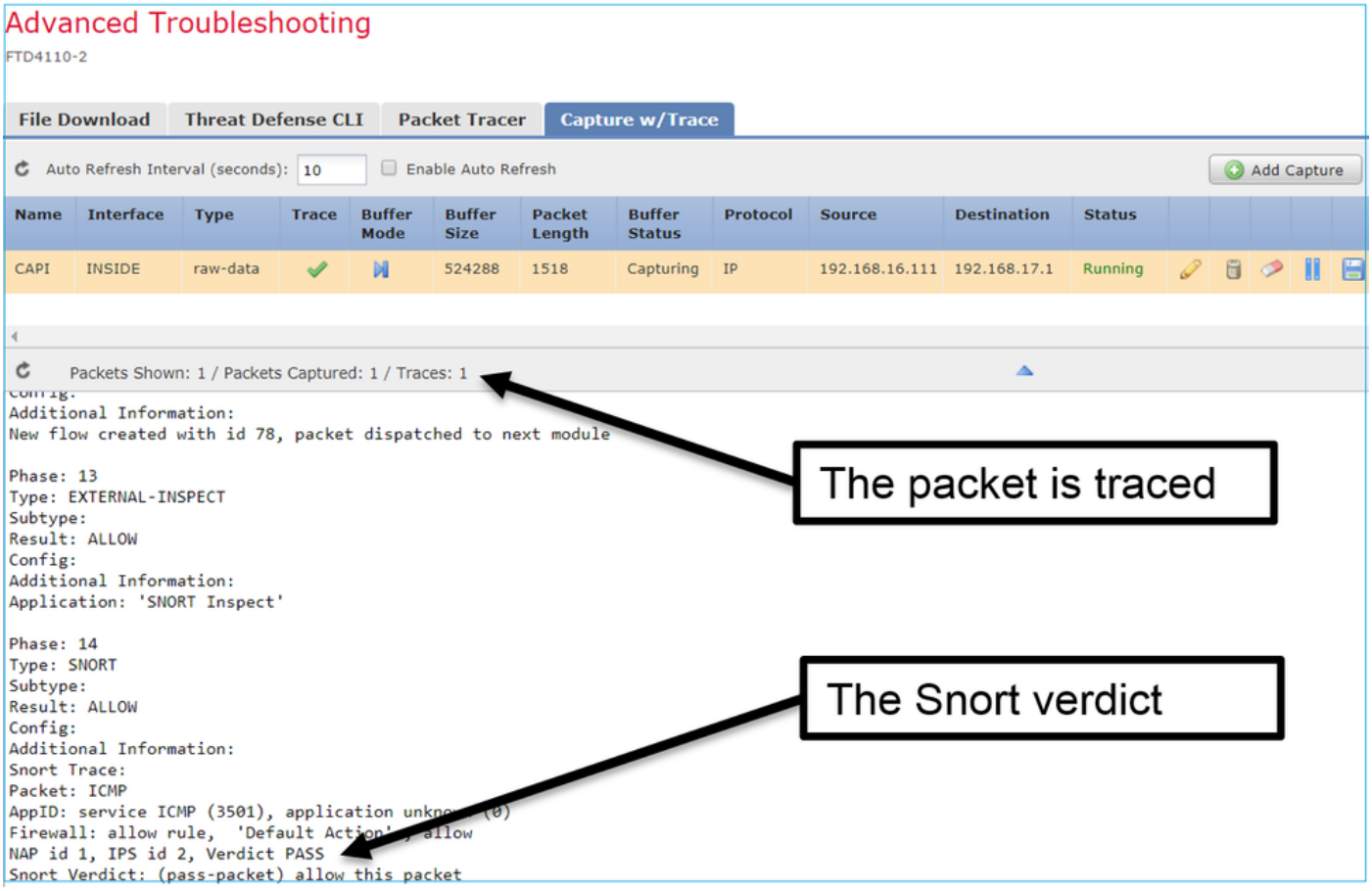
```
<#root>

> 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
>
```

تتبع حزمة حقيقية على FMC بعد 6.2

في FMC 6.2.x، يتيح لك معالج الالتقاط w/Trace التقاط الحزم الحقيقية وتتبعها على FTD:



يمكنك التحقق من الحزمة التي تم تتبعها في واجهة مستخدم FMC:



الأداة المساعدة FTD Packet Tracer

المتطلبات

أستخدم الأداة المساعدة Packet Tracer لهذا التدفق وفحص كيفية معالجة الحزمة داخليا:

واجهة الدخول	داخل
البروتوكول	طلب صدى ICMP
IP المصدر	192.168.103.1
IP الوجهة	192.168.101.1

الحل

تقوم Packet Tracer بإنشاء حزمة ظاهرية. كما هو موضح في هذا المثال، تخضع الحزمة إلى فحص الشرخ. تظهر عملية التقاط أخذت في نفس الوقت على مستوى snort (capture-traffic) طلب صدى 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

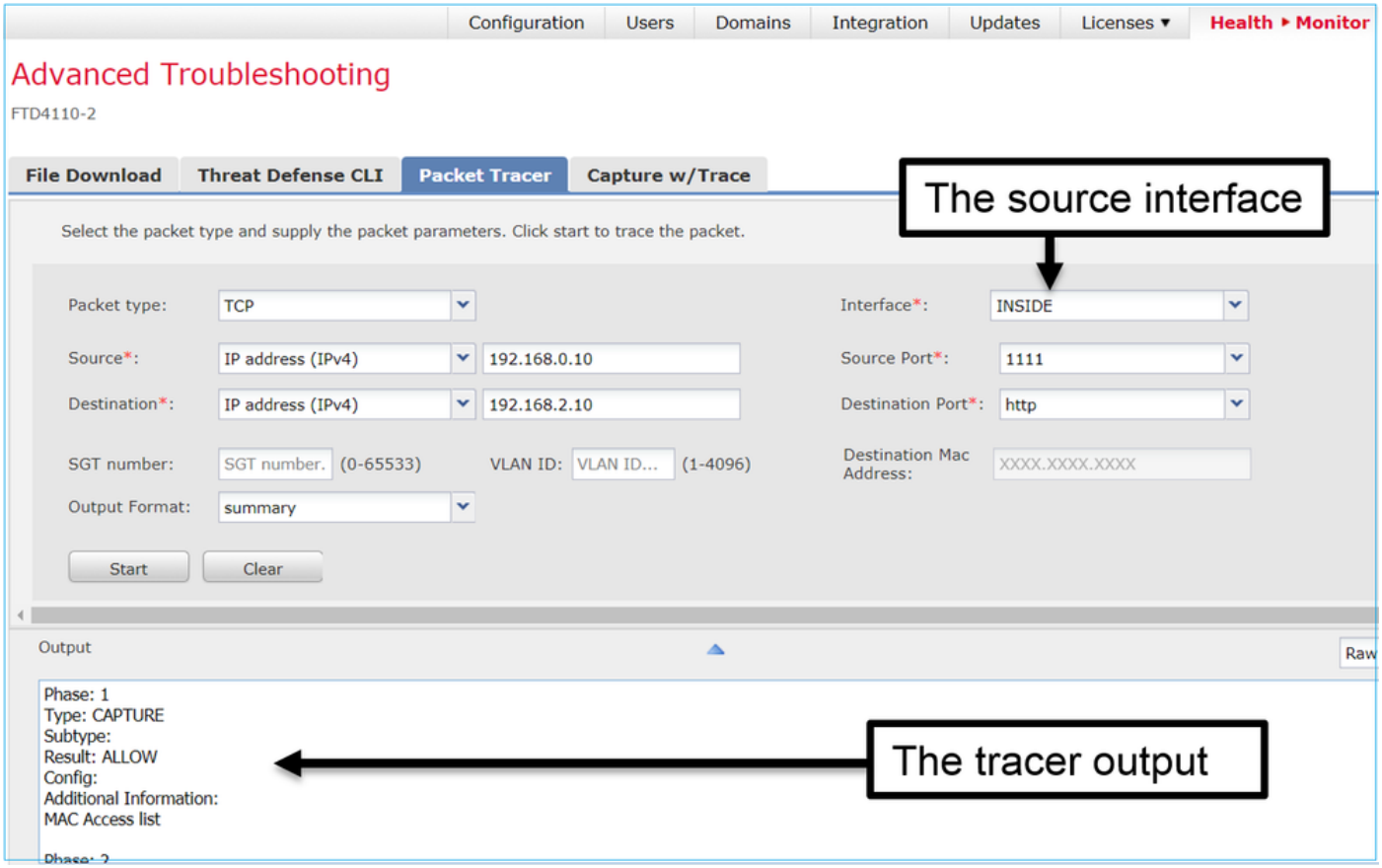
```
NAP id 2, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet


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

>
```

يظهر التقاط مستوى snort في وقت إختبار packet-tracer الحزمة الظاهرية:

```
<#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
```

أداة واجهة المستخدم لحزم البيانات Packet Tracer UI في إصدارات برامج FMC بعد 6.2

في إصدار FMC 6.2.x تم تقديم أداة واجهة المستخدم لتتبع الحزم. يمكن الوصول إلى الأداة بنفس الطريقة التي يتم بها الوصول إلى أداة التقاط وتسمح لك بتشغيل Packet Tracer على FTD من واجهة مستخدم FMC:



معلومات ذات صلة

- [الدليل المرجعي لقيادة الدفاع ضد التهديد الناري FIREPOWER]
- [ملاحظات حول إصدار نظام Firepower، الإصدار 6.1.0]
- [دليل تكوين Firepower Threat Defense من Cisco لإدارة أجهزة Firepower، الإصدار 6.1]
- [الدعم التقني والمستندات - Cisco Systems]

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).