المرحلة 2 من أستكشاف أخطاء مسار بيانات Firepower وإصلاحها: طبقة DAQ

المحتويات

المقدمة

هذه المقالة هي جزء من سلسلة مقالات توضح كيفية أستكشاف مسار البيانات في أنظمة FirePOWER وإصلاحها بشكل منهجي لتحديد ما إذا كانت مكونات FirePOWER قد تؤثر على حركة المرور. يرجى الرجوع إلى [مقالة "نظرة عامة"](#) للحصول على معلومات حول بنية الأنظمة الأساسية FirePOWER وارتباطاتها بمقالات "أستكشاف أخطاء مسارات البيانات وإصلاحها" الأخرى.

في هذه المقالة، سننظر إلى المرحلة الثانية من أستكشاف أخطاء مسار بيانات Firepower وإصلاحها: طبقة DAQ (محاكم حماية البيانات).

دليل المنصات

يصف الجدول التالي المنصات التي تغطيها هذه المقالة.

اسم رمز النظام الأساسي	الوصف	قابل للتطبيق الأجهزة الأنظمة الأساسية	ملاحظات
SFR	ASA مع تثبيت وحدة FirePOWER	سلسلة ASA-5500-X	غير متوفر

	Services (SFR) النمطية.		
FTD (الكل)	ينطبق على جميع منصات الدفاع ضد تهديد الطاقة النارية (FTD)	الفئة ASA-5500-X، الأنظمة الأساسية الظاهرية لبطاقة رسومات الشبكة (NGFW)، FPR-2100، FPR-9300، FPR-4100	غير متوفر
FTD (بخلاف SSP و FPR-2100)	صورة FTD مثبتة على ASA أو نظام أساسي ظاهري	سلسلة ASA-5500-X، أنظمة NGFW الظاهرية، FPR-2100	غير متوفر
FTD (SSP)	تم تثبيت برنامج الإرسال فائق السرعة (FTD) كجهاز منطقي على هيكل قائم على نظام التشغيل القابل للتشغيل (FXOS) Firepower	FPR-9300 و FPR-4100	لا تستخدم السلسلة 2100 برنامج FXOS Chassis Manager

أستكشاف أخطاء مرحلة DAQ الخاصة ب FirePOWER وإصلاحها

ان طبقة DAQ (محكمة تأديب البيانات) هي مكون من قوة النار التي تترجم الحزم إلى شكل يمكن ان يفهمه الشيخ. وهو يعالج الحزمة في البداية عندما ترسل إلى الشيخ. لذلك، إذا كانت الحزم تدخل ولكن لا تخرج جهاز FirePOWER أو أن أستكشاف أخطاء مدخل الحزمة وإصلاحها لم ينتج عنها نتائج مفيدة، فيمكن أن يكون أستكشاف أخطاء DAQ وإصلاحها مفيدا.

التقاط حركة المرور في طبقة DAQ

للحصول على موجه الأمر الذي يتم تشغيل الالتقاط منه، يجب عليك أولا الاتصال باستخدام SSH ب SFR أو عنوان IP الخاص ب FTD.

> **ملاحظة**: في أجهزة FPR-9300 و 4100، أدخل **اتصال ftd** أولا، لينتهي في انفذة مطالبة ثانية. يمكنك أيضا إدخال SSH في برووتوكول IP الخاص بمدير هيكل FXOS، ثم إدخال **وحدة التحكم 1 الخاصة بالاتصال**، يتبعها **اتصال ftd**.

يشرح هذا المقال كيفية تجميع تجميع تجميع الحزم على مستوى DAQ ل FirePOWER.

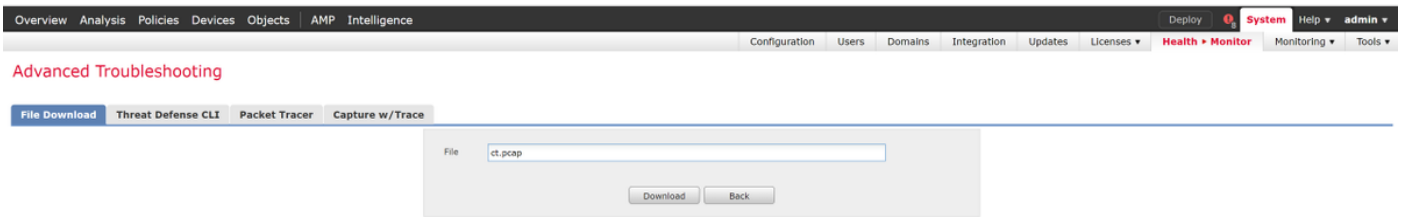
الحظ أن الصياغة ليست نفس الأمر **capture** المستخدم على ASA وكذلك جانب LINA من منصة FTD. وفيما يلي مثال على تشغيل التقاط حزمة DAQ من جهاز FTD:

```
> system support capture-traffic

Please choose domain to capture traffic from:
  0 - br1
  1 - Router
  2 - my-inline inline set


Selection? 2


Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: -s 1518 -w ct.pcap

> expert
admin@ciscoasa:~$ ls /ngfw/var/common/
ct.pcap
```

كما هو موضح في لقطة الشاشة أعلاه، تم كتابة التقاط بتنسيق PCAP يسمى ct.pcap إلى الدليل **/ngfw/var/الملتقط** (**/var/common** على منصة SFR). يمكن نسخ ملفات الالتقاط هذه من جهاز FirePOWER من نافذة مطالبة > باستخدام الاتجاهات الواردة في [القرص](#) المذكورة أعلاه.

بدلا من ذلك، في مركز إدارة Firepower (FMC) في الإصدار 6.2.0 من FirePOWER والإصدارات الأحدث، يمكنك التنقل إلى **الأجهزة > إدارة الأجهزة**. ثم انقر فوق الرمز الموجود بجوار الجهاز المعني، يتبع **أستكشاف الأخطاء وإصلاحها المتقدم > تنزيل الملف**.

يمكنك بعد ذلك إدخال اسم ملف الالتقاط وانقر تنزيل.



كيفية تجاوز قوة النيران

إذا كانت FirePOWER ترى حركة المرور، ولكن تم تحديد أن الحزم لا تعرض الجهاز أو أن هناك مشكلة أخرى مع حركة المرور، فإن الخطوة التالية ستكون تجاوز مرحلة فحص FirePOWER لتأكيد أن أحد مكونات FirePOWER يسقط حركة المرور. وفيما يلي تفصيل لأسرع طريقة لجعل حركة المرور تتجاوز قوة النيران على مختلف المنصات.

SFR - وضع الوحدة النمطية FirePOWER في وضع المراقبة فقط

على ال ASA الذي يستضيف SFR، أنت يستطيع وضعت ال SFR وحدة نمطية في مدرب-only أسلوب عن طريق ال ASA أمر خط قران (CLI) أو ال cisco أداة مدير (ASDM) معدل. وهذا يتسبب في إرسال نسخة من الحزم المباشرة إلى الوحدة النمطية SFR فقط.

من أجل وضع وحدة SFR في وضع جهاز العرض فقط عبر واجهة سطر الأوامر (CLI) الخاصة ب ASA، يجب أولا تحديد خريطة الفئة وخريطة السياسة المستخدمة لإعادة توجيه SFR من خلال تشغيل الأمر **show service-policy sfr**.

```
# show service-policy sfr

Global policy:
 Service-policy: global_policy
   Class-map: sfr
     SFR: card status Up, mode fail-open
       packet input 10000, packet output 9900, drop 100, reset-drop 0
```

يوضح الإخراج أن خريطة policy global_policy تقوم بفرض إجراء فتح فشل SFR على خريطة فئة "sfr".

> **ملاحظة**: "Fail-close" هو أيضا وضع يمكن فيه تشغيل SFR، ولكنه ليس شائع الاستخدام لأنه يمنع كل حركة المرور إذا كانت وحدة SFR معطلة أو غير مستجيبة.

in order to وضعت ال SFR وحدة نمطية داخل مدرب-only أسلوب، أنت يستطيع أصدرت هذا أمر أن يبطل الحالي SFR تشكيل وأدخل ال مدرب-only تشكيل:

```
# configure terminal
(config)# policy-map global_policy
(config-pmap)# class sfr
(config-pmap-c)# no sfr fail-open
(config-pmap-c)# sfr fail-open monitor-only

INFO: The monitor-only mode prevents SFR from denying or altering traffic.

(config-pmap-c)# write memory
Building configuration...
```

بمجرد وضع الوحدة النمطية في وضع المراقبة فقط، يمكن التحقق منها في إخراج **show service-policy sfr**.

```
# sh service-policy sfr

Global policy:
 Service-policy: global_policy
   Class-map: sfr
     SFR: card status Up, mode fail-open monitor-only
       packet input 0, packet output 100, drop 0, reset-drop 0
```

> **ملاحظة**: لإعادة وحدة SFR إلى الوضع المضمن، قم بإصدار الأمر **no sfr fail-open monitor-only** من تنفيذ مطالبة **(config-pmap-c)#**الموضحة أعلاه، متبوعة ب **SFR {failed-open | failed-close}** الأمر الذي كان موجودا في الأصل.

بدلا من ذلك، يمكنك وضع الوحدة النمطية في جهاز العرض فقط عبر ASM بالتنقل إلى

التكوين > جدار الحماية > قواعد سياسة الخدمة. ثم انقر فوق القاعدة المعنية. بعد ذلك، انتقل إلى صفحة **إجراءات القواعد** وانقر فوق علامة التبويب **ASA FirePOWER Inspection**. وبمجرد الوصول، يمكن تحديد **جهاز العرض فقط**.

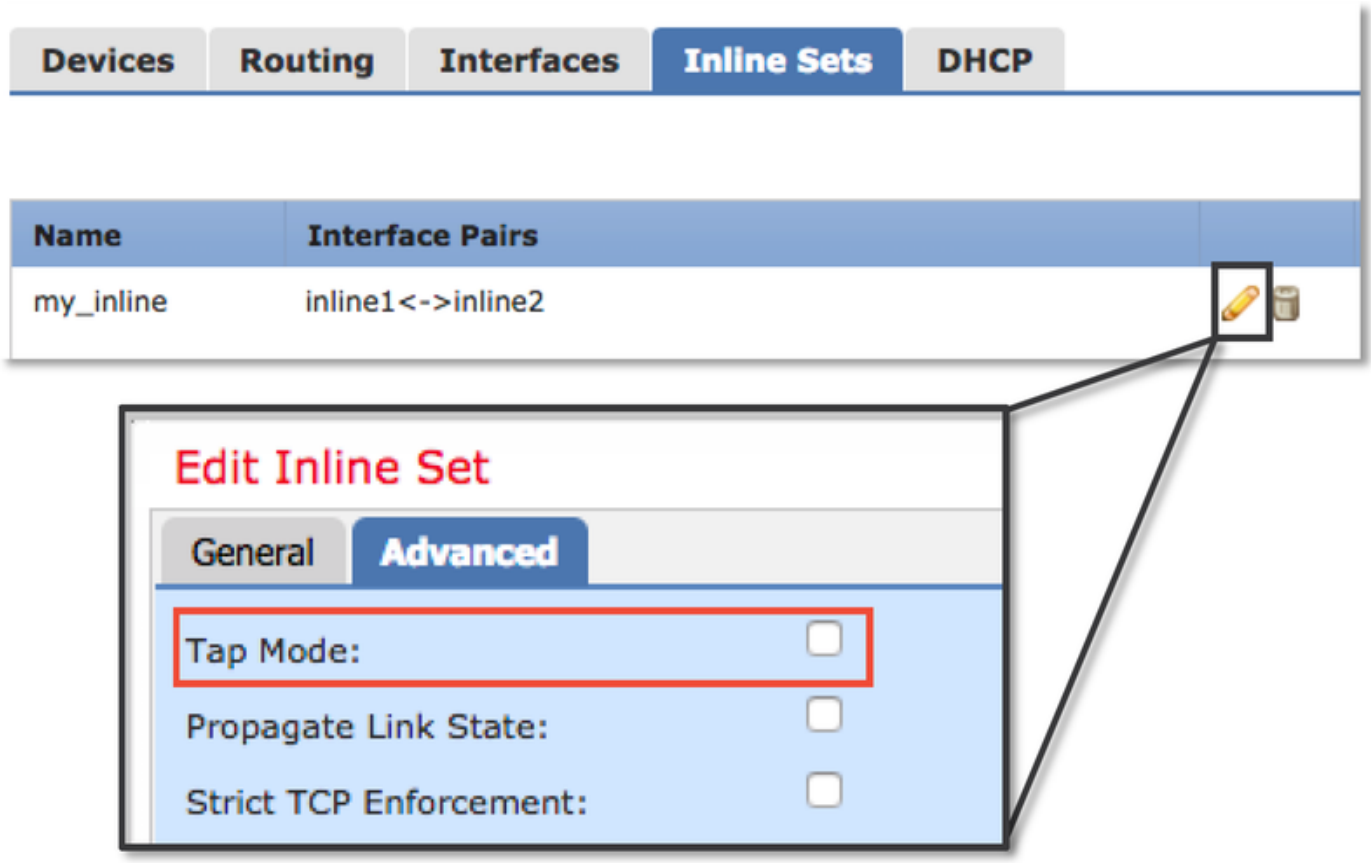
إن يبقى الحركة مرور إصدار حتى بعد أن ال SFR نمطية يتلقى يكون في مدرب فقط أسلوب، ال firepower وحدة نمطية ال يسبب المشكلة. بعد ذلك، يمكن تشغيل تعقب الحزمة لمزيد من تشخيص المشكلات على مستوى ASA.

إذا لم تعد المشكلة قائمة، فإن الخطوة التالية ستكون أستكشاف أخطاء مكونات برنامج FirePOWER وإصلاحها.

FTD (الكل) - وضع مجموعات في السطر في وضع TAP

إذا كانت حركة المرور تمر عبر أزواج الواجهة التي تم تكوينها في مجموعات الأسطر، يمكن وضع المجموعة المضمنة في وضع TAP. وهذا يؤدي بشكل أساسي إلى عدم إتخاذ FirePOWER إجراء على الحزمة المباشرة. ال يطبق على مسحاج تخديد أو أسلوب شفاف دون مسحاج تخديد داخلي بما أن الأداة ينبغي عدلت الربط قبل أن يرسلها إلى الخطوة تالي و ال يستطيع كنت وضعت في مجرى جانبي أسلوب دون يسقط حركة مرور. بالنسبة للوضع الموجه والشفاف بدون مجموعات الأسطر، قم بالمتابعة مع خطوة متتبع الحزمة.

لتكوين وضع TAP من واجهة مستخدم FMC (UI)، انتقل إلى **الأجهزة > إدارة الأجهزة**، ثم قم بتحرير الجهاز المعني. تحت علامة التبويب **مجموعات في السطر**، قم بإيقاف تشغيل الخيار **لوضع الضغط**.



إذا قام وضع TAP بحل المشكلة، فإن الخطوة التالية ستكون أستكشاف أخطاء مكونات برنامج FirePOWER وإصلاحها.

إذا لم يحل وضع TAP المشكلة، فسيكون الإصدار خارج برنامج FirePOWER. بعد ربط tracer يستطيع كنت استعملت أن يزيد من تشخيص الإصدار.

إستخدام أداة تتبع الحزم لاستكشاف أخطاء حركة المرور التي تم محاكاتها وإصلاحها

Packet Tracer هي أداة مساعدة يمكن أن تساعد في تحديد موقع إسقاط الحزمة. إنها محاكي، وبالتالي فإنها تقوم بتتبع حزمة اصطناعية.

SFR - تشغيل تتبع الحزم على ASA CLI

هنا مثال على كيفية تشغيل متتبع الحزم على ASA CLI لحركة مرور SSH. لمزيد من المعلومات التفصيلية حول صياغة أمر تعقب الحزمة، يرجى الرجوع إلى هذا القسم في دليل مرجع أوامر سلسلة ASA.

```
asa# packet-tracer input inside tcp 192.168.62.60 10000 10.10.10.10 ssh

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.151.37.1 using egress ifc  outside

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: SFR
Subtype:
Result: ALLOW
Config:
class-map inspection_default
 match any
policy-map global_policy
 class inspection_default
  sfr fail-open
service-policy global_policy global
Additional Information:
```

```
Phase: 6
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
class-map inspection_default
 match any
policy-map global_policy
 class inspection_default
  inspect icmp
service-policy global_policy global
Additional Information:

Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 756, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

في المثال أعلاه، نرى على حد سواء وحدة ASA و SFR التي تسمح بالحزم بالإضافة إلى معلومات مفيدة حول كيفية معالجة ASA لتدفق الحزمة.

FTD (all) - تشغيل أداة تعقب الحزم على واجهة سطر الأوامر (CLI) في FTD

على جميع الأنظمة الأساسية ل FTD، يمكن تشغيل الأمر packet tracer من واجهة سطر الأوامر (CLI) الخاصة ب FTD.

```
> packet-tracer input inside tcp 192.168.62.60 10000 10.10.10.10 ssh

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.100.1 using egress ifc  outside
```

```
Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434433
access-list CSM_FW_ACL_ remark rule-id 268434433: ACCESS POLICY:
My_AC_Policy - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268434433: L7 RULE: Block urls
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will
be reached

Phase: 4
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Config:
class-map class-default
 match any
policy-map global_policy
 class class-default
  set connection advanced-options UM_STATIC_TCP_MAP
service-policy global_policy global
Additional Information:
```

```
Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
object network 62_network
 nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 192.168.62.60/10000 to 192.168.100.51/10000

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 8
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 10
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 612016, packet dispatched to next module
```

```
Phase: 11
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 12
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: TCP, SYN, seq 1821549761
Reputation: packet blacklisted, drop
Snort: processed decoder alerts or actions queue, drop
IPS Event: gid 136, sid 1, drop
Snort detect_drop: gid 136, sid 1, drop
NAP id 1, IPS id 0, Verdict BLACKLIST, Blocked by Reputation
Snort Verdict: (black-list) black list this flow
```

في هذا المثال، ربط tracer الا يبدي السبب للسقوط. في هذه الحالة، هي القائمة السوداء IP ضمن ميزة "معلومات الأمان" في FirePOWER التي تمنع الحزمة. تتمثل الخطوة التالية في استكشاف أخطاء مكون برنامج FirePOWER الفردي الذي يتسبب في الإسقاط وإصلاحها.

استخدام Capture مع Trace لاستكشاف أخطاء حركة المرور المباشرة وإصلاحها

كما يمكن تعقب حركة المرور المباشرة عبر ميزة الالتقاط مع ميزة التتبع، والتي توفر عدى جميع الأنظمة الأساسية عبر واجهة سطر الأوامر (CLI). أدناه مثال على تشغيل التقاط مع تتبع مقابل حركة مرور SSH.

```
> capture ssh_traffic trace interface inside match tcp any any eq 22
> show capture ssh_traffic

7 packets captured

   1: 01:17:38.498906       192.168.62.70.48560 > 10.83.180.173.22: S 4250994241:4250994241(0) win 29200 <mss 1460,sackOK,timestamp 1045829951
0,nop,wscale 7>
   2: 01:17:38.510898       10.83.180.173.22 > 192.168.62.70.48560: S 903999422:903999422(0) ack 4250994242 win 17896 <mss 1380,sackOK,timestamp
513898266 1045829951,nop,wscale 7>
   3: 01:17:38.511402       192.168.62.70.48560 > 10.83.180.173.22: . ack 903999423 win 229 <nop,nop,timestamp 1045829956 513898266>
   4: 01:17:38.511982       192.168.62.70.48560 > 10.83.180.173.22: P 4250994242:4250994283(41) ack 903999423 win 229 <nop,nop,timestamp
1045829957 513898266>
   5: 01:17:38.513294       10.83.180.173.22 > 192.168.62.70.48560: . ack 4250994283 win 140 <nop,nop,timestamp 513898268 1045829957>
   6: 01:17:38.528125       10.83.180.173.22 > 192.168.62.70.48560: P 903999423:903999444(21) ack 4250994283 win 140 <nop,nop,timestamp 513898282
1045829957>
   7: 01:17:38.528613       192.168.62.70.48560 > 10.83.180.173.22: . ack 903999444 win 229 <nop,nop,timestamp 1045829961 513898282>
```

```
> show capture ssh_traffic packet-number 4 trace

7 packets captured

   4: 01:17:38.511982      192.168.62.70.48560 > 10.83.180.173.22: P
4250994242:4250994283(41) ack 903999423 win 229 <nop,nop,timestamp
1045829957 513898266>
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: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found flow with id 626406, using existing flow

Phase: 4
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'
```

```
Phase: 5
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: TCP, ACK, seq 4250994242, ack 903999423
AppID: service SSH (846), application unknown (0)
Firewall: starting rule matching, zone 1 -> 2, geo 0 -> 0, vlan 0, sgt 65535, user 2, icmpType 0, icmpCode 0
Firewall: trust/fastpath rule, id 268435458, allow
NAP id 1, IPS id 0, Verdict WHITELIST
Snort Verdict: (fast-forward) fast forward this flow

Result:
input-interface: inside
input-status: up
input-line-status: up
Action: allow
```

في هذا المثال، تم تتبع الحزمة الرابعة في الالتقاط، نظرا لأن هذه هي الحزمة الأولى مع بيانات التطبيق المعرفة. كما هو موضح، فإن الحزمة تنتهي إلى البياض من طرف الشخير، مما يعني أنه ليس من الضروري فحص الشخير مرة أخرى للتدفق، ويسمح بشكل عام.

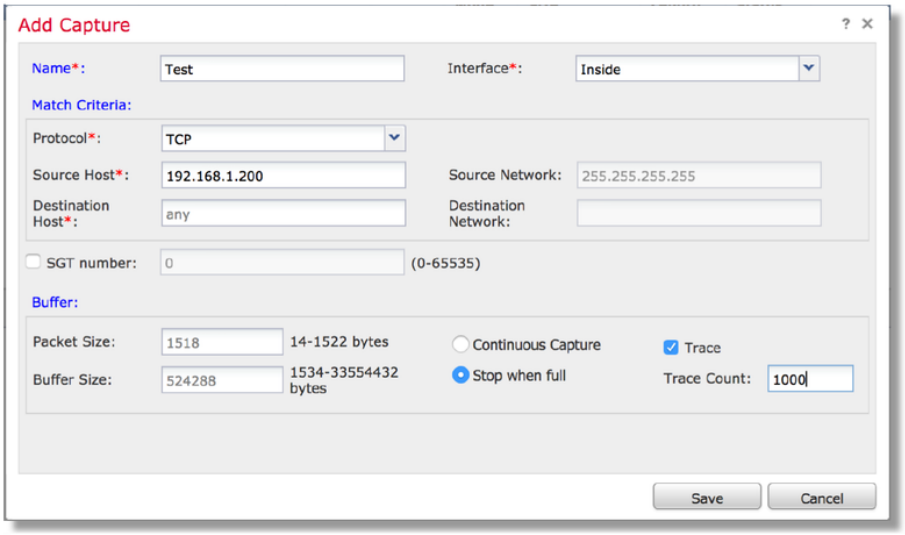
لمزيد من المعلومات حول الالتقاط بصيغة التتبع، يرجى الرجوع إلى هذا القسم في دليل مرجع أوامر سلسلة ASA.

FTD (الكل) - تشغيل الالتقاط باستخدام تتبع على واجهة المستخدم الرسومية (GUI) ل FMC

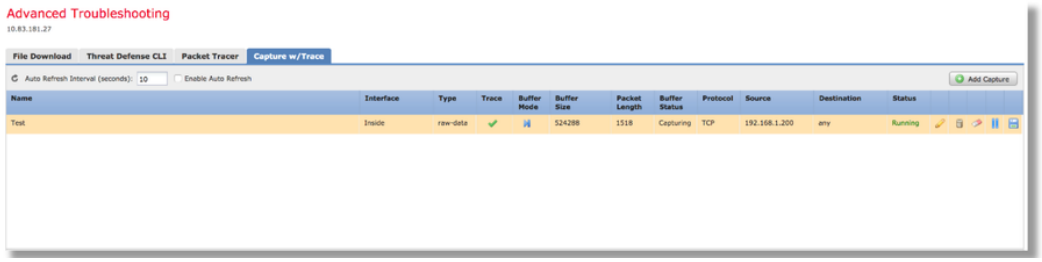
على أنظمة FTD الأساسية، يمكن تشغيل الالتقاط بالتتبع على واجهة مستخدم FMC. للوصول إلى الأداة المساعدة، انتقل إلى **الأجهزة > إدارة الأجهزة**.

ثم انقر فوق الرمز الموجود بجوار الجهاز المعني، يتبع **أستكشاف الأخطاء وإصلاحها المتقدم > التقاط و/تتبع**.

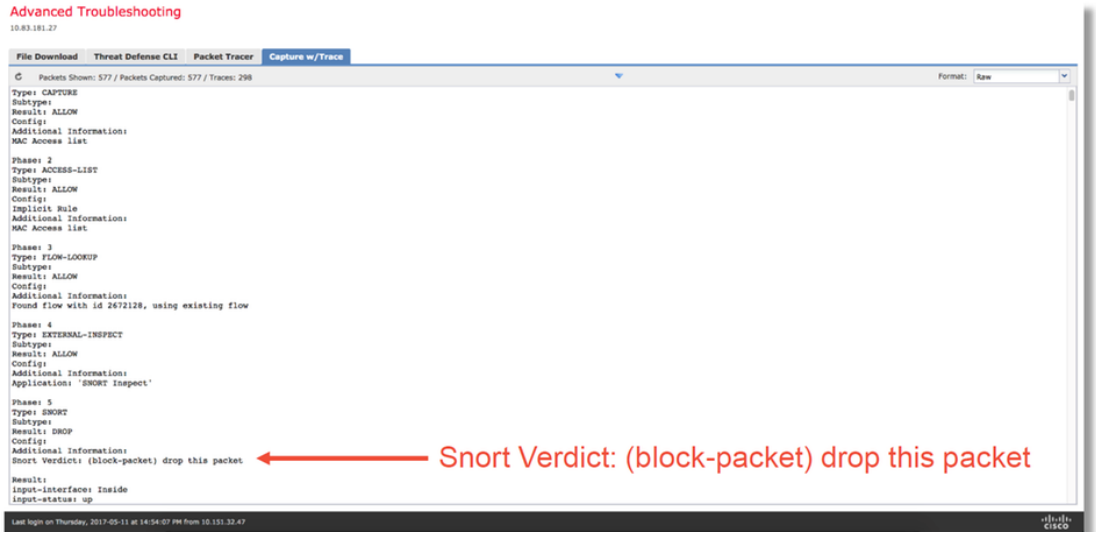
أدناه مثال على كيفية تشغيل التقاط باستخدام تتبع عبر واجهة المستخدم الرسومية.



Clicking **Add Capture** button will display this popup window



View of all current captures



Example output shows the packet was blocked by Snort

إذا أظهر الالتقاط مع التتبع سبب إسقاط الحزمة، فإن الخطوة التالية ستكون أستكشاف أخطاء مكونات البرامج الفردية وإصلاحها.

إن ال يظهر وه واضح السبب من الإصدار، الخطوة تالي يكون أن يسرع حركة مرور.

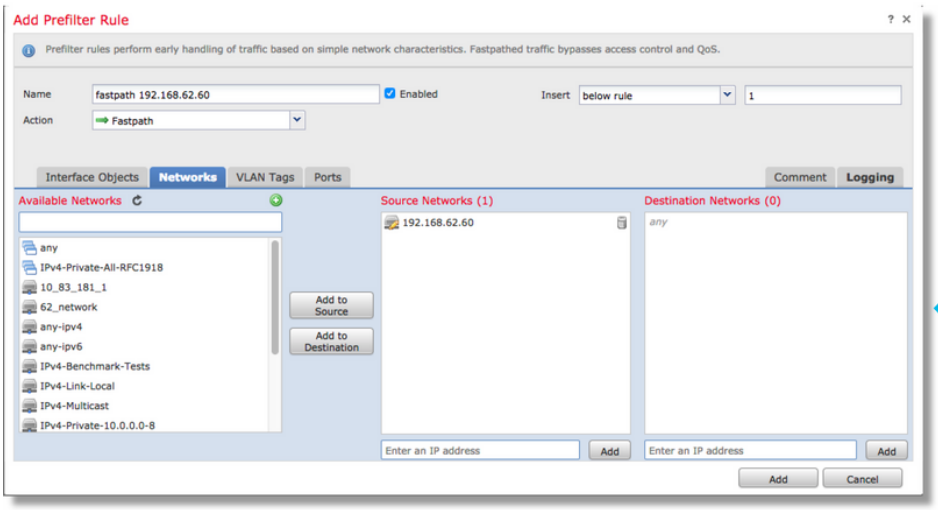
إنشاء قاعدة مسار سريع ل PreFilter في FTD

على جميع منصات FTD، هناك سياسة ما قبل التصفية، والتي يمكن إستخدامها لتحويل حركة المرور من تفتيش FirePOWER (snort).

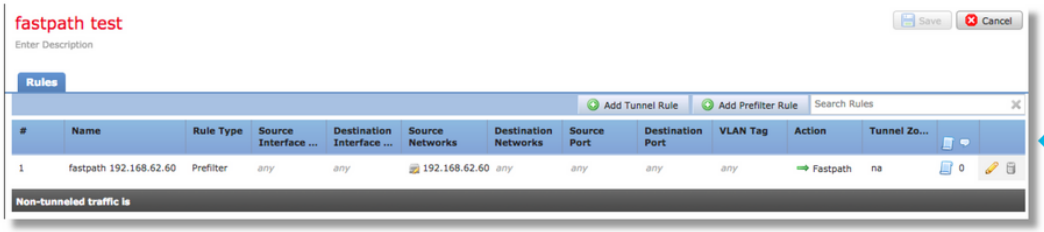
في FMC، يوجد ذلك ضمن **السياسات > التحكم في الوصول > Prefilter**. ال يمكن تحرير نهج التصفية المسبقة الافتراضي، لذا سيلزم إنشاء نهج مخصص.

بعد ذلك، يجب إقران نهج PreFilter الذي تم إنشاؤه حديثا بنهج التحكم في الوصول. يتم تكوين هذا ضمن عالمة التبويب "خيارات متقدمة" الخاصة بنهج التحكم بالوصول في قسم **إعدادات نهج عامل التصفية المسبق**.

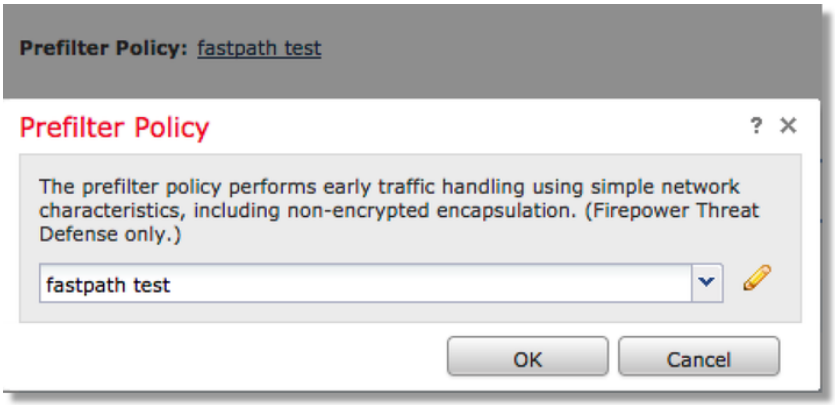
فيما يلي مثال على كيفية إنشاء قاعدة FastPath داخل نهج PreFilter والتحقق من عدد مرات الوصول.



Clicking **Add Prefilter Rule** button will display this popup window.



View of all rules in the **fastpath test** Prefilter policy



From AC policy make sure the Prefilter Policy is set to the custom Prefilter Policy

View of connection events matching prefilter rule

First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Prefilter Policy	Tunnel/Prefilter Rule
2017-05-15 16:05:14	2017-05-15 16:05:14	Fastpath		192.168.62.60	10.83.180.173	48480 / tcp	22 (ssh) / tcp	fastpath test	fastpath 192.168.62.60

انقر هنا للحصول على مزيد من التفاصيل حول تشغيل نهج التصفية المسبقة وتكوينها.

إذا أدت إضافة نهج PreFilter إلى حل مشكلة حركة مرور البيانات، يمكن ترك القاعدة في مكانها إذا كان ذلك مطلوبا. ومع ذلك، لم يتم إجراء أي فحص آخر لذلك التدفق. يلزم إجراء المزيد من أستكشاف أخطاء برنامج FirePOWER وإصلاحها.

إذا لم تحل إضافة نهج عامل التصفية المسبق المشكلة، يمكن تشغيل الحزمة ذات خطوة التتبع مرة أخرى لتتبع المسار الجديد للحزمة.

البيانات التي سيتم تقديمها إلى TAC

البيانات	تعليمات
مخرجات القيادة	طالع هذه المقالة للحصول على تعليمات
التقاط الحزم	بالنسبة إلى ASA/LINA: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-firewalls/118097-configure-asa-00.html بالنسبة إلى Firepower: http://www.cisco.com/c/en/us/support/docs/security/sourcefire-fire technote-sourcefire-00.html
خرج ASA "show tech"	قم بتسجيل الدخول إلى ASA CLI وتمتع بحفظ جلسة عمل المحطة الطرفية في سجل المحطة الطرفية جلسة إنتاج مبرد إلى TAC. يمكن حفظ هذا الملف على القرص أو نظام تخزين خارجي باستخدام هذا الأمر. show tech | إعادة توجيه القرص0:/show_tech.log
أستكشاف أخطاء الملف وإصلاحها من جهاز FirePOWER الذي يقوم بفحص حركة المرور	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-techn

الخطوة التالية

وإذا ما تبين أن أحد مكونات برنامج الطاقة النارية هو السبب وراء هذه القضية، فإن الخطوة التالية سوف تتلخص في إستبعاد كل عنصر بشكل منهجي، بدءا باستخبارات الأمن.

انقر هنا لمتابعة الدليل التالي.

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).