توضيح إجراءات قواعد سياسة التحكم في الوصول إلى برنامج Firepower Threat Defense

المحتويات

المقدمة

يصف هذا المستند الإجراءات المتنوعة المتاحة على سياسة التحكم في الوصول (ACP) إلى Firepower Threat Defense (FTD) وسياسة التصفية المسبقة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- إلغاء تحميل التدفق
- التقاط الحزم على أجهزة الدفاع ضد تهديد FirePOWER
- أداة تتبع الحزم والتقاط باستخدام خيار التتبع على أجهزة FTD

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco Firepower 4110 Threat Defense، الإصدار 6.4.0 (Build 113) و 6.6.0 (Build 90)
- مركز إدارة Firepower (FMC)، الإصدار 6.4.0 (Build 113) و 6.6.0 (Build 90)

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.

المنتجات ذات الصلة

هذا وثيقة يستطيع أيضا كنت استعملت مع هذا جهاز وبرمجية صيغة:

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR1000 و FPR2100 و FPR4100 و FPR9300
- VMware (ESXi) وخدمات الويب من Amazon (AWS) والأجهزة الافتراضية القائمة على Kernel (KVM)
- الوحدة النمطية لموجه الخدمة المدمجة (ISR) Router Module
- برنامج FTD الإصدار 6.1.x والإصدارات الأحدث

> **ملاحظة**: يتم دعم إلغاء تحميل التدفق فقط على المثيلات الأصلية لتطبيقات ASA و FTD وعلى الأنظمة الأساسية FPR4100 و FPR9300. لا تدعم مثيلات حاوية FTD إلغاء تحميل التدفق.

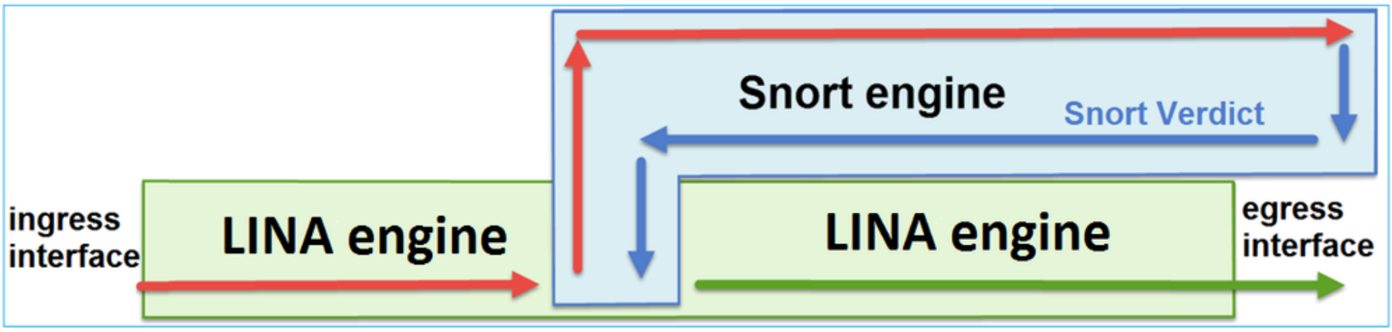
معلومات أساسية

يتم فحص عملية الخلفية لكل إجراء مع تفاعلاها مع الميزات الأخرى مثل إلغاء تحميل التدفق والبروتوكولات التي تفتح الاتصالات الثانوية.

FTD هو صورة برنامج موحدة تتكون من محركين رئيسيين:

- محرك لينا
- محرك الشخير

يوضح هذا الرقم كيفية تفاعل المحركين:



- تدخل الحزمة واجهة الدخول ويتم معالجتها بواسطة محرك LINA
- إذا كان مطلوبا من قبل سياسة FTD، يتم فحص الحزمة بواسطة محرك snort
- يقوم محرك الشبكة بإرجاع الحكم (قائمة السماح أو قائمة الحظر) للحزمة
- يقوم محرك LINA بإسقاط الحزمة أو إعادة توجيهها بناء على قرار الشخير

كيفية نشر ACP

يتم تكوين نهج FTD على FMC عند إستخدام الإدارة خارج المربع (عن بعد) أو Firepower Device Manager (FDM) عند إستخدام الإدارة المحلية. وفي كلا السيناريوهين، يتم نشر ACP على النحو التالي:

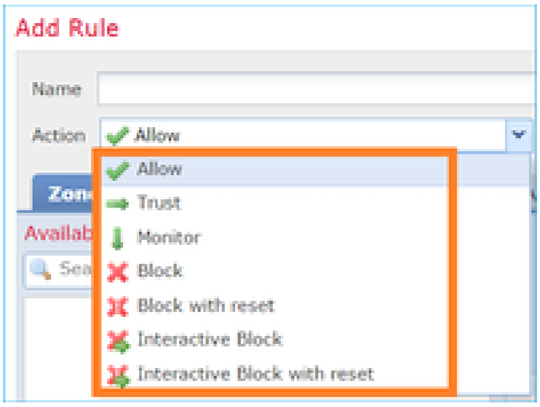
- قائمة تحكم في الوصول العالمي (ACL) باسم CSM_FW_ACL_ إلى محرك FTD LINA
- قواعد التحكم في الوصول (AC) في ملف /ngfw/var/sf/detection_engines/<uuid>/ngfw.rules إلى محرك التطفل FTD

التكوين

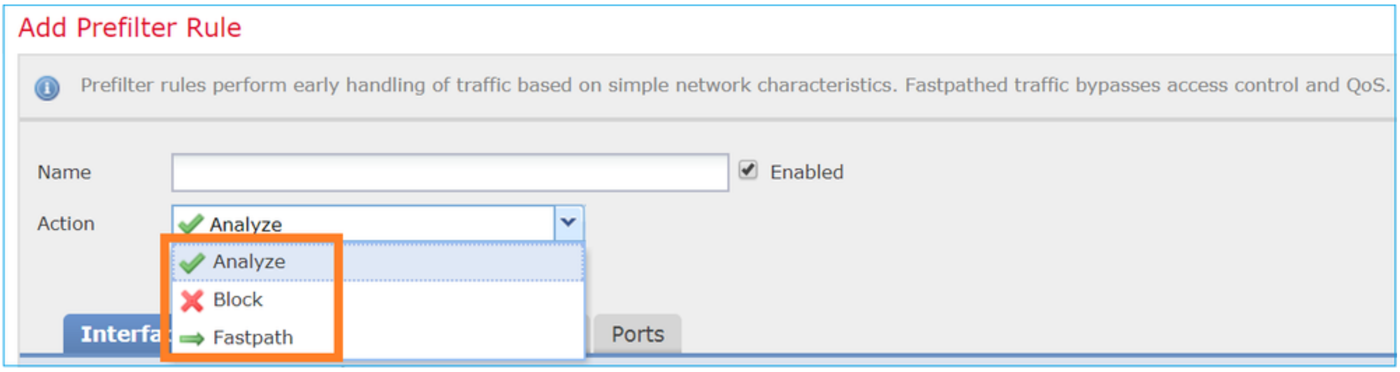
الإجراءات المتوفرة ل ACP

تحتوي قائمة التحكم بالوصول (ACP) ل FTD على قاعدة واحدة أو أكثر ويمكن أن تحتوي كل قاعدة على أحد هذه الإجراءات كما هو موضح في الصورة:

- **Allow**
- **Trust**
- **Monitor**
- **Block**
- **Block with reset**
- **Interactive Block**
- **Interactive Block with reset**



وبالمثل، يمكن أن يحتوي نهج PreFilter على قاعدة واحدة أو أكثر ويتم عرض الإجراءات المحتملة في الصورة:


Add Prefilter Rule
Prefilter rules perform early handling of traffic based on simple network characteristics. Fastpathed traffic bypasses access control and QoS.
Name
☑ Enabled
Action
Analyze
Analyze
Block
Fastpath
Interfa
Ports

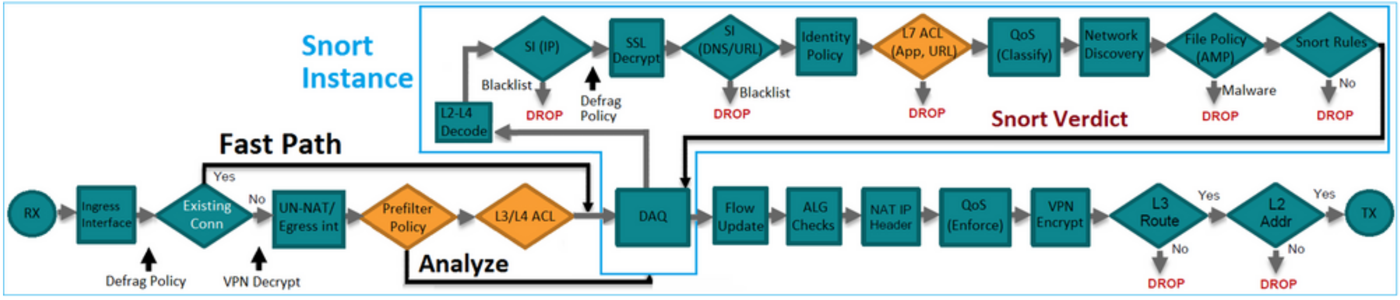
كيفية التفاعل بين سياسة ACP و Prefilter

تم إدخال نهج Prefilter في الإصدار 6.1 وهو يخدم غرضين رئيسيين:

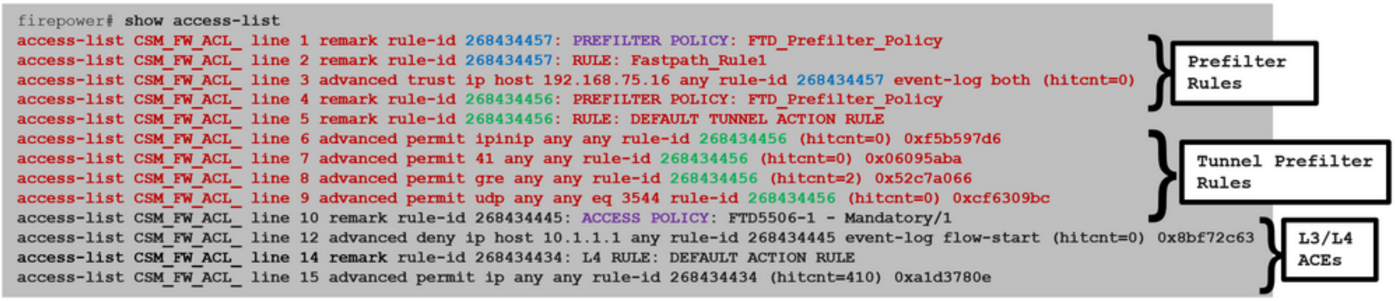
1. وهو يسمح بفحص حركة المرور النفقي حيث يقوم محرك FTD LINA بالتحقق من رأس IP الخارجي بينما يتحقق محرك الشخير من رأس IP الداخلي. وبشكل أكثر تحديدا، في حالة حركة المرور النفقي (على سبيل المثال GRE)، تعمل القواعد الموجودة في نهج عامل التصفية المسبق دائما على **outer headers**, بينما تسري القواعد الموجودة في قائمة التحكم بالوصول (ACP) دائما على الجلسات الداخلية **(inner headers)**. تشير حركة المرور النفقي إلى هذه البروتوكولات:

- GRE
- IP في IP
- IPv6-in-IP
- منفذ Teredo طراز 3544

2. وهو يوفر التحكم في الوصول المبكر (EAC) الذي يسمح للتدفق بتجاوز محرك الشخير بشكل كامل كما هو موضح في الصورة.



يتم نشر قواعد عامل التصفية الأولي على FTD على هيئة عناصر التحكم في الوصول (ACEs) إلى L3/L4 وتسبق إدخالات التحكم في الوصول (ACEs) التي تم تكوينها من المستوى الثالث/الرابع كما هو موضح في الصورة:

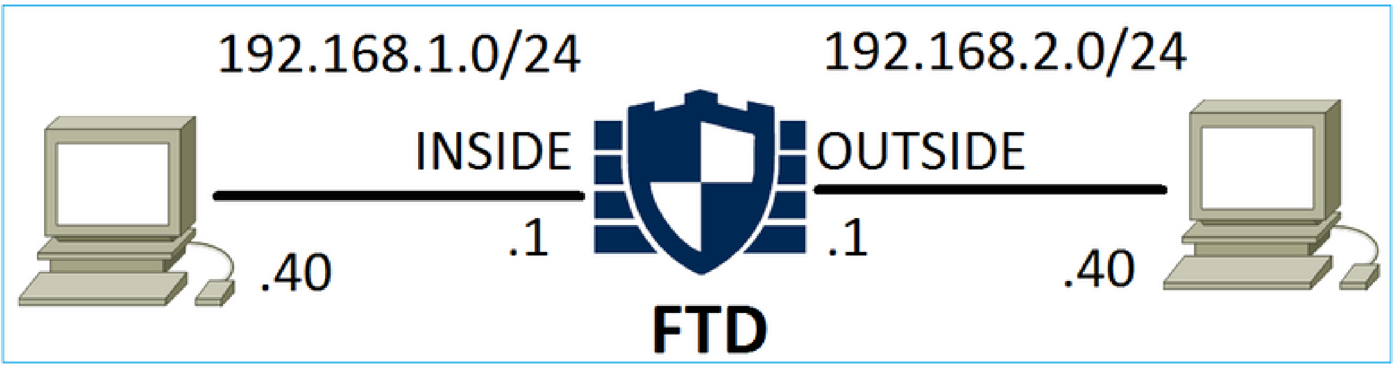


```
firepower# show access-list
access-list CSM_FW_ACL_ line 1 remark rule-id 268434457: PREFILTER POLICY: FTD_Prefilter_Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 268434457: RULE: Fastpath_Rule1
access-list CSM_FW_ACL_ line 3 advanced trust ip host 192.168.75.16 any rule-id 268434457 event-log both (hitcnt=0)
access-list CSM_FW_ACL_ line 4 remark rule-id 268434456: PREFILTER POLICY: FTD_Prefilter_Policy
access-list CSM_FW_ACL_ line 5 remark rule-id 268434456: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 6 advanced permit ipinip any any rule-id 268434456 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 7 advanced permit 41 any any rule-id 268434456 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 8 advanced permit gre any any rule-id 268434456 (hitcnt=2) 0x52c7a066
access-list CSM_FW_ACL_ line 9 advanced permit udp any any eq 3544 rule-id 268434456 (hitcnt=0) 0xcf6309bc
access-list CSM_FW_ACL_ line 10 remark rule-id 268434445: ACCESS POLICY: FTD5506-1 - Mandatory/1
access-list CSM_FW_ACL_ line 12 advanced deny ip host 10.1.1.1 any rule-id 268434445 event-log flow-start (hitcnt=0) 0x8bf72c63
access-list CSM_FW_ACL_ line 14 remark rule-id 268434434: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ line 15 advanced permit ip any any rule-id 268434434 (hitcnt=410) 0xa1d3780e
```

ملاحظة: يتم تطبيق قواعد ACP الخاصة ب PreFilter V/s = التطابق الأول.

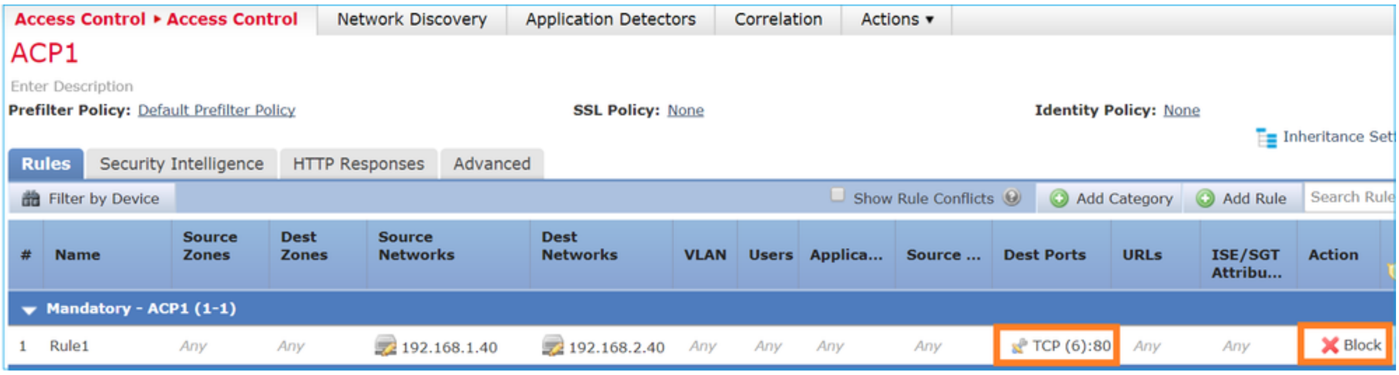
إجراء حظر ACP

ضع في الاعتبار المخطط المعروض في هذه الصورة:



السيناريو 1. قطرة الكتان المبكرة

تحتوي قائمة التحكم بالوصول (ACP) على قاعدة حظر تستخدم شرط L4 (غاية ميناء TCP 80) كما هو موضح في الصورة:



ACP1

Enter Description

Prefilter Policy: Default Prefilter Policy **SSL Policy:** None **Identity Policy:** None

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	TCP (6):80	Any	Any	✗ Block

السياسة المنشورة في Snort:

```
268435461 deny any 192.168.1.40 32 any any 192.168.2.40 32 80 any 6
```

نهج النشر في LINA. لاحظ أنه يتم دفع القاعدة ك **deny** الإجراء:

```
firepower# show access-list
…
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L4 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced deny tcp host 192.168.1.40 host 192.168.2.40 eq www
rule-id 268435461 event-log flow-start (hitcnt=0) 0x6149c43c
```

التحقق من السلوك:

عندما يحاول host-A (192.168.1.40) فتح جلسة HTTP إلى host-B (192.168.2.40) يتم إسقاط حزم مزامنة TCP (SYN) بواسطة محرك FTD LINA وتصل إلى محرك snort أو الوجهة:

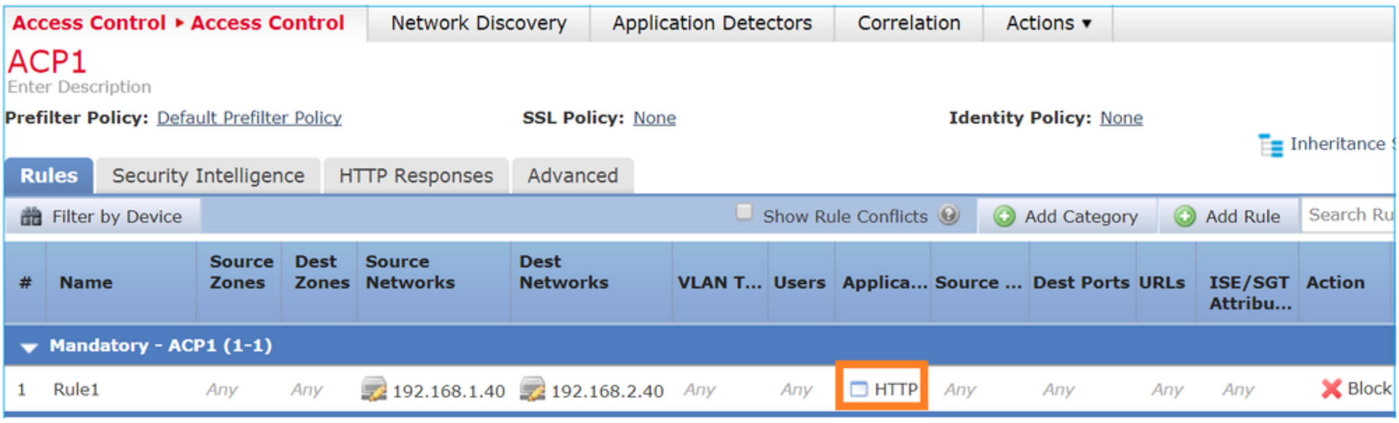
```
firepower# show capture
capture CAPI type raw-data buffer 33554432 trace trace-count 100 interface INSIDE [Capturing -
430 bytes]
  match ip host 192.168.1.40 any
capture CAPO type raw-data buffer 33554432 trace trace-count 100 interface OUTSIDE [Capturing -
0 bytes]
  match ip host 192.168.1.40 any
```

```
firepower# show capture CAPI
   1: 11:08:09.672801  192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4060517 0>
   2: 11:08:12.672435  192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4063517 0>
   3: 11:08:18.672847  192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4069517 0>
   4: 11:08:30.673610  192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4081517 0>
```

```
firepower# show capture CAPI packet-number 1 trace
   1: 11:08:09.672801  192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4060517 0>
...

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny tcp host 192.168.1.40 host 192.168.2.40 eq www rule-id
268435461 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268435461: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268435461: L4 RULE: Rule1
Additional Information:
                             <- No Additional Information = No Snort Inspection

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

السيناريو 2. إسقاط الحكم بسبب الشخير

تحتوي قائمة التحكم بالوصول (ACP) على قاعدة حظر تستخدم شرط L7 (تطبيق HTTP) كما هو موضح في الصورة:



Access Control ▸ Access Control | Network Discovery | Application Detectors | Correlation | Actions ▾

ACP1

Enter Description

Prefilter Policy: Default Prefilter Policy   SSL Policy: None   Identity Policy: None

Inheritance

Rules | Security Intelligence | HTTP Responses | Advanced

Filter by Device   □ Show Rule Conflicts   Add Category   Add Rule   Search Ru

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
▾ Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	HTTP	Any	Any	Any	Any	✗ Block

السياسة المنشورة في Snort:

```
268435461 deny any 192.168.1.40 32 any any 192.168.2.40 32 any any any  (appid 676:1)
```

AppID 676:1 = HTTP

نهج النشر في LINA.

> **ملاحظة**: يتم دفع القاعدة ك **permit** الإجراء لأن LINA لا يمكنه تحديد أن الجلسة تستخدم HTTP. في FTD، توجد آلية اكتشاف التطبيقات في محرك snort.

```
firepower# show access-list
…
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L7 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435461 (hitcnt=0) 0xb788b786
```

لقاعدة حظر تستخدم **Application** كشرط، يظهر تتبع الحزمة الحقيقية أن الجلسة سقطت من قبل LINA بسبب الحكم محرك الشخير.

> **ملاحظة**: لتحديد التطبيق، يجب على محرك الشخير فحص بعض الحزم (عادة من 3 إلى 10 التي تعتمد على أداة فك الترميز للتطبيق). وبالتالي يتم السماح ببضع حزم من خلال FTD وتجعلها تصل إلى الوجهة. لا تزال الحزم المسموح بها تخضع لفحص "سياسة التسلل" استنادا إلى **Access Policy > Advanced > 'Intrusion Policy used before Access Control rule is determined'** خيار.

التحقق من السلوك:

عندما يحاول المضيف-A (192.168.1.40) إنشاء جلسة عمل HTTP مع المضيف-B (192.168.2.40) يظهر التقاط مدخل LINA:

```
firepower# show capture CAPI
```

```
8 packets captured

   1: 11:31:19.825564  192.168.1.40.32790 > 192.168.2.40.80: S 357753151:357753151(0) win 2920
<mss 1460,sackOK,timestamp 5450579 0>
   2: 11:31:19.826403  192.168.2.40.80 > 192.168.1.40.32790: S 1283931030:1283931030(0) ack
357753152 win 2896 <mss 1380,sackOK,timestamp 5449236 5450579>
   3: 11:31:19.826556  192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5450580 5449236>
   4: 11:31:20.026899  192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5450781 5449236>
   5: 11:31:20.428887  192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5451183 5449236>
 ...
```

أسر المخرج:

```
firepower# show capture CAPO

5 packets captured

   1: 11:31:19.825869  192.168.1.40.32790 > 192.168.2.40.80: S 1163713179:1163713179(0) win 2920
<mss 1380,sackOK,timestamp 5450579 0>
   2: 11:31:19.826312  192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5449236 5450579>
   3: 11:31:23.426049  192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5452836 5450579>
   4: 11:31:29.426430  192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5458836 5450579>
   5: 11:31:41.427208  192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5470836 5450579>
```

يظهر التتبع أن الحزمة الأولى (TCP SYN) مسموح بها من قبل الشورت نظرا لأنه لم يتم الوصول إلى قرار اكتشاف التطبيق بعد:

```
firepower# show capture CAPI packet-number 1 trace
   1: 11:31:19.825564  192.168.1.40.32790 > 192.168.2.40.80: S 357753151:357753151(0) win 2920
<mss 1460,sackOK,timestamp 5450579 0>
...

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435461
access-list CSM_FW_ACL_ remark rule-id 268435461: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268435461: L7 RULE: Rule1
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will be reached
...
Phase: 10
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 23194, packet dispatched to next module
…
```

```
Phase: 12
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: TCP, SYN, seq 357753151
AppID: service unknown (0), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 0, icmpCode 0
Firewall: pending rule-matching, id 268435461, pending AppID
NAP id 1, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet

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

نفس الشيء لحزمة TCP syn/ACK:

```
firepower# show capture CAPO packet-number 2 trace
   2: 11:31:19.826312 192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5449236 5450579>
…

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found flow with id 23194, using existing flow
…

Phase: 5
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: TCP, SYN, ACK, seq 1283931030, ack 357753152
AppID: service unknown (0), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 0, icmpCode 0
Firewall: pending rule-matching, id 268435461, pending AppID
NAP id 1, 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: INSIDE
output-status: up
output-line-status: up
```

```
Action: allow
```

يقوم الشخير بإرجاع الحكم الصادر في DROP بمجرد اكتمال فحص الحزمة الثالثة:

```
firepower# show capture CAPI packet-number 3 trace
   3: 11:31:19.826556  192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5450580 5449236>

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found flow with id 23194, using existing flow

Phase: 5
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: TCP, ACK, seq 357753152, ack 1283931031
AppID: service HTTP (676), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0(0) -> 0, vlan 0, sgt 65535, user 9999997,
url http://192.168.2.40/128k.html
Firewall: block rule, id 268435461, drop
Snort: processed decoder alerts or actions queue, drop
NAP id 1, IPS id 0, Verdict BLOCKLIST, Blocked by Firewall
Snort Verdict: (block-list) block list this flow

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
Action: drop
Drop-reason: (firewall) Blocked by the firewall preprocessor
```

يمكنك أيضا تشغيل الأمر **system support trace** من وضع FTD CLISH. توفر هذه الأداة دالتين:

- إظهار الحكم على الشخر لكل حزمة عند إرسالها إلى مكتبة الحصول على البيانات (DAQ) ورأيتها في LINA. DAQ هو مكون يقع بين محرك FTD LINA ومحرك الشخير
- يسمح بالتشغيل **system support firewall-engine-debug** في نفس الوقت لرؤية ما يحدث داخل محرك الشخير نفسه

هنا هو المخرج:

```
> system support trace

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.1.40
Please specify a client port:
Please specify a server IP address: 192.168.2.40
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

Tracing enabled by Lina
```

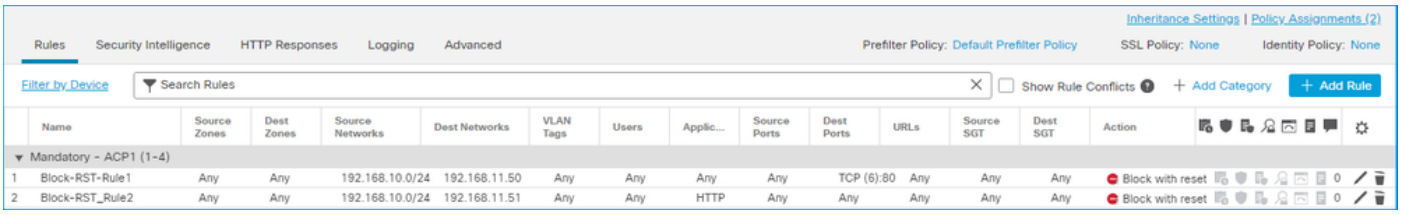
```
192.168.2.40-80 - 192.168.1.40-32791 6 Packet: TCP, SYN, seq 2620409313
192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 New session
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', and SrcZone
first with zones -1 -> -1, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0,
payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 ->
0, vlan 0, sgt 65535, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 pending rule order 2, 'Rule1', AppID
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: pending rule-matching, 'Rule1', pending AppID
192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
Trace buffer and verdict reason are sent to DAQ's PDTS

Tracing enabled by Lina
192.168.2.40-80 - 192.168.1.40-32791 6 Packet: TCP, SYN, ACK, seq 3700371680, ack 2620409314
192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', and SrcZone
first with zones -1 -> -1, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0,
payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 ->
0, vlan 0, sgt 65535, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 pending rule order 2, 'Rule1', AppID
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: pending rule-matching, 'Rule1', pending AppID
192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
Trace buffer and verdict reason are sent to DAQ's PDTS

Tracing enabled by Lina
192.168.2.40-80 - 192.168.1.40-32791 6 Packet: TCP, ACK, seq 2620409314, ack 3700371681
192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service HTTP (676), application unknown (0)
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', and SrcZone
first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc
676, payload 0, client 686, misc 0, user 9999997, url http://192.168.2.40/128k.html, xff
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0(0)
-> 0, vlan 0, sgt 65535, user 9999997, url http://192.168.2.40/128k.html
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 match rule order 2, 'Rule1', action Block
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 deny action
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: block rule, 'Rule1', drop
192.168.1.40-32791 > 192.168.2.40-80 6 Snort: processed decoder alerts or actions queue, drop
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Deleting session
192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict BLOCKLIST
192.168.1.40-32791 > 192.168.2.40-80 6 ===> Blocked by Firewall
```

ملخص

- يتم نشر "إجراء حظر قائمة التحكم في الوصول (ACP)" كقاعدة السماح أو الرفض في LINA التي تعتمد على شروط القاعدة
- إذا كانت الشروط من L3/L4، فعندئذ يقوم LINA بحظر الحزمة. في حالة TCP، يتم حظر الحزمة الأولى (TCP SYN)
- إذا كانت الشروط هي L7 فيتم إعادة توجيه الحزمة إلى محرك snort لمزيد من الفحص. في حالة TCP، يتم السماح ببضعة حزم من خلال FTD حتى يصل الشخر إلى قرار. لا تزال الحزم المسموح بها تخضع لفحص "سياسة التسلل" استنادا إلى **Access Policy > Advanced > 'Intrusion Policy used before Access Control rule is determined'** خيار.

كتلة ACP مع إجراء إعادة الضبط

تم تكوين كتلة مع قاعدة الراحة على واجهة مستخدم FMC:



Inheritance Settings | Policy Assignments (2)

Rules | Security Intelligence | HTTP Responses | Logging | Advanced

Prefilter Policy: Default Prefilter Policy   SSL Policy: None   Identity Policy: None

Filter by Device   Search Rules   □ Show Rule Conflicts   + Add Category   + Add Rule

	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action		
▼ Mandatory - ACP1 (1-4)																
1	Block-RST-Rule1	Any	Any	192.168.10.0/24	192.168.11.50	Any	Any	Any	Any	TCP (6):80	Any	Any	Any	Block with reset	0	
2	Block-RST_Rule2	Any	Any	192.168.10.0/24	192.168.11.51	Any	Any	HTTP	Any	Any	Any	Any	Any	Block with reset	0	

يتم نشر كتلة قاعدة إعادة التعيين على محرك FTD LINA ك **permit** و إلى محرك الشخير ك **reset** القاعدة:

```
firepower# show access-list
…
access-list CSM_FW_ACL_ line 10 advanced permit tcp 192.168.10.0 255.255.255.0 host
192.168.11.50 eq www rule-id 268438864 (hitcnt=0) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268438865: L7 RULE: Block-RST_Rule2
access-list CSM_FW_ACL_ line 13 advanced permit ip 192.168.10.0 255.255.255.0 host 192.168.11.51
rule-id 268438865 (hitcnt=0) 0x622350d0
```

محرك الشخير:

```
admin@firepower:~$ cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules
…
# Start of AC rule.
268438864 reset any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6
# End rule 268438864
268438865 reset any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1)
(ip_protos 6, 17)
# End rule 268438865
```

عندما تطابق الحزمة الكتلة مع قاعدة إعادة ضبط يرسل FTD **TCP Reset** الحزمة أو **ICMP Type 3 Code 13** رسالة الوجهة التي يتعذر الوصول إليها (تمت تصفيتها إداريا):

```
root@kali:~/tests# wget 192.168.11.50/file1.zip
--2020-06-20 22:48:10--  http://192.168.11.50/file1.zip
Connecting to 192.168.11.50:80... failed: Connection refused.
```

وفيما يلي التقاط على واجهة مدخل FTD:

```
firepower# show capture CAPI
2 packets captured
1: 21:01:00.977259 802.1Q vlan#202 P0 192.168.10.50.41986 > 192.168.11.50.80: S
3120295488:3120295488(0) win 29200 <mss 1460,sackOK,timestamp 3740873275 0,nop,wscale 7>
2: 21:01:00.978114 802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.41986: R 0:0(0) ack
3120295489 win 0 2 packets shown
```

System support trace يظهر الإخراج، في هذه الحالة، أن الحزمة سقطت بسبب حكم الشخر:

```
> system support trace

Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.50
Please specify a client port:
```

```
Please specify a server IP address: 192.168.11.50
Please specify a server port:
Monitoring packet tracer and firewall debug messages


192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 3387496622
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 new firewall session
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 using HW or preset rule order 2, 'Block-RST-
Rule1', action Reset and prefilter rule 0
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 HitCount data sent for rule id: 268438864,
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 reset action
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 deleting firewall session flags = 0x0,
fwFlags = 0x0
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: block w/ reset rule, 'Block-RST-
Rule1', drop
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions
queue, drop
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 9, NAP id 1, IPS id 0, Verdict
BLOCKLIST
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 ===> Blocked by Firewall
Verdict reason is sent to DAQ
```

حالات الاستخدام

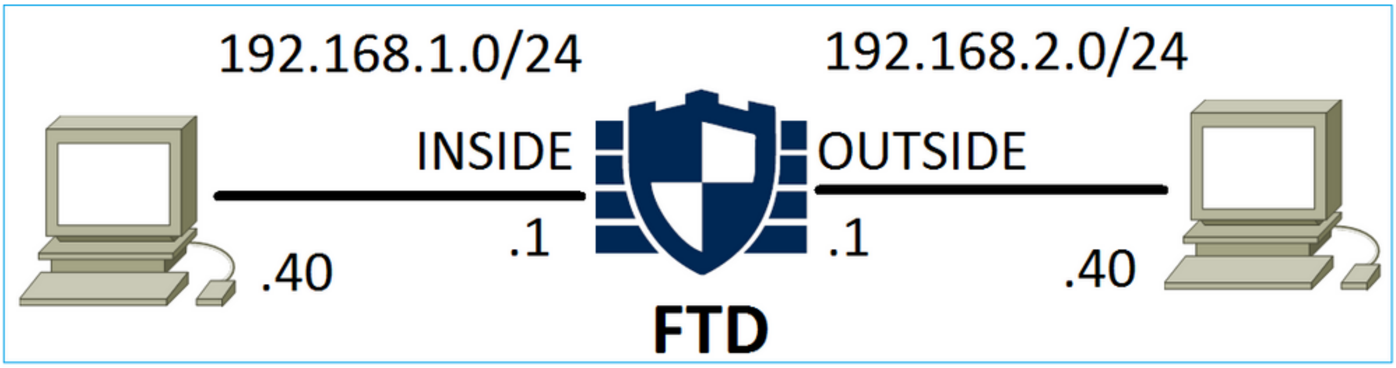
نفس **Block** إجراء، ولكنه ينهي الاتصال فورا.

إجراء السماح ل ACP

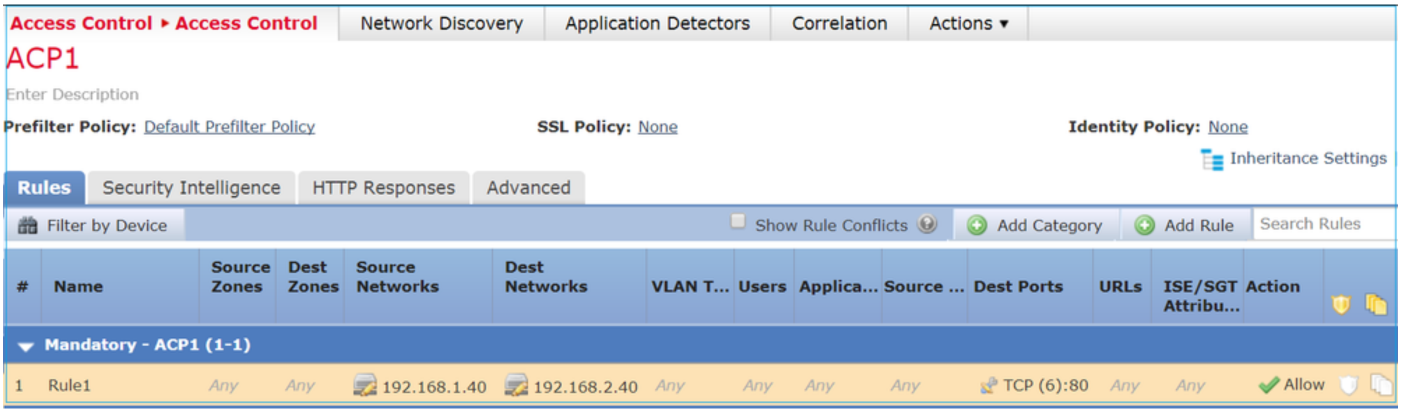
السيناريو 1. إجراء السماح ل ACP (شروط L3/L4)

عادة، تقوم بتكوين قاعدة السماح لتحديد عمليات فحص إضافية مثل نهج التسلل و/أو نهج الملف. يوضح هذا السيناريو الأول تشغيل قاعدة السماح عند تطبيق شرط L3/L4.

ضع في حسبانك هذا المخطط كما هو موضح في الصورة:



يتم تطبيق هذا النهج كما هو موضح في الصورة:



Access Control ▸ Access Control | Network Discovery | Application Detectors | Correlation | Actions ▾

ACP1

Enter Description

Prefilter Policy: Default Prefilter Policy   SSL Policy: None   Identity Policy: None

Inheritance Settings

Rules | Security Intelligence | HTTP Responses | Advanced

Filter by Device   □ Show Rule Conflicts   Add Category   Add Rule   Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	TCP (6):80	Any	Any	✓ Allow

السياسة المنشورة في Snort. لاحظ أنه يتم نشر القاعدة ك **allow** الإجراء:

```
# Start of AC rule.
268435461 allow any 192.168.1.40 32 any any 192.168.2.40 32 80 any 6
```

السياسة في لينا.

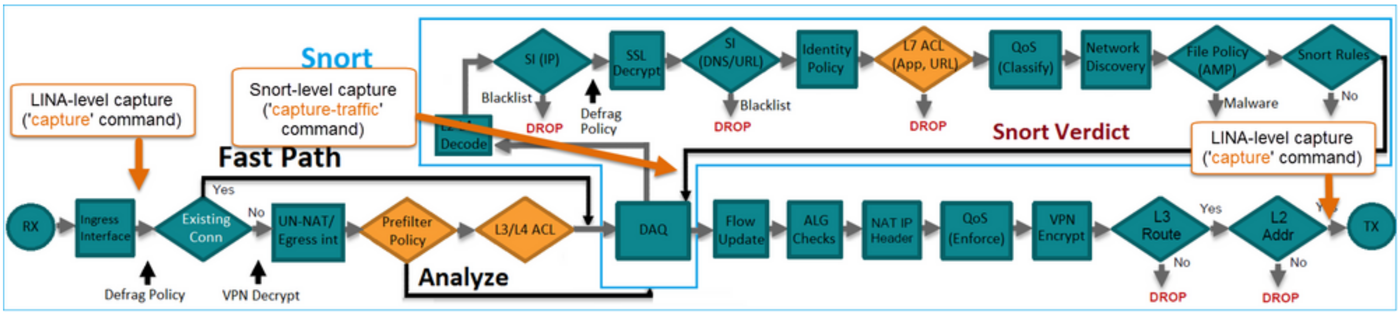
> **ملاحظة**: يتم نشر القاعدة ك **permit** فعل يعني أساسا إعادة التوجيه إلى الشورت لمزيد من التفتيش.

```
firepower# show access-list
…
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L7 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced permit tcp host 192.168.1.40 host 192.168.2.40 eq www
rule-id 268435461 (hitcnt=1) 0x641a20c3
```

لمعرفة كيفية معالجة FTD لتدفق يطابق قاعدة السماح، هناك عدة طرق:

- التحقق من إحصائيات الشخير
- باستخدام أداة CLISH لتتبع دعم النظام
- مع إستخدام الالتقاط مع خيار التتبع في LINA واختياريا مع التقاط حركة مرور البيانات في محرك الشبكة

التقاط LINA مقابل حركة مرور بيانات الشخير:



التحقق من السلوك:

مسح إحصائيات الشخر، تمكين **system support trace** from CLISH, and initiate an HTTP flow from host-A (192.168.1.40) to host-B (192.168.2.40). All the packets are forwarded to the Snort engine and get the PASS verdict by the Snort:

```
firepower# clear snort statistics

> system support trace

Please specify an IP protocol:
Please specify a client IP address: 192.168.1.40
Please specify a client port:
Please specify a server IP address: 192.168.2.40
Please specify a server port:
Enable firewall-engine-debug too? [n]:
Monitoring packet tracer debug messages

Tracing enabled by Lina
192.168.2.40-80 - 192.168.1.40-32797 6 Packet: TCP, SYN, seq 361134402
192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow
192.168.1.40-32797 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
Trace buffer and verdict reason are sent to DAQ's PDTS

Tracing enabled by Lina
192.168.2.40-80 - 192.168.1.40-32797 6 Packet: TCP, SYN, ACK, seq 1591434735, ack 361134403
192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow
192.168.1.40-32797 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
Trace buffer and verdict reason are sent to DAQ's PDTS

Tracing enabled by Lina
192.168.2.40-80 - 192.168.1.40-32797 6 Packet: TCP, ACK, seq 361134403, ack 1591434736
192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service HTTP (676), application unknown (0)
192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow
192.168.1.40-32797 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
```

تزداد عدادات حزم المرور:

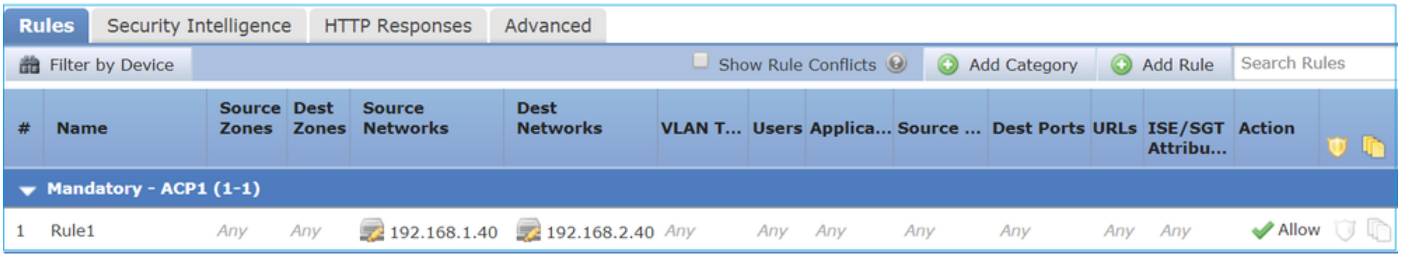
```
> show snort statistics

Packet Counters:
  Passed Packets                                                  54
  Blocked Packets                                                  0
  Injected Packets                                                 0
  Packets bypassed (Snort Down)                                    0
  Packets bypassed (Snort Busy)                                    0

Flow Counters:
  Fast-Forwarded Flows                                             0
  Blocklisted Flows                                                0
...
```

الحزم التي تم تمريرها = تم فحصها بواسطة محرك الشخير

السيناريو 2. إجراء السماح ل ACP (شروط L3-7)

ويتم ملاحظة سلوك مماثل عند نشر قاعدة "السماح" كما يلي.

شرط L3/L4 فقط كما هو موضح في الصورة:

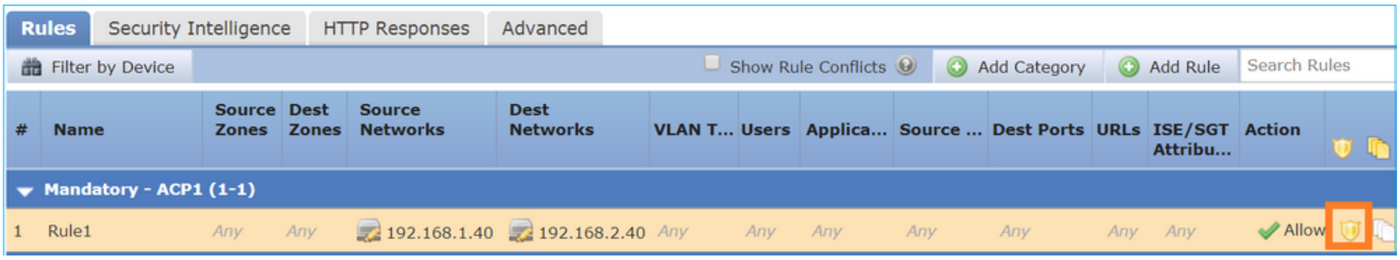


Rules | Security Intelligence | HTTP Responses | Advanced

Filter by Device □ Show Rule Conflicts Add Category Add Rule Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
▼ Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	Any	Any	Any	✓ Allow

يتم عرض شرط L7 (على سبيل المثال، سياسة التطفل ونهج الملف والتطبيق وما إلى ذلك) في الصورة:



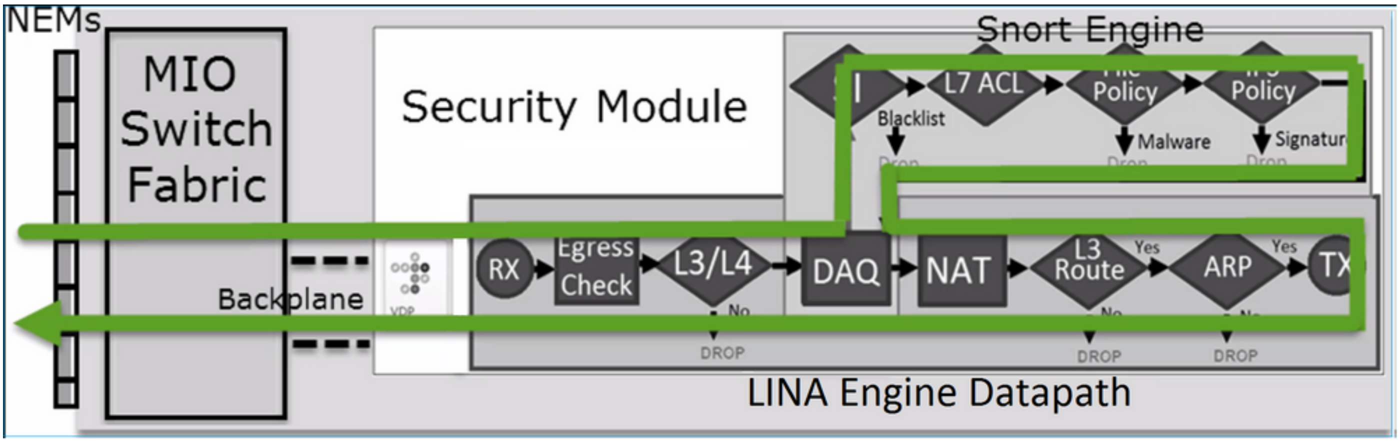
Rules | Security Intelligence | HTTP Responses | Advanced

Filter by Device □ Show Rule Conflicts Add Category Add Rule Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
▼ Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	Any	Any	Any	✓ Allow

ملخص

من أجل التلخيص، هذه هي الطريقة التي تتم بها معالجة تدفق ما بواسطة FTD الذي يتم نشره على FP4100/9300 عندما تتم مطابقة قاعدة السماح كما هو موضح في الصورة:



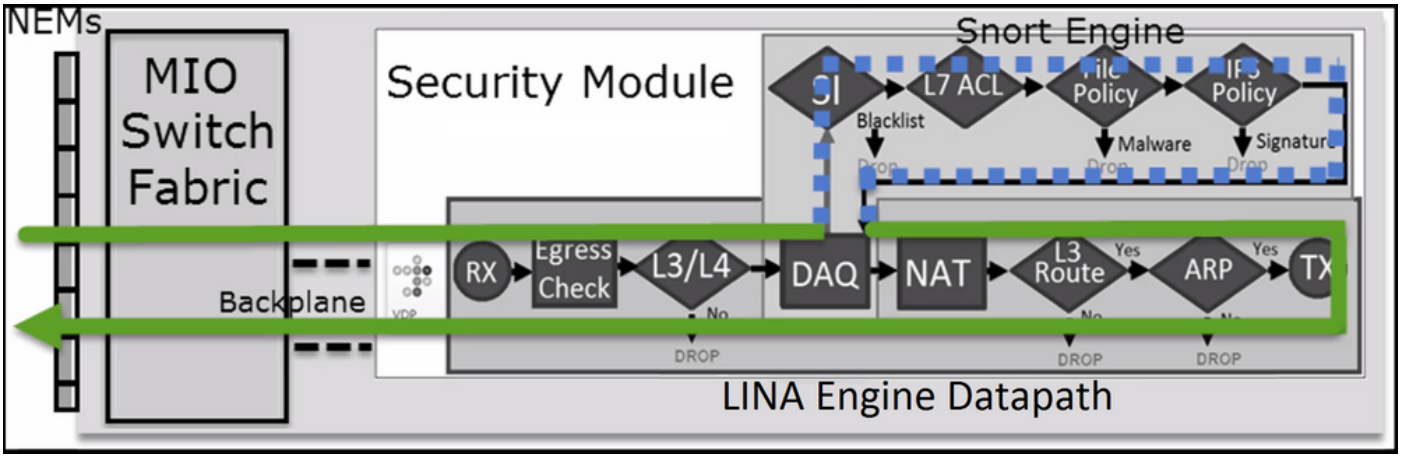
ملاحظة: يقصد ب Management Input Output (MIO) المحرك المشرف لهيكل FirePOWER.

السيناريو 3. إعادة توجيه الحكم بسرعة مع السماح

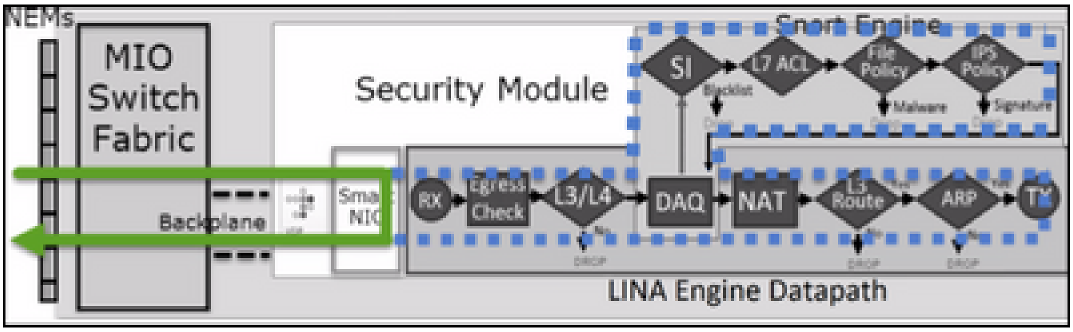
هناك سيناريوهات محددة حيث يعطي محرك FTD Snort حكما لقائمة التحكم (بشكل سريع للأمام) ويتم تحميل باقي التدفق إلى محرك LINA (في بعض الحالات، يتم إلغاء تحميله إلى مسرع HW - SmartNIC). وهذه هي:

1. حركة مرور SSL دون تكوين نهج SSL
2. تجاوز التطبيقات الذكية (IAB)

هذا هو التمثيل البصري من الربط ممر:



أو في بعض الحالات:



النقاط الأساسية

- يتم نشر قاعدة السماح ك **allow** في سنورت و **permit** في لينا
- في معظم الحالات، تتم إعادة توجيه جميع حزم الجلسة إلى محرك الشخر من أجل فحص إضافي

حالات الاستخدام

يمكنك تكوين قاعدة السماح عندما تحتاج إلى فحص L7 بواسطة محرك الشخير مثل:

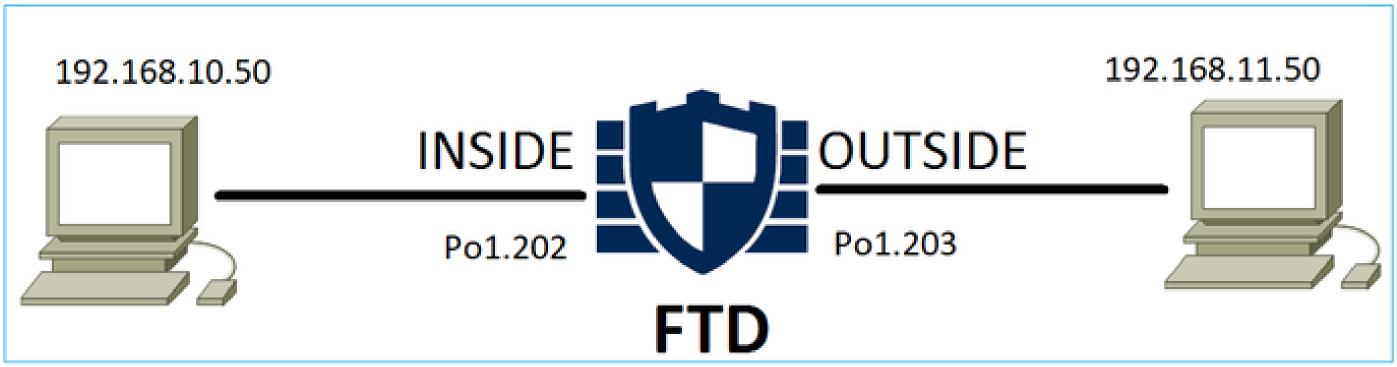
- سياسة الاقتحام
- نهج الملف

إجراءات الثقة الخاصة ب ACP

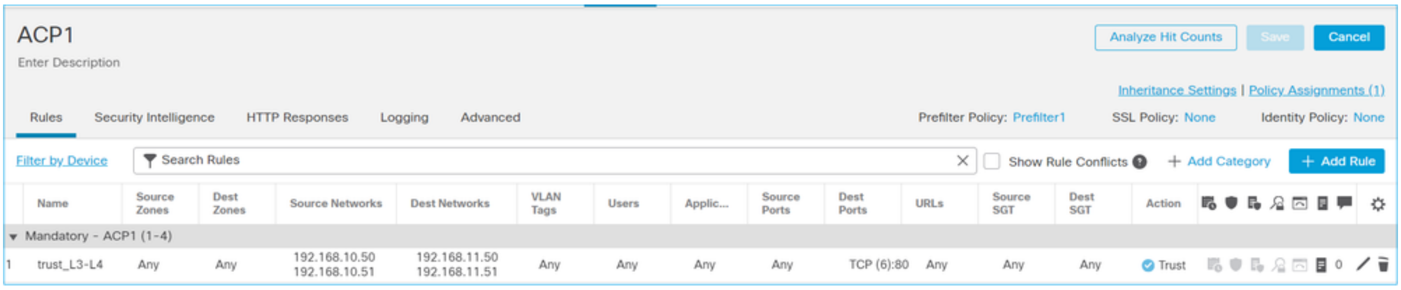
السيناريو 1. إجراءات الثقة الخاصة ب ACP

إذا لم تكن ترغب في تطبيق فحص L7 المتقدم على مستوى الشبكة (على سبيل المثال، نهج التطفل ونهج الملفات واكتشاف الشبكة)، لكنك لا تزال ترغب في إستخدام ميزات مثل ذكاء الأمان (SI) ونهج الهوية وجودة الخدمة (QoS) وما إلى ذلك، يوصى باستخدام إجراء الثقة في قاعدتك.

الطوبولوجيا:



النهج الذي تم تكوينه:



Prefilter Policy: Prefilter1 SSL Policy: None Identity Policy: None

	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action
▾ Mandatory - ACP1 (1-4)														
1	trust_L3-L4	Any	Any	192.168.10.50 192.168.10.51	192.168.11.50 192.168.11.51	Any	Any	Any	Any	TCP (6):80	Any	Any	Any	✓ Trust

قاعدة الثقة عند نشرها في محرك تنصت FTD:

```
# Start of AC rule.
268438858 fastpath any 192.168.10.50 31 any any 192.168.11.50 31 80 any 6 (log dcforward
flowend)
```

> **ملاحظة**: الرقم 6 هو البروتوكول (TCP).

القاعدة في FTD LINA:

```
firepower# show access-list | i 268438858
access-list CSM_FW_ACL_ line 17 remark rule-id 268438858: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 18 remark rule-id 268438858: L7 RULE: trust_L3-L4
access-list CSM_FW_ACL_ line 19 advanced permit tcp object-group FMC_INLINE_src_rule_268438858
object-group FMC_INLINE_dst_rule_268438858 eq www rule-id 268438858 (hitcnt=19) 0x29588b4f
  access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.50 host 192.168.11.50 eq
www rule-id 268438858 (hitcnt=19) 0x9d442895
  access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.50 host 192.168.11.51 eq
www rule-id 268438858 (hitcnt=0) 0xd026252b
  access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.51 host 192.168.11.50 eq
www rule-id 268438858 (hitcnt=0) 0x0d785cc4
  access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.51 host 192.168.11.51 eq
www rule-id 268438858 (hitcnt=0) 0x3b3234f1
```

التحقق:

تمكين **system support trace** وبدء جلسة HTTP من المضيف-A (192.168.10.50) إلى المضيف-B (192.168.11.50). توجد 3 حزم تمت إعادة توجيهها إلى محرك الشبكة. يرسل محرك الشوكة إلى LINA الحكم لقائمة التحكم الذي يقوم أساسا بإلغاء تحميل بقية التدفق إلى محرك LINA:

```
> system support trace

Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.50
Please specify a client port:
Please specify a server IP address: 192.168.11.50
Please specify a server port: 80
Monitoring packet tracer and firewall debug messages

192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 453426648
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 new firewall session
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 using HW or preset rule order 5, 'trust_L3-
L4', action Trust and prefilter rule 0
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 HitCount data sent for rule id: 268438858,
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-
L4', allow
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0, Verdict
PASS

192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Packet: TCP, SYN, ACK, seq 2820426532, ack
453426649
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-
L4', allow
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0, Verdict
PASS

192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 453426649, ack
2820426533
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-
L4', allow
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0, Verdict
PERMITLIST
```

بمجرد إنهاء الاتصال، يحصل مشغل snort على معلومات بيانات التعريف من محرك LINA ويحذف الجلسة:

```
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 Got end of flow event from hardware with
flags 00010001. Rule Match Data: rule_id 0, rule_action 0 rev_id 0, rule_flags 3
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 Logging EOF for event from hardware with
rule_id = 268438858 ruleAction = 3 ruleReason = 0
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 : Received EOF, deleting the snort session.

192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: deleting snort session, reason:
timeout
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 deleting firewall session flags = 0x10003,
fwFlags = 0x1115
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: deleted snort session using 0
bytes; protocol id:(-1) : LWstate 0xf LWFlags 0x6007
```

يعرض التقاط الشخير الحزم الثلاثة التي تنتقل إلى محرك الشخير:

```
> capture-traffic

Please choose domain to capture traffic from:
  0 - management0
  1 - management1
  2 - Global

Selection? 2

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: -n vlan and (host 192.168.10.50 and host 192.168.11.50)
10:26:16.525928 IP 192.168.10.50.42144 > 192.168.11.50.80: Flags [S], seq 3065553465, win 29200,
options [mss 1380,sackOK,TS val 3789188468 ecr 0,nop,wscale 7], length 0
10:26:16.525928 IP 192.168.11.50.80 > 192.168.10.50.42144: Flags [S.], seq 3581351172, ack
3065553466, win 8192, options [mss 1380,nop,wscale 8,sackOK,TS val 57650410 ecr 3789188468],
length 0
10:26:16.525928 IP 192.168.10.50.42144 > 192.168.11.50.80: Flags [.], ack 1, win 229, options
[nop,nop,TS val 3789188470 ecr 57650410], length 0
```

يظهر التقاط LINA التدفق الذي يمر خلاله:

```
firepower# show capture CAPI

437 packets captured

   1: 09:51:19.431007  802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: S
2459891187:2459891187(0) win 29200 <mss 1460,sackOK,timestamp 3787091387 0,nop,wscale 7>
   2: 09:51:19.431648  802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: S
2860907367:2860907367(0) ack 2459891188 win 8192 <mss 1380,nop,wscale 8,sackOK,timestamp
57440579 3787091387>
   3: 09:51:19.431847  802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: . ack
2860907368 win 229 <nop,nop,timestamp 3787091388 57440579>
   4: 09:51:19.431953  802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: P
2459891188:2459891337(149) ack 2860907368 win 229 <nop,nop,timestamp 3787091388 57440579>
   5: 09:51:19.444816  802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: .
2860907368:2860908736(1368) ack 2459891337 win 256 <nop,nop,timestamp 57440580 3787091388>
   6: 09:51:19.444831  802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: .
2860908736:2860910104(1368) ack 2459891337 win 256 <nop,nop,timestamp 57440580 3787091388>

…
```

تتبع الحزم من LINA هو طريقة أخرى لرؤية أحكام الشخير. حصلت الحزمة الأولى على حكم المرور:

```
firepower# show capture CAPI packet-number 1 trace | i Type|Verdict
Type: CAPTURE
Type: ACCESS-LIST
Type: ROUTE-LOOKUP
Type: ACCESS-LIST
Type: CONN-SETTINGS
Type: NAT
Type: NAT
Type: IP-OPTIONS
Type: CAPTURE
Type: CAPTURE
Type: NAT
Type: CAPTURE
Type: NAT
```

```
Type: IP-OPTIONS
Type: CAPTURE
Type: FLOW-CREATION
Type: EXTERNAL-INSPECT
Type: SNORT
Snort id 22, NAP id 2, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Type: ADJACENCY-LOOKUP
Type: CAPTURE
```

تتبع حزمة TCP SYN/ACK على الواجهة الخارجية:

```
firepower# show capture CAPO packet-number 2 trace | i Type|Verdict
Type: CAPTURE
Type: ACCESS-LIST
Type: FLOW-LOOKUP
Type: EXTERNAL-INSPECT
Type: SNORT
Snort id 22, NAP id 2, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Type: ADJACENCY-LOOKUP
Type: CAPTURE
```

يحصل TCP ACK على حكم قائمة السماح:

```
firepower# show capture CAPI packet-number 3 trace | i Type|Verdict
Type: CAPTURE
Type: ACCESS-LIST
Type: FLOW-LOOKUP
Type: EXTERNAL-INSPECT
Type: SNORT
Snort id 22, NAP id 2, IPS id 0, Verdict PERMITLIST
Snort Verdict: (fast-forward) fast forward this flow
Type: CAPTURE
```

هذا هو الناتج الكامل من الحكم على النقش (الحزمة #3)

```
firepower# show capture CAPI packet-number 3 trace | b Type: SNORT
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: TCP, ACK, seq 687485179, ack 1029625865
AppID: service unknown (0), application unknown (0)
Firewall: trust/fastpath rule, id 268438858, allow
Snort id 31, NAP id 2, IPS id 0, Verdict PERMITLIST
Snort Verdict: (fast-forward) fast forward this flow
```

لم تتم إعادة توجيه الحزمة الرابعة إلى محرك الشبكة نظرا لأن الحكم تم تخزينه مؤقتا بواسطة محرك LINA:

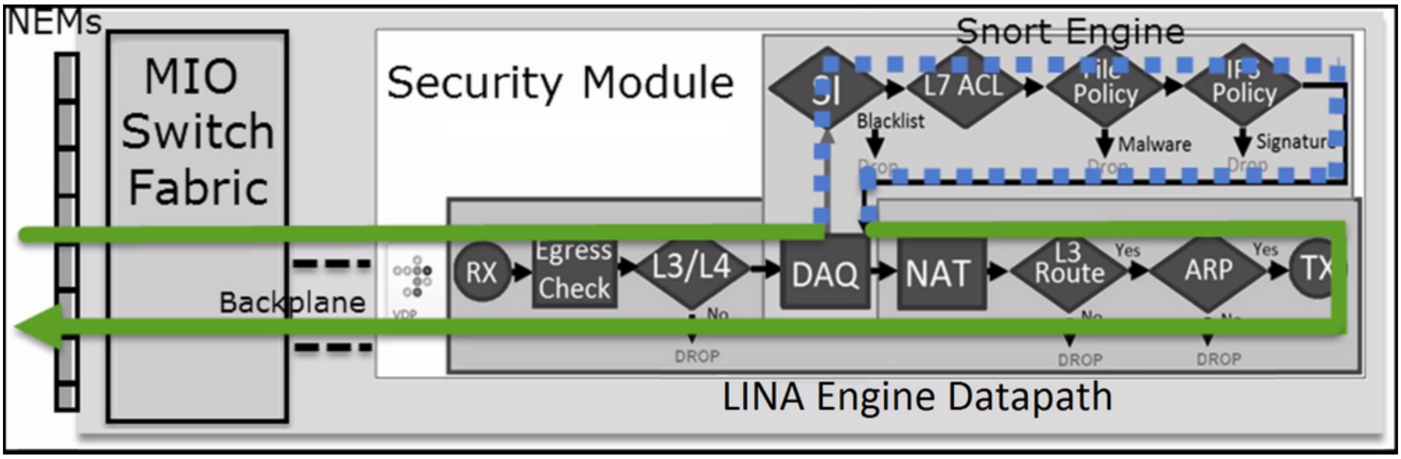
```
firepower# show capture CAPI packet-number 4 trace

441 packets captured

   4: 10:34:02.741523       802.1Q vlan#202 P0 192.168.10.50.42158 > 192.168.11.50.80: P
164375589:164375738(149) ack 3008397532 win 229 <nop,nop,timestamp 3789654678 57697031>
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 1254, using existing flow

Phase: 4
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (fast-forward) fast forward this flow

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
Action: allow


1 packet shown
```

تؤكد إحصاءات الشخير ما يلي:

```
firepower# show snort statistics

Packet Counters:
  Passed Packets                                                      2
  Blocked Packets                                                     0
  Injected Packets                                                    0
  Packets bypassed (Snort Down)                                       0
  Packets bypassed (Snort Busy)                                       0

Flow Counters:
  Fast-Forwarded Flows                                                1
  Blacklisted Flows                                                   0
```

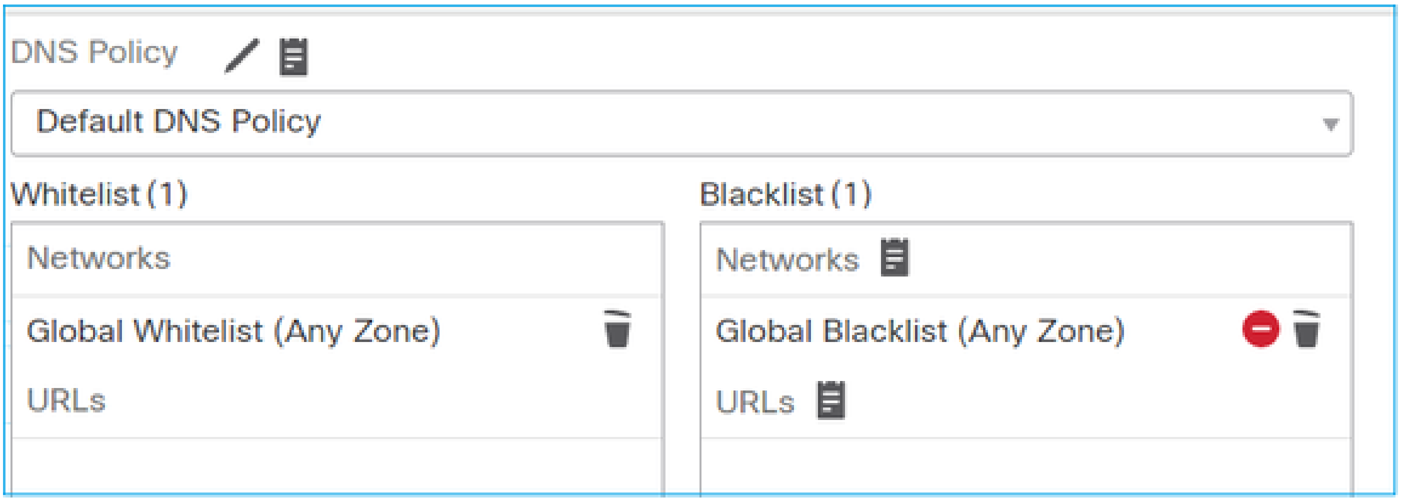
```
Miscellaneous Counters:
  Start-of-Flow events                                            0
  End-of-Flow events                                              1
  Denied flow events                                              0
  Frames forwarded to Snort before drop                           0
  Inject packets dropped                                          0
```

تدفق الحزمة باستخدام قاعدة الثقة. يتم فحص بعض الحزم بواسطة الشورت ويتم فحص الباقي بواسطة LINA:



السيناريو 2. ACP Trust Action (بدون SI، و QoS، و Identity Policy)

في حالة ما إذا كنت تريد من FTD تطبيق تحققات ذكاء الأمان (SI) على جميع التدفقات، يتم تمكين SI بالفعل على مستوى ACP ويمكنك تحديد مصادر SI (TALOS، موجز الويب، القوائم، وما إلى ذلك). من ناحية أخرى، في حالة رغبتك في تعطيله، تقوم بتعطيل SI للشبكات بشكل عام لكل ACP، SI ل URL، و SI ل DNS. يتم تعطيل SI للشبكات و URL كما هو موضح في الصورة:



DNS Policy

Default DNS Policy

Whitelist (1)

Networks

Global Whitelist (Any Zone)

URLs

Blacklist (1)

Networks

Global Blacklist (Any Zone)

URLs

في هذه الحالة، يتم نشر قاعدة الضمان إلى LINA كثقة:

```
> show access-list
...
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L4 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced trust ip host 192.168.1.40 host 192.168.2.40 rule-id
268435461 event-log flow-end (hitcnt=0) 0x5c1346d6
```

ملاحظة: اعتبارا من تاريخ 6.2.2، كان FTD يدعم TID. يعمل TID بطريقة مماثلة ل SI، ولكن في حالة تعطيل SI، فإنه لا "يفرض" إعادة توجيه الحزمة إلى محرك snort لفحص TID.

التحقق من السلوك

ابدأ جلسة HTTP من المضيف-A (192.168.1.40) إلى المضيف-B (192.168.2.40). بما أن هذا هو FP4100 ويدعم إلغاء التحميل المتدفق في الأجهزة، فإن هذه الأمور تحدث:

- تتم إعادة توجيه بعض الحزم من خلال محرك FTD LINA ويتم إلغاء تحميل باقي التدفق إلى SmartNIC (مسرع الأجهزة)
- لا تتم إعادة توجيه أي حزم إلى محرك الشبكة

لاحظ جدول اتصال FTD LINA العلامة ‘o هذا يعني أنه تم تفريغ التدفق إلى الأجهزة. أيضا، لاحظ غياب ‘N علم |||ي. وهذا يعني في الأساس "عدم إعادة توجيه الشخير":

```
firepower# show conn
1 in use, 15 most used

TCP OUTSIDE  192.168.2.40:80 INSIDE  192.168.1.40:32809, idle 0:00:00, bytes 949584, flags UIOo
```

لاحظ إحصائيات الشخير أحداث التسجيل فقط في بداية الجلسة ونهايتها:

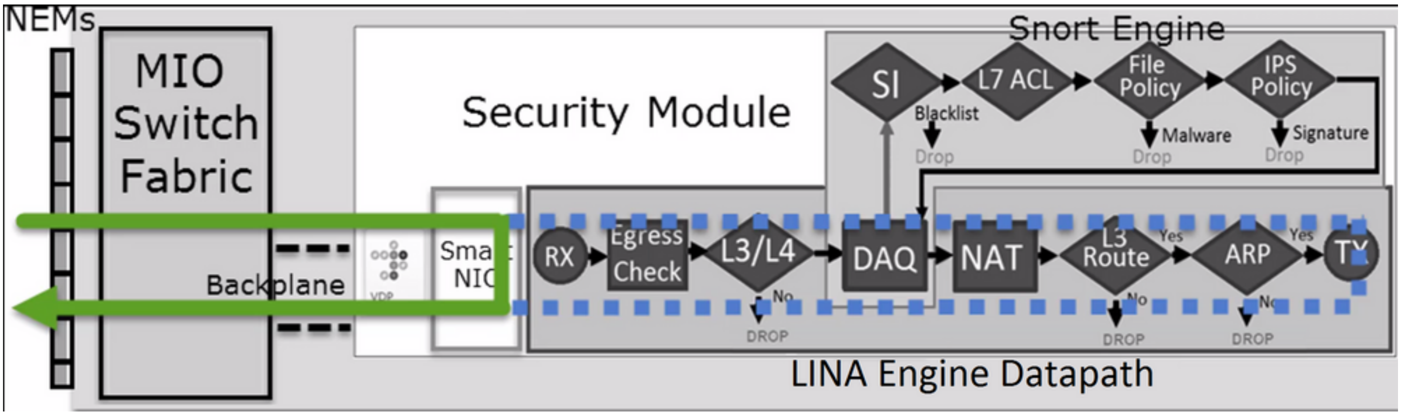
```
firepower# show snort statistics

Packet Counters:
  Passed Packets                                          0
  Blocked Packets                                         0
  Injected Packets                                        0
  Packets bypassed (Snort Down)                           0
  Packets bypassed (Snort Busy)                           0

Flow Counters:
  Fast-Forwarded Flows                                    0
  Blacklisted Flows                                       0

Miscellaneous Counters:
  Start-of-Flow events                                    1
  End-of-Flow events                                      1
```

لاحظ سجلات FTD LINA أنه في كل جلسة عمل كان هناك 2 عملية تدفق (واحد لكل إتجاه) يتم تحميلها إلى الجهاز:

```
Sep 27 2017 20:16:05: %ASA-7-609001: Built local-host INSIDE:192.168.1.40
Sep 27 2017 20:16:05: %ASA-6-302013: Built inbound TCP connection 25384 for
INSIDE:192.168.1.40/32809 (192.168.1.40/32809) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Sep 27 2017 20:16:05: %ASA-6-805001: Offloaded TCP Flow for connection 25384 from
INSIDE:192.168.1.40/32809 (192.168.1.40/32809) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Sep 27 2017 20:16:05: %ASA-6-805001: Offloaded TCP Flow for connection 25384 from
OUTSIDE:192.168.2.40/80 (192.168.2.40/80) to INSIDE:192.168.1.40/32809 (192.168.1.40/32809)
Sep 27 2017 20:16:05: %ASA-6-805002: TCP Flow is no longer offloaded for connection 25384 from
OUTSIDE:192.168.2.40/80 (192.168.2.40/80) to INSIDE:192.168.1.40/32809 (192.168.1.40/32809)
Sep 27 2017 20:16:05: %ASA-6-805002: TCP Flow is no longer offloaded for connection 25384 from
INSIDE:192.168.1.40/32809 (192.168.1.40/32809) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Sep 27 2017 20:16:05: %ASA-6-302014: Teardown TCP connection 25384 for INSIDE:192.168.1.40/32809
```

```
to OUTSIDE:192.168.2.40/80 duration 0:00:00 bytes 1055048 TCP FINs
Sep 27 2017 20:16:05: %ASA-7-609002: Teardown local-host INSIDE:192.168.1.40 duration 0:00:00
```

تدفق الحزمة مع نشر قاعدة الثقة ك **trust** الفعل في لينا. يتم فحص بعض الحزم بواسطة LINA ويتم تحميل الباقي إلى SmartNIC (FP4100/FP9300):

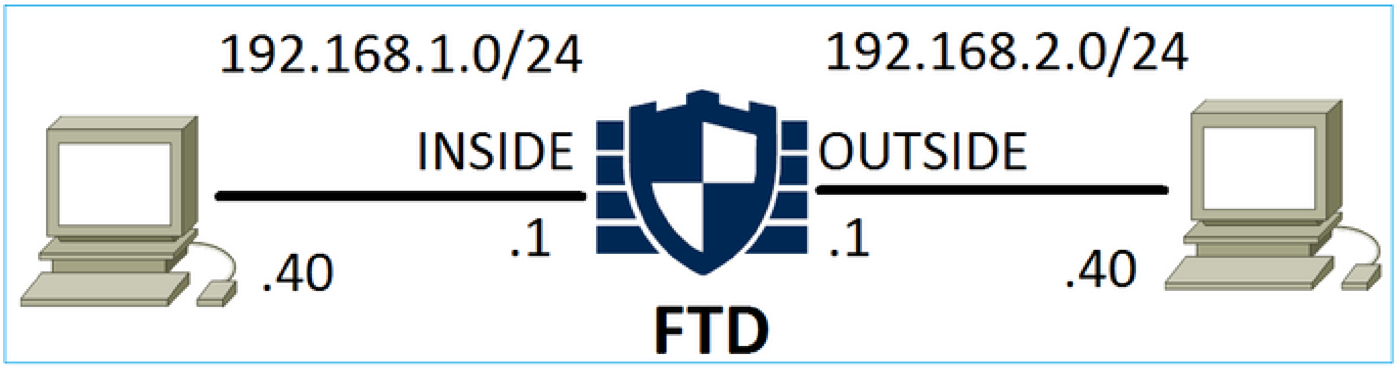


حالات الاستخدام

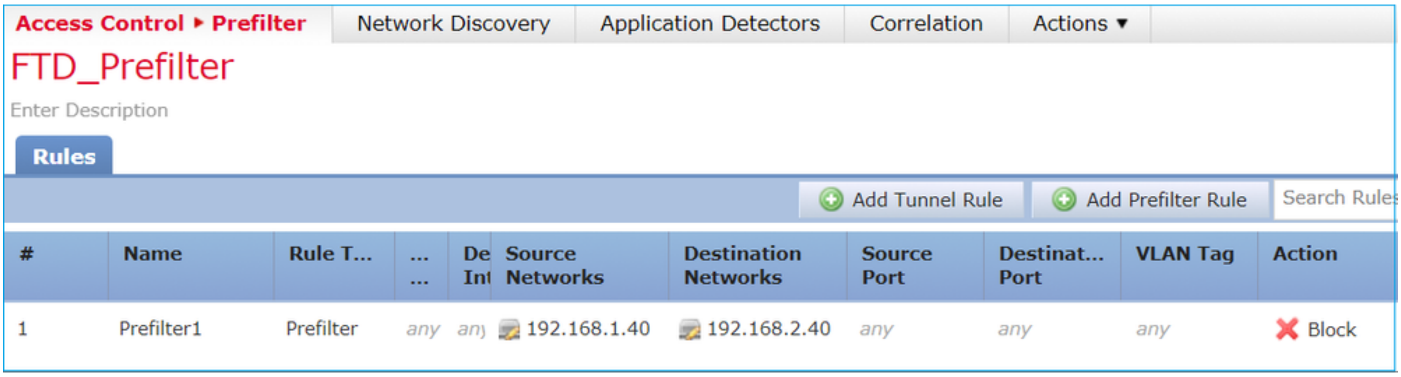
- يجب عليك إستخدام **Trust** إجراء عند إحتياجك إلى فحص حزم قليلة فقط بواسطة محرك الشخير (على سبيل المثال اكتشاف التطبيقات، التحقق بواسطة SI) ويتم إلغاء تحميل باقي التدفق إلى محرك LINA
- إذا كنت تستخدم FTD على FP4100/9300 وتريد أن يتجاوز التدفق فحص الشخر بشكل كامل ثم ضع في الاعتبار قاعدة Prefilter مع **Fastpath** إجراء (راجع القسم المرتبط في هذا المستند)

إجراء حظر نهج عامل التصفية المسبق

ضع في حسبانك المخطط كما هو موضح في الصورة:



فكر أيضا في السياسة كما هو موضح في الصورة:



FTD_Prefilter

Enter Description

#	Name	Rule T...	... ...	De Int	Source Networks	Destination Networks	Source Port	Destinat... Port	VLAN Tag	Action
1	Prefilter1	Prefilter	any	any	192.168.1.40	192.168.2.40	any	any	any	✗ Block

هذا وه النهج الذي تم نشره في محرك FTD Snort (ملف ngfw.rules):

```
# Start of tunnel and priority rules.
# These rules are evaluated by LINA. Only tunnel tags are used from the matched rule id.
268437506 deny any 192.168.1.40 32 any any 192.168.2.40 32 any any any  (tunnel -1
```

في لينا:

```
access-list CSM_FW_ACL_ line 1 remark rule-id 268437506: PREFILTER POLICY: FTD_Prefilter
access-list CSM_FW_ACL_ line 2 remark rule-id 268437506: RULE: Prefilter1
access-list CSM_FW_ACL_ line 3 advanced deny ip host 192.168.1.40 host 192.168.2.40 rule-id
268437506 event-log flow-start (hitcnt=0) 0x76476240
```

عند تعقب ةمزح افتراضية، فإنها رهظت نأ الحزمة يتم إسقاطها ةطساوب LINA الو تتم إعادة توجيهها إلى الشخير أبدا:

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
…
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip host 192.168.1.40 host 192.168.2.40 rule-id 268437506
event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268437506: PREFILTER POLICY: FTD_Prefilter
access-list CSM_FW_ACL_ remark rule-id 268437506: RULE: Prefilter1
Additional Information:

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

تظهر إحصاءات الشخير:

```
firepower# show snort statistics

Packet Counters:
  Passed Packets                                                0
  Blocked Packets                                               0
  Injected Packets                                              0
  Packets bypassed (Snort Down)                                 0
  Packets bypassed (Snort Busy)                                 0

Flow Counters:
  Fast-Forwarded Flows                                          0
  Blacklisted Flows                                             0

Miscellaneous Counters:
  Start-of-Flow events                                 0
  End-of-Flow events                                   0
  Denied flow events                                   1
```

عرض عمليات إسقاط ASP لدينا:

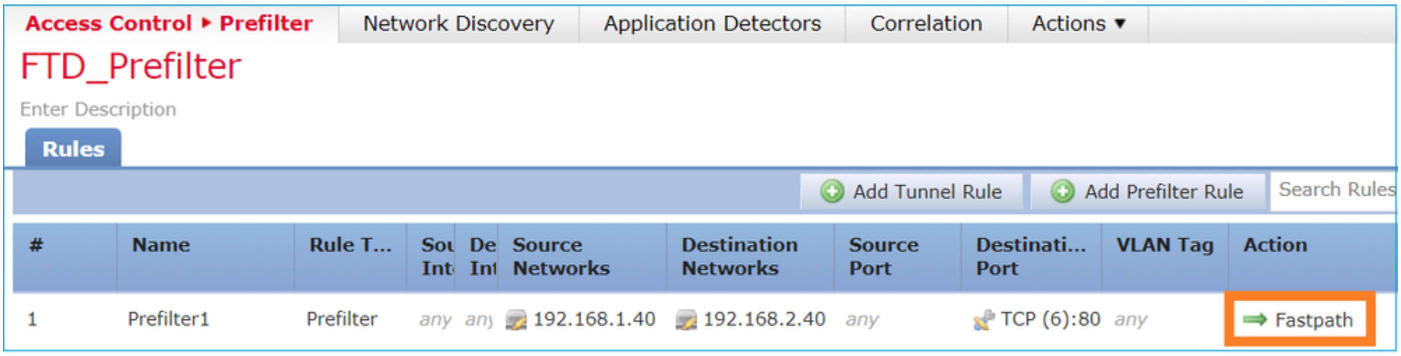
```
firepower# show asp drop

Frame drop:
  Flow is denied by configured rule (acl-drop)                 1
```

حالات الاستخدام

يمكنك إستخدام قاعدة كتلة عامل التصفية المسبق عندما تريد حظر حركة المرور استنادا إلى شروط L3/L4 دون الحاجة إلى إجراء أي فحص فحص تقريبي لحركة المرور.

إجراء FastPath لنھج ما قبل التصفية

ضع في الاعتبار قاعدة نھج عامل التصفية المسبق كما ھو موضح في الصورة:



#	Name	Rule T...	Sou Int	De Int	Source Networks	Destination Networks	Source Port	Destinati... Port	VLAN Tag	Action
1	Prefilter1	Prefilter	any	an	192.168.1.40	192.168.2.40	any	TCP (6):80	any	Fastpath

ھذه ھي السياسة التي تم نشرها في محرك FTD Snort:

```
268437506 fastpath any any any any any any any any (log dcforward flowend) (tunnel -1)
```

في FTD LINA:

```
access-list CSM_FW_ACL_ line 1 remark rule-id 268437506: PREFILTER POLICY: FTD_Prefilter
access-list CSM_FW_ACL_ line 2 remark rule-id 268437506: RULE: Prefilter1
access-list CSM_FW_ACL_ line 3 advanced trust tcp host 192.168.1.40 host 192.168.2.40 eq www
rule-id 268437506 event-log flow-end (hitcnt=0) 0xf3410b6f
```

التحقق من السلوك

عندما يحاول المضيف-A (192.168.1.40) فتح جلسة HTTP إلى المضيف-B (192.168.2.40) تمر بعض الحزم عبر LINA ويتم تحميل الباقي إلى SmartNIC. في ھذه الحالة **system support trace** مع **firewall-engine-debug** تمكين العروض:

```
> system support trace

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.1.40
Please specify a client port:
```

```
Please specify a server IP address: 192.168.2.40
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

192.168.1.40-32840 > 192.168.2.40-80 6 AS 1 I 8 Got end of flow event from hardware with flags
04000000
```

تظهر سجلات LINA التدفق الذي تم إلغاء تحميله:

```
Oct 01 2017 14:36:51: %ASA-7-609001: Built local-host INSIDE:192.168.1.40
Oct 01 2017 14:36:51: %ASA-7-609001: Built local-host OUTSIDE:192.168.2.40
Oct 01 2017 14:36:51: %ASA-6-302013: Built inbound TCP connection 966 for
INSIDE:192.168.1.40/32840 (192.168.1.40/32840) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Oct 01 2017 14:36:51: %ASA-6-805001: Offloaded TCP Flow for connection 966 from
INSIDE:192.168.1.40/32840 (192.168.1.40/32840) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Oct 01 2017 14:36:51: %ASA-6-805001: Offloaded TCP Flow for connection 966 from
OUTSIDE:192.168.2.40/80 (192.168.2.40/80) to INSIDE:192.168.1.40/32840 (192.168.1.40/32840)
```

عمليات التقاط LINA تظهر 8 حزم تمر عبر:

```
firepower# show capture
capture CAPI type raw-data buffer 33554432 trace trace-count 100 interface INSIDE [Capturing -
3908 bytes]
  match ip host 192.168.1.40 host 192.168.2.40
capture CAPO type raw-data buffer 33554432 trace trace-count 100 interface OUTSIDE [Capturing -
3908 bytes]
  match ip host 192.168.1.40 host 192.168.2.40


firepower# show capture CAPI

8 packets captured

   1: 14:45:32.700021  192.168.1.40.32842 > 192.168.2.40.80: S 3195173118:3195173118(0) win 2920
<mss 1460,sackOK,timestamp 332569060 0>
   2: 14:45:32.700372  192.168.2.40.80 > 192.168.1.40.32842: S 184794124:184794124(0) ack
3195173119 win 2896 <mss 1380,sackOK,timestamp 332567732 332569060>
   3: 14:45:32.700540  192.168.1.40.32842 > 192.168.2.40.80: P 3195173119:3195173317(198) ack
184794125 win 2920 <nop,nop,timestamp 332569060 332567732>
   4: 14:45:32.700876  192.168.2.40.80 > 192.168.1.40.32842: . 184794125:184795493(1368) ack
3195173317 win 2698 <nop,nop,timestamp 332567733 332569060>
   5: 14:45:32.700922  192.168.2.40.80 > 192.168.1.40.32842: P 184795493:184796861(1368) ack
3195173317 win 2698 <nop,nop,timestamp 332567733 332569060>
   6: 14:45:32.701425  192.168.2.40.80 > 192.168.1.40.32842: FP 184810541:184810851(310) ack
3195173317 win 2698 <nop,nop,timestamp 332567733 332569061>
   7: 14:45:32.701532  192.168.1.40.32842 > 192.168.2.40.80: F 3195173317:3195173317(0) ack
184810852 win 2736 <nop,nop,timestamp 332569061 332567733>
   8: 14:45:32.701639  192.168.2.40.80 > 192.168.1.40.32842: . ack 3195173318 win 2697
<nop,nop,timestamp 332567734 332569061>
```

تظهر إحصائيات تدفق-إلغاء تحميل FTD 22 حزمة تم إلغاء تحميلها إلى الأجهزة:

```
firepower# show flow-offload statistics
```

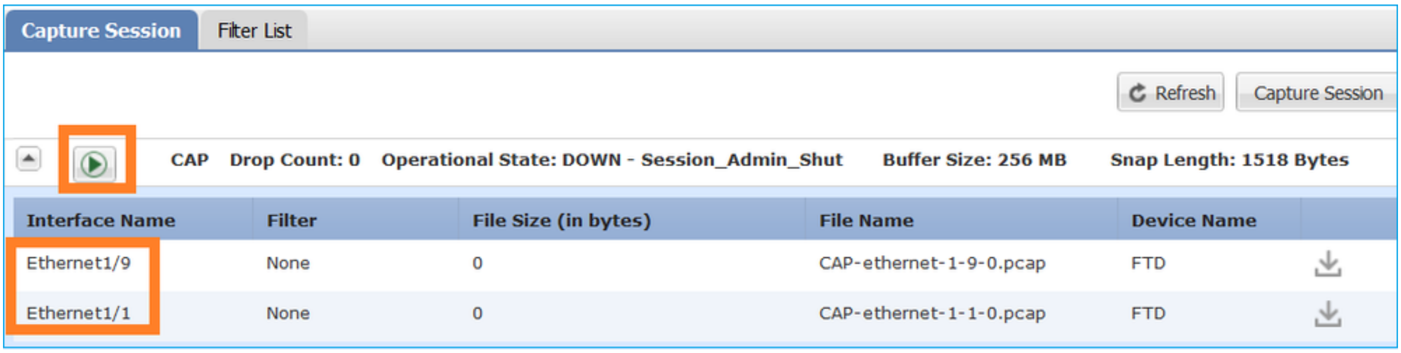
```
 Packet stats of port : 0
        Tx Packet count                  :             22
        Rx Packet count                  :             22
        Dropped Packet count             :              0
        VNIC transmitted packet          :             22
        VNIC transmitted bytes           :          15308
        VNIC Dropped packets             :              0
        VNIC erroneous received          :              0
        VNIC CRC errors                  :              0
        VNIC transmit failed             :              0
        VNIC multicast received          :              0
```

يمكنك أيضا إستخدام **show flow-offload flow** أمر لرؤية معلومات إضافية متعلقة بالتدفق غير المحمل. فيما يلي مثال:

```
firepower# show flow-offload flow
Total offloaded flow stats: 2 in use, 4 most used, 20% offloaded, 0 collisions
TCP intfc 103 src 192.168.1.40:39301 dest 192.168.2.40:20, static, timestamp 616063741, packets
33240, bytes 2326800
TCP intfc 104 src 192.168.2.40:20 dest 192.168.1.40:39301, static, timestamp 616063760, packets
249140, bytes 358263320
firepower# show conn
5 in use, 5 most used
Inspect Snort:
       preserve-connection: 1 enabled, 0 in effect, 4 most enabled, 0 most in effect

TCP OUTSIDE  192.168.2.40:21 INSIDE  192.168.1.40:40988, idle 0:00:00, bytes 723, flags UIO
TCP OUTSIDE  192.168.2.40:21 INSIDE  192.168.1.40:40980, idle 0:02:40, bytes 1086, flags UIO
TCP OUTSIDE  192.168.2.40:80 INSIDE  192.168.1.40:49442, idle 0:00:00, bytes 86348310, flags UIO
N1
TCP OUTSIDE  192.168.2.40:20 INSIDE  192.168.1.40:39301, idle 0:00:00, bytes 485268628, flags Uo
<- offloaded flow
TCP OUTSIDE  192.168.2.40:20 INSIDE  192.168.1.40:34713, idle 0:02:40, bytes 821799360, flags
UFRIO
```

- تعتمد النسبة المئوية على '**show conn**إخراج '. على سبيل المثال، إذا تم تحميل 5 مخروطيات بشكل إجمالي من خلال محرك FTD LINA وتم إلغاء تحميل واحد منها، فهذا يعني أنه تم الإبلاغ عن 20٪ على أنها تم إلغاء تحميلها
- يعتمد الحد الأقصى للجلسات التي تم إلغاء تحميلها على إصدار البرنامج (على سبيل المثال، ASA 9. 8. 3 ودعم FTD 6. 2. 3 ل 4 ملايين عملية تدفق غير محملة (أو 8 ملايين عملية تدفق أحادي الإتجاه)
- في حالة وصول عدد التدفقات غير المحملة إلى الحد (على سبيل المثال 4 ملايين عملية تدفق ثنائية الإتجاه)، لا يتم إلغاء تحميل أي إتصالات جديدة حتى تتم إزالة الاتصالات الحالية من الجدول غير المحمل

لترى كل الحزم على FP4100/9300 التي تمر عبر FTD (إلغاء التحميل + LINA)، هناك حاجة لتمكين الالتقاط على مستوى الهيكل كما هو موضح في الصورة:



CAP   Drop Count: 0   Operational State: DOWN - Session_Admin_Shut   Buffer Size: 256 MB   Snap Length: 1518 Bytes

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/9	None	0	CAP-ethernet-1-9-0.pcap	FTD
Ethernet1/1	None	0	CAP-ethernet-1-1-0.pcap	FTD

يظهر التقاط اللوحة الخلفية للهيكل لكلا الاتجاهين. بسبب بنية التقاط FXOS (2 نقاط التقاط لكل إتجاه) يتم عرض كل حزمة **مرتين** كما هو موضح في الصورة:

إحصائيات الحزمة:

- إجمالي الحزم عبر FTD: 30
- الحزم عبر FTD LINA: 8
- الحزم التي تم إلغاء تحميلها إلى مسرع الأجهزة SmartNIC: 22

في حالة وجود نظام أساسي مختلف عن FP4100/FP9300، تتم معالجة جميع الحزم بواسطة محرك LINA نظرا لأن تدفق-إلغاء التحميل غير مدعوم (لاحظ غياب علامة **o**):

```
FP2100-6# show conn addr 192.168.1.40
33 in use, 123 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 2 most enabled, 0 most in effect

TCP OUTSIDE  192.168.2.40:80 INSIDE  192.168.1.40:50890, idle 0:00:09, bytes 175, flags UxIO
```

لا تعرض LINA syslogs سوى إعداد الاتصال وأحداث إنهاء الاتصال:

```
FP2100-6# show log | i 192.168.2.40
Jun 21 2020 14:29:44: %FTD-6-302013: Built inbound TCP connection 6914 for
INSIDE:192.168.1.40/50900 (192.168.11.101/50900) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Jun 21 2020 14:30:30: %FTD-6-302014: Teardown TCP connection 6914 for INSIDE:192.168.1.40/50900
to OUTSIDE:192.168.2.40/80 duration 0:00:46 bytes 565 TCP FINs from OUTSIDE
```

حالات الاستخدام

- إستخدام **Prefilter Fastpath** عندما تريد تجاوز فحص الشخر بالكامل. عادة ما ترغب في القيام بذلك للتدفقات الكبيرة من البيانات التي تثق بها مثل عمليات النسخ الاحتياطي ونقل قواعد البيانات، وما إلى ذلك
- في أجهزة FP4100/9300 **Fastpath** تؤدي العملية إلى تشغيل إلغاء تحميل التدفق ويمر عدد قليل من الحزم فقط من خلال محرك FTD LINA. ويتم التعامل مع الباقي بواسطة بطاقة واجهة الشبكة (SmartNIC) التي تعمل على تقليل زمن الوصول

إجراء FastPath لنهج ما قبل التصفية (مجموعة أسطر)

في حالة تطبيق إجراء PreFilter Policy FastPath على حركة المرور التي تمر عبر مجموعة داخلية (واجهات NGIPS)، يجب أخذ هذه النقاط في الاعتبار:

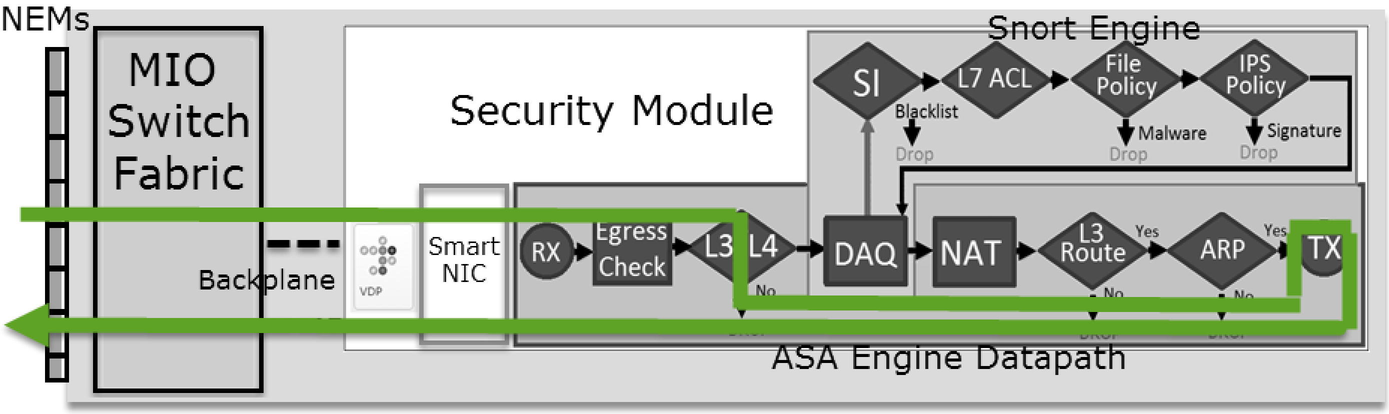
- يتم تطبيق القاعدة على محرك LINA ك **trust** الإجراء
- لم يتم فحص التدفق بواسطة محرك الشخير
- لا يحدث إلغاء تحميل التدفق (تسريع HW) نظرا لأن إلغاء تحميل التدفق غير قابل للتطبيق على واجهات NGIPS

هنا مثال من ربط تتبع في حالة ما إذا كان إجراء FastPath ل PreFilter مطبق على مجموعة في السطر:

```
firepower# packet-tracer input inside tcp 192.168.1.40 12345 192.168.1.50 80 detailed

Phase: 1
```

```
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied
Forward Flow based lookup yields rule:
in id=0x2ad7ac48b330, priority=501, domain=ips-mode, deny=false
hits=2, user_data=0x2ad80d54abd0, cs_id=0x0, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=inside, output_ifc=any

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced trust ip object 192.168.1.0 object 192.168.1.0 rule-id
268438531 event-log flow-end
access-list CSM_FW_ACL_ remark rule-id 268438531: PREFILTER POLICY: PF1
access-list CSM_FW_ACL_ remark rule-id 268438531: RULE: 1
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ad9f9f8a7f0, priority=12, domain=permit, trust
hits=1, user_data=0x2ad9b23c5d40, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=192.168.1.0, mask=255.255.255.0, port=0, tag=any, ifc=any
dst ip/id=192.168.1.0, mask=255.255.255.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 3
Type: NGIPS-EGRESS-INTERFACE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
Ingress interface inside is in NGIPS inline mode.
Egress interface outside is determined by inline-set configuration

Phase: 4
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 7, packet dispatched to next module
Module information for forward flow ...
snp_fp_ips_tcp_state_track_lite
snp_fp_ips_mode_adj
snp_fp_tracer_drop
snp_ifc_stat

Module information for reverse flow ...
snp_fp_ips_tcp_state_track_lite
snp_fp_ips_mode_adj
snp_fp_tracer_drop
snp_ifc_stat

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

هذا هو التمثيل البصري من الربط ممر:



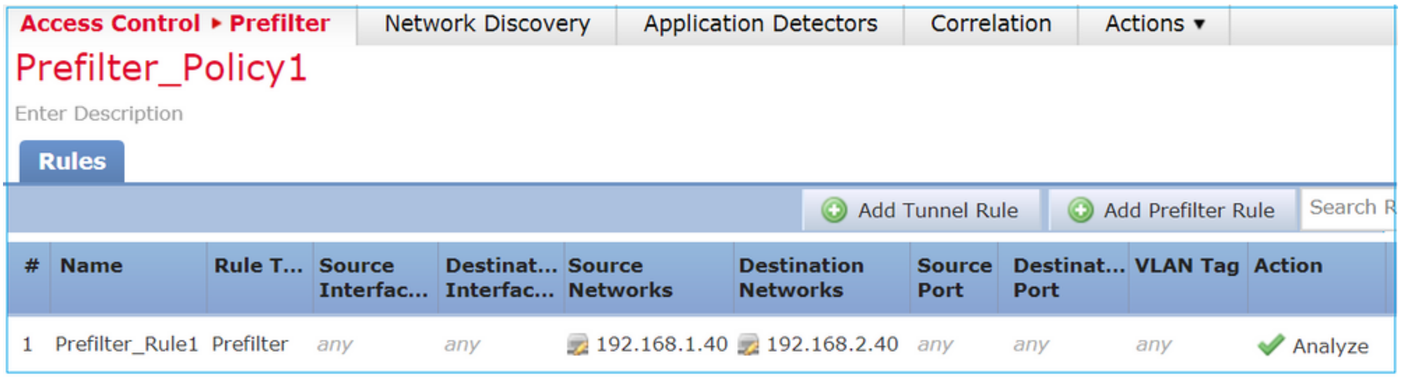
إجراء FastPath لنهج ما قبل التصفية (مجموعة الأسطر مع TAP)

نفس حالة المجموعة الداخلية

إجراء تحليل نهج عامل التصفية المسبق

السيناريو 1. تحليل ما قبل التصفية باستخدام قاعدة كتلة ACP

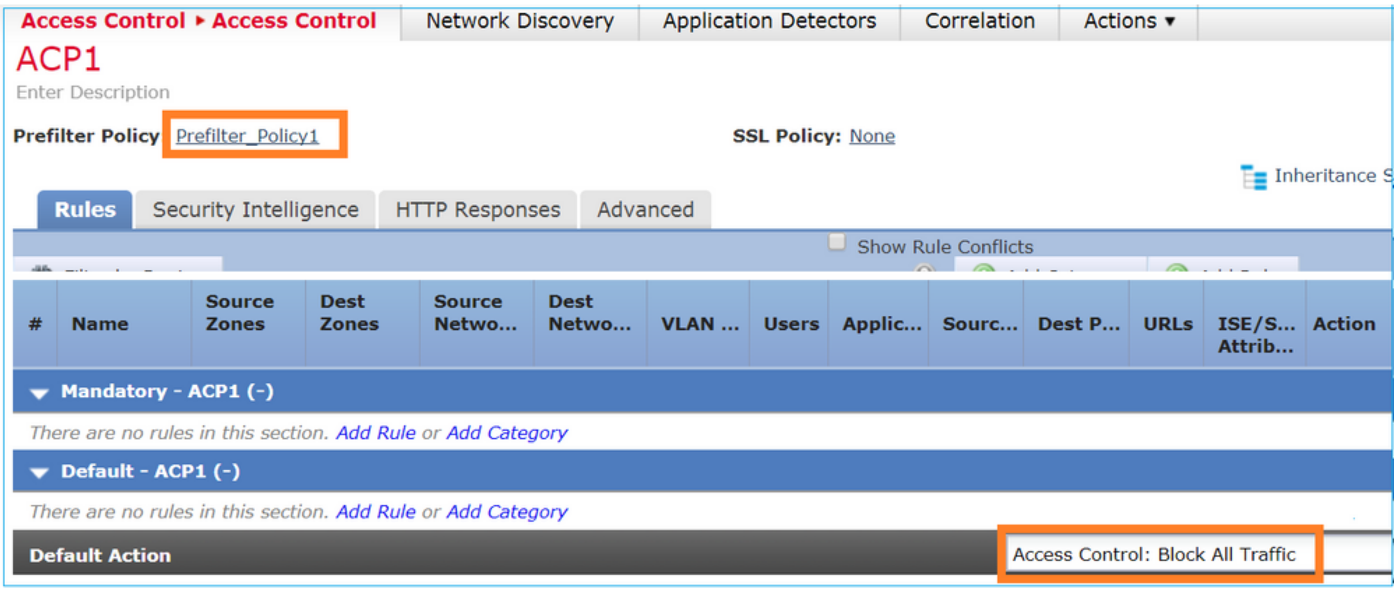
ضع في الاعتبار نهج عامل التصفية المسبق الذي يحتوي على قاعدة تحليل كما هو موضح في الصورة:



Prefilter_Policy1

#	Name	Rule T...	Source Interfac...	Destinat... Interfac...	Source Networks	Destination Networks	Source Port	Destinat... Port	VLAN Tag	Action
1	Prefilter_Rule1	Prefilter	any	any	192.168.1.40	192.168.2.40	any	any	any	✓ Analyze

تحتوي قائمة التحكم بالوصول (ACP) فقط على القاعدة الافتراضية التي تم تعيينها على **Block All Traffic** كما هو موضح في الصورة:



Access Control ▸ Access Control | Network Discovery | Application Detectors | Correlation | Actions ▾

ACP1

Enter Description

Prefilter Policy: Prefilter_Policy1

SSL Policy: None

Inheritance S

Rules | Security Intelligence | HTTP Responses | Advanced

□ Show Rule Conflicts

#	Name	Source Zones	Dest Zones	Source Netwo...	Dest Netwo...	VLAN ...	Users	Applic...	Sourc...	Dest P...	URLs	ISE/S... Attrib...	Action

▼ Mandatory - ACP1 (-)

There are no rules in this section. Add Rule or Add Category

▼ Default - ACP1 (-)

There are no rules in this section. Add Rule or Add Category

Default Action: Access Control: Block All Traffic

هذا هو النهج الذي تم نشره في محرك FTD Snort (ملف ngfw.rules):

```
# Start of tunnel and priority rules.
# These rules are evaluated by LINA. Only tunnel tags are used from the matched rule id.
268435460 allow any 192.168.1.40 32 any any 192.168.2.40 32 any any any  (tunnel -1)
268435459 allow any any  1025-65535 any any  3544 any 17  (tunnel -1)
268435459 allow any any  3544 any any  1025-65535 any 17  (tunnel -1)
268435459 allow any any  any any any  any any 47  (tunnel -1)
268435459 allow any any  any any any  any any 41  (tunnel -1)
268435459 allow any any  any any any  any any 4  (tunnel -1)
# End of tunnel and priority rules.
# Start of AC rule.
268435458 deny any any  any any any  any any any  (log dcforward flowstart)
# End of AC rule.
```

هذا هو النهج الذي تم نشره في محرك FTD LINA Engine:

```
access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435460 (hitcnt=0) 0xb788b786
```

التحقق من السلوك

يظهر Packet-tracer أن الحزمة مسموح بها بواسطة LINA، تتم إعادة توجيهها إلى محرك snort (بسبب **permit** الدالة ACTION) و SNORT Engine ترجع **Block** الحكم بما أن الإجراء الافتراضي من AC مطابق.

> **ملاحظة**: لا يقيم الشروط حركة المرور استنادا إلى قواعد النفق

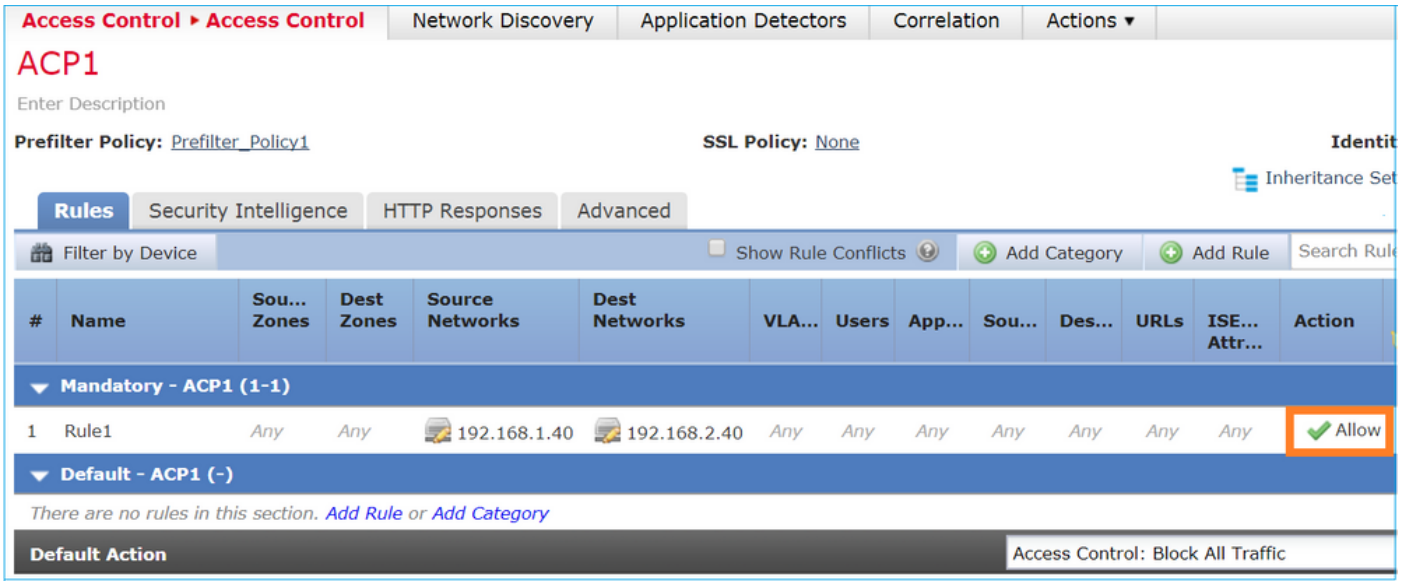
عندما يتتبع أنت ربط هو يكشف ال نفسه:

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
```

```
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will be reached

…
Phase: 14
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: ICMP
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 8, icmpCode 0
Firewall: block rule, id 268435458, drop
Snort: processed decoder alerts or actions queue, drop
NAP id 1, IPS id 0, Verdict BLOCKLIST, Blocked by Firewall
Snort Verdict: (block-list) block list this flow

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: drop
Drop-reason: (firewall) Blocked by the firewall preprocessor
```

السيناريو 2. تحليل ما قبل التصفية باستخدام قاعدة السماح ل ACP

إذا كان الهدف هو السماح للحزمة بالمرور عبر FTD، هناك حاجة لإضافة قاعدة في قائمة التحكم في الوصول (ACP). يمكن أن تكون العملية إما "سماح" أو "ثقة" تعتمد على الهدف (على سبيل المثال، إذا كنت تريد تطبيق فحص L7 يجب عليك إستخدامه **Allow** عملية) كما هو موضح في الصورة:



ACP1

Enter Description

Prefilter Policy: Prefilter_Policy1 SSL Policy: None Identit

#	Name	Sou... Zones	Dest Zones	Source Networks	Dest Networks	VLA...	Users	App...	Sou...	Des...	URLs	ISE... Attr...	Action
Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	Any	Any	Any	✓ Allow
Default - ACP1 (-)													
There are no rules in this section. Add Rule or Add Category													
Default Action													Access Control: Block All Traffic

السياسة المنشورة في محرك التشغيل FTD Snort:

```
# Start of AC rule.
268435461 allow any 192.168.1.40 32 any any 192.168.2.40 32 any any any
268435458 deny any any  any any any  any any any  (log dcforward flowstart)
# End of AC rule.
```

في محرك لينا:

```
access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435460 (hitcnt=1) 0xb788b786
```

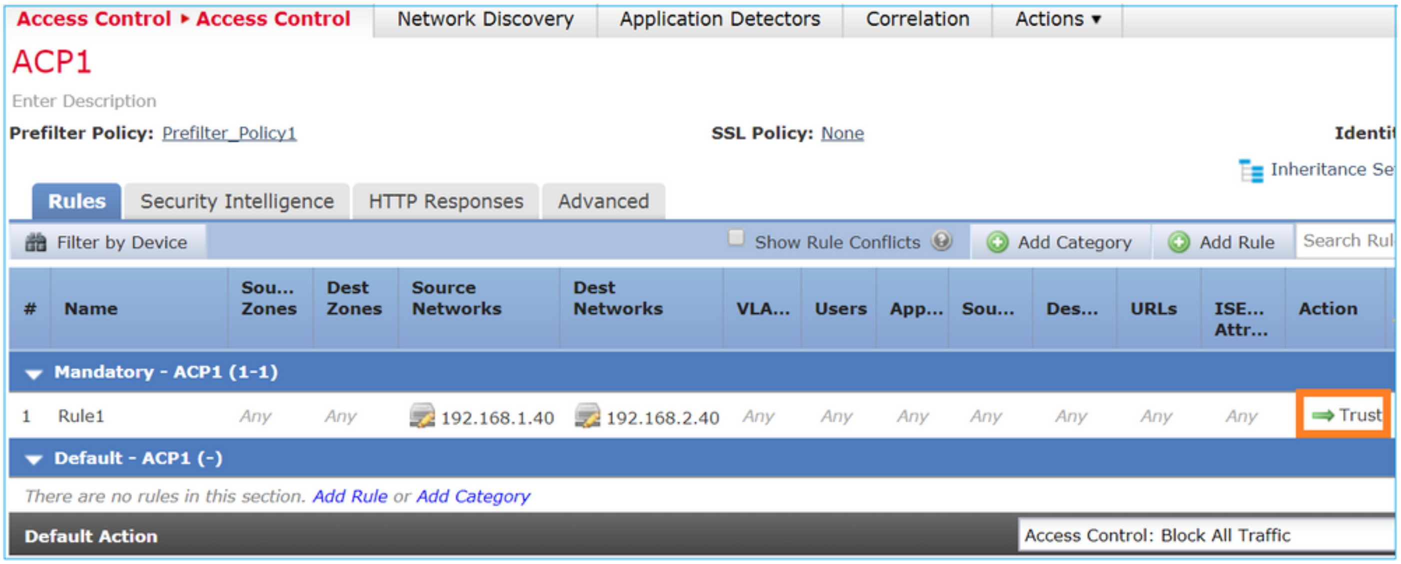
التحقق من السلوك

يظهر Packet-tracer أن الحزمة تطابق القاعدة **268435460** في لينا و **268435461** في محرك الشخير:

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will be reached
…
Phase: 14
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: ICMP
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 8, icmpCode 0
Firewall: allow rule, id 268435461, allow
NAP id 1, 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
```

السيناريو 3. تحليل ما قبل التصفية باستخدام قاعدة الثقة في ACP

في حالة إحتواء قائمة التحكم في الوصول (ACP) على قاعدة "الثقة"، فهذا كما هو موضح في الصورة:



ACP1

Enter Description

Prefilter Policy: Prefilter_Policy1

SSL Policy: None

#	Name	Sou... Zones	Dest Zones	Source Networks	Dest Networks	VLA...	Users	App...	Sou...	Des...	URLs	ISE... Attr...	Action
Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	Any	Any	Any	Trust
Default - ACP1 (-)													
There are no rules in this section. Add Rule or Add Category													

Default Action: Access Control: Block All Traffic

ترون:

```
# Start of AC rule.
268435461 fastpath any 192.168.1.40 32 any any 192.168.2.40 32 any any any
268435458 deny any any  any any any  any any any  (log dcforward flowstart)
# End of AC rule.
```

لينا:

```
access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435460 (hitcnt=2) 0xb788b786
```

تذكر أنه نظرا لتمكين si بشكل افتراضي، يتم نشر قاعدة الثقة ك **permit** إجراء على LINA بحيث يتم إعادة توجيه بعض الحزم على الأقل إلى محرك الشخر للتفتيش.

التحقق من السلوك

يظهر Packet-tracer أن مشغل snort يسمح بالحزمة ويلغي تحميل بقية التدفق إلى LINA:

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will be reached
…
Phase: 14
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
```

```
Packet: ICMP
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 8, icmpCode 0
Firewall: trust/fastpath rule, id 268435461, allow
NAP id 1, IPS id 0, Verdict PERMITLIST
Snort Verdict: (fast-forward) fast forward this flow
…
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow
```

السيناريو 4. تحليل ما قبل التصفية باستخدام قاعدة الثقة في ACP

في هذا السيناريو، تم تعطيل SI يدويا.

تم نشر القاعدة في Snort على النحو التالي:

```
# Start of AC rule.
268435461 fastpath any 192.168.1.40 32 any any 192.168.2.40 32 any any any
268435458 deny any any  any any any  any any any  (log dcforward flowstart)
# End of AC rule.
```

في LINA يتم نشر القاعدة كعنصر ثقة. على الرغم من أن الحزمة تطابق قاعدة السماح (راجع عدد مرات وصول ACE) التي يتم نشرها بسبب تحليل قاعدة عامل التصفية الأولي ويتم فحص الحزمة بواسطة محرك snort:

```
access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435460 (hitcnt=3) 0xb788b786
...
access-list CSM_FW_ACL_ line 13 advanced trust ip host 192.168.1.40 host 192.168.2.40 rule-id
268435461 event-log flow-end (hitcnt=0) 0x5c1346d6
...
access-list CSM_FW_ACL_ line 16 advanced deny ip any any rule-id 268435458 event-log flow-start
(hitcnt=0) 0x97aa021a
```

التحقق من السلوك

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will be reached
```

```
...
Phase: 14
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: ICMP
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 8, icmpCode 0
Firewall: trust/fastpath rule, id 268435461, allow
NAP id 1, IPS id 0, Verdict PERMITLIST
Snort Verdict: (fast-forward) fast forward this flow
…
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow
```

النقاط الأساسية

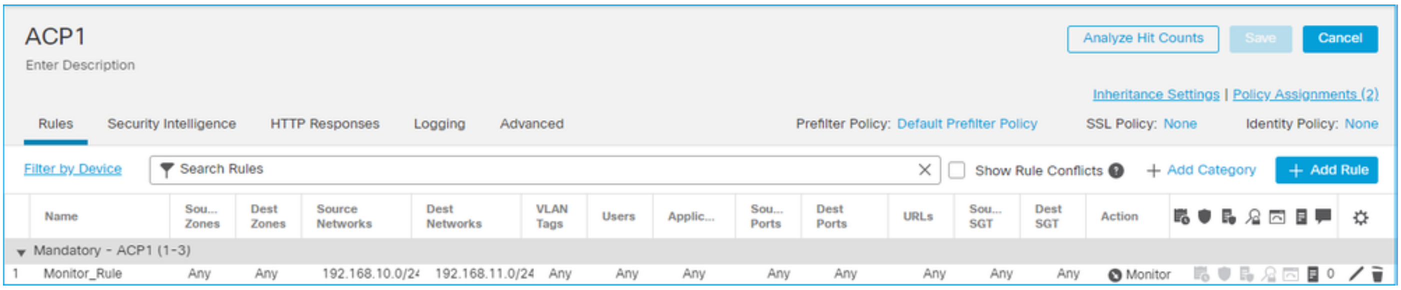
- يعرض الأمر **Analyze** يتم نشر الإجراء كقاعدة تصريح في محرك LINA. هذا له تأثير على الربط أن يكون أرسلت إلى ال snort محرك للتفتيش
- يعرض الأمر **Analyze** ال يقوم الإجراء بنشر أي قاعدة في محرك Snort لذلك تحتاج إلى التأكد من تكوين قاعدة في ACP تطابق قاعدة في Snort<
- يعتمد على قاعدة ACP التي يتم نشرها في محرك الشخير (**block** في مقابل **allow** في مقابل **fastpath**) ال شيء أو كل أو بضعة حزم مسموح بها من قبل الشخير

حالات الاستخدام

- حالة إستخدام ل **Analyze** الإجراء هو عندما يكون لديك قاعدة FastPath واسعة في سياسة ما قبل التصفية وتريد وضع بعض الاستثناءات لتدفقات معينة بحيث يتم فحصها بواسطة الشخير

إجراء مراقبة ACP

قاعدة مراقبة تم تكوينها على واجهة مستخدم FMC:



	Name	Sou... Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Sou... Ports	Dest Ports	URLs	Sou... SGT	Dest SGT	Action	
▾	Mandatory - ACP1 (1-3)														
1	Monitor_Rule	Any	Any	192.168.10.0/24	192.168.11.0/24	Any	Any	Any	Any	Any	Any	Any	Any	Monitor	0

يتم نشر قاعدة جهاز العرض على محرك FTD LINA ك **permit** و على محرك الشخير **audit** الإجراء.

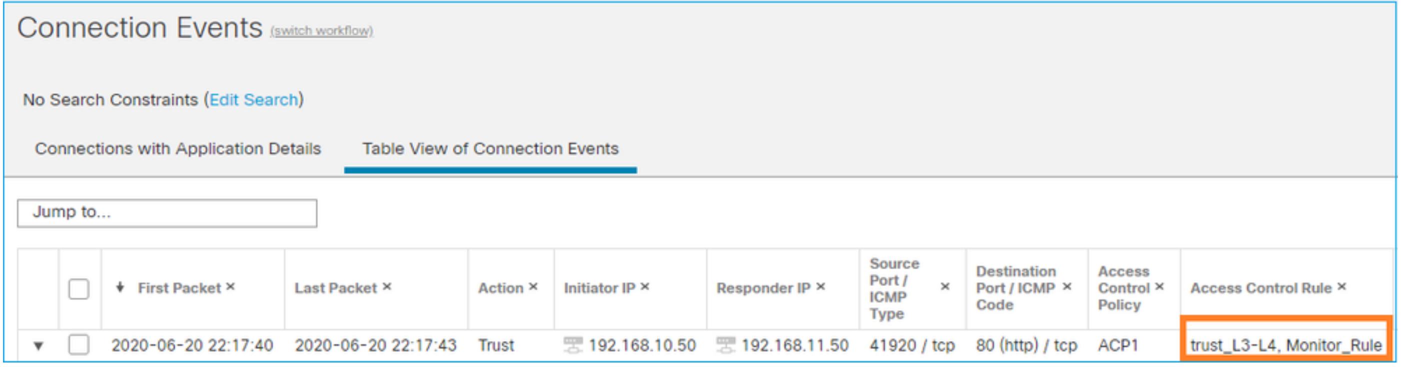
```
firepower# show access-list
…
access-list CSM_FW_ACL_ line 10 advanced permit ip 192.168.10.0 255.255.255.0 192.168.11.0
255.255.255.0 rule-id 268438863 (hitcnt=0) 0x61bbaf0c
```

قاعدة الشخير:

```
admin@firepower:~$ cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules
…
# Start of AC rule.
268438863 audit any 192.168.10.0 24 any any 192.168.11.0 24 any any any (log dcforward flowend)
# End rule 268438863
```

النقاط الأساسية

- لا تقوم قاعدة المراقبة بإسقاط حركة المرور أو السماح بها ولكنها تقوم بإنشاء حدث اتصال. يتم التحقق من الحزمة مقابل القواعد التالية ويتم إما السماح بها أو إسقاطها
- تظهر أحداث اتصال FMC أن الحزمة طابقت قاعدتين:



Connection Events (switch workflow)

No Search Constraints (Edit Search)

Connections with Application Details | Table View of Connection Events

Jump to...

		↓ First Packet ×	Last Packet ×	Action ×	Initiator IP ×	Responder IP ×	Source Port / ICMP Type ×	Destination Port / ICMP Code ×	Access Control Policy ×	Access Control Rule ×
▼	□	2020-06-20 22:17:40	2020-06-20 22:17:43	Trust	192.168.10.50	192.168.11.50	41920 / tcp	80 (http) / tcp	ACP1	trust_L3-L4, Monitor_Rule

System support trace يظهر الإخراج أن الحزم تطابق كلا القاعدتين:

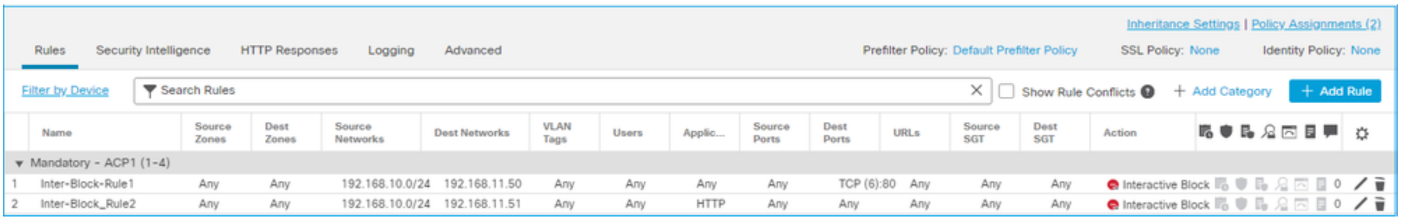
```
> system support trace

Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.50
Please specify a client port:
Please specify a server IP address: 192.168.11.50
Please specify a server port:
Monitoring packet tracer and firewall debug messages


192.168.10.50-41922 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 419031630
192.168.10.50-41922 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.50-41922 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 new firewall session
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 Starting AC with minimum 2, 'Monitor_Rule',
and IPProto first with zone           s -1 -> -1, geo 0 -> 0, vlan 0, source sgt type: 0, source
sgt tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest sgt tag: 0,            svc 0, payload 0,
client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 match rule order 2, 'Monitor_Rule', action
Audit
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 match rule order 3, 'trust_L3-L4', action
Trust
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 MidRecovery data sent for rule id:
268438858,rule_action:3, rev id:1078           02206, rule_match flag:0x2
```

حالات الاستخدام

يستخدم لمراقبة نشاط الشبكة وإنشاء حدث اتصال

إجراء الحظر التفاعلي ل ACP

قاعدة كتل تفاعلية تم تكوينها على واجهة مستخدم FMC:



Prefilter Policy: Default Prefilter Policy   SSL Policy: None   Identity Policy: None

	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action
▾	Mandatory - ACP1 (1-4)													
1	Inter-Block-Rule1	Any	Any	192.168.10.0/24	192.168.11.50	Any	Any	Any	Any	TCP (6):80	Any	Any	Any	Interactive Block 0
2	Inter-Block_Rule2	Any	Any	192.168.10.0/24	192.168.11.51	Any	Any	HTTP	Any	Any	Any	Any	Any	Interactive Block 0

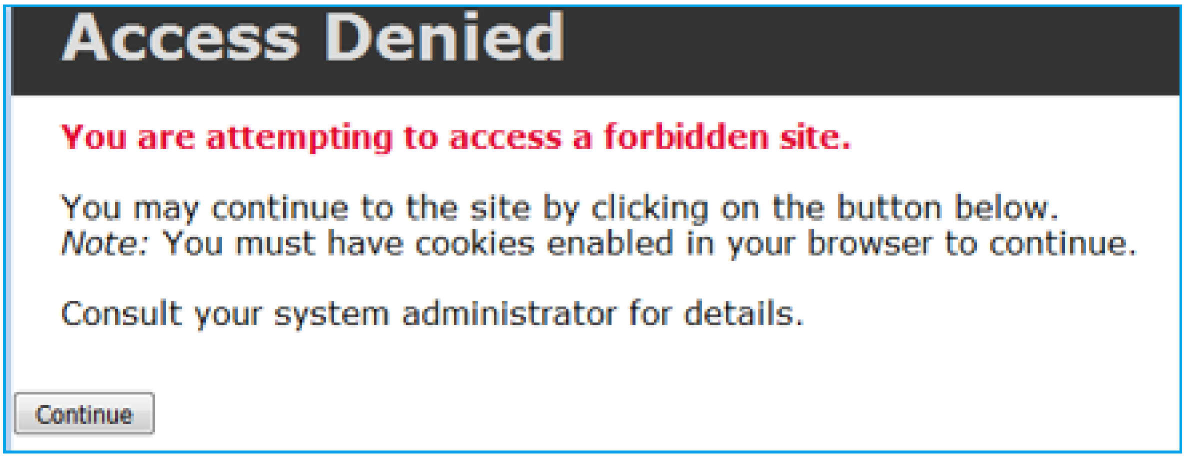
يتم نشر قاعدة الحظر التفاعلي على محرك FTD LINA كمشغل **permit** و إلى محرك الشخير كقاعدة مجازة:

```
firepower# show access-list
…
access-list CSM_FW_ACL_ line 9 remark rule-id 268438864: L7 RULE: Inter-Block-Rule1
access-list CSM_FW_ACL_ line 10 advanced permit tcp 192.168.10.0 255.255.255.0 host
192.168.11.50 eq www rule-id 268438864 (hitcnt=3) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268438865: L7 RULE: Inter-Block_Rule2
access-list CSM_FW_ACL_ line 13 advanced permit ip 192.168.10.0 255.255.255.0 host 192.168.11.51
rule-id 268438865 (hitcnt=0) 0x622350d0
```

محرك الشخير:

```
admin@firepower:~$ cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules
…
# Start of AC rule.
268438864 bypass any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6
# End rule 268438864
268438865 bypass any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1)
(ip_protos 6, 17)
# End rule 268438865
```

تطالبك "قاعدة الحظر التفاعلية" بحظر الوجهة



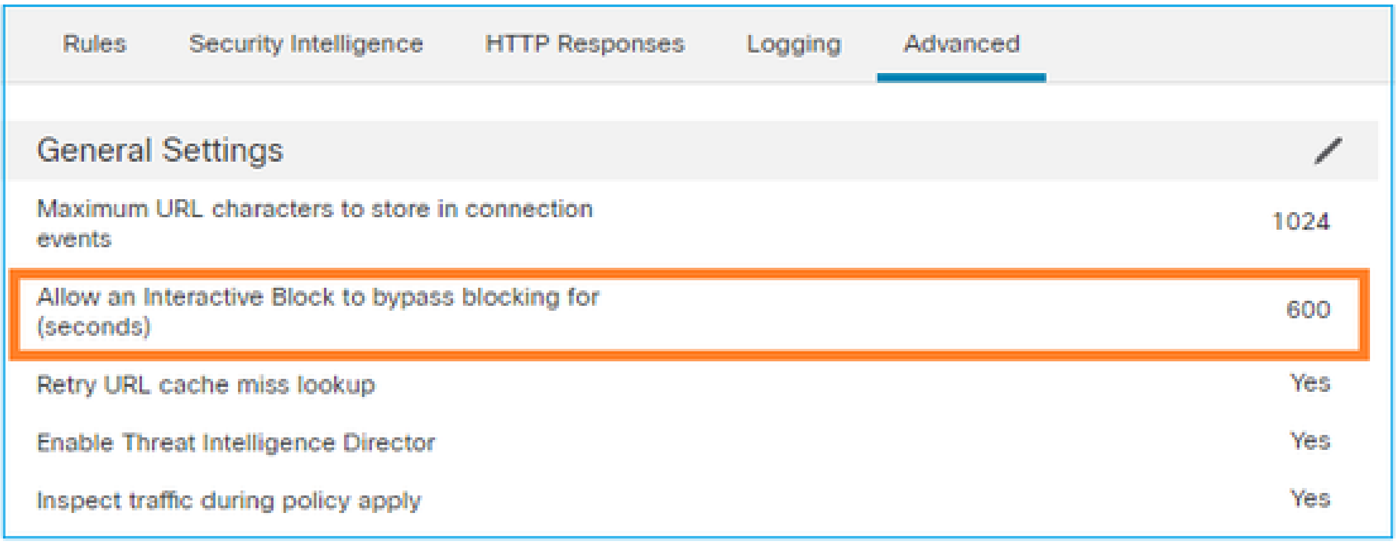
Access Denied

You are attempting to access a forbidden site.

You may continue to the site by clicking on the button below.
Note: You must have cookies enabled in your browser to continue.

Consult your system administrator for details.

بشكل افتراضي، يسمح جدار الحماية بتجاوز الكتلة لمدة 600 ثانية:



General Settings

Maximum URL characters to store in connection events 1024

Allow an Interactive Block to bypass blocking for (seconds) 600

Retry URL cache miss lookup Yes

Enable Threat Intelligence Director Yes

Inspect traffic during policy apply Yes

في **system support trace** إخراج أنت يستطيع رأيت أن في البداية جدار الحماية يمنع حركة المرور ويظهر صفحة الحظر:

```
> system support trace
…
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 983273680, ack
2014879580
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt
tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589,
misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 match rule order 2, 'Inter-Block-Rule1',
action Interactive
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 bypass action sending HTTP interactive
response of 1093 bytes
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive block rule, 'Inter-
Block-Rule1', drop
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions
queue, drop
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 deleting firewall session flags = 0x800,
fwFlags = 0x1002
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 22, NAP id 1, IPS id 0, Verdict
BLACKLIST
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 ===> Blocked by Firewall
Verdict reason is sent to DAQ
```

بمجرد تحديد المستخدم **Continue** (أو تحديث صفحة المستعرض) يظهر تصحيح الأخطاء أن الحزم مسموح بها بواسطة القاعدة نفسها التي تحاكي و **Allow** الإجراء:

```
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 1357413630, ack
2607625293
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt
tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589,
misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
```

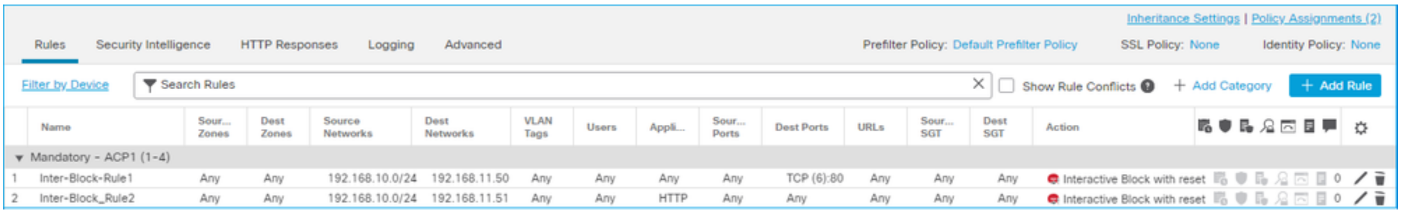
```
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 match rule order 2, 'Inter-Block-Rule1',
action Interactive
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 bypass action interactive bypass
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 allow action
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1',
allow
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-
Block-Rule1', allow
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 8, NAP id 1, IPS id 0, Verdict
PASS
```

حالات الاستخدام

إظهار صفحة تحذير لمستخدمي ويب وإعطائهم خيار المتابعة.

الكتلة التفاعلية ل ACP مع إجراء إعادة الضبط

كتلة تفاعلية مع قاعدة إعادة الضبط التي تم تكوينها على واجهة مستخدم FMC:



	Name	Sour... Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Appli...	Sour... Ports	Dest Ports	URLs	Sour... SGT	Dest SGT	Action	
▼	Mandatory - ACP1 (1-4)														
1	Inter-Block-Rule1	Any	Any	192.168.10.0/24	192.168.11.50	Any	Any	Any	Any	TCP (6):80	Any	Any	Any	Interactive Block with reset	0
2	Inter-Block_Rule2	Any	Any	192.168.10.0/24	192.168.11.51	Any	Any	HTTP	Any	Any	Any	Any	Any	Interactive Block with reset	0

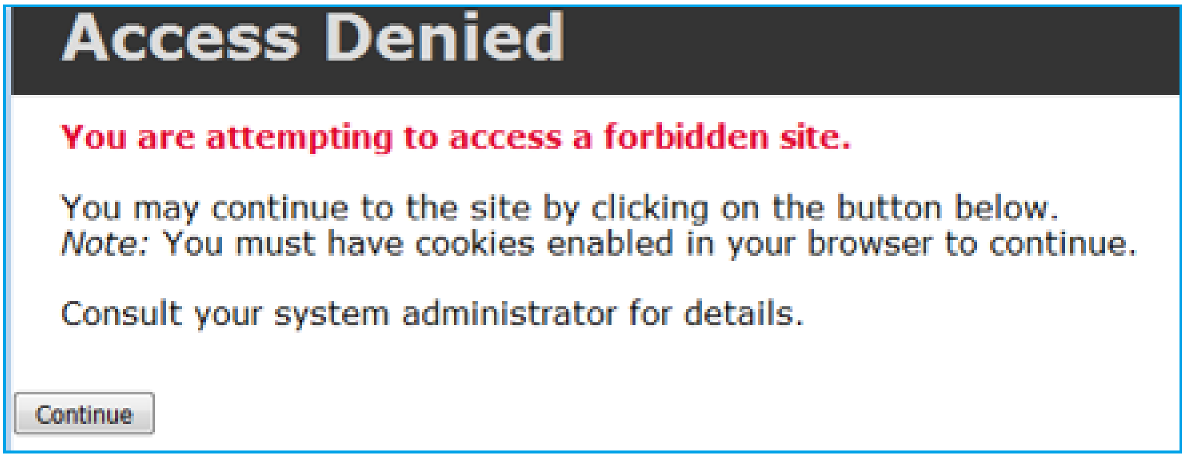
يتم نشر الحظر التفاعلي مع قاعدة إعادة الضبط على محرك FTD LINA كمشغل **permit** الإجراء و إلى Snort محرك كقاعدة إعادة تعيين:

```
firepower# show access-list
…
access-list CSM_FW_ACL_ line 9 remark rule-id 268438864: L7 RULE: Inter-Block-Rule1
access-list CSM_FW_ACL_ line 10 advanced permit tcp 192.168.10.0 255.255.255.0 host
192.168.11.50 eq www rule-id 268438864 (hitcnt=13) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268438865: L7 RULE: Inter-Block_Rule2
access-list CSM_FW_ACL_ line 13 advanced permit ip 192.168.10.0 255.255.255.0 host 192.168.11.51
rule-id 268438865 (hitcnt=0) 0x622350d0
```

محرك الشخير:

```
# Start of AC rule.
268438864 intreset any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6
# End rule 268438864
268438865 intreset any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1)
(ip_protos 6, 17)
# End rule 268438865
```

كما هو الحال مع "الحظر" مع "إعادة التعيين"، يمكن للمستخدم تحديد **Continue** الخيار:



Access Denied

You are attempting to access a forbidden site.

You may continue to the site by clicking on the button below.
Note: You must have cookies enabled in your browser to continue.

Consult your system administrator for details.

في تصحيح أخطاء البرنامج، يتم عرض الإجراء في إعادة التعيين التفاعلي:

```
> system support trace

Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.52
Please specify a client port:
Please specify a server IP address: 192.168.11.50
Please specify a server port:
Monitoring packet tracer and firewall debug messages


192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 3232128039
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 new firewall session
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0 -> 0, vlan 0, source sgt type: 0, source
sgt tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest sgt tag: 0, svc 0, payload 0, client 0,
misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 match rule order 2, 'Inter-Block-Rule1',
action Interactive Reset
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 MidRecovery data sent for rule id:
268438864,rule_action:8, rev id:1099034206, rule_match flag:0x0
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 HitCount data sent for rule id: 268438864,
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
PASS

192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 Packet: TCP, SYN, ACK, seq 2228213518, ack
3232128040
192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
PASS

192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3232128040, ack
2228213519
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
PASS

192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3232128040, ack
2228213519
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application
```

```
unknown (0)
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt
tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589,
misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 match rule order 2, 'Inter-Block-Rule1',
action Interactive Reset
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 bypass action sending HTTP interactive
response of 1093 bytes
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive block rule, 'Inter-
Block-Rule1', drop
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions
queue, drop
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 deleting firewall session flags = 0x800,
fwFlags = 0x1002
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
BLACKLIST
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 ===> Blocked by Firewall
Verdict reason is sent to DAQ
```

عند هذه النقطة، يتم عرض صفحة الحظر على المستخدم النهائي. إذا قام المستخدم بتحديد **Continue** (أو تحديث صفحة الويب) تتطابق نفس القاعدة التي تسمح هذه المرة لحركة المرور عبر:

```
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 1593478294, ack
3135589307
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt
tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589,
misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 match rule order 2, 'Inter-Block-Rule1',
action Interactive Reset
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 bypass action interactive bypass
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 allow action
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1',
allow
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-
Block-Rule1', allow
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 14, NAP id 1, IPS id 0, Verdict
PASS

192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3135589307, ack
1593478786
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1',
allow
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-
Block-Rule1', allow
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Snort id 14, NAP id 1, IPS id 0, Verdict
PASS
```

تقوم الكتلة التفاعلية مع قاعدة إعادة الضبط بإرسال TCP RST إلى حركة مرور البيانات غير الخاصة بالويب:

```
firepower# show cap CAPI | i 11.50
   2: 22:13:33.112954       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: S
```

```
3109534920:3109534920(0) win 29200 <mss 1460,sackOK,timestamp 3745225378 0,nop,wscale 7>
   3: 22:13:33.113626       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: S
3422362500:3422362500(0) ack 3109534921 win 8192 <mss 1380,nop,wscale 8,sackOK,timestamp
53252448 3745225378>
   4: 22:13:33.113824       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362501 win 229 <nop,nop,timestamp 3745225379 53252448>
   5: 22:13:33.114953       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P
3422362501:3422362543(42) ack 3109534921 win 256 <nop,nop,timestamp 53252448 3745225379>
   6: 22:13:33.114984       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P
3422362543:3422362549(6) ack 3109534921 win 256 <nop,nop,timestamp 53252448 3745225379>
   7: 22:13:33.114984       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P
3422362549:3422362570(21) ack 3109534921 win 256 <nop,nop,timestamp 53252448 3745225379>
   8: 22:13:33.115182       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362543 win 229 <nop,nop,timestamp 3745225381 53252448>
   9: 22:13:33.115411       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362549 win 229 <nop,nop,timestamp 3745225381 53252448>
  10: 22:13:33.115426       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362570 win 229 <nop,nop,timestamp 3745225381 53252448>
  12: 22:13:34.803699       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: P
3109534921:3109534931(10) ack 3422362570 win 229 <nop,nop,timestamp 3745227069 53252448>
  13: 22:13:34.804523       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: R
3422362570:3422362570(0) ack 3109534931 win 0
```

إتصالات FTD الثانوية و ثقوب

في الإصدارات الأقدم (على سبيل المثال 6.2.2 و 6.2.3، وما إلى ذلك)، لا يقوم محرك Snort بفتح ثقوب الاتصالات الثانوية (على سبيل المثال بيانات FTD) إذا كنت تستخدم **Trust** الإجراء. في الإصدارات الأخيرة، يتم تغيير هذا السلوك ويفتح محرك الشخير ثقوبا حتى مع **Trust** الإجراء.

إرشادات قواعد FTD

- أستخدم قواعد Prefilter Policy FastPath لتدفقات الدهون الكبيرة ولتقليل زمن الوصول من خلال المربع
- إستخدام قواعد كتلة عامل التصفية المسبق لحركة المرور التي يجب حظرها استنادا إلى شروط L3/L4
- أستخدم قواعد الثقة ب ACP إذا كنت تريد تجاوز العديد من عمليات التحقق من التصريف، ولكن مع الاستمرار في الاستفادة من ميزات مثل نهج الهوية، جودة الخدمة، SI، اكتشاف التطبيقات، عامل تصفية URL
- ضع القواعد التي تؤثر بشكل أقل على أداء جدار الحماية في الجزء العلوي من سياسة التحكم في الوصول باستخدام الإرشادات التالية:

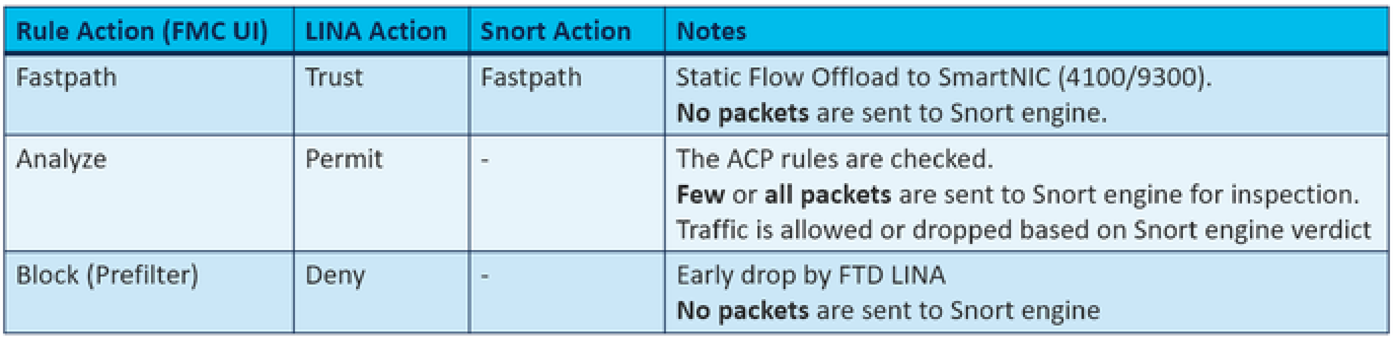
1. حظر القواعد (الطبقات 1-4) - حظر مرشح أولي
2. السماح بالقواعد (الطبقات 1-4) - مسار التثبيت قبل التصفية
3. قواعد كتل ACP (الطبقات 1-4)
4. قواعد الثقة (الطبقات 1-4)
5. حظر القواعد (الطبقات من 5 إلى 7 - اكتشاف التطبيق، تصفية URL)
6. السماح بالقواعد (الطبقات 1-7 - اكتشاف التطبيقات وتصفية عنوان URL ونهج التسلل/نهج الملفات)
7. قاعدة الحظر (القاعدة الافتراضية)

- تجنب التسجيل الزائد (تسجيل الدخول في البداية أو النهاية وتجنب كليهما في نفس الوقت)
- كن على علم بتوسيع القاعدة، للتحقق من عدد القواعد في LINA

```
firepower# show access-list | include elements
access-list CSM_FW_ACL_; 7 elements; name hash: 0x4a69e3f3
```

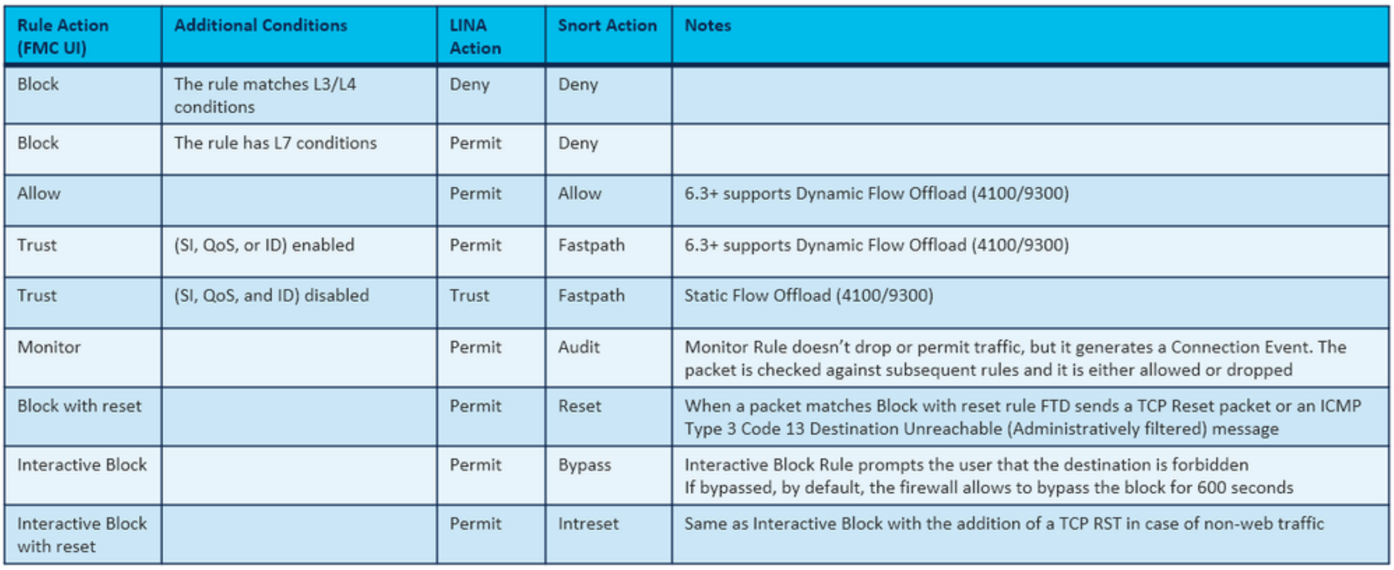
ملخص

إجراءات التصفية المسبقة



Rule Action (FMC UI)	LINA Action	Snort Action	Notes
Fastpath	Trust	Fastpath	Static Flow Offload to SmartNIC (4100/9300). **No packets** are sent to Snort engine.
Analyze	Permit	-	The ACP rules are checked. **Few** or **all packets** are sent to Snort engine for inspection. Traffic is allowed or dropped based on Snort engine verdict
Block (Prefilter)	Deny	-	Early drop by FTD LINA **No packets** are sent to Snort engine

إجراءات ACP



Rule Action (FMC UI)	Additional Conditions	LINA Action	Snort Action	Notes
Block	The rule matches L3/L4 conditions	Deny	Deny	
Block	The rule has L7 conditions	Permit	Deny	
Allow		Permit	Allow	6.3+ supports Dynamic Flow Offload (4100/9300)
Trust	(SI, QoS, or ID) enabled	Permit	Fastpath	6.3+ supports Dynamic Flow Offload (4100/9300)
Trust	(SI, QoS, and ID) disabled	Trust	Fastpath	Static Flow Offload (4100/9300)
Monitor		Permit	Audit	Monitor Rule doesn't drop or permit traffic, but it generates a Connection Event. The packet is checked against subsequent rules and it is either allowed or dropped
Block with reset		Permit	Reset	When a packet matches Block with reset rule FTD sends a TCP Reset packet or an ICMP Type 3 Code 13 Destination Unreachable (Administratively filtered) message
Interactive Block		Permit	Bypass	Interactive Block Rule prompts the user that the destination is forbidden If bypassed, by default, the firewall allows to bypass the block for 600 seconds
Interactive Block with reset		Permit	Intreset	Same as Interactive Block with the addition of a TCP RST in case of non-web traffic

ملاحظة: بدءا من الإصدار 6.3 من برنامج FTD، يمكن أن يعمل إلغاء التحميل الديناميكي للتدفق على إلغاء تحميل الاتصالات التي تفي بالمعايير الإضافية، على سبيل المثال، الحزم الموثوق بها التي تتطلب فحص الشفرة. راجع قسم "إلغاء تحميل الاتصالات الكبيرة (التدفقات)" من دليل تكوين مركز إدارة Firepower للحصول على مزيد من التفاصيل

معلومات ذات صلة

- قواعد التحكم في الوصول إلى FTD
- نهج التصفية المسبقة والتصفية المسبقة ل FTD

- تحليل لقطات جدار حماية FirePOWER لاستكشاف أخطاء الشبكة وإصلاحها بفعالية
- العمل باستخدام إمكانات الدفاع ضد تهديد نظام التشغيل FirePOWER (FTD) وإمكانات اقتفاء حزم البيانات
- تكوين تسجيل الدخول إلى FTD عبر FMC
- الدعم التقني والمستندات - Cisco Systems
- إلغاء تحميل الاتصالات الكبيرة

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).