تكوين سياسات عامل التصفية المسبق لـ FTD وتشغيلها

المحتويات

المقدمة

يصف هذا المستند تكوين سياسات التصفية المسبقة للدفاع عن تهديد FirePOWER (FTD) وتشغيلها.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- ASA5506X الذي يشغل FTD رمز 6.1.0-195
- FireSIGHT Management Center (FMC) الذي يشغل الإصدار 6.1.0-195
- موجهات 3925 Cisco IOS® التي تشغل 15.2 صورة

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

معلومات أساسية

سياسة ما قبل التصفية هي ميزة تم إدخالها في إصدار 6.1 وتخدم ثلاثة أغراض رئيسية:

1. مطابقة حركة المرور استنادا إلى كل من الرؤوس الداخلية والخارجية
2. توفير التحكم بالوصول المبكر الذي يسمح للتدفق بتجاوز محرك الشيخ بشكل كامل
3. العمل كعنصر نائب لإدخالات التحكم في الوصول (ACEs) التي يتم ترحيلها من أداة الترحيل من خلال أجهزة الأمان المعدلة (ASA).

التكوين

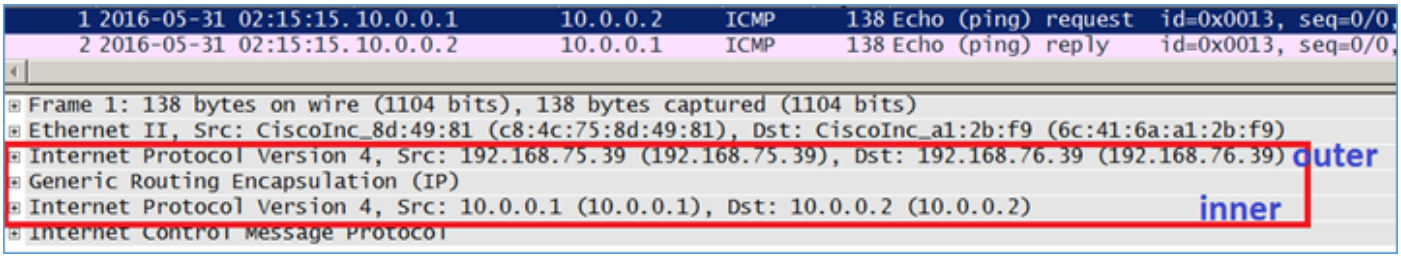
حالة إستخدام نهج عامل التصفية المسبق 1

يمكن لنهج PreFilter إستخدام نوع قاعدة النفق التي تسمح ل FTD بالتصفية استنادا إلى كل من حركة المرور النفقي لرأس IP الداخلية و/أو الخارجية. وقت كتابة هذه المقالة، تشير حركة المرور النفقي إلى:

- تضمين التوجيه العام (GRE)
- IP-in-IP
- IPv6-in-IP
- منفذ Teredo 3544

ضع في اعتبارك نفق GRE كما هو موضح في الصورة.

عند إختبار الاتصال من R1 إلى R2 باستخدام نفق GRE، تمر حركة المرور عبر جدار الحماية كما هو موضح في الصورة.



إذا كان جدار الحماية جهاز ASA، فإنه يتحقق من رأس IP الخارجي كما هو موضح في الصورة.

```
<#root>

ASA#

show conn

GRE OUTSIDE 192.168.76.39:0 INSIDE  192.168.75.39:0

, idle 0:00:17, bytes 520, flags
```

إذا كان جدار الحماية جهاز FirePOWER، فإنه يتحقق من عنوان IP الداخلي كما هو موضح في الصورة.

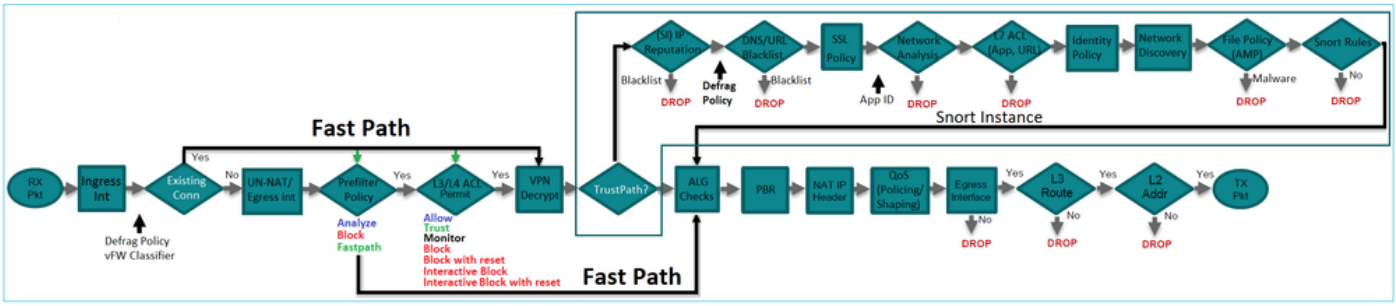
باستخدام نهج عامل التصفية المسبق، يمكن لجهاز FTD مطابقة حركة مرور البيانات استنادا إلى كل من الرؤوس الداخلية والخارجية.

النقطة الرئيسية:

في المثال التالي	شيكات
ASA	IP الخارجي
Snort	IP الداخلي
نظام Firepower Threat Defense (FTD)	خارجي (Prefilter) + IP داخلي (سياسة التحكم في الوصول (ACP))

حالة إستخدام نهج التصفية المسبقة 2

يمكن لنهج PreFilter إستخدام نوع قاعدة Prefilter التي يمكنها توفير التحكم بالوصول المبكر والسماح للتدفق بتجاوز محرك الشخير تماما كما هو موضح في الصورة.



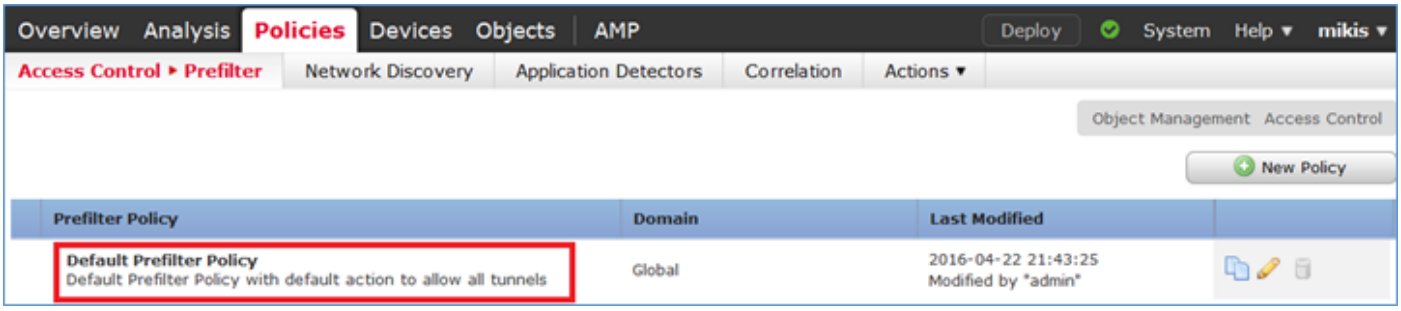
المهمة 1. التحقق من نهج PreFilter الافتراضي

متطلبات المهمة:

التحقق من نهج التصفية المسبقة الافتراضي

الحل:

الخطوة 1. انتقل إلى السياسات > التحكم في الوصول > Prefilter. يوجد نهج افتراضي لـ Prefilter بالفعل كما هو موضح في الصورة.



الخطوة 2. أختر تحرير لترى إعدادات النهج كما هو موضح في الصورة.

الخطوة 3. تم إرفاق "نهج عامل التصفية المسبقة" بالفعل بنهج التحكم بالوصول كما هو موضح في الصورة.

التحقق من CLI (LINA)

تتم إضافة قواعد عامل التصفية المسبق فوق قوائم التحكم في الوصول (ACLs):

```
<#root>

firepower#

show access-list

access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list CSM_FW_ACL_; 5 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998:

PREFILTER POLICY:

 Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit 41 any any rule-id 9998 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 5 advanced permit gre any any rule-id 9998 (hitcnt=5) 0x52c7a066
access-list CSM_FW_ACL_ line 6 advanced permit udp any any eq 3544 rule-id 9998 (hitcnt=0) 0xcf6309bc
```

المهمة 2. حظر حركة المرور النفقي باستخدام العلامة

متطلبات المهمة:

حظر حركة مرور ICMP التي يتم إنشاء قنوات لها داخل نفق GRE.

الحل:

الخطوة 1. إذا قمت بتطبيق قائمة التحكم في الوصول (ACP) هذه، فيمكنك أن ترى حركة مرور بروتوكول رسائل التحكم في الإنترنت (ICMP) محظورة، بغض النظر عما إذا كانت تمر عبر نفق GRE أم لا، كما هو موضح في الصورة.

<#root>

R1#

ping 192.168.76.39

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.76.39, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

<#root>

R1#

ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:

.....
Success rate is 0 percent (0/5)

في هذه الحالة، يمكنك إستخدام نهج PreFilter للوفاء بمتطلبات المهمة. والمنطق هنا هو كالتالي:

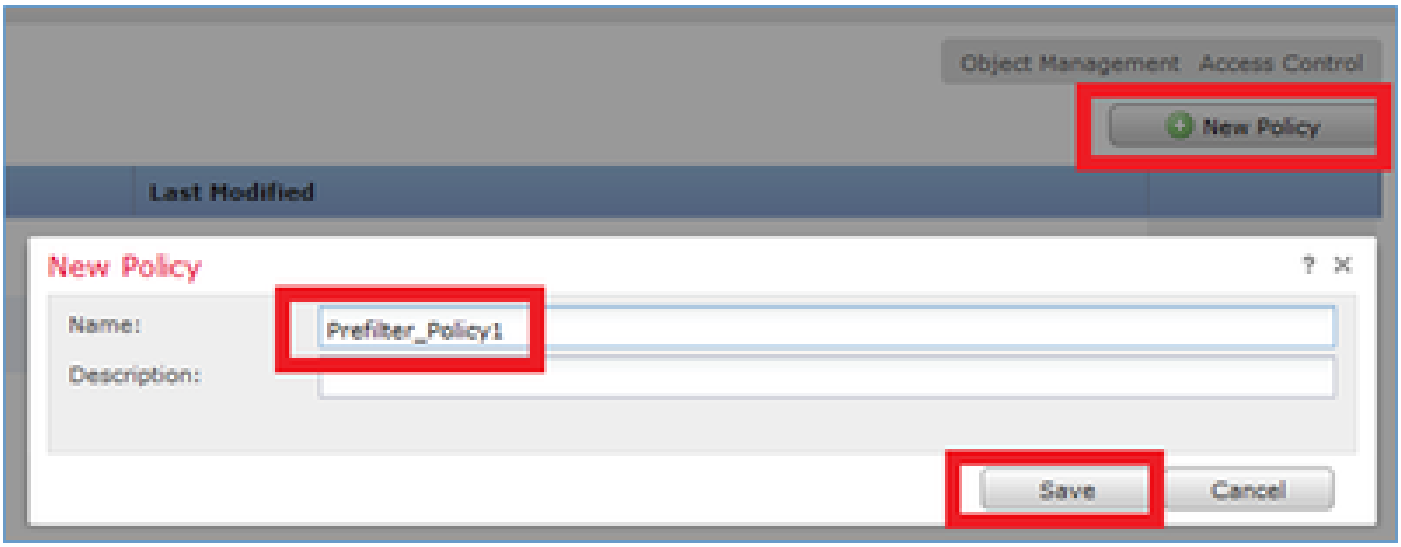
1. وتمييز جميع الحزم التي يتم تضمينها داخل GRE.
2. أنت تقوم بإنشاء سياسة التحكم في الوصول التي تطابق الحزم المميزة وتمنع ICMP.

من وجهة نظر الهندسة المعمارية، فإن الحزم يتم فحصها مقابل قواعد التصفية المسبقة ACP، وأخيرا يقوم LINA بالتنسيب مع LInux (LINA)، ثم شطب قواعد التصفية المسبقة

الشخير بتوجيه LINA للإسقاط. تصل الحزمة الأولى من خلال جهاز FTD.

الخطوة 1. حدد علامة تحرك المرور النفقي.

انتقل إلى السياسات > التحكم في الوصول > PreFilter وقم بإنشاء سياسة Prefilter جديدة. تذكر أنه لا يمكن تحرير نهج Prefilter الافتراضي كما هو موضح في الصورة.

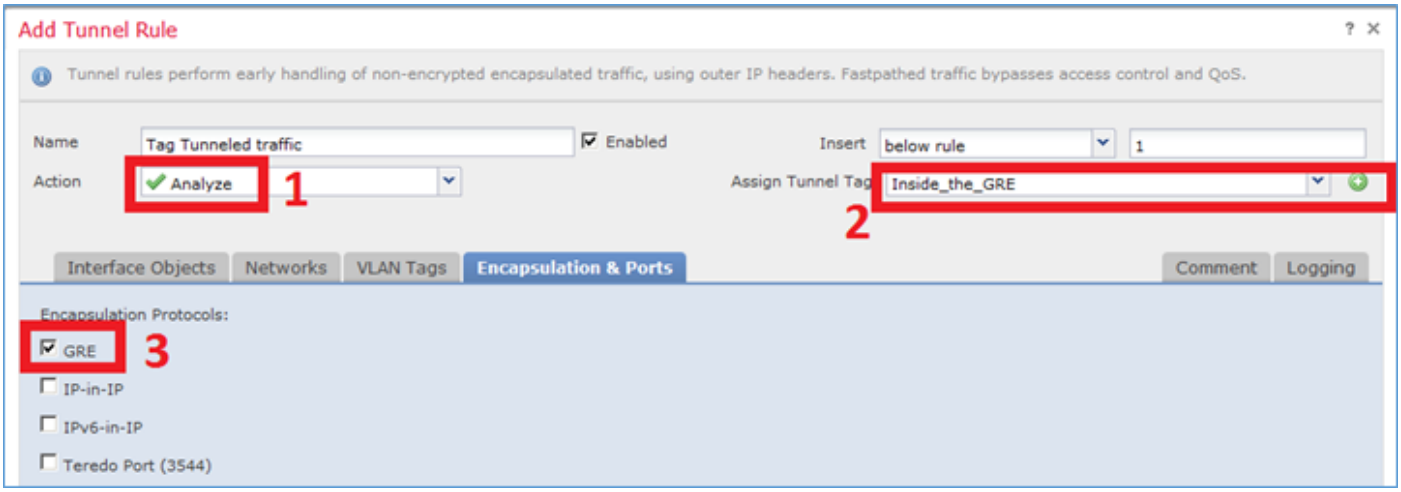


في نهج عامل التصفية المسبق، يمكنك تحديد نوعين من القواعد:

1. قاعدة النفق
2. قاعدة عامل التصفية المسبق

يمكنك التفكير في هذين السمتين على أنهما مميزات مختلفة تمامًا يمكن تكوينها في نهج PreFilter.

لهذه المهمة، من الضروري تعريف قاعدة نفق كما هو موضح في الصورة.



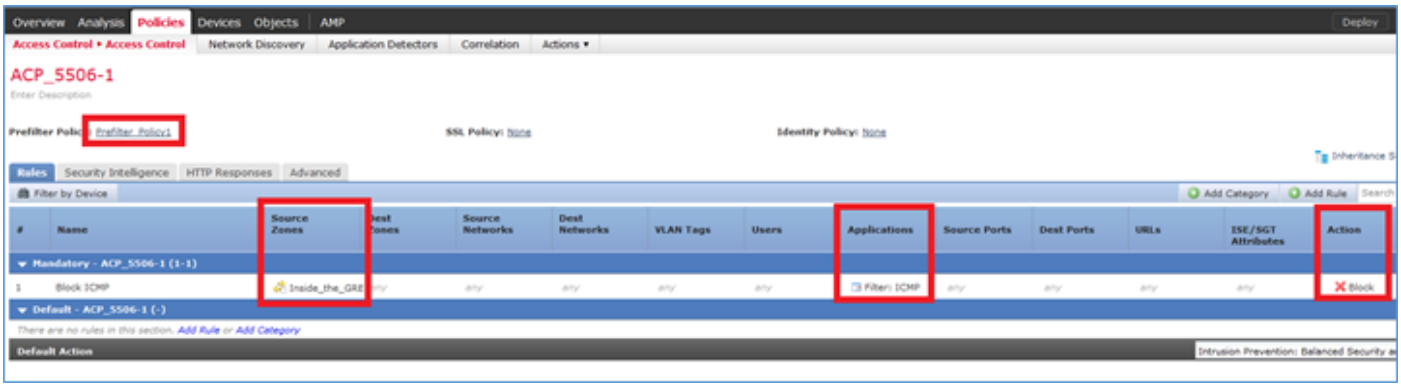
فيما يتعلق بالإجراءات:

الإجراء	الوصف

حللن	بعد LINA، يتم التحقق من التدفق بواسطة محرك الشيخ. إختياري، يمكن تعيين علامة نفق لحركة المرور النفقي.
حظر	تم حظر التدفق بواسطة LINA. يجب التحقق من الرأس الخارجي.
مسار سريع	يتم التعامل مع التدفق بواسطة LINA فقط دون الحاجة إلى الاتصال بمحرك Snort.

الخطوة 2. حدد سياسة التحكم في الوصول لحركة المرور ذات العلامات.

على الرغم من أنه ال يمكن أن يكون بديهيا للغاية في البداية، إال أنه يمكن إستخدام علامة النفق من قبل قاعدة سياسة التحكم بالوصول كمنطقة مصدر. انتقل إلى السياسات > التحكم في الوصول وأنشئ قاعدة تمنع ICMP لحركة المرور ذات عالمات التمييز كما هو موضح في الصورة.



ملاحظة: يتم إرفاق نهج PreFilter الجديد بنهج التحكم في الوصول.

التحقق:

تمكين االلتقاط على LINA وعلى CLISH:

```
<#root>

firepower#

show capture

capture CAPI type raw-data trace interface inside [Capturing - 152 bytes]
capture CAPO type raw-data trace interface outside [Capturing - 152 bytes]
```

```
<#root>

>

capture-traffic
```

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

Selection?

1


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

-n
```

من R1، حاول إختبار اتصال نقطة نهاية نفق GRE البعيد. فشل إختبار الاتصال:

```
<#root>

R1#

ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:

.....
Success rate is 0 percent (0/5)
```

يظهر التقاط CLISH أن أول طلب echo مر عبر FTD وأن الرد تم حظره:

```
<#root>

Options: -n
18:21:07.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo

18:21:07.759939 IP 192.168.76.39 > 192.168.75.39: GREv0, length 104: IP 10.0.0.2 > 10.0.0.1: ICMP echo r

18:21:09.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo
18:21:11.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo
18:21:13.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo
18:21:15.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo
```

ويؤكد التقاط LINA ذلك:

```
<#root>

>

show capture CAPI | include ip-proto-47

 102: 18:21:07.767523  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104
 107: 18:21:09.763739  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104
```

```
 111: 18:21:11.763769  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104
 115: 18:21:13.763784  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104
 120: 18:21:15.763830  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104
>
>
```

show capture CAPO | include ip-proto-47

```
  93: 18:21:07.768133  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104
```

** 94: 18:21:07.768438 192.168.76.39 > 192.168.75.39: ip-proto-47, length 104**

قم بتمكين جدار حماية CLISH-engine-debug ومسح عدادات الإسقاط ل LINA ASP وإجراء نفس الاختبار. ظهر تصحيح أخطاء CLISH أنه بالنسبة إلى Echo-Request، قمت بمطابقة قاعدة عامل التصفية المسبق وقاعدة ACP الخاصة بالرد على الارتداد:

<#root>

```
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0
```

New session

```
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0
```

uses prefilter rule 268434441 with tunnel zone 1

```
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 Starting with minimum 0, id 0 and SrcZone first with zones 1 -> -1,
```

icmpType 8, icmpCode 0

```
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 pending rule order 3, 'Block ICMP', AppId
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0
```

uses prefilter rule 268434441 with tunnel zone 1

```
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 Starting with minimum 0, id 0 and SrcZone first with zones 1 -> -1,
```

icmpType 0, icmpCode 0

```
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0
```

match rule order 3, 'Block ICMP', action Block

```
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 deny action
```

يوضح إسقاط ASP أن Snort أسقط الحزم:

<#root>

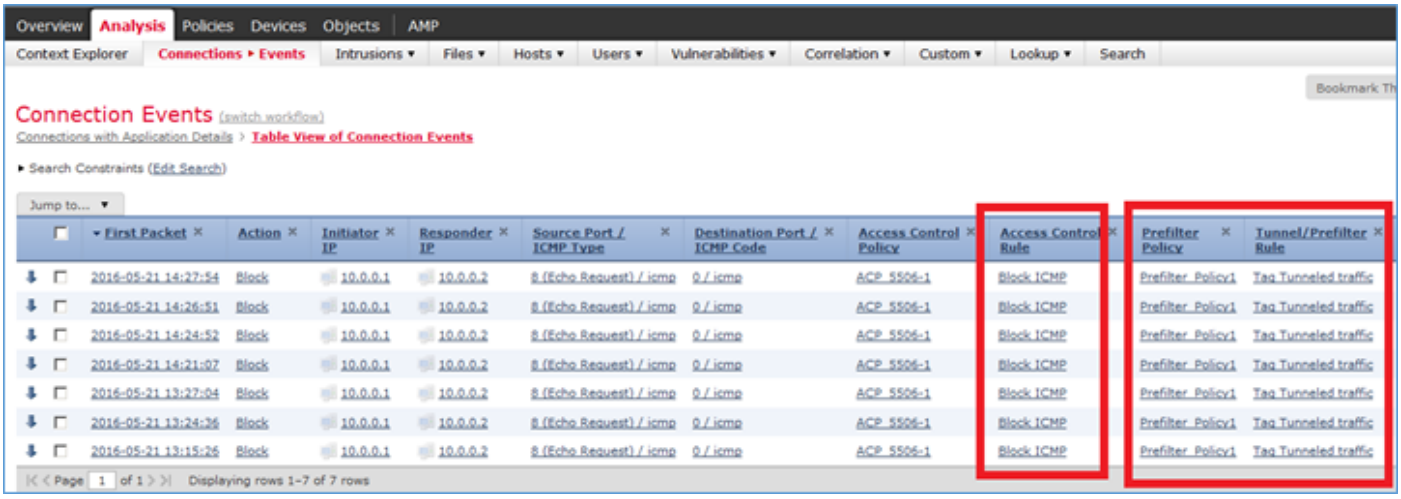
```
>
```

show asp drop

```
Frame drop:
  No route to host (no-route)                                   366
  Reverse-path verify failed (rpf-violated)                       2
  Flow is denied by configured rule (acl-drop)                    2
```

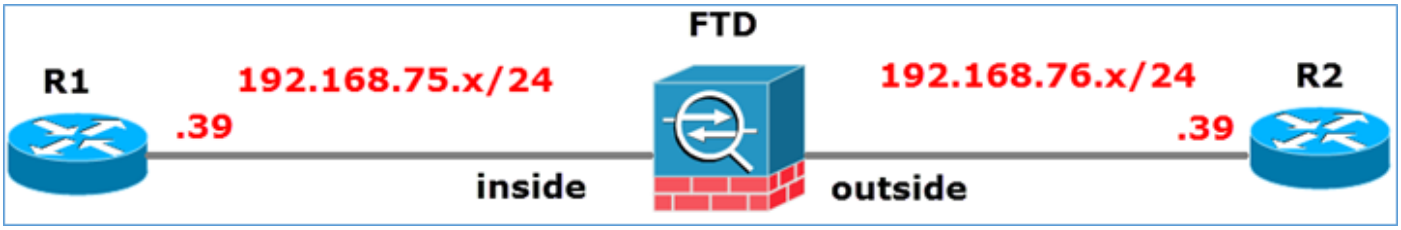
```
Snort requested to drop the frame (snort-drop)                5
```

في "أحداث الاتصال"، يمكنك مشاهدة "نهج وأسس Prefilter" التي قمت بمطابقتها كما هو موضح في الصورة.



المهمة 3. تجاوز Snort Engine باستخدام قواعد FastPath Prefilter

الرسم التخطيطي للشبكة

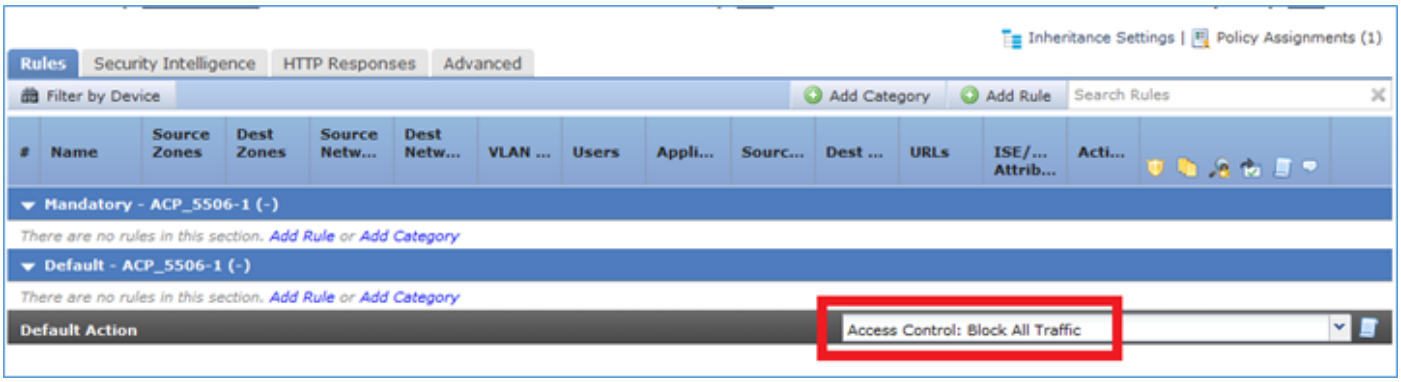


متطلبات المهمة:

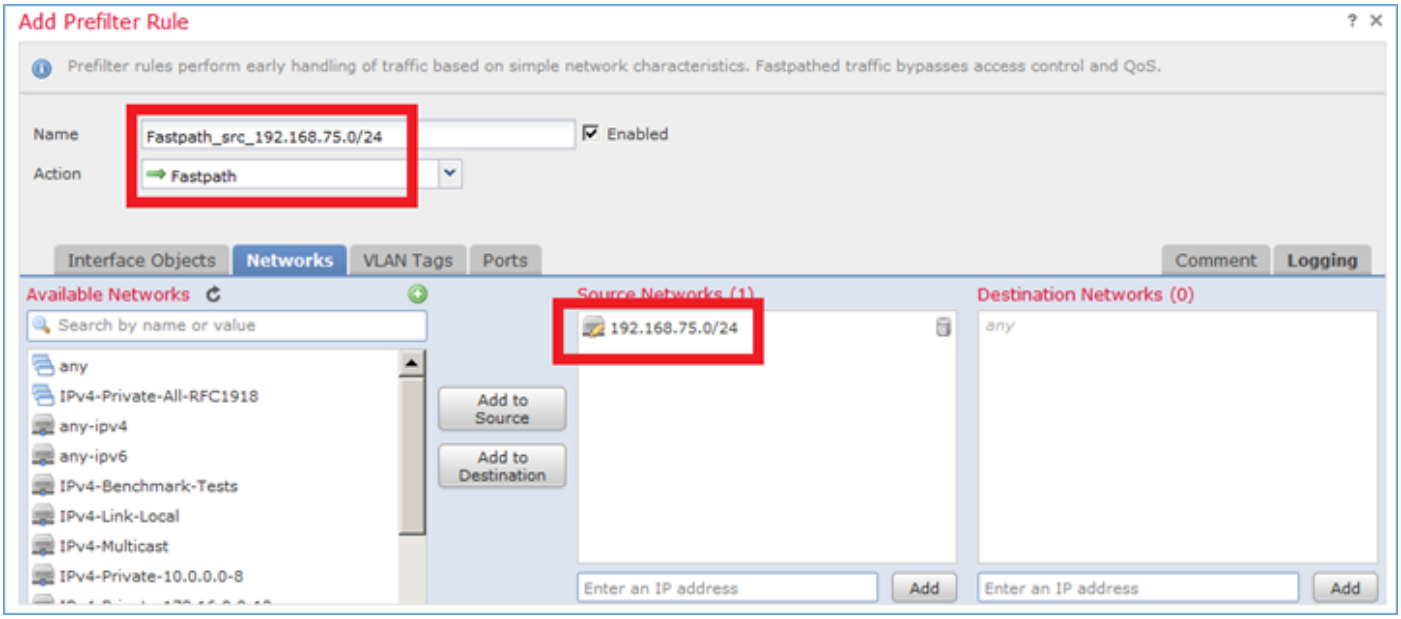
1. قم بإزالة قواعد نهج التحكم بالوصول الحالية وإضافة قاعدة "نهج التحكم بالوصول" التي تمنع حركة المرور بالكامل.
2. قم بتكوين قاعدة نهج Prefilter التي تتجاوز Snort Engine لحركة مرور البيانات التي يتم الحصول عليها من شبكة 192.168.75.0/24.

الحل:

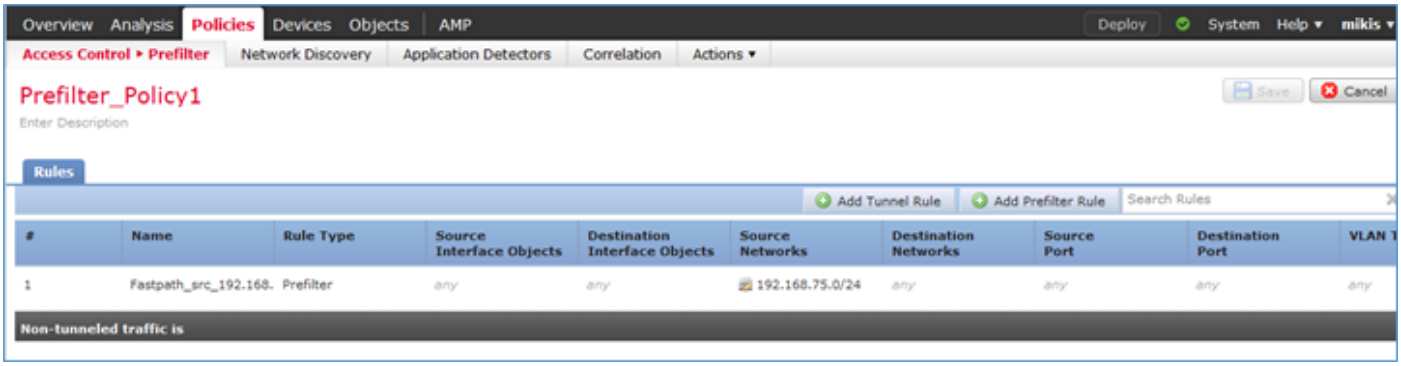
الخطوة 1. يتم وضع نهج التحكم في الوصول الذي يمنع حركة مرور البيانات بالكامل كما هو موضح في الصورة.



الخطوة 2. قم بإضافة قاعدة Prefilter مع FastPath كإجراء لشبكة المصدر 192.168.75.0/24 كما هو موضح في الصورة.



الخطوة 3. النتيجة كما هو موضح في الصورة.



الخطوة 4. حفظ ونشر.

تمكين الالتقاط باستخدام تتبع على كل من واجهات FTD:

<#root>

firepower#

capture CAPI int inside trace match icmp any any

```
firepower#

capture CAPO int outsid trace match icmp any any
```

حاول إختبار الاتصال من R1 (192.168.75.39) إلى R2 (192.168.76.39) من خلال FTD. فشل إختبار الاتصال:

```
<#root>

R1#

ping 192.168.76.39

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.76.39, timeout is 2 seconds:

.....
Success rate is 0 percent (0/5)
```

التقاط على الواجهة الداخلية يوضح:

```
<#root>

firepower#

show capture CAPI


5 packets captured

   1: 23:35:07.281738   192.168.75.39 > 192.168.76.39: icmp: echo request
   2: 23:35:09.278641   192.168.75.39 > 192.168.76.39: icmp: echo request
   3: 23:35:11.279251   192.168.75.39 > 192.168.76.39: icmp: echo request
   4: 23:35:13.278778   192.168.75.39 > 192.168.76.39: icmp: echo request
   5: 23:35:15.279282   192.168.75.39 > 192.168.76.39: icmp: echo request
5 packets shown
```

تتبع أول حزمة (echo-request) عرض (النقاط المهمة المميزة):

مفسد (إبراز إلى القراءة)

تتبع Firepower# show capture CAPI Packet-Number 1

5 حزم ملتقطة

1: 23:35:07.281738 192.168.75.39 > 192.168.76.39: ICMP: طلب echo

المرحلة: 1

النوع: الالتقاط

النوع الفرعي:

النتيجة: السماح

التكوين:

معلومات إضافية:

قائمة الوصول إلى MAC

المرحلة: 2

النوع: قائمة الوصول

النوع الفرعي:

النتيجة: السماح

التكوين:

قاعدة ضمنية

معلومات إضافية:

قائمة الوصول إلى MAC

المرحلة: 3

النوع: بحث المسار

النوع الفرعي: حل واجهة الخروج

النتيجة: السماح

التكوين:

معلومات إضافية:

تم العثور على الخطوة التالية 192.168.76.39 يستخدم مخرج IFC خارج

المرحلة: 4

النوع: قائمة الوصول

النوع الفرعي: السجل

النتيجة: السماح

التكوين:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ Advanced Trust IP 192.168.75.0 255.255.255.0 أي قاعدة-id 26843448

الك ثادحألا لجس

access-list CSM_FW_ACL_ مظحالم rule-id 26843448: نمض ام قبل التصفية: prefilter_policy1

access-list csm_fw_acl_ مظحالم rule-id 26843448: الدعاقلا: FastPath_src_192.168.75.0/24

معلومات إضافية:

المرحلة: 5

النوع: conn-settings

النوع الفرعي:

النتيجة: السماح

التكوين:

الفئة-خريطة الافتراضي لفئة

مطابقة أي

خريطة السياسة العامة العامة_السياسة

الفئة الافتراضية

ضبط الاتصال خيارات متقدمة UM_STATIC_TCP_MAP

عمومي_policy-service-policy

معلومات إضافية:

المرحلة: 6

النوع: NAT

النوع الفرعي: لكل جلسة

النتيجة: السماح

التكوين:

معلومات إضافية:

المرحلة: 7

النوع: خيارات IP

النوع الفرعي:

النتيجة: السماح

التكوين:

معلومات إضافية:

المرحلة: 8

النوع: التفتيش

النوع الفرعي: np-inspection

النتيجة: السماح

التكوين:

class-map inspection_default

مطابقة فحص افتراضي-حركة مرور

خريطة السياسة العامة العامة_السياسة

class inspection_default

فحص ICMP

عمومي_policy-service-policy

معلومات إضافية:

المرحلة: 9

النوع: التفتيش

النوع الفرعي: np-inspection

النتيجة: السماح

التكوين:

معلومات إضافية:

المرحلة: 10

النوع: NAT

النوع الفرعي: لكل جلسة

النتيجة: السماح

التكوين:

معلومات إضافية:

المرحلة: 11

النوع: خيارات IP

النوع الفرعي:

النتيجة: السماح

التكوين:

معلومات إضافية:

المرحلة: 12

النوع: إنشاء التدفق

النوع الفرعي:

النتيجة: السماح

التكوين:

معلومات إضافية:

تم إنشاء تدفق جديد باستخدام المعرف 52، يتم إرسال الحزمة إلى الوحدة النمطية التالية

المرحلة: 13

النوع: قائمة الوصول

النوع الفرعي: السجل

النتيجة: السماح

التكوين:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ Advanced Trust IP 192.168.75.0 255.255.255.0 أي قاعدة-id 26843448 سجل الكل الأحداث

access-list CSM_FW_ACL_ ملاحظة rule-id 26843448: من جهة ما قبل التصفية: prefilter_policy1

access-list csm_fw_acl_ ملاحظة rule-id 26843448: القاعدة: FastPath_src_192.168.75.0/24

معلومات إضافية:

المرحلة: 14

النوع: conn-settings

النوع الفرعي:

النتيجة: السماح

التكوين:

الفئة-خريطة الافتراضي لفئة

مطابقة أي

خريطة السياسة العامة العامة_السياسة

الفئة الافتراضية

ضبط الاتصال خيارات متقدمة UM_STATIC_TCP_MAP

عمومي_policy-service-policy

معلومات إضافية:

المرحلة: 15

النوع: NAT

النوع الفرعي: لكل جلسة

النتيجة: السماح

التكوين:

معلومات إضافية:

المرحلة: 16

النوع: خيارات IP

النوع الفرعي:

النتيجة: السماح

التكوين:

معلومات إضافية:

المرحلة: 17

النوع: بحث المسار

النوع الفرعي: حل واجهة الخروج

النتيجة: السماح

التكوين:

معلومات إضافية:

تم العثور على الخطوة التالية 192.168.76.39 يستخدم خرج IFC خارج

المرحلة: 18

النوع: التواجد-البحث

النوع الفرعي: الخطوة التالية والتواجد

النتيجة: السماح

التكوين:

معلومات إضافية:

نشاط التواجد

عنوان MAC للخطوة التالية 004.deab.681b يضرب 140372416161507

المرحلة: 19

النوع: الالتقاط

النوع الفرعي:

النتيجة: السماح

التكوين:

معلومات إضافية:

قائمة الوصول إلى MAC

النتيجة:

واجهة الإدخال: خارج

حالة الإدخال: لأعلى

حالة خط الإدخال: للأعلى

واجهة الإخراج: خارج

حالة الإخراج: لأعلى

حالة خط الإخراج: لأعلى

الإجراء: السماح

تم عرض حزمة واحدة

Firepower#

Firepower# show capture capi packet-number 1 trace 5 packet capture 1: 23:35:07.281738 192.168.75.39 > 192.168.76.39: icmp: echo request phase: 1 type: capture subtype: result: allow config: معلومات إضافية: mac access list phase: 2type: access-list subtype: result: allow config: Implicit rule additional information: mac access phase: النوع 3: النوع الفرعي للبحث عن المسار: حل نتيجة واجهة الخروج: السماح بالتكوين: معلومات إضافية: تستخدم الخطوة

التالية 192.168.76.39 egress ifc جراخ المرحلة: النوع 4: النوع الفرعي قائمة الوصول: نتيجة السجل: السماح بالتكوين: access-group csm_fw_acl_ global access-list csm_fw_acl_advanced trust ip 192.168.75.255.255.55.5 0 أي سجل أحداث لمعرف القاعدة 268434448 الك نم قائمة الوصول CSM_FW_ACL_ المظلة قاعدة-id 268434448: نهج PREFILTER: PreFilter_Policy1 access-list CSM_FW_ACL_ المظلة قاعدة-id 268434448: القاعدة: FastPath_src_192.168.75.0/24 معلومات إضافية: المرحلة 5: النوع: CONN-Settings subtype: السماح بالنوع: config: class-map class-default مطابقة أي سياسة-map global_policy class-default مجموعة اتصال متقدم-options UM_STATIC_TCP_MAP service-policy global_policy معلومات إضافية: المرحلة: 6 نوع: NAT subtype: لك جلسة نتيجة: السماح بالتconfig: معلومات إضافية: المرحلة 7: النوع: ip-options subtype: النتيجة: السماح بالتكوين: المرحلة 8: فحص النوع الفرعي: np-inspection نتيجة: السماح للتكوين: class-map_inspection_match-default-inspection-traffic-policy-class فحص معلومات إضافية عمومية ICMP service-policy global_policy: المرحلة: 9 النوع: فحص النوع الفرعي: np-inspection result: Allow config: معلومات إضافية: المرحلة 10: النوع الفرعي nat: لك جلسة نتيجة: Allow config: معلومات إضافية: المرحلة 11: النوع الفرعي: IP-Options: النتيجة: Allow config: معلومات إضافية: المرحلة 12 النوع: النوع الفرعي إنشاء التدفق: النتيجة: Allow config: معلومات إضافية: نوع 13: المرحلة التالية الوحدة إلى أرسلت حزمة، 52 معرف باستخدام جديد تدفق إنشاء تم Access-list subtype: log result: allow config: access-group csm_fw_acl_ global access-list csm_fw_acl_ advanced trust ip 192.168.75.0 255.255.255.0 any rule-id 26843448 event-log الك access-list CSM_FW_ACL المظلة rule-id 268444448: نهج ما قبل التصفية: PreFilter_Policy1 access-list CSM_FW_ACL_ المظلة قاعدة-id 26843448: القاعدة: FastPath_src_192.168.75.0/24 معلومات إضافية: المرحلة: 14 النوع: CONN-Settings subtype: النتيجة: السماح بالتكوين: class-map-default مطابقة أي نهج-map_global_policy class-default مجموعة اتصال متقدم-options UM_STATIC_TCP_MAP service-policy_global معلومات إضافية: المرحلة 15: نوع فرعي ل NAT: لك جلسة عمل: يسمح config: معلومات إضافية: المرحلة: 16 نوع: IP-options subtype: النتيجة: يسمح config: معلومات إضافية: المرحلة 17: النوع الفرعي: حل نقطة الوصول: حل نقطة الوصول نتيجة: يسمح بالتكوين: معلومات إضافية: تم العثور على المرحلة التالية 192.168.76.39 يستخدم مخرج IFC جراخ المرحلة: 18 النوع: التجاور-البحث الفرعي: عنوان MAC من خلال إضافية: معلومات: يسمح بالتكوين: التجاور نتيجة والتالية الخطوة التالية 14004.deab.681b: 140372416161507: النوع الخطوة التالية النشطة في التجاور إلى المرحلة 19: النوع الفرعي ل CAPTURE: النتيجة: السماح بالتكوين: معلومات إضافية: نتيجة قائمة الوصول إلى MAC: وضع الإدخال-interface: حالة خط الإدخال: وضع خط الإدخال لأعلى: حالة الإخراج: حالة خط الإخراج لأعلى: الإجراء: السماح بحزمة عرض FirePower#

التقاط على الواجهة الخارجية يوضح:

<#root>

```
firepower#
```

show capture CAPO

```
10 packets captured

   1: 23:35:07.282044   192.168.75.39 > 192.168.76.39: icmp: echo request
   2: 23:35:07.282227   192.168.76.39 > 192.168.75.39: icmp: echo reply
   3: 23:35:09.278717   192.168.75.39 > 192.168.76.39: icmp: echo request
   4: 23:35:09.278962   192.168.76.39 > 192.168.75.39: icmp: echo reply
   5: 23:35:11.279343   192.168.75.39 > 192.168.76.39: icmp: echo request
   6: 23:35:11.279541   192.168.76.39 > 192.168.75.39: icmp: echo reply
```

```
   7: 23:35:13.278870   192.168.75.39 > 192.168.76.39: icmp: echo request
   8: 23:35:13.279023   192.168.76.39 > 192.168.75.39: icmp: echo reply
   9: 23:35:15.279373   192.168.75.39 > 192.168.76.39: icmp: echo request
  10: 23:35:15.279541   192.168.76.39 > 192.168.75.39: icmp: echo reply
10 packets shown
```

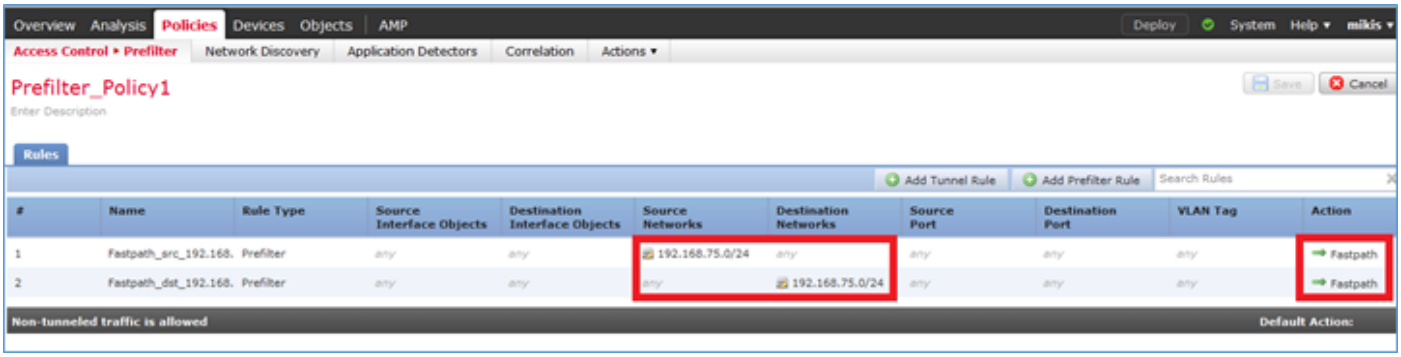
يظهر تتبع الحزمة المرتجعة أنها تطابق التدفق الحالي (52)، ولكن تم حظرها بواسطة قائمة التحكم في الوصول (ACL):

```
<#root>

firepower#

show capture CAPO packet-number 2 trace


10 packets captured



2: 23:35:07.282227       192.168.76.39 > 192.168.75.39: icmp: echo reply

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 52, uses current flow


Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: DROP

Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip any any rule-id 268434432 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: ACP_5506-1 - Default/1
```

```
access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
Additional Information:

Result:
input-interface: outside
input-status: up
input-line-status: up
Action: drop
```

Drop-reason: (acl-drop) Flow is denied by configured rule

الخطوة 5. قم بإضافة قاعدة عامل تصفية مسبق أخرى لحركة المرور العائدة. النتيجة كما هو موضح في الصورة.



الآن تتبع الحزمة المرتجعة التي تراها (النقاط المهمة مبرزة):

مفسد (إبراز إلى القراءة)

تتبع Firepower# show capture CAPO Packet-2

10 حزم ملتقطة

2: 00:01:38.873123 192.168.76.39 > 192.168.75.39: ICMP: رد echo

المرحلة: 1

النوع: االلتقاط

النوع الفرعي:

النتيجة: السماح

التكوين:

معلومات إضافية:

قائمة الوصول إلى MAC

المرحلة: 2

النوع: قائمة الوصول

النوع الفرعي:

النتيجة: السماح

التكوين:

قاعدة ضمنية

معلومات إضافية:

قائمة الوصول إلى MAC

المرحلة: 3

النوع: Flow-lookup

النوع الفرعي:

النتيجة: السماح

التكوين:

معلومات إضافية:

تم العثور على تدفق بالمعرف 62، يستخدم التدفق الحالي

المرحلة: 4

النوع: قائمة الوصول

النوع الفرعي: السجل

النتيجة: السماح

التكوين:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ Advanced Trust IP any 192.168.75.0 255.255.255.0 rule-id 26843450 event-log الكل

access-list CSM_FW_ACL_ مطابقة rule-id 268434450: نهج ما قبل التصفية: prefilter_policy1

access-list csm_fw_acl_ مطابقة rule-id 268434450: القاعدة: FastPath_dst_192.168.75.0/24

معلومات إضافية:

المرحلة: 5

النوع: conn-settings

النوع الفرعي:

النتيجة: السماح

التكوين:

الفئة-خريطة الافتراضي لفئة

أي مطابقة

خريطة السياسة العامة العامة_السياسة

الفئة الافتراضية

ضبط الاتصال خيارات متقدمة UM_STATIC_TCP_MAP

عمومي_policy-service-policy

معلومات إضافية:

المرحلة: 6

النوع: NAT

النوع الفرعي: لكل جلسة

النتيجة: السماح

التكوين:

معلومات إضافية:

المرحلة: 7

النوع: خيارات IP

النوع الفرعي:

النتيجة: السماح

التكوين:

معلومات إضافية:

المرحلة: 8

النوع: بحث المسار

النوع الفرعي: حل واجهة الخروج

النتيجة: السماح

التكوين:

معلومات إضافية:

تم العثور على الخطوة التالية 192.168.75.39 تستخدم مخرج IFC من الداخل

المرحلة: 9

النوع: التجاوز-البحث

النوع الفرعي: الخطوة التالية والتجاوز

النتيجة: السماح

التكوين:

معلومات إضافية:

نشاط التجاوز

عنوان MAC للخطوة التالية c84c.758d.4981 بضرب 140376711128802

المرحلة: 10

النوع: التالقاط

النوع الفرعي:

النتيجة: السماح

التكوين:

معلومات إضافية:

قائمة الوصول إلى MAC

النتيجة:

واجهة الإدخال: من الداخل

حالة الإدخال: ألعلى

حالة خط الإدخال: للألعلى

واجهة الإخراج: من الداخل

حالة الإخراج: ألعلى

حالة خط الإخراج: ألعلى

الإجراء: السماح

Firepower# show capture capo packet-number 2 trace 10 packet capture 2: 00:01:38.873123 192.168.76.39 > 192.168.75.39: icmp: echo response phase: 1 type: capture subtype: result: allow config: معلومات إضافية: mac access list phase: 2 type: access-list subtype: result: allow config: Implicit rule إضافي معلومات: mac access list المرحلة: 3 النوع: النوع الفرعي: Flow-Lookup: النتيجة: Allow config: معلومات إضافية: تم العثور عليها باستخدام المعرف 62، يستخدم

مرحلة التدفق الحالية: 4 نوع: Access-LIST subtype: log result: allow config: access-group csm_fw_acl_ global access-list csm_fw_acl_ advanced trust ip any 192.168.75.0 255.255.255.0 rule-id 2684405 سجل الأحداث كل من access-list csm_FW_ACL_ مطابقة rule-id 268434450: PREfilter Policy: Prefilter_Policy1 access-list CSM_FW_ACL_ مطابقة rule-id 268434450: القاعدة: FastPath_dst_192.168.75.0/24 معلومات إضافية: المرحلة 5: النوع الفرعي: CONN-SETTINGS: النتيجة: السماح للCONFIG: CLASS-MAP-DEFAULT أي مطابقة POLICY-MAP_CLASS DEFAULT الاتصال ADVANCED-OPTIONS UM_STATIC_TCP_MAP service-policy global_policy معلومات إضافية: المرحلة: 6 نوع: NAT subtype: لكل جلسة نتيجة: يسمح config: معلومات إضافية: المرحلة 7: النوع الفرعي: IP-OPTIONS: النتيجة: السماح بالتconfig: معلومات إضافية: المرحلة: النوع 8: ROUTE-LOOKUP subtype: حل مشكلة واجهة الخروج نتيجة: السماح 192.168.75.39 يستخدم config: معلومات إضافية: تم العثور على الخطوة التالية الخطوة التالية ونتيجة EGRESS داخل المرحلة: النوع 9: النوع الفرعي للبحث عن التجاوز: الخطوة التالية عنوان MAC التجاوز: السماح بالتكوين: معلومات إضافية: التجاوز نشط من الخطوة التالية 14037671128802 المرحلة: النوع 10: التقاط نوع فرعي: النتيجة: c84c.758d.4981 يضرب السماح بالتكوين: معلومات إضافية: قائمة الوصول إلى MAC نتيجة: واجهة الإدخال: حالة خط الإدخال: وضع خط الإدخال التصاعدي: حالة الإخراج في الداخل: وضع خط الإخراج: وضع خط الإخراج الإدخال: السماح الإجراء ألعلى:

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

وقد تم شرح عملية التحقق في أقسام المهام ذات الصلة.

استكشاف الأخطاء وإصلاحها

هناك حاليا ما من معلومة محددة يتوفر أن يتحرى هذا تشكيل.

معلومات ذات صلة

- يمكن العثور على جميع إصدارات دليل تكوين Cisco Firepower Management Center هنا:

التنقل عبر وثائق الدفاع عن تهديد جدار الحماية الآمن من Cisco

- يوصي مركز المساعدة التقنية العالمي (TAC) من Cisco بشدة بهذا الدليل المرئي للمعرفة العملية المتعمقة حول تقنيات أمان الجيل التالي من Cisco Firepower، والتي تتضمن التقنيات المذكورة في هذه المقالة:

الدفاع ضد تهديد FirePOWER (FTD) من Cisco

- لجميع عمليات التهيئة واستكشاف أخطاء المالحظات التقنية وإصالحها:

مركز إدارة جدار الحماية الآمن من Cisco

- الدعم التقني والمستندات - Cisco Systems

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