تحليل التقاط جدار حماية FirePOWER لاستكشاف أخطاء الشبكة وإصلاحها

المحتويات

المقدمة

يصف هذا المستند تقنيات تحليل مختلفة لالتقاط الحزم تهدف إلى استكشاف مشكلات الشبكة وإصلاحها بفاعلية.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- بنية النظام الأساسي Firepower
- سجلات NGFW
- NGFW Packet-tracer

بالإضافة إلى ذلك، قبل البدء في تحليل التقاط الحزم، من المستحسن بشدة تلبية هذه المتطلبات:

- تعرف عملية البروتوكول - ال تبدأ في التحقق من التقاط حزمة إذا لم تفهم كيفية عمل البروتوكول الذي تم االستيالء عليه.
- تعرف المخطط - يجب أن تعرف أجهزة النقل من نهاية إلى نهاية. إذا لم يكن هذا ممكنا، فيجب عليك على الأقل معرفة أجهزة تدفق البيانات من الخادم والتدفق.
- تعرف على الجهاز - يجب أن تعرف كيفية معالجة جهازك للحزم، وما هي الواجهات المعنية (الدخول/الخروج)، وما هي بنية الجهاز، وما هي نقاط االلتقاط المختلفة.
- تعرف التكوين - يجب أن تعرف كيفية التعامل مع تدفق الحزمة بواسطة الجهاز فيما يتعلق ب:
  - واجهة التوجيه/الخروج

- السياسات المطبقة
- ترجمة عنوان الشبكة (NAT)

- تعرف الأدوات المتاحة - بجانب عمليات الالتقاط، يوصى بأن تكون جاهزة لتطبيق الأدوات والتقنيات الأخرى (مثل التسجيل وتتبع الأثر) وإذا لزم الأمر، قم بربطها بالحزم التي تم التقاطها.

المكونات المستخدمة

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

- تستند معظم السيناريوهات إلى FP4140 الذي يشغل برنامج FTD الإصدار 6.5.x.
- برنامج تشغيل FMC الإصدار 6.5.x.

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

التقاط الحزمة هو أحد أدوات أستكشاف الأخطاء وإصلاحها الأكثر إهمالا المتوفرة اليوم. يوميا، يحل TAC من Cisco العديد من المشاكل مع تحليل البيانات الملتقطة.

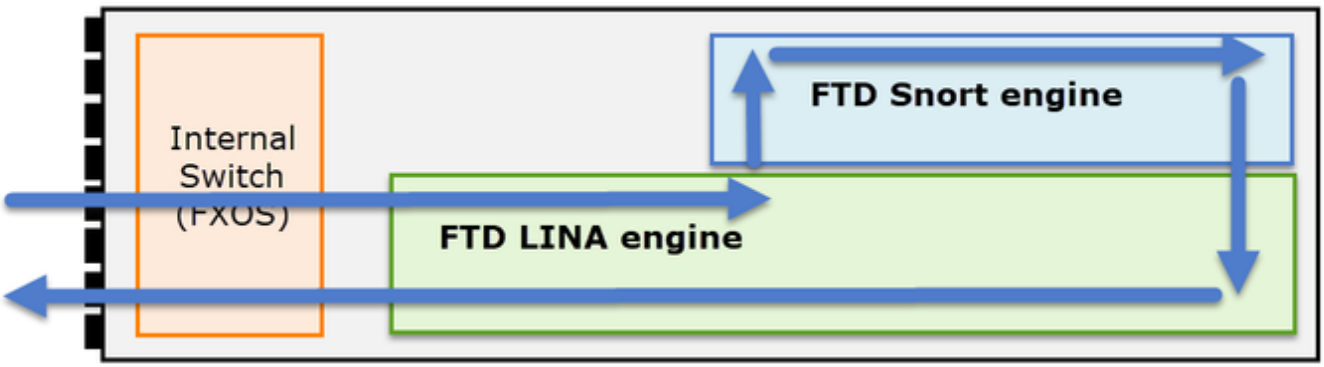
الهدف من هذا المستند هو مساعدة مهندسي الشبكة والأمان في تحديد مشاكل الشبكة الشائعة واستكشاف أخطائها وإصلاحها استنادا إلى تحليل التقاط الحزم أساسا.

تستند جميع السيناريوهات المقدمة في هذا المستند إلى حالات مستخدم حقيقي شوهدت في مركز المساعدة التقنية (TAC) من Cisco.

يغطي المستند عمليات التقاط الحزمة من وجهة نظر جدار حماية الجيل التالي (NGFW) من Cisco، ولكن يتم تطبيق نفس المفاهيم على أنواع الأجهزة الأخرى أيضا.

كيف يمكنك تجميع صور على مجموعة منتجات جدار الحماية من الجيل التالي (NGFW) وتصديرها؟

في حالة جهاز أمان FirePOWER (1xxx، 21xx، 41xx، 93xx) وتطبيق Firepower Threat Defense (FTD)، يمكن عرض معالجة الحزمة كما هو موضح في الصورة.



1. تدخل الحزمة واجهة الدخول ويتم معالجتها بواسطة المحول الداخلي للهيكل.
2. تدخل الحزمة إلى محرك FTD Lina الذي يقوم أساسا بالتحقق من L3/L4.
3. إذا كان النهج يتطلب فحص الحزمة بواسطة محرك snort (فحص L7 بشكل أساسي).
4. يرجع محرك الشيخ حكما للحزمة.
5. يقوم محرك LINA بإسقاط الحزمة أو إعادة توجيهها بناءً على قرار Snort.
6. تعمل الحزمة على تركيب الهيكل من خلال محول الهيكل الداخلي.

استنادا إلى البنية الموضحة، يمكن التقاط "برنامج الإرسال فائق السرعة (FTD)" في ثلاثة (3) أماكن مختلفة:

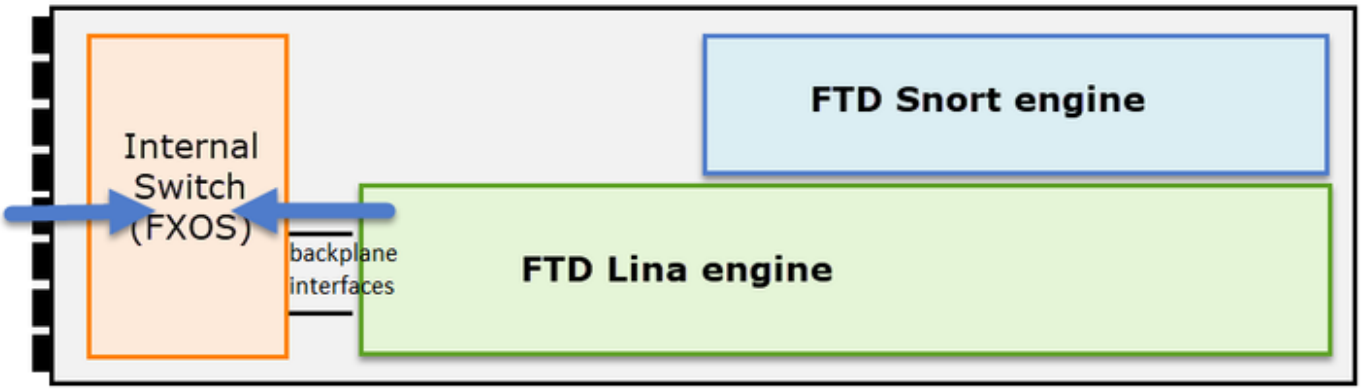
- FXOS
- محرك FTD Lina
- محرك شيخ FTD

تجميع التقاط FXOS

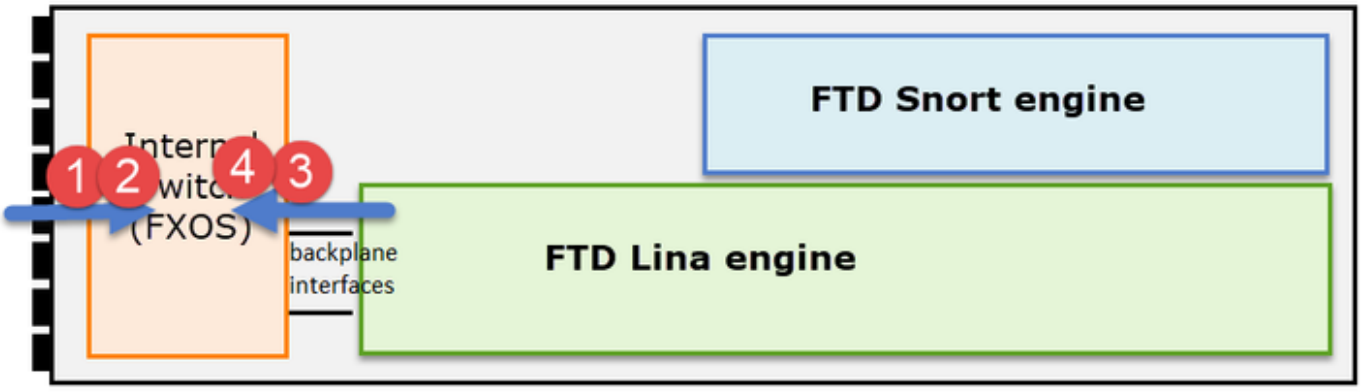
يتم وصف العملية في هذا المستند:

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos271/web-guide/b_GUI_FXOS_ConfigGuide_271/troubleshooting.html#concept_E8823CC63C934A909BBC0DF12F

يمكن التقاط FXOS فقط أن تؤخذ في إتجاه المدخل من نقطة عرض المحول الداخلي تظهر في الصورة هنا.



كما هو موضح هنا، هاتان نقطتا التقاط لكل إتجاه (بسبب بنية المحول الداخلي).



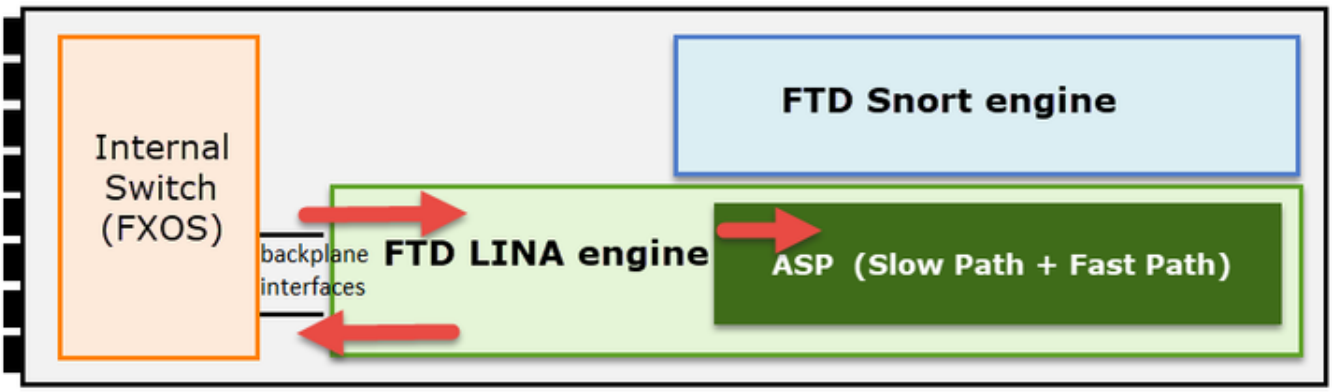
تتضمن الحزم الملتقطة في النقاط 2، 3، و 4 علامة شبكة ظاهرية (VNTag).

ملاحظة: تتوفر التقاط مستوى الهيكل بنظام FXOS فقط على الأنظمة الأساسية FP41xx و FP93xx. لا تتوفر FP1xxx و FP21xx هذه الإمكانية.

تمكين وتجميع عمليات التقاط FTD Lina

نقاط الالتقاط الرئيسية:

- واجهة الدخول
- واجهة الخروج
- مسار الأمان السريع (ASP)



يمكنك إستخدام واجهة المستخدم الخاصة ب Firepower Management Center (واجهة مستخدم FMC) أو واجهة سطر الأوامر (CLI) الخاصة ب FTD لتمكين وتجميع عمليات الالتقاط الخاصة ب FTD Lina.

تمكين الالتقاط من CLI على الواجهة الداخلية:

```
<#root>

firepower#

capture CAPI interface INSIDE match icmp host 192.168.103.1 host 192.168.101.1
```

يتطابق هذا الالتقاط مع حركة المرور بين IPs 192.168.103.1 و 192.168.101.1 في كلا الاتجاهين.

تمكين التقاط ASP لرؤية جميع الحزم التي تم إسقاطها بواسطة محرك FTD Lina:

```
<#root>

firepower#

capture ASP type asp-drop all
```

تصدير التقاط خط FTD إلى خادم FTP:

```
<#root>

firepower#

copy /pcap capture:CAPI ftp://ftp_username:ftp_password@192.168.78.73/CAPI.pcap
```

تصدير التقاط خط FTD إلى خادم TFTP:

```
<#root>

firepower#

copy /pcap capture:CAPI tftp://192.168.78.73
```

بدءا من إصدار FMC 6.2.x، يمكن تمكين وتجميع مجموعات FTD Lina من واجهة مستخدم FMC.

هناك طريقة أخرى لتجميع لقطات FTD من جدار حماية تتم إدارته من قبل FMC، وهي:

الخطوة 1

في حالة LINA أو ASP التقاط انسخ التقاط إلى قرص FTD.

```
<#root>

firepower#

copy /pcap capture:capin disk0:capin.pcap

Source capture name [capin]?

Destination filename [capin.pcap]?
!!!!
```

الخطوة 2

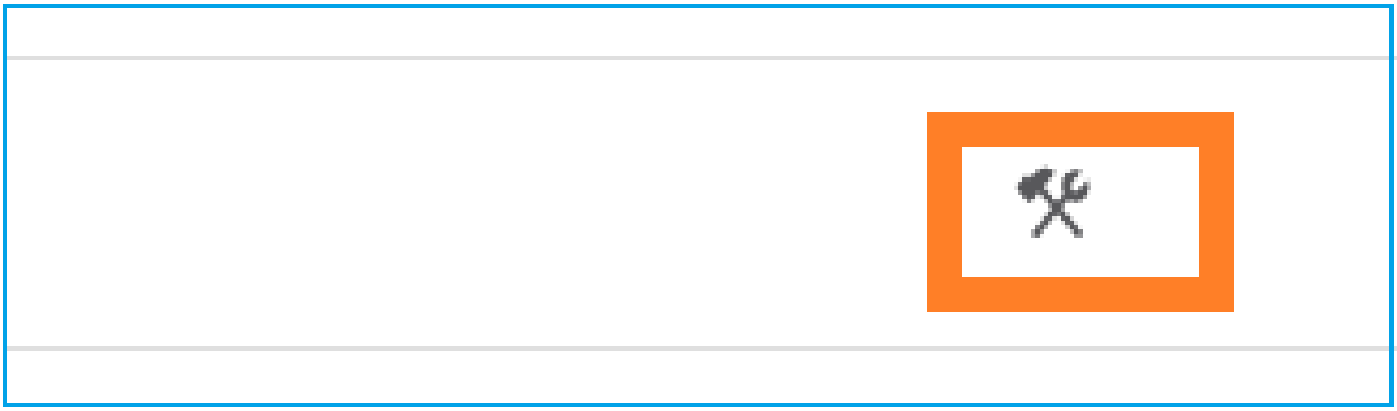
انتقل إلى وضع الخبير، وحدد مكان التقاط المحفوظ، ثم انسخه إلى موقع /ngfw/var/shared:

```
<#root>

firepower#

Console connection detached.

>
```

```
expert

admin@firepower:~$

sudo su

Password:
root@firepower:/home/admin#

 cd /mnt/disk0

root@firepower:/mnt/disk0#

ls -al | grep pcap

-rwxr-xr-x 1 root root     24 Apr 26 18:19 CAPI.pcap
-rwxr-xr-x 1 root root  30110 Apr  8 14:10

capin.pcap

-rwxr-xr-x 1 root root   6123 Apr  8 14:11 capin2.pcap
root@firepower:/mnt/disk0#

cp capin.pcap /ngfw/var/common
```

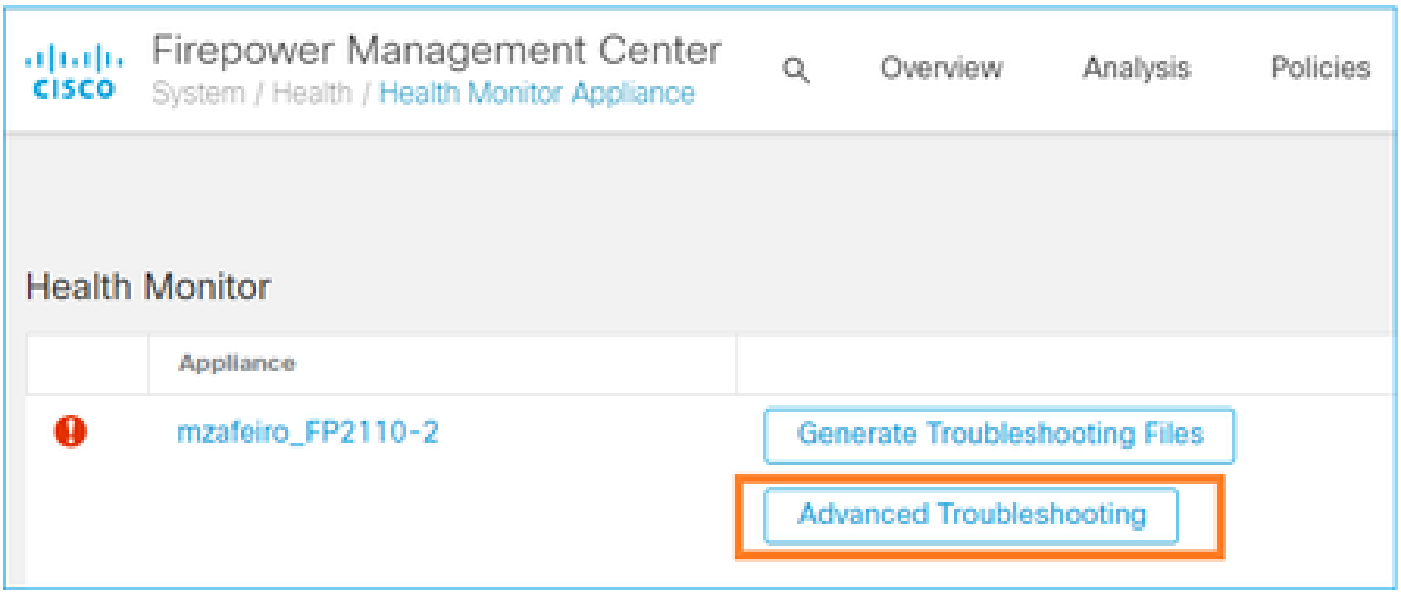
الخطوة 3

قم بتسجيل الدخول إلى وحدة التحكم في الإدارة (FMC) التي تدير بروتوكول FTD وتنقل إلى الأجهزة > إدارة الأجهزة. حدد موقع جهاز FTD وحدد أيقونة أستكشاف الأخطاء وإصلاحها:

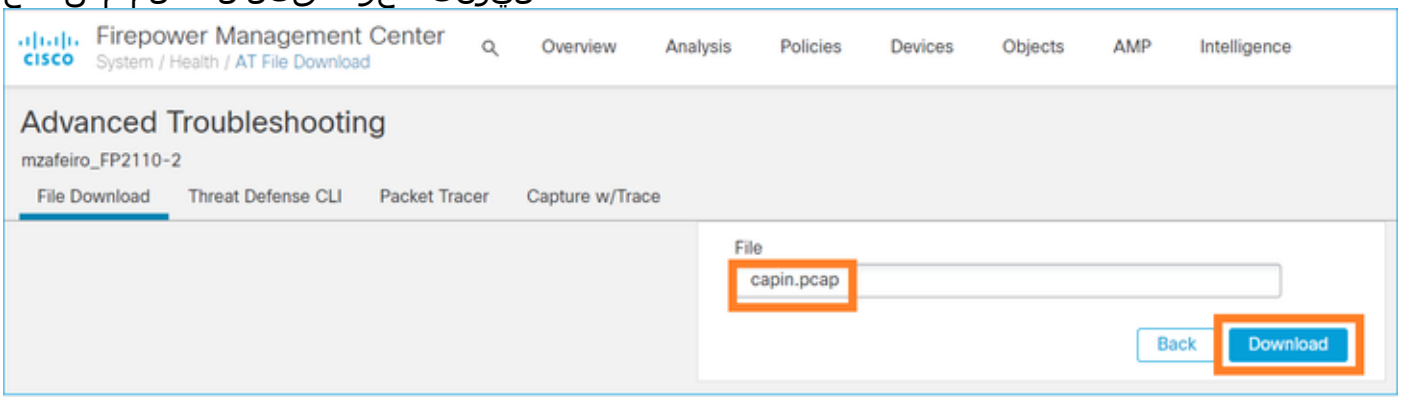


الخطوة 4

تحديد أستكشاف الأخطاء وإصلاحها المتقدم:



حدد اسم ملف الالتقاط وحدد تنزيل:

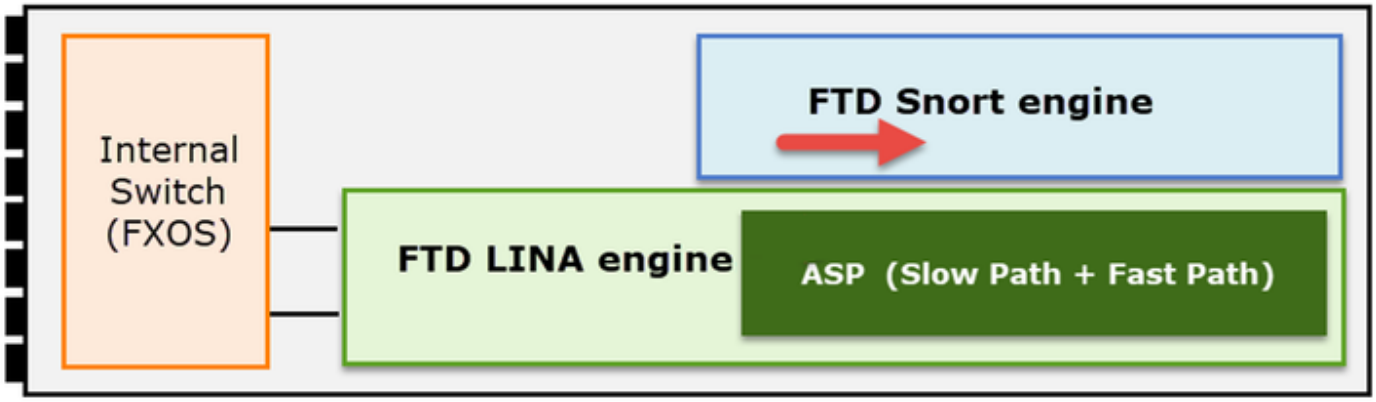


للحصول على مزيد من المعلومات حول كيفية تمكين/تجميع الالتقاط من واجهة مستخدم FMC، تحقق من هذا المستند:

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html

تمكين وتجميع لقطات ويب ل FTD

تظهر نقطة الالتقاط في الصورة هنا.



تمكين التقاط مستوى Snort:

```
<#root>

>

capture-traffic


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

Selection?

1


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

-n host 192.168.101.1
```

لكتابة االلتقاط إلى ملف باسم capture.pcap ونسخه من خالل FTP إلى خادم بعيد:

```
<#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:

-w capture.pcap host 192.168.101.1


CTRL + C <- to stop the capture


>

file copy 10.229.22.136 ftp / capture.pcap

Enter password for ftp@10.229.22.136:
Copying capture.pcap
Copy successful.
```

>

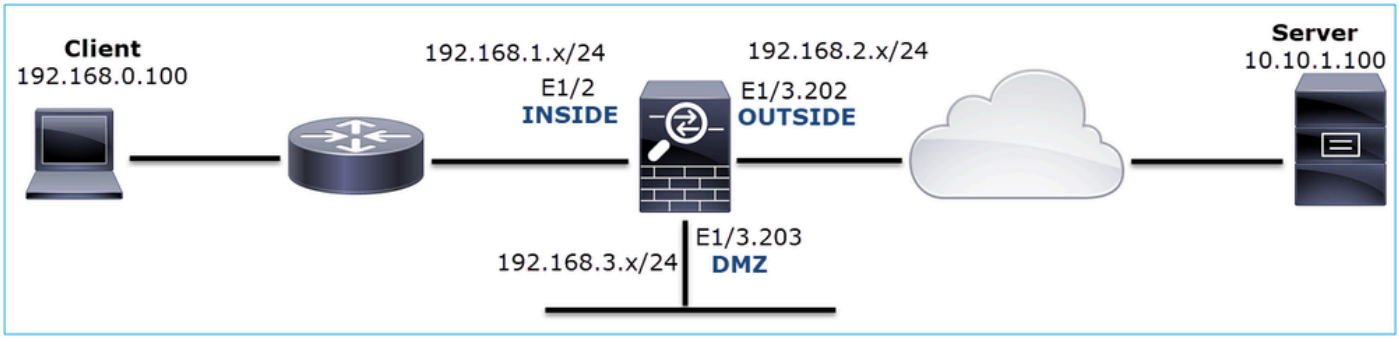
لمزيد من أمثلة الالتقاط على مستوى الشيخ التي تتضمن عوامل تصفية الالتقاط مختلفة تحقق من هذا المستند:

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html

استكشاف الأخطاء وإصلاحها

الحالة 1. لا يوجد TCP SYN على واجهة الخروج

المخطط موضح في الصورة هنا:



وصف المشكلة: HTTP لا يعمل

التدفق المتأثر:

SRC IP: 192.168.0.100

بروتوكول DST IP: 10.10.1.100

البروتوكول: بروتوكول TCP 80

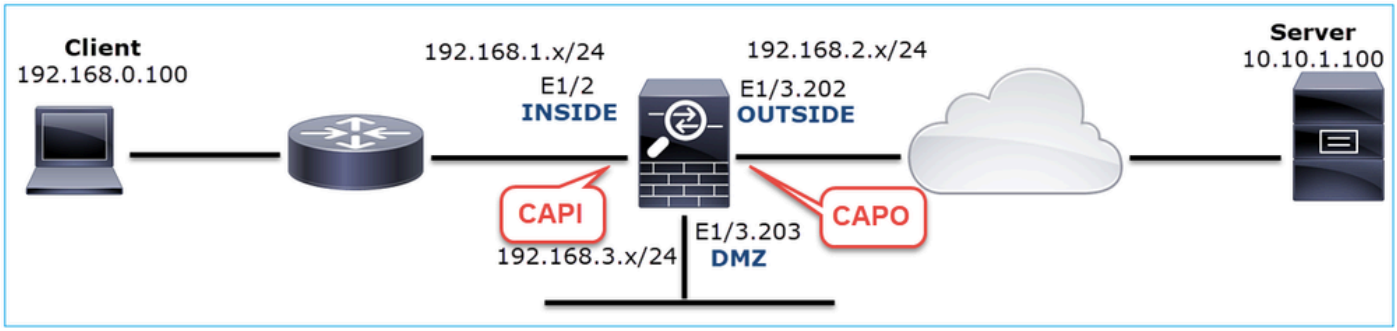
تحليل أسر

تمكين الالتقاط على محرك FTD LINA:

<#root>

```
firepower#
capture CAPI int INSIDE match ip host 192.168.0.100 host 10.10.1.100
firepower#
```

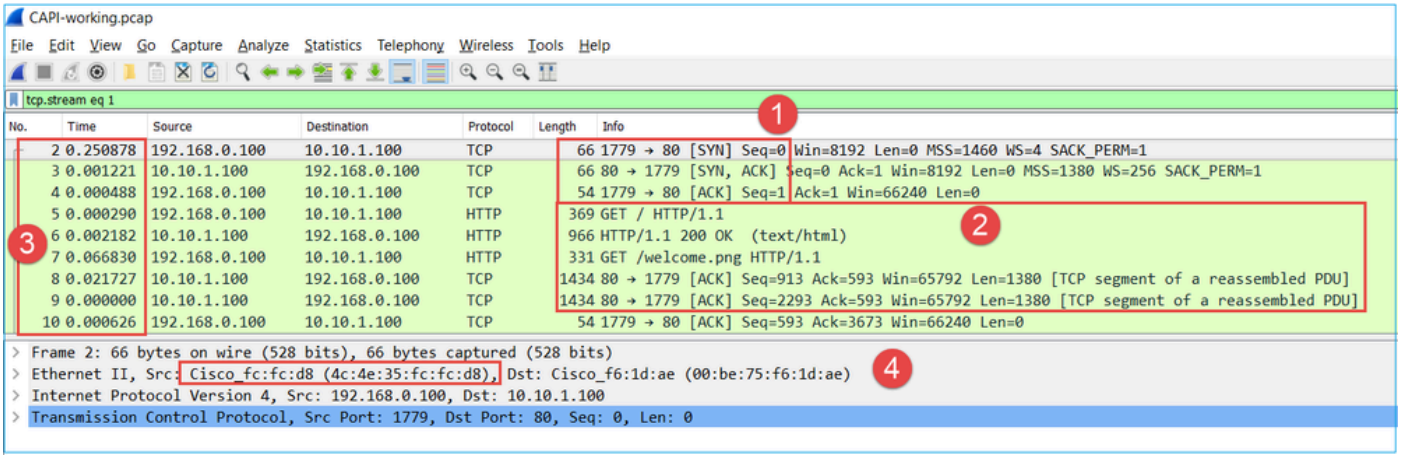
```
capture CAPO int OUTSIDE match ip host 192.168.0.100 host 10.10.1.100
```



التقاط - السيناريو الوظيفي:

كخط أساس، من المفيد جدا دائما أن تحصل على لقطات من سيناريو وظيفي.

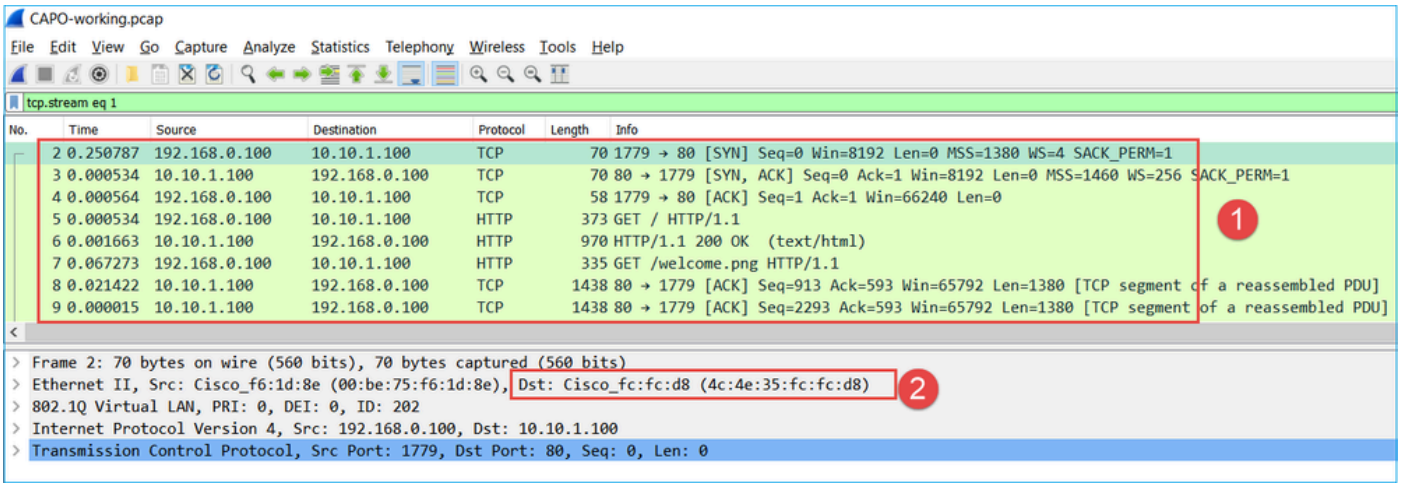
يتم التقاط واجهة NGFW Inside على النحو الموضح في الصورة:



النقاط الرئيسية:

1. مصافحة TCP 3-way.
2. تبادل البيانات ثنائي الإتجاه.
3. لا توجد تأخيرات بين الحزم (استنادا إلى فرق الوقت بين الحزم).
4. MAC المصدر هو الجهاز الصحيح لتدفق البيانات.

يتم عرض التقاط الواجهة الخارجية ل NGFW، في الصورة هنا:



النقاط الرئيسية:

1. نفس البيانات الموجودة في التقاط CAPI.
2. MAC الوجهة هو جهاز المنبع الصحيح.

التقاط - سيناريو لا يعمل

من خلال واجهة سطر الأوامر (CLI) الخاصة بالجهاز، تبدو الصور بهذا الشكل:

```
<#root>

firepower#

show capture

capture CAPI type raw-data interface INSIDE

[Capturing - 484 bytes]

  match ip host 192.168.0.100 host 10.10.1.100
capture CAPO type raw-data interface OUTSIDE

[Capturing - 0 bytes]

  match ip host 192.168.0.100 host 10.10.1.100
```

محتويات CAPI:

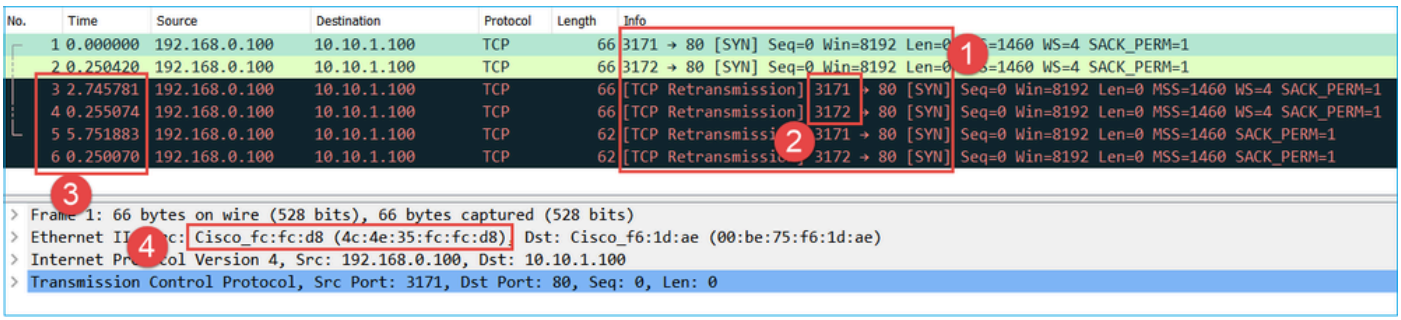
```
<#root>

firepower#

show capture CAPI

6 packets captured

   1: 11:47:46.911482    192.168.0.100.3171 > 10.10.1.100.80:

S
```

```
 1089825363:1089825363(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
   2: 11:47:47.161902   192.168.0.100.3172 > 10.10.1.100.80:

S

 3981048763:3981048763(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
   3: 11:47:49.907683   192.168.0.100.3171 > 10.10.1.100.80:

S

 1089825363:1089825363(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
   4: 11:47:50.162757   192.168.0.100.3172 > 10.10.1.100.80:

S

 3981048763:3981048763(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
   5: 11:47:55.914640   192.168.0.100.3171 > 10.10.1.100.80:

S

 1089825363:1089825363(0) win 8192 <mss 1460,nop,nop,sackOK>
   6: 11:47:56.164710   192.168.0.100.3172 > 10.10.1.100.80:

S

 3981048763:3981048763(0) win 8192 <mss 1460,nop,nop,sackOK>
```

<#root>

```
firepower#

show capture CAPO


0 packet captured


0 packet shown
```

هذه صورة لالتقاط CAPI في Wireshark:



النقاط الرئيسية:

1. يتم عرض حزم نظام TCP فقط (لا يوجد مصافحة TCP ثلاثية الإتجاه).
2. هناك جلستان لـ TCP (منفذ المصدر 3171 و 3172) لا يمكن إنشاؤهما. يقوم العميل المصدر بإعادة إرسال حزم TCP syn. يتم تعريف هذه الحزم التي تمت إعادة إرسالها بواسطة Wireshark كعمليات إعادة إرسال TCP.

3. تحدث عمليات إعادة إرسال بروتوكول TCP كل ما يقارب 3 ثم 6 ثوان وما إلى ذلك.
4. مصدر عنوان MAC من الجهاز الصحيح لتدفق البيانات.

واستنادا إلى الفصلين، يمكن إستنتاج ما يلي:

- تصل حزمة من 5 قنوات معينة (SRC/dst IP، ومنفذ src/dst، والبروتوكول) إلى جدار الحماية على الواجهة المتوقعة (في الداخل).
- لا تترك الحزمة جدار الحماية على الواجهة المتوقعة (الخارجية).

الإجراءات الموصى بها

والغرض من الإجراءات الواردة في هذا القسم هو زيادة تضييق نطاق هذه المسألة.

الإجراء 1. تحقق من تتبع حزمة محاكية.

أستخدم أداة packet-tracer لمعرفة كيفية معالجة حزمة بواسطة جدار الحماية. في حالة إسقاط الحزمة بواسطة نهج الوصول إلى جدار الحماية، يبدو تتبع الحزمة المحاكية مماثلا لهذا الإخراج:

```
<#root>

firepower#

packet-tracer input INSIDE tcp 192.168.0.100 11111 10.10.1.100 80


Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.2.72 using egress ifc  OUTSIDE

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 268439946 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268439946: ACCESS POLICY: FTD_Policy - Default
access-list CSM_FW_ACL_ remark rule-id 268439946: L4 RULE: DEFAULT ACTION RULE
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, Drop-location: frame 0x00005647a4f4b120 flow
```

الإجراء 2. تحقق من آثار الحزم الحية.

قم بتمكين تتبع الحزمة للتحقق من كيفية معالجة حزم TCP syn الحقيقية بواسطة جدار الحماية. بشكل افتراضي، يتم تتبع أول 50 حزمة مدخل فقط:

```
<#root>

firepower#

capture CAPI trace
```

مسح مخزن الالتقاط المؤقت:

```
<#root>

firepower#

clear capture /all
```

في حالة إسقاط الحزمة بواسطة نهج الوصول إلى جدار الحماية، يبدو التتبع مشابهًا لهذا الإخراج:

```
<#root>

firepower#

show capture CAPI packet-number 1 trace

6 packets captured
```

```
   1: 12:45:36.279740       192.168.0.100.3630 > 10.10.1.100.80: S 2322685377:2322685377(0) win 8192 <m
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.2.72 using egress ifc  OUTSIDE

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 268439946 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268439946: ACCESS POLICY: FTD_Policy - Default
access-list CSM_FW_ACL_ remark rule-id 268439946: L4 RULE: DEFAULT ACTION RULE
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, Drop-location: frame 0x00005647a4f4b120 flow


1 packet shown
```

الإجراء 3. تحقق من سجلات FTD Lina.

لتكوين Syslog على FTD عبر FMC، تحقق من هذا المستند:

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200479-Configure-Logging-

on-FTD-via-FMC.html

من المستحسن بشدة أن يتم تكوين خادم syslog خارجي لسجلات FTD Lina. في حالة عدم تكوين خادم syslog عن بعد، قم بتمكين السجلات المخزنة المؤقتة المحلية على جدار الحماية أثناء أستكشاف الأخطاء وإصلاحها. تكوين السجل الظاهر في هذا المثال هو نقطة بداية جيدة:

```
<#root>

firepower#

show run logging

…
logging enable
logging timestamp
logging buffer-size 1000000
logging buffered informational
```

اضبط جهاز النداء الطرفي على 24 سطرا للتحكم في جهاز النداء الطرفي:

```
<#root>

firepower#

terminal pager 24
```

مسح مخزن الالتقاط المؤقت:

```
<#root>

firepower#

clear logging buffer
```

اختبر الاتصال وفحص السجلات باستخدام عامل تصفية المحلل. في هذا المثال، يتم إسقاط الحزم بواسطة نهج الوصول إلى جدار الحماية:

```
<#root>

firepower#

show logging | include 10.10.1.100

Oct 09 2019 12:55:51: %FTD-4-106023: Deny tcp src INSIDE:192.168.0.100/3696 dst OUTSIDE:10.10.1.100/80
Oct 09 2019 12:55:51: %FTD-4-106023: Deny tcp src INSIDE:192.168.0.100/3697 dst OUTSIDE:10.10.1.100/80
```

```
Oct 09 2019 12:55:54: %FTD-4-106023: Deny tcp src INSIDE:192.168.0.100/3696 dst OUTSIDE:10.10.1.100/80
Oct 09 2019 12:55:54: %FTD-4-106023: Deny tcp src INSIDE:192.168.0.100/3697 dst OUTSIDE:10.10.1.100/80
```

الإجراء 4. تحقق من عمليات إسقاط ASP لجدار الحماية.

إذا كنت تشك في أن الحزمة سقطت من جدار الحماية، فيمكنك رؤية عدادات جميع الحزم التي أسقطتها جدار الحماية على مستوى البرنامج:

```
<#root>

firepower#

show asp drop


Frame drop:
  No route to host (no-route)                                          234
  Flow is denied by configured rule (acl-drop)                          71

Last clearing: 07:51:52 UTC Oct 10 2019 by enable_15

Flow drop:

Last clearing: 07:51:52 UTC Oct 10 2019 by enable_15
```

يمكنك تمكين عمليات الالتقاط لعرض جميع عمليات إسقاط مستوى برنامج ASP:

```
<#root>

firepower#

capture ASP type asp-drop all buffer 33554432 headers-only
```

تلميح: إذا لم تكن مهتما بمحتويات الحزمة يمكنك التقاط رؤوس الحزمة فقط (خيار رؤوس فقط). وهذا يتيح لك التقاط المزيد من الحزم في مخزن الالتقاط المؤقت. بالإضافة إلى ذلك، يمكنك زيادة حجم مخزن الالتقاط المؤقت (بشكل افتراضي وهو 500 كيلوبايت) إلى قيمة تصل إلى 32 ميجابايت (خيار المخزن المؤقت). أخيرا، بدءا من الإصدار 6.3 لـ FTD، يتيح لك خيار حجم الملف تكوين ملف التقاط حتى 10 جيجابايت. في تلك الحالة يمكنك فقط رؤية محتويات الالتقاط بتنسيق PCAP.

للتحقق من محتويات الالتقاط، يمكنك استخدام مرشح التضييق نطاق البحث:

```
<#root>

firepower#

show capture ASP | include 10.10.1.100
```

```
  18: 07:51:57.823672   192.168.0.100.12410 > 10.10.1.100.80: S 1870382552:1870382552(0) win 8192 <mss
  19: 07:51:58.074291   192.168.0.100.12411 > 10.10.1.100.80: S 2006489005:2006489005(0) win 8192 <mss
  26: 07:52:00.830370   192.168.0.100.12410 > 10.10.1.100.80: S 1870382552:1870382552(0) win 8192 <mss
  29: 07:52:01.080394   192.168.0.100.12411 > 10.10.1.100.80: S 2006489005:2006489005(0) win 8192 <mss
  45: 07:52:06.824282   192.168.0.100.12410 > 10.10.1.100.80: S 1870382552:1870382552(0) win 8192 <mss
  46: 07:52:07.074230   192.168.0.100.12411 > 10.10.1.100.80: S 2006489005:2006489005(0) win 8192 <mss
```

في هذه الحالة، بما أن الحزم يتم تعقبها بالفعل على مستوى الواجهة، فلا يتم ذكر سبب الإسقاط في التقاط ASP. تذكر أنه يمكن تعقب الحزمة فقط في مكان واحد (واجهة الدخول أو إسقاط ASP). في هذه الحالة، يوصى بأخذ عمليات إسقاط ASP متعددة وتعيين سبب إسقاط ASP محدد. وفي ما يلي النهج الموصى به:

1. قم بمسح عدادات إسقاط ASP الحالية:

```
<#root>

firepower#

clear asp drop
```

2. إرسال التدفق الذي تقوم باستكشاف أخطائه وإصلاحها من خلال جدار الحماية (تشغيل الاختبار).

3. تحقق مرة أخرى من عدادات إسقاط ASP ولاحظ أنها قد تمت زيادتها.

```
<#root>

firepower#

show asp drop

Frame drop:
  No route to host (

no-route

)                                              234
  Flow is denied by configured rule (

acl-drop

)                                  71
```

4. تمكين التقاط (التقاط) ASP لعمليات الإسقاط المحددة التي يتم رؤيتها:

```
<#root>

firepower#

capture ASP_NO_ROUTE type asp-drop no-route
```

```
firepower#
capture ASP_ACL_DROP type asp-drop acl-drop
```

5. إرسال التدفق الذي تقوم باستكشاف الأخطاء وإصلاحها من خلال جدار الحماية (تشغيل إختبار).

6. تحقق من مجموعات ASP. في هذه الحالة، تم إسقاط الحزم بسبب مسار غير موجود:

```
<#root>
firepower#
show capture ASP_NO_ROUTE | include 192.168.0.100.*10.10.1.100

  93: 07:53:52.381663   192.168.0.100.12417 > 10.10.1.100.80: S 3451917925:3451917925(0) win 8192 <mss
  95: 07:53:52.632337   192.168.0.100.12418 > 10.10.1.100.80: S 1691844448:1691844448(0) win 8192 <mss
 101: 07:53:55.375392   192.168.0.100.12417 > 10.10.1.100.80: S 3451917925:3451917925(0) win 8192 <mss
 102: 07:53:55.626386   192.168.0.100.12418 > 10.10.1.100.80: S 1691844448:1691844448(0) win 8192 <mss
 116: 07:54:01.376231   192.168.0.100.12417 > 10.10.1.100.80: S 3451917925:3451917925(0) win 8192 <mss
 117: 07:54:01.626310   192.168.0.100.12418 > 10.10.1.100.80: S 1691844448:1691844448(0) win 8192 <mss
```

الإجراء 5. تحقق من جدول اتصال FTD Lina.

يمكن أن يكون هناك حالات تتوقع فيها أن تخرج الحزمة واجهة 'X'، ولكن لأي سبب كان فإنها تعرض الواجهة 'Y'. يستند تحديد واجهة مخرج جدار الحماية إلى ترتيب التشغيل هذا:

1. بحث الاتصال المنشأ
2. البحث عن ترجمة عنوان الشبكة (NAT) - تأخذ مرحلة UN-NAT (غاية NAT) الأولوية على PBR وبحث المسار.
3. التوجيه القائم على السياسة (PBR)
4. بحث جدول التوجيه

للتحقق من جدول اتصال FTD:

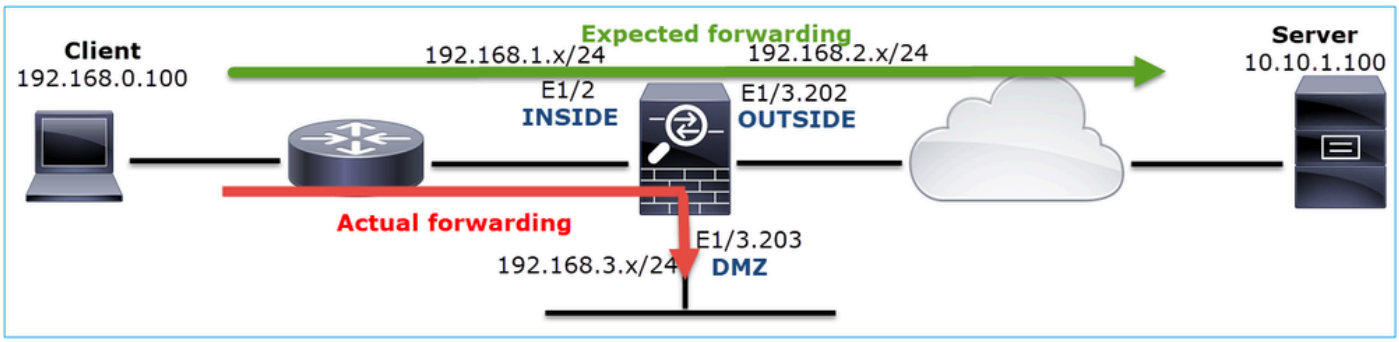
```
<#root>
firepower#
show conn

2 in use, 4 most used
Inspect Snort:
        preserve-connection: 2 enabled, 0 in effect, 4 most enabled, 0 most in effect

TCP
DMZ
 10.10.1.100:
80
```

```
INSIDE
 192.168.0.100:
11694
, idle 0:00:01, bytes 0, flags
aA N1
TCP
DMZ
 10.10.1.100:80
INSIDE
 192.168.0.100:
11693
, idle 0:00:01, bytes 0, flags
aA N1
```

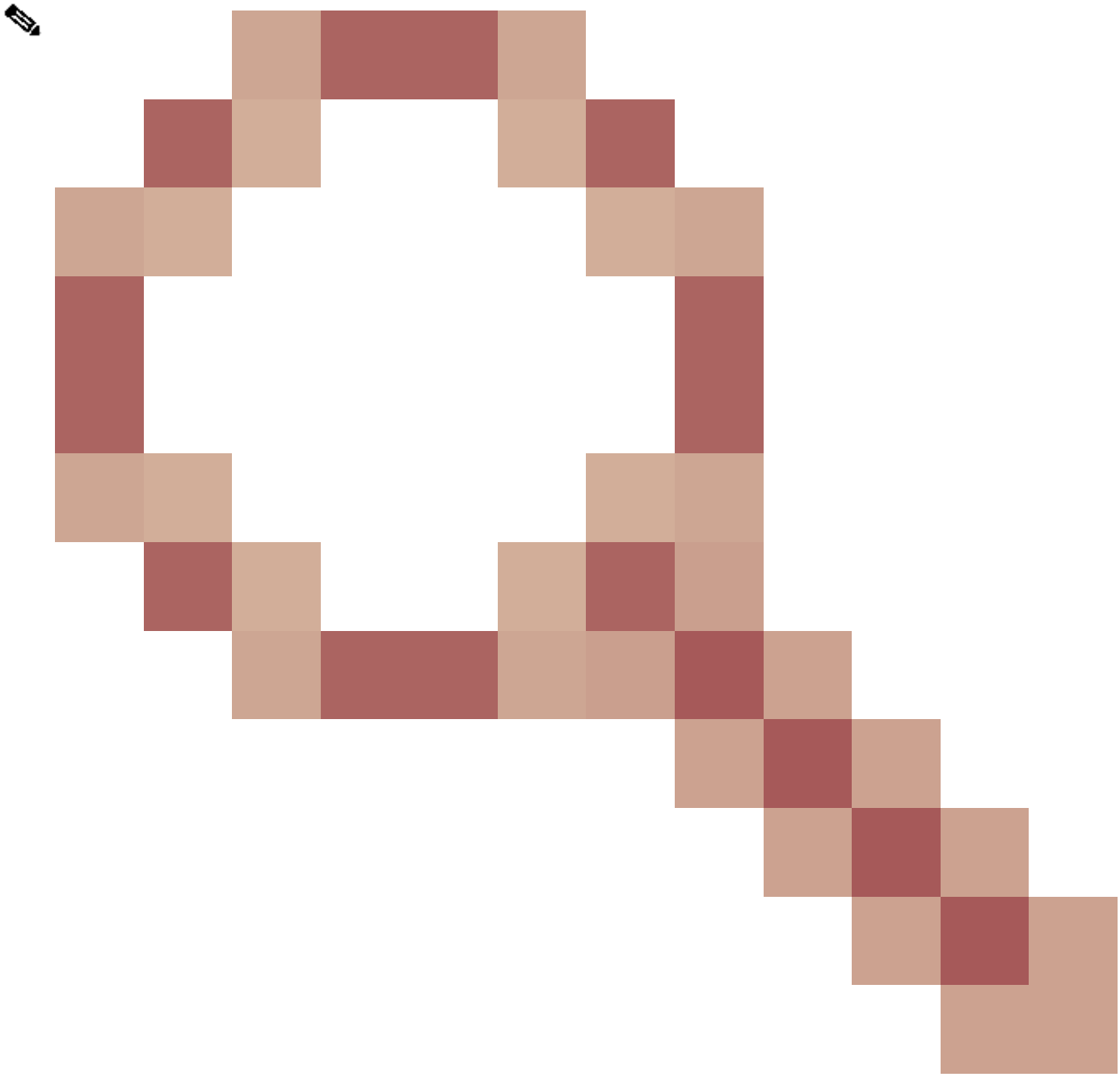
النقاط الرئيسية:

- استنادا إلى علامات التمييز (A)، فإن الاتصال جنيني (تم فتحه نصف - لم يظهر إلا TCP SYN بواسطة جدار الحماية).
- بناء على المصدر/الغاية ميناء المدخل قارن داخل و المخرج قارن وه DMZ.

يمكن تصور هذا في الصورة هنا:



ملاحظة: بما أن جميع واجهات FTD تحتوي على مستوى أمان من 0 أمر الواجهة في إخراج show conn يعتمد على رقم الواجهة. وعلى وجه الخصوص، يتم تحديد الواجهة ذات رقم واجهة النظام الأساسي الظاهري (VPIF-num) الأعلى على أنها داخلية بينما يتم تحديد الواجهة ذات رقم واجهة النظام الأساسي الظاهري (VPIF-num الأقل) على أنها خارجية. أنت يستطيع رأيت القارن vpif قيمة مع العرض قارن تفصيل أمر. التحسينات ذات الصلة، معرف تصحيح الأخطاء من Cisco CSCvi15290



إنه: يعرض FTD إتجاه الاتصال في إخراج "show conn" ل FTD

<#root>

```
firepower#

show interface detail | i Interface number is|Interface [P|E].*is up

...
Interface Ethernet1/2 "INSIDE", is up, line protocol is up
        Interface number is

19

Interface Ethernet1/3.202 "OUTSIDE", is up, line protocol is up
        Interface number is

 20

Interface Ethernet1/3.203 "DMZ", is up, line protocol is up
```

```
        Interface number is
22
```

ملاحظة: كما هو الحال في إصدار برنامج FirePOWER الإصدار 6.5، وفرت الإصدار 9.13.x من ASA مخرجات الأمر show conn long و show conn detail معلومات حول بادئ الاتصال والمستجيب

الناتج 1:

```
<#root>

firepower#

show conn long

...
TCP OUTSIDE: 192.168.2.200/80 (192.168.2.200/80) INSIDE: 192.168.1.100/46050 (192.168.1.100/46050), fla

Initiator: 192.168.1.100, Responder: 192.168.2.200

  Connection lookup keyid: 228982375
```

الناتج 2:

```
<#root>

firepower#

show conn detail

...
TCP OUTSIDE: 192.168.2.200/80 INSIDE: 192.168.1.100/46050,
    flags aA N1, idle 4s, uptime 11s, timeout 30s, bytes 0

Initiator: 192.168.1.100, Responder: 192.168.2.200

  Connection lookup keyid: 228982375
```

وبالإضافة إلى ذلك، يعرض العرض طويل NATed IPs داخل أقواس في حالة ترجمة عنوان الشبكة:

```
<#root>

firepower#

show conn long

...
```

```
TCP OUTSIDE: 192.168.2.222/80 (192.168.2.222/80) INSIDE: 192.168.1.100/34792 (192.168.2.150/34792), fla
  Initiator: 192.168.1.100, Responder: 192.168.2.222
  Connection lookup keyid: 262895
```

الإجراء 6. تحقق من ذاكرة التخزين المؤقت لبروتوكول تحليل عنوان جدار الحماية (ARP).

إذا تعذر على جدار الحماية حل المرحلة التالية، يقوم جدار الحماية بإسقاط الحزمة الأصلية (TCP SYN في هذه الحالة) بشكل صامت وإرسال طلبات ARP باستمرار حتى يقوم بحل المرحلة التالية.

لعرض ذاكرة التخزين المؤقت ل ARP لجدار الحماية، أستخدم الأمر:

```
<#root>

firepower#

show arp
```

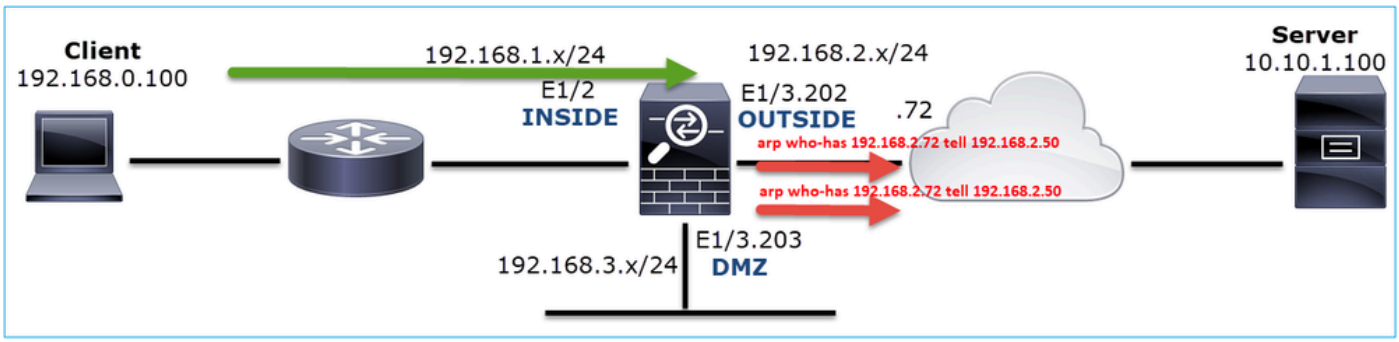
بالإضافة إلى ذلك، للتحقق من وجود مضيفين غير محاليين، يمكنك إستخدام الأمر:

```
<#root>

firepower#

 show arp statistics

        Number of ARP entries in ASA: 0

        Dropped blocks in ARP: 84
        Maximum Queued blocks: 3
        Queued blocks: 0
        Interface collision ARPs Received: 0
        ARP-defense Gratuitous ARPS sent: 0
        Total ARP retries:

182             < indicates a possible issue for some hosts

        Unresolved hosts:

1


< this is the current status

        Maximum Unresolved hosts: 2
```

إذا كنت تريد إجراء مزيد من الفحص لعملية ARP، فيمكنك تمكين التقاط خاص ب ARP:

```
<#root>

firepower#

capture ARP ethernet-type arp interface OUTSIDE

firepower#

show capture ARP

...
   4: 07:15:16.877914       802.1Q vlan#202 P0 arp

who-has 192.168.2.72 tell 192.168.2.50

   5: 07:15:18.020033       802.1Q vlan#202 P0 arp who-has 192.168.2.72 tell 192.168.2.50
```

في هذا الإخراج، يحاول جدار الحماية (192.168.2.50) حل المرحلة التالية (192.168.2.72)، ولكن لا يوجد رد ARP



تعرض المخرجات هنا سيناريو وظيفي بدقة ARP المناسبة:

```
<#root>

firepower#

show capture ARP

2 packets captured

   1: 07:17:19.495595       802.1Q vlan#202 P0

arp who-has 192.168.2.72 tell 192.168.2.50

   2: 07:17:19.495946       802.1Q vlan#202 P0

arp reply 192.168.2.72 is-at 4c:4e:35:fc:fc:d8

2 packets shown
```

```
<#root>

firepower#

show arp

        INSIDE 192.168.1.71 4c4e.35fc.fcd8 9
```

```
        OUTSIDE 192.168.2.72 4c4e.35fc.fcd8 9
```

في حالة عدم وجود إدخال ARP في المكان يظهر تتبع لحزمة TCP SYN المباشرة:

```
<#root>

firepower#

show capture CAPI packet-number 1 trace


6 packets captured

   1: 07:03:43.270585

192.168.0.100.11997 > 10.10.1.100.80

: S 4023707145:4023707145(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.2.72 using egress ifc  OUTSIDE
…
Phase: 14
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 4814, packet dispatched to next module
…
Phase: 17
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.2.72 using egress ifc  OUTSIDE
```

```
Result:
input-interface: INSIDE
input-status: up
input-line-status: up

output-interface: OUTSIDE

output-status: up
output-line-status: up

Action: allow
```

كما يمكن أن يرى في الإنتاج، التتبع الإجراءي المظهر: يسمح حتى عندما لا يكون من الممكن الوصول إلى الخوادم التالية وتم إسقاط الحزمة بصمت بواسطة جدار الحماية! في هذه الحالة، الربط-tracer أداة ينبغي أيضا فحصت بما أن هو يوفر أكثر دقة إنتاج:

<#root>

```
firepower#

packet-tracer input INSIDE tcp 192.168.0.100 1111 10.10.1.100 80

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.2.72 using egress ifc  OUTSIDE
…

Phase: 14
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 4816, packet dispatched to next module
…
Phase: 17
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
```

```
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.2.72 using egress ifc  OUTSIDE

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: (no-v4-adjacency) No valid V4 adjacency, Drop-location: frame 0x00005647a4e86109 flow (NA)/
```

في إصدارات ASA/FirePOWER الأخيرة، تم تحسين الرسالة السابقة ل:

<#root>

```
Drop-reason: (no-v4-adjacency) No valid V4 adjacency.

Check ARP table (show arp) has entry for nexthop

., Drop-location: f
```

ملخص الأسباب المحتملة والإجراءات الموصى بها

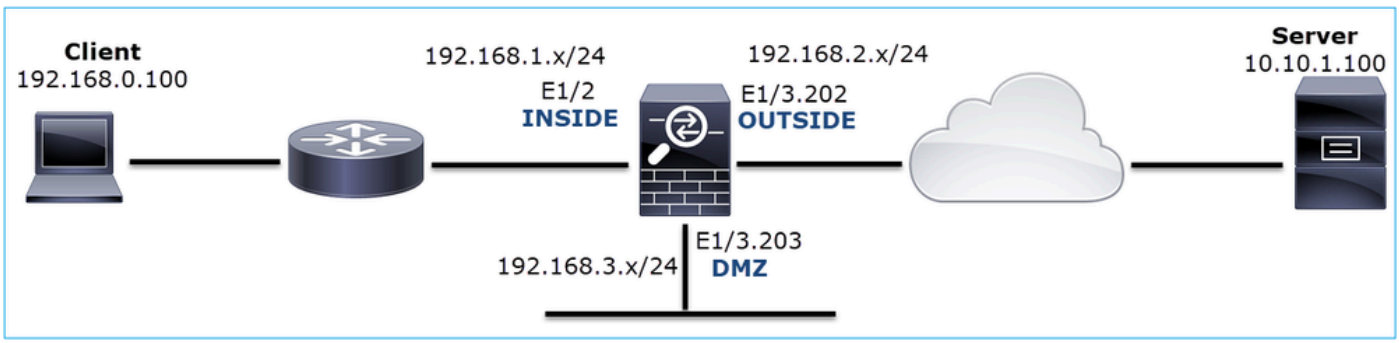
إن يري أنت فقط TCP syn رطب علي المدخل قارن، غير أن ام من TCP syn رطب يرسل من ال يتوقع مخرج قارن بعض يمكن سبب:

السبب المحتمل	الإجراءات الموصى بها
يتم إسقاط الحزمة بواسطة نهج الوصول إلى جدار الحماية.	• أستخدم packet-tracer أو capture w/trace لمعرفة كيفية معالجة جدار الحماية للحزمة. • تحقق من سجلات جدار الحماية. • تحقق من عمليات إسقاط ASP لجدار الحماية (show asp drop أو capture type asp-drop). • تحقق من أحداث اتصال FMC. هذا يفترض أن القاعدة تحتوي على تسجيل ممكن.
عامل تصفية الالتقاط غير صحيح.	• استعملت packet-tracer أو علي قبض w/trace أن يعدل nat ترجمة هناك يكون إن يري أن ip. في تلك الحالة، اضبط الوجهة أو المصدر مرشح الالتقاط.
	• يعرض إخراج الأمر show conn long عناوين IP الخاصة ب NATed.

أرسلت الربط إلى قارن مخرج مختلف.	• أستخدم packet-tracer أو capture w/trace لمعرفة كيفية معالجة جدار الحماية للحزمة. تذكر ترتيب العمليات الذي يضع في الاعتبار تحديد واجهة المخرج والاتصال الحالي وبحث جدول التوجيه و UN-NAT و PBR. • تحقق من سجلات جدار الحماية. • تحقق من جدول اتصال جدار الحماية (show conn). إذا تم إرسال الحزمة إلى واجهة خاطئة لأنها تطابق اتصال حالي، فاستخدم الأمر clear conn address وحدد السلسلة 5 من الاتصال الذي تريد مسحه.
لا يوجد طريق إلى الوجهة.	• أستخدم packet-tracer أو capture w/trace لمعرفة كيفية معالجة جدار الحماية للحزمة. • تحقق من عمليات إسقاط ASP لجدار الحماية (show asp drop) للحصول على سبب إسقاط المسار.
لا يوجد إدخال ARP على واجهة المخرج.	• تحقق من ذاكرة التخزين المؤقت ل ARP لجدار الحماية (show arp). • أستخدم packet-tracer لمعرفة ما إذا كان هناك تجاوز صالح.
قارن المخرج معطل.	تحقق من إخراج الأمر show interface ip brief على جدار الحماية وتحقق من حالة الواجهة.

حالة 2. TCP syn من عميل، TCP RST من نادل

تعرض هذه الصورة المخطط:



وصف المشكلة: HTTP لا يعمل

التدفق المتأثر:

SRC IP: 192.168.0.100

بروتوكول DST IP: 10.10.1.100

البروتوكول: بروتوكول TCP 80

تحليل أسر

قم بتمكين عمليات الالتقاط على محرك FTD LINA.

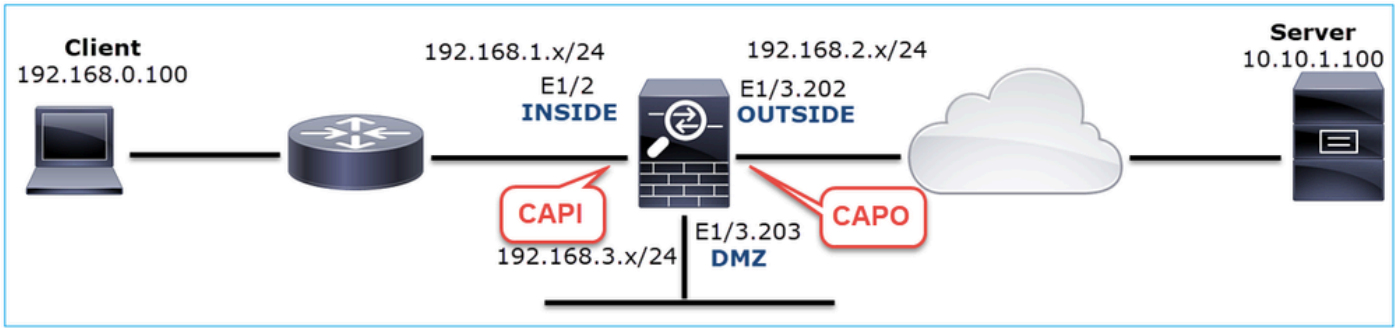
<#root>

firepower#

capture CAPI int INSIDE match ip host 192.168.0.100 host 10.10.1.100

firepower#

capture CAPO int OUTSIDE match ip host 192.168.0.100 host 10.10.1.100



التقاط - سيناريو العمل:

هذه هي الطريقة التي تبدو بها عمليات الالتقاط من واجهة سطر الأوامر الخاصة بالجهاز:

<#root>

firepower#

show capture

capture CAPI type raw-data trace interface INSIDE [Capturing -

834 bytes

]
  match ip host 192.168.0.100 host 10.10.1.100
capture CAPO type raw-data interface OUTSIDE [Capturing -

878 bytes

```
]
  match ip host 192.168.0.100 host 10.10.1.100
```

محتويات CAPI:

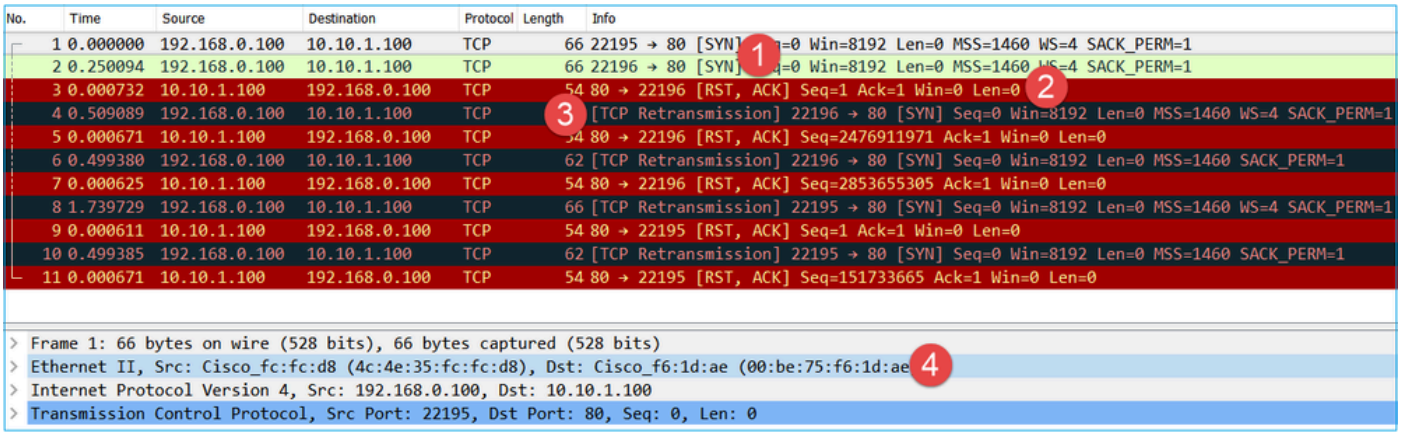
```
<#root>

firepower#

show capture CAPI

   1: 05:20:36.654217   192.168.0.100.22195 > 10.10.1.100.80:

S

 1397289928:1397289928(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
   2: 05:20:36.904311   192.168.0.100.22196 > 10.10.1.100.80:

S

 2171673258:2171673258(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
   3: 05:20:36.905043   10.10.1.100.80 > 192.168.0.100.22196:

R

 1850052503:1850052503(0) ack 2171673259 win 0
   4: 05:20:37.414132   192.168.0.100.22196 > 10.10.1.100.80:

S

 2171673258:2171673258(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
   5: 05:20:37.414803   10.10.1.100.80 > 192.168.0.100.22196:

R

 31997177:31997177(0) ack 2171673259 win 0
   6: 05:20:37.914183   192.168.0.100.22196 > 10.10.1.100.80:

S

 2171673258:2171673258(0) win 8192 <mss 1460,nop,nop,sackOK>
...
```

محتويات CAPO:

```
<#root>

firepower#

show capture CAPO

   1: 05:20:36.654507   802.1Q vlan#202 P0 192.168.0.100.22195 > 10.10.1.100.80:

S

 2866789268:2866789268(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
   2: 05:20:36.904478   802.1Q vlan#202 P0 192.168.0.100.22196 > 10.10.1.100.80:

S
```

```
4785344:4785344(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
  3: 05:20:36.904997   802.1Q vlan#202 P0 10.10.1.100.80 > 192.168.0.100.22196:

R

0:0(0) ack 4785345 win 0
  4: 05:20:37.414269   802.1Q vlan#202 P0 192.168.0.100.22196 > 10.10.1.100.80:

S

4235354730:4235354730(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
  5: 05:20:37.414758   802.1Q vlan#202 P0 10.10.1.100.80 > 192.168.0.100.22196:

R

0:0(0) ack 4235354731 win 0
  6: 05:20:37.914305   802.1Q vlan#202 P0 192.168.0.100.22196 > 10.10.1.100.80:

S

4118617832:4118617832(0) win 8192 <mss 1380,nop,nop,sackOK>
```

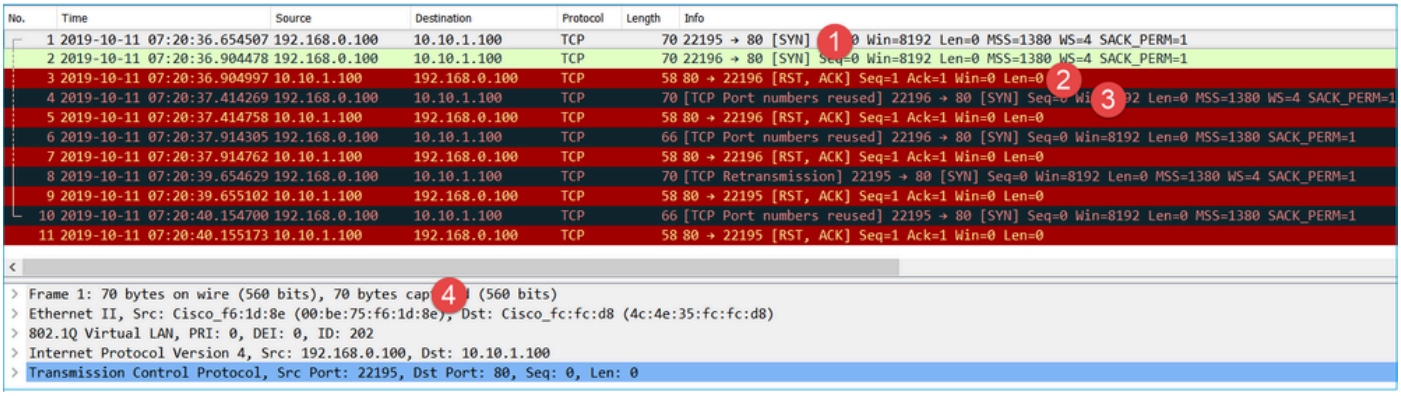
تظهر هذه الصورة التقاط CAPI في Wireshark.



النقاط الرئيسية:

1. يرسل المصدر حزمة TCP syn.
2. يتم إرسال TCP RST نحو المصدر.
3. يرسل المصدر حزم TCP syn.
4. عناوين MAC صحيحة (على حزم الدخول ينتمي عنوان MAC المصدر إلى موجه البث، ينتمي عنوان MAC الوجهة إلى جدار الحماية داخل الواجهة).

تظهر هذه الصورة التقاط CAPO في Wireshark:



النقاط الرئيسية:

1. يرسل المصدر حزمة TCP syn.
2. يصل TCP RST إلى الواجهة الخارجية.
3. يرسل المصدر حزم TCP syn.
4. عناوين MAC صحيحة (على حزم الخروج يكون جدار الحماية الخارجي هو مصدر MAC، موجه البث هو الغاية MAC).

واستنادا إلى الفصلين، يمكن إستنتاج ما يلي:

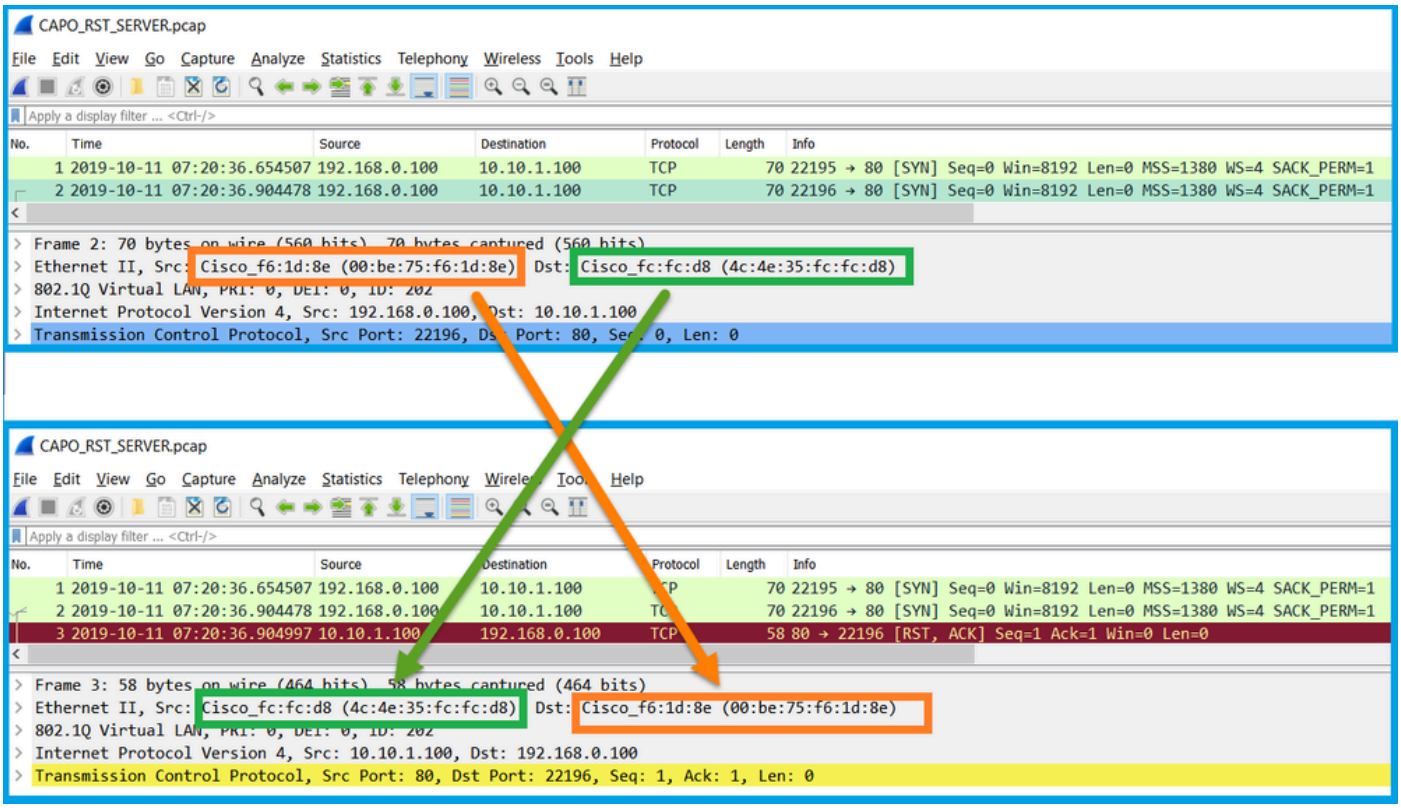
- لا يتم إكمال تأكيد اتصال TCP الثلاثي الإتجاه بين العميل والخادم
- هناك TCP RST الذي يصل إلى واجهة مخرج جدار الحماية
- جدار الحماية "يتحدث" إلى أجهزة تدفق البيانات من الخادم (استنادا إلى عناوين MAC)

الإجراءات الموصى بها

والغرض من الإجراءات الواردة في هذا القرع هو زيادة تضييق نطاق هذه المسألة.

إجراء 1. تحقق من عنوان MAC المصدر الذي يرسل TCP RST.

دققت أن الغاية {upper}mac يرى في ال TCP syn ربط ال نفسه بما أن المصدر {upper}mac قد رأى في ال TCP rst ربط.

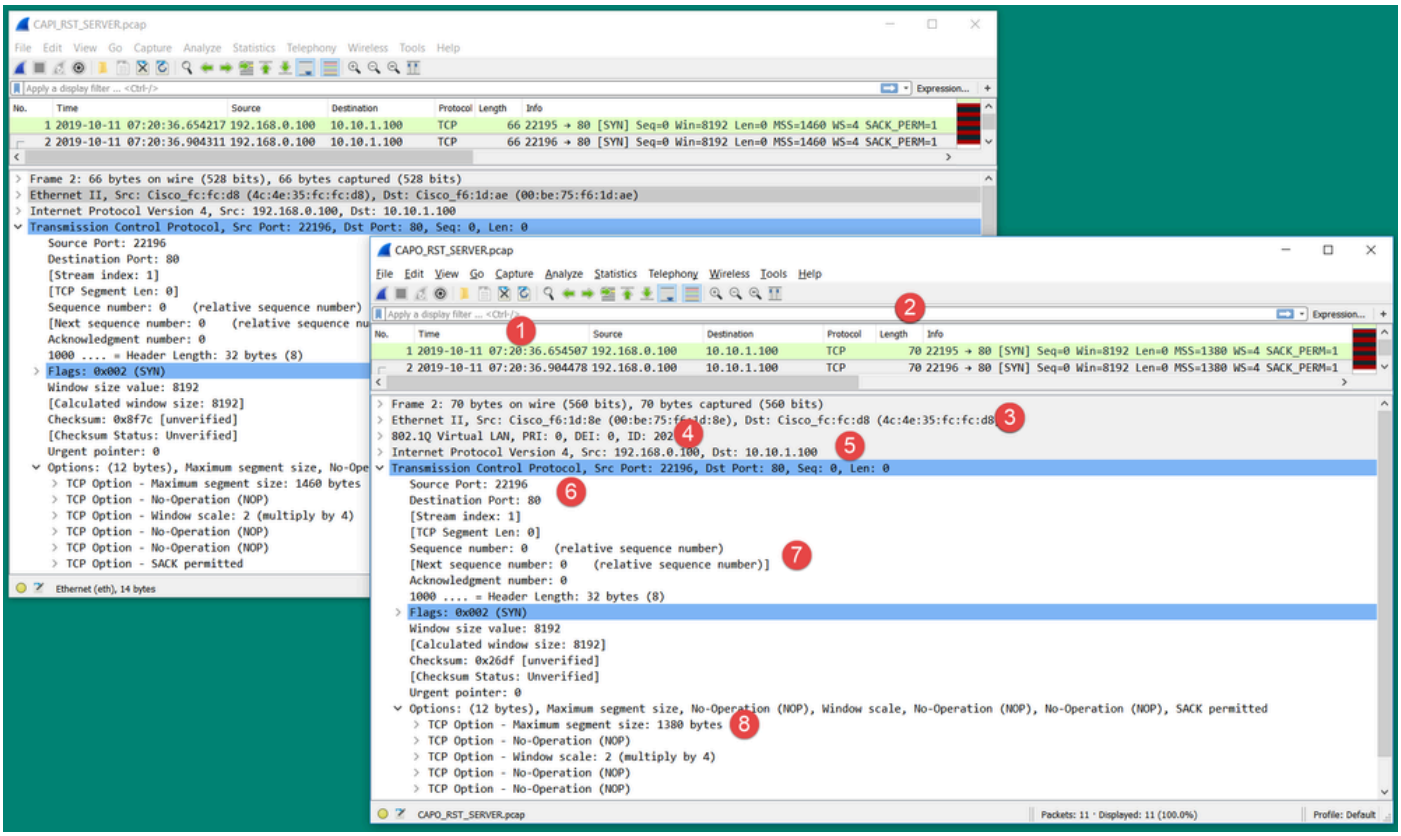


يهدف هذا الفحص إلى تأكيد أمرين:

- تحقق من عدم وجود تدفق غير متناظر.
- تحقق من انتماء MAC إلى جهاز تدفق البيانات المتوقع.

الإجراء 2. مقارنة حزم الدخول والخروج.

قارن الربط 2 على Wireshark بصريا للتحقق من أن جدار الحماية لا يعدل/يفسد الربط. يتم إبراز بعض الفروق المتوقعة.



النقاط الرئيسية:

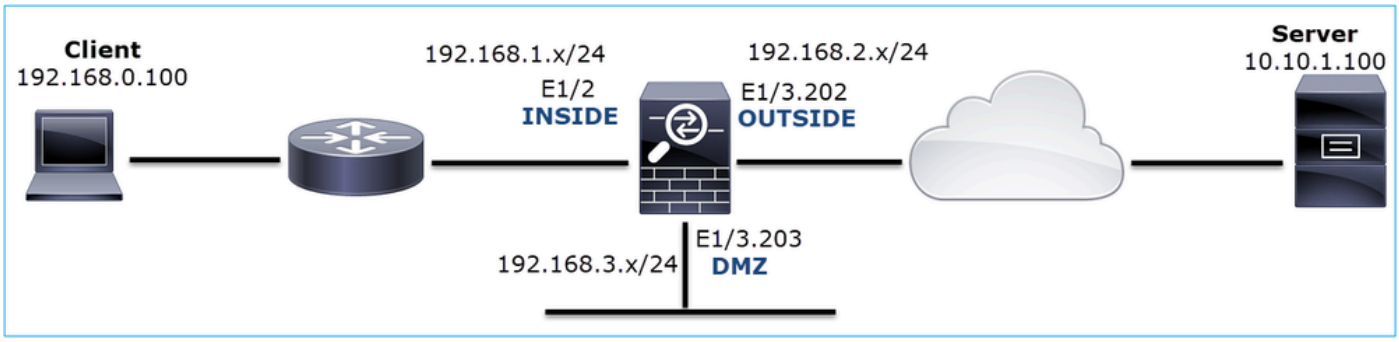
1. الطوابع الزمنية مختلفة. ومن ناحية أخرى، لا بد أن يكون الفارق ضئيلا ومعقولا. يعتمد هذا على المميزات وفحص السياسة المطبقة على الحزمة مثل الحمل على الجهاز.
2. يختلف طول الحزم خاصة إذا كان هناك رأس dot1Q تمت إضافته/إزالته بواسطة جدار الحماية على جانب واحد فقط.
3. عناوين MAC مختلفة.
4. يمكن أن يكون رأس dot1Q في مكانه إذا تم الالتقاط على واجهة فرعية.
5. ال ip عنوان (عناوين) مختلف في حالة NAT أو أيسر عنوان ترجمة (ضرب) طبقت إلى الربط.
6. المصدر أو غاية مختلف ميناء في حالة NAT أو ضرب طبقت إلى الربط.
7. إذا قمت بتعطيل خيار رقم التسلسل النسبي ل Wireshark، فسترى أن أرقام تسلسل/أرقام الإقرار TCP يتم تعديلها بواسطة جدار الحماية بسبب عشوائية رقم التسلسل الأولي (IS).
8. يمكن الكتابة فوق بعض خيارات TCP. على سبيل المثال، يعمل جدار الحماية بشكل افتراضي على تغيير الحد الأقصى لحجم مقطع TCP (MSS) إلى 1380 لتجنب تجزئة الحزمة في مسار النقل.

الإجراء 3. التقاط في الوجهة.

إن أمكن، إلتقط صورة في الوجهة نفسها. إذا لم يكن هذا ممكنا فخذ التقاط أقرب ما يمكن إلى الوجهة. الهدف هنا هو التحقق من من الذي يرسل TCP RST (هل خادم الوجهة أو من أحد الأجهزة الأخرى في المسار؟).

الحالة 3. مصافحة TCP 3-way + RST من نقطة نهاية واحدة

تعرض هذه الصورة المخطط:



وصف المشكلة: HTTP لا يعمل

التدفق المتأثر:

SRC IP: 192.168.0.100

بروتوكول DST IP: 10.10.1.100

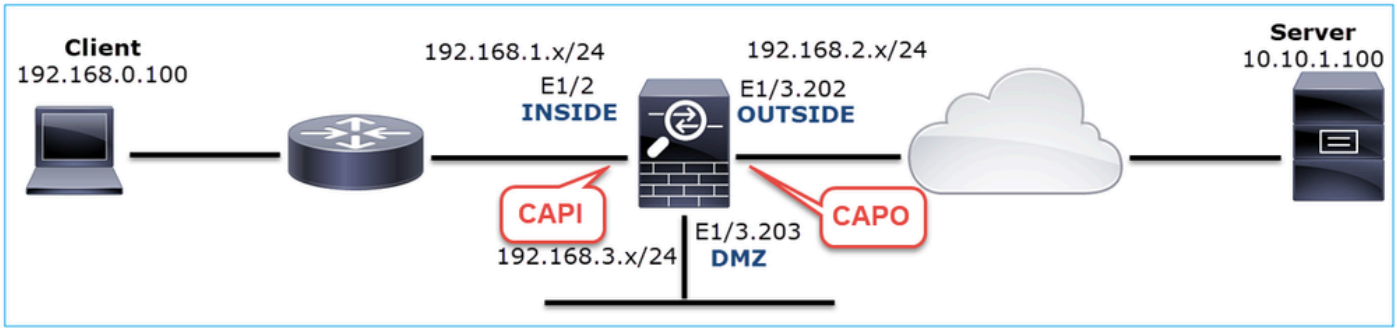
البروتوكول: بروتوكول TCP 80

تحليل أسر

قم بتمكين عمليات الالتقاط على محرك FTD LINA.

<#root>

```
firepower#
 capture CAPI int INSIDE match ip host 192.168.0.100 host 10.10.1.100
firepower#
 capture CAPO int OUTSIDE match ip host 192.168.0.100 host 10.10.1.100
```

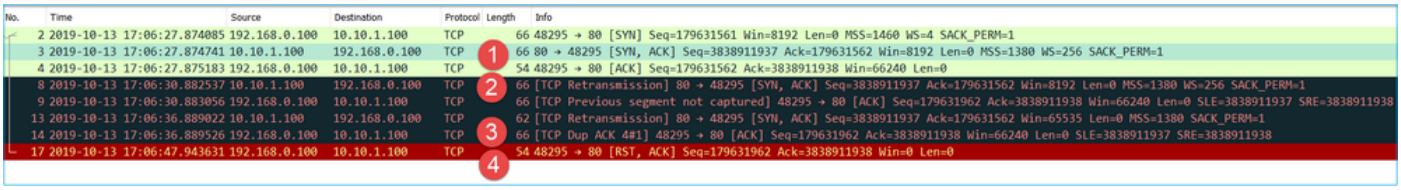


التقاط - سيناريو لا يعمل:

هناك طريقتان مختلفتان يمكن لهذه المشكلة أن تظهر في عمليات التقاط.

3.1 - مصافحة TCP 3-way + RST المؤجلة من العميل

يحتوي كل من جدار الحماية على CAPI و CAPO على الحزم نفسها، كما هو موضح في الصورة.



النقاط الرئيسية:

1. تمر مصافحة TCP 3-way عبر جدار الحماية.
2. يرسل الخادم SYN/ACK.
3. يرسل الزبون الطعام.
4. بعد حوالي 20 ثانية، يتخلى العميل عن بروتوكول TCP RST ويرسل إليه.

الإجراءات الموصى بها

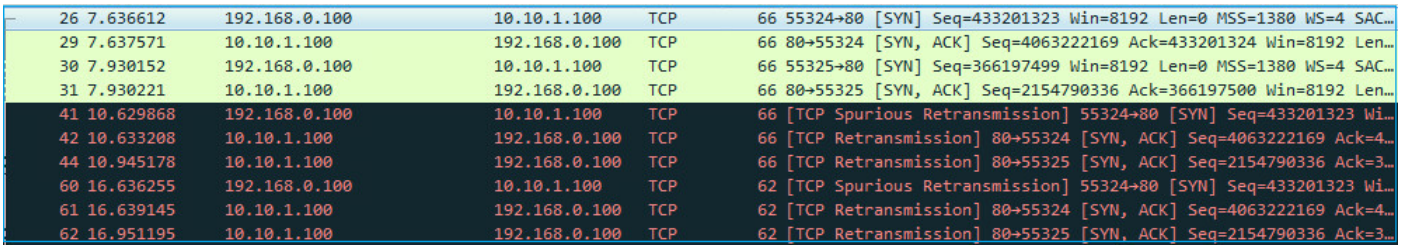
والغرض من الإجراءات الواردة في هذا الفرع هو زيادة تضييق نطاق هذه المسألة.

الإجراء 1. التقاط الصور أقرب ما يمكن إلى نقطتي النهاية.

تشير لقطات جدار الحماية إلى أن الخادم لم يعالج ACK الخاص بالعميل. وهذا مبني على هذه الحقائق:

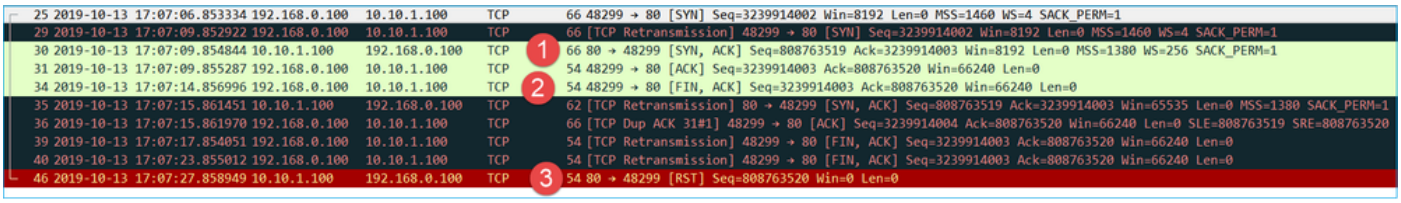
- يرسل الخادم SYN/ACK.
- يرسل الزبون الطعام.
- يرسل العميل TCP RST أو FIN/ACK قبل أي بيانات.

يظهر الالتقاط على الخادم المشكلة. لم يصل أبدا ACK العميل من تأكيد اتصال TCP الثلاثي:



3.2 - المصافحة ثلاثية الإتجاه ل TCP + الزعنفة/المكدس المؤجل من العميل + RST المؤجل من الخادم

يحتوي كل من جدار الحماية على CAPI و CAPO على الحزم نفسها، كما هو موضح في الصورة.



النقاط الرئيسية:

1. تمر مصافحة TCP 3-way عبر جدار الحماية.
2. بعد حوالي 5 ثوان يرسل العميل زعنفة/ACK.
3. بعد حوالي 20 ثانية، ينتهي الخادم من وضع TCP RST ويرسل إليه.

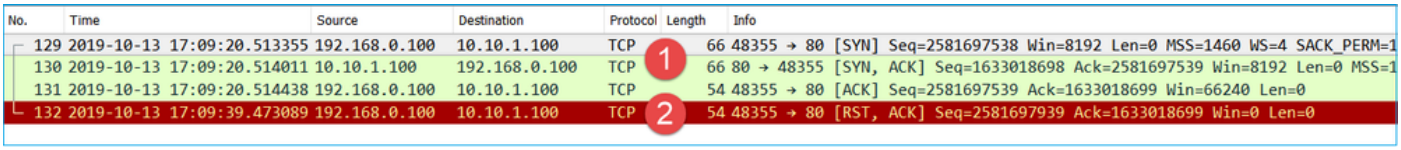
بناء على هذا السيناريو، يمكن الاستنتاج بأنه على الرغم من وجود مصافحة TCP ثلاثية الاتجاه عبر جدار الحماية، يبدو أنه لا يتم إتمامها في الواقع على نقطة نهاية واحدة (تشير عمليات إعادة الإرسال إلى ذلك).

الإجراءات الموصى بها

نفس الشيء في الحالة 3.1

3.3 - مصافحة TCP 3-way + RST المؤجلة من العميل

يحتوي كل من جدار الحماية على CAPI و CAPO على الحزم نفسها، كما هو موضح في الصورة.



النقاط الرئيسية:

1. تمر مصافحة TCP 3-way عبر جدار الحماية.
2. بعد حوالي 20 ثانية، يتخلى العميل عن بروتوكول TCP RST ويرسل إليه.

واستنادا إلى هذه الصور، يمكن إستنتاج ما يلي:

- بعد 5-20 ثانية، تتوقف نقطة نهاية واحدة وتقرر إنهاء الاتصال.

الإجراءات الموصى بها

نفس الشيء في الحالة 3.1

3.4 - المصافحة ثلاثية الإتجاه ل TCP + RST الفوري من الخادم

يحتوي كل من جدار الحماية على CAPI و CAPO على هذه الحزم، كما هو موضح في الصورة.

No.	Time	Source	Destination	Protocol	Length	Info
26	2019-10-13 17:07:07.104410	192.168.0.100	10.10.1.100	TCP	66	48300 → 80 [SYN] Seq=2563435279 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
27	2019-10-13 17:07:07.105112	10.10.1.100	192.168.0.100	TCP	66	80 → 48300 [SYN, ACK] Seq=3757137497 Ack=2563435280 Win=8192 Len=0 MSS=1380
28	2019-10-13 17:07:07.105554	192.168.0.100	10.10.1.100	TCP	54	48300 → 80 [ACK] Seq=2563435280 Ack=3757137498 Win=66240 Len=0
41	2019-10-13 17:07:07.106325	10.10.1.100	192.168.0.100	TCP	54	80 → 48300 [RST] Seq=2563435280 Win=0 Len=0

النقاط الرئيسية:

1. تمر مصافحة TCP 3-way عبر جدار الحماية.
2. هناك TCP RST من الخادم بعد حزمة ACK بفاصل زمني ثانية.

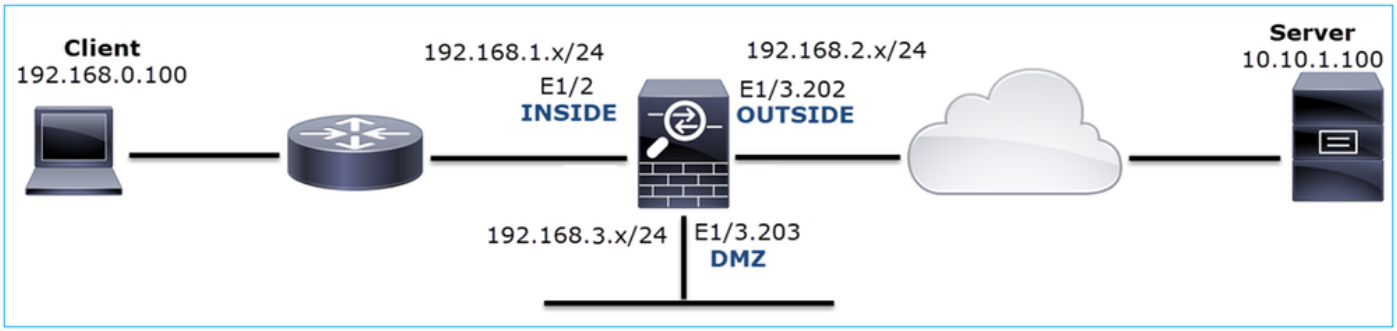
الإجراءات الموصى بها

الإجراء: التقاط الصور أقرب ما يمكن إلى الخادم.

يمكن أن يشير TCP RST الفوري من الخادم إلى وجود خادم أو جهاز في المسار الذي يرسل TCP RST. قم بالتقاط على الخادم نفسه وحدد مصدر TCP RST.

الحالة 4. TCP RST من العميل

تعرض هذه الصورة المخطط:



وصف المشكلة: لا يعمل HTTP.

التدفق المتأثر:

SRC IP: 192.168.0.100

بروتوكول DST IP: 10.10.1.100

البروتوكول: بروتوكول TCP 80

تحليل أسر

قم بتمكين عمليات الالتقاط على محرك FTD LINA.

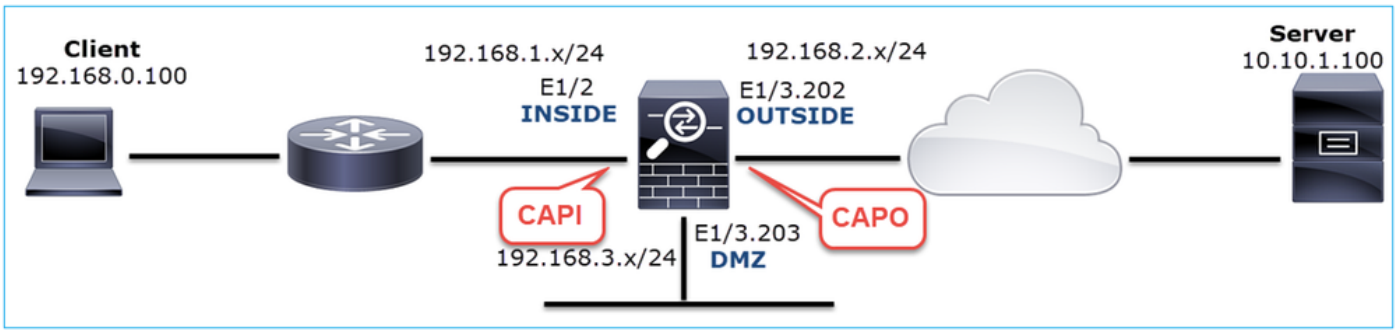
<#root>

```
firepower#
```

```
capture CAPI int INSIDE match ip host 192.168.0.100 host 10.10.1.100
```

```
firepower#
```

```
capture CAPO int OUTSIDE match ip host 192.168.0.100 host 10.10.1.100
```



التقاط - سيناريو لا يعمل:

هذه هي محتويات CAPI.

<#root>

```
firepower#
```

```
show capture CAPI
```

```
14 packets captured

   1: 12:32:22.860627   192.168.0.100.47078 > 10.10.1.100.80: S 4098574664:4098574664(0) win 8192 <mss
   2: 12:32:23.111307   192.168.0.100.47079 > 10.10.1.100.80: S 2486945841:2486945841(0) win 8192 <mss
   3: 12:32:23.112390   192.168.0.100.47079 > 10.10.1.100.80: R 3000518858:3000518858(0) win 0
   4: 12:32:25.858109   192.168.0.100.47078 > 10.10.1.100.80: S 4098574664:4098574664(0) win 8192 <mss
   5: 12:32:25.868698   192.168.0.100.47078 > 10.10.1.100.80: R 1386249853:1386249853(0) win 0
   6: 12:32:26.108118   192.168.0.100.47079 > 10.10.1.100.80: S 2486945841:2486945841(0) win 8192 <mss
   7: 12:32:26.109079   192.168.0.100.47079 > 10.10.1.100.80: R 3000518858:3000518858(0) win 0
   8: 12:32:26.118295   192.168.0.100.47079 > 10.10.1.100.80: R 3000518858:3000518858(0) win 0
   9: 12:32:31.859925   192.168.0.100.47078 > 10.10.1.100.80: S 4098574664:4098574664(0) win 8192 <mss
  10: 12:32:31.860902   192.168.0.100.47078 > 10.10.1.100.80: R 1386249853:1386249853(0) win 0
  11: 12:32:31.875229   192.168.0.100.47078 > 10.10.1.100.80: R 1386249853:1386249853(0) win 0
  12: 12:32:32.140632   192.168.0.100.47079 > 10.10.1.100.80: R 3000518858:3000518858(0) win 0
  13: 12:32:32.159995   192.168.0.100.47079 > 10.10.1.100.80: S 2486945841:2486945841(0) win 8192 <mss
  14: 12:32:32.160956   192.168.0.100.47079 > 10.10.1.100.80: R 3000518858:3000518858(0) win 0
14 packets shown
```

هذه هي محتويات CAPO:

<#root>

```
firepower#
```

```
show capture CAPO
```

```
11 packets captured

   1: 12:32:22.860780   802.1Q vlan#202 P0 192.168.0.100.47078 > 10.10.1.100.80: S 1386249852:138624985
   2: 12:32:23.111429   802.1Q vlan#202 P0 192.168.0.100.47079 > 10.10.1.100.80: S 3000518857:300051885
```

```
   3: 12:32:23.112405   802.1Q vlan#202 P0 192.168.0.100.47079 > 10.10.1.100.80: R 3514091874:351409187
   4: 12:32:25.858125   802.1Q vlan#202 P0 192.168.0.100.47078 > 10.10.1.100.80: S 1386249852:138624985
   5: 12:32:25.868729   802.1Q vlan#202 P0 192.168.0.100.47078 > 10.10.1.100.80: R 2968892337:296889233
   6: 12:32:26.108240   802.1Q vlan#202 P0 192.168.0.100.47079 > 10.10.1.100.80: S 3822259745:382225974
   7: 12:32:26.109094   802.1Q vlan#202 P0 192.168.0.100.47079 > 10.10.1.100.80: R 40865466:40865466(0)
   8: 12:32:31.860062   802.1Q vlan#202 P0 192.168.0.100.47078 > 10.10.1.100.80: S 4294058752:429405875
   9: 12:32:31.860917   802.1Q vlan#202 P0 192.168.0.100.47078 > 10.10.1.100.80: R 1581733941:158173394
  10: 12:32:32.160102   802.1Q vlan#202 P0 192.168.0.100.47079 > 10.10.1.100.80: S 4284301197:428430119
  11: 12:32:32.160971   802.1Q vlan#202 P0 192.168.0.100.47079 > 10.10.1.100.80: R 502906918:502906918(
11 packets shown
```

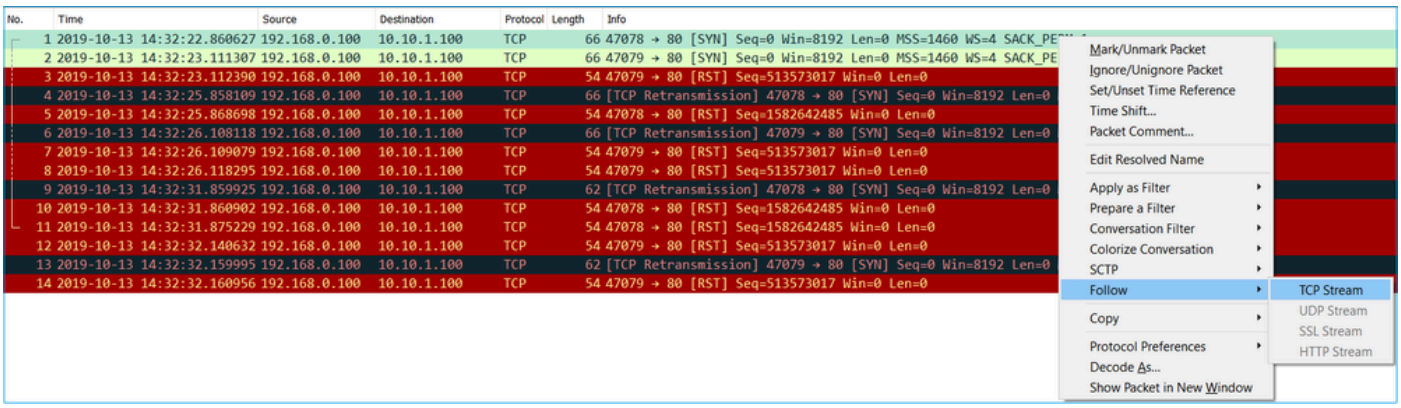
تظهر سجلات جدار الحماية:

```
<#root>

firepower#

show log | i 47741

Oct 13 2019 13:57:36: %FTD-6-302013: Built inbound TCP connection 4869 for INSIDE:192.168.0.100/47741 (
Oct 13 2019 13:57:36: %FTD-6-302014: Teardown TCP connection 4869 for INSIDE:192.168.0.100/47741 to OUT

TCP Reset-O from INSIDE

Oct 13 2019 13:57:39: %FTD-6-302013: Built inbound TCP connection 4870 for INSIDE:192.168.0.100/47741 (
Oct 13 2019 13:57:39: %FTD-6-302014: Teardown TCP connection 4870 for INSIDE:192.168.0.100/47741 to OUT

TCP Reset-O from INSIDE

Oct 13 2019 13:57:45: %FTD-6-302013: Built inbound TCP connection 4871 for INSIDE:192.168.0.100/47741 (
Oct 13 2019 13:57:45: %FTD-6-302014: Teardown TCP connection 4871 for INSIDE:192.168.0.100/47741 to OUT
```

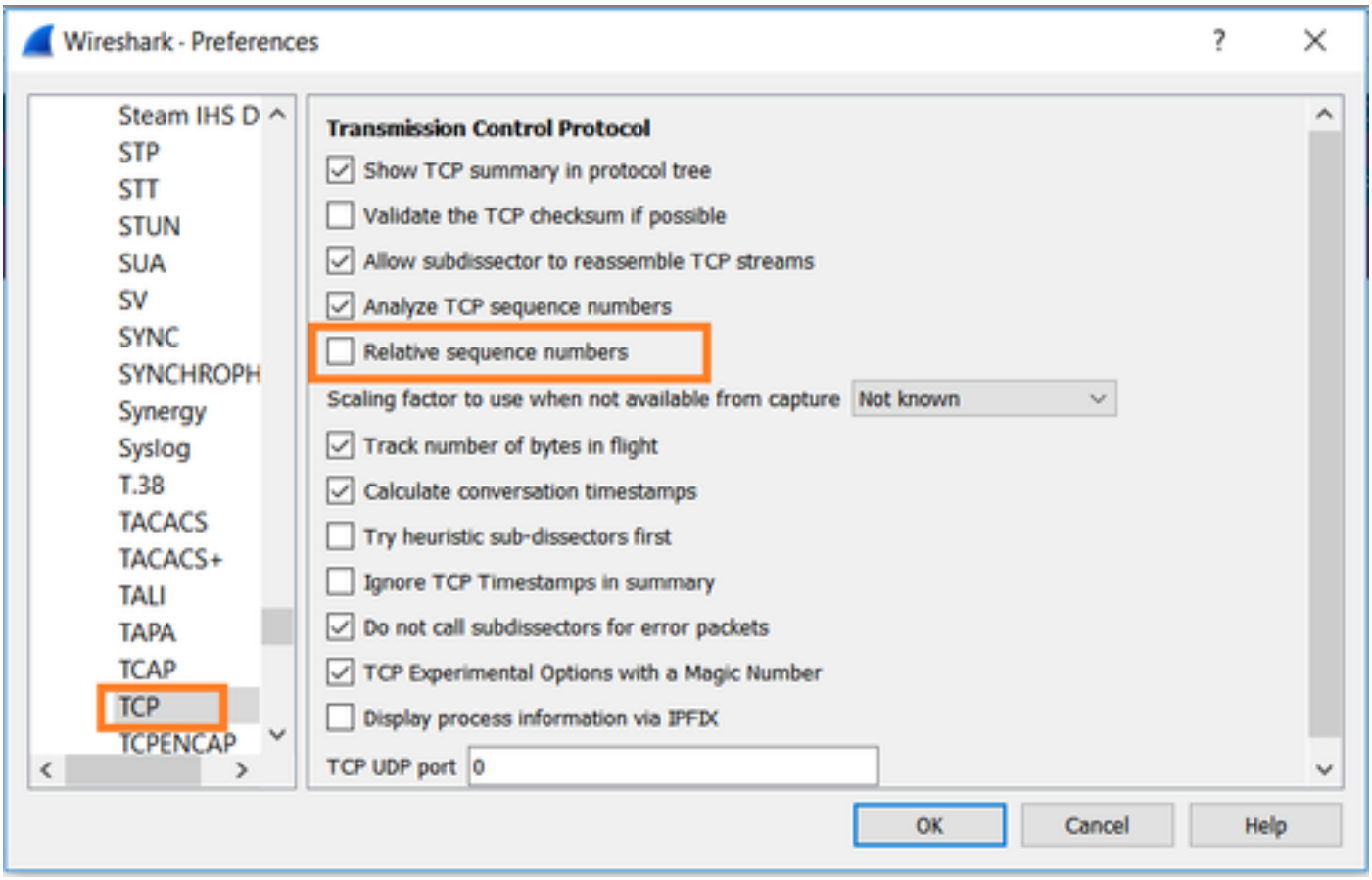
تشير هذه السجلات إلى وجود TCP RST يصل إلى واجهة جدار الحماية الداخلية

أسر CAPI في Wireshark:

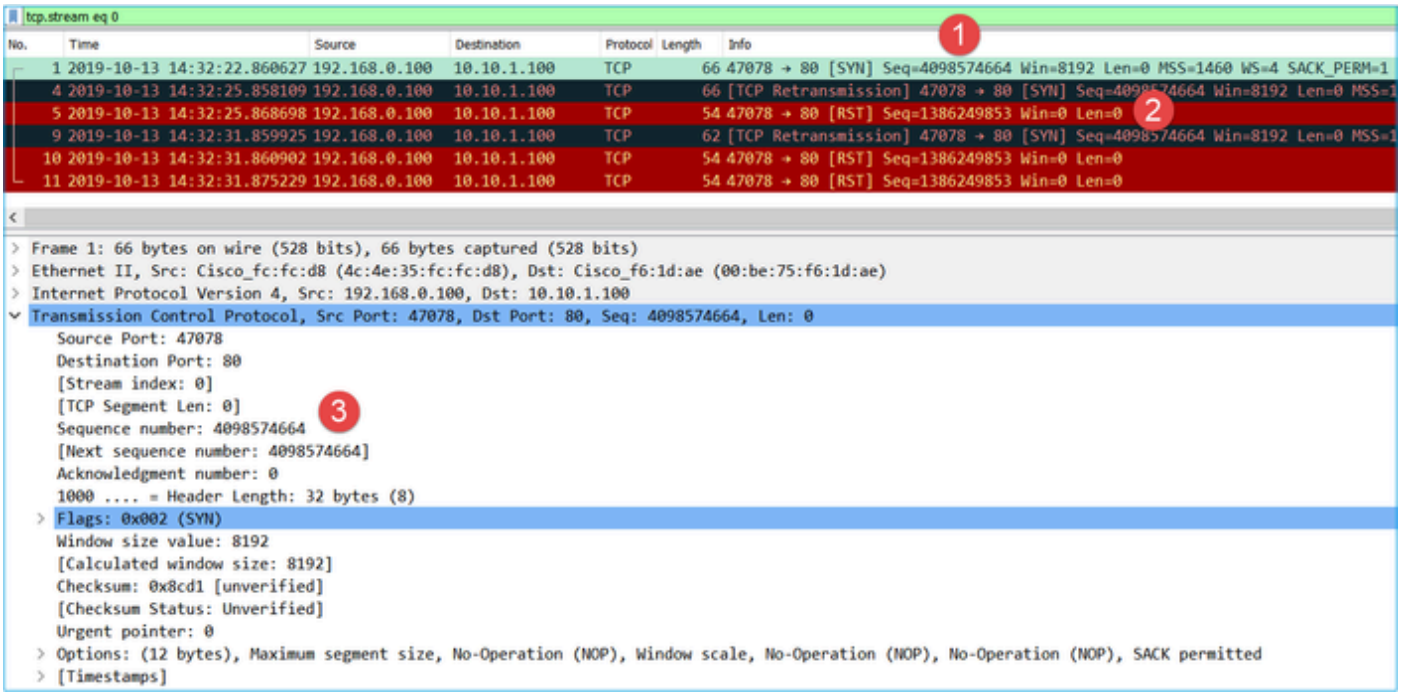
اتبع تدفق TCP الأول، كما هو موضح في الصورة.



تحت Wireshark، انتقل إلى تحرير > تفضيلات > بروتوكولات > TCP وألغي تحديد خيار أرقام التسلسل النسبية كما هو موضح في الصورة.



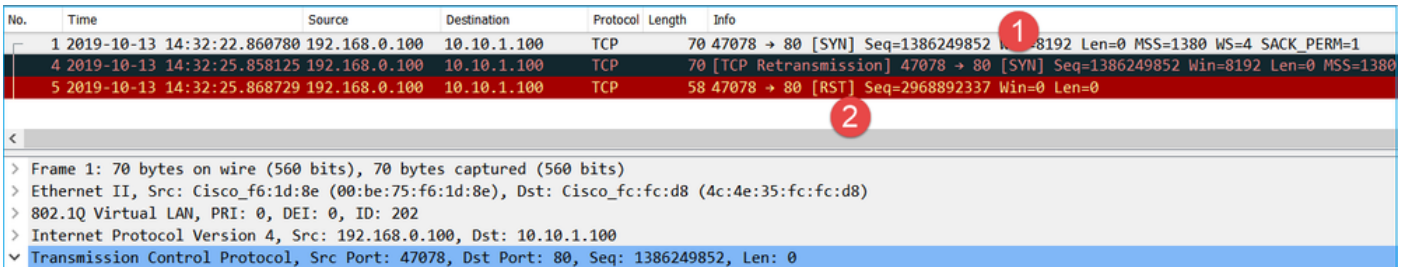
تظهر هذه الصورة محتويات التدفق الأول في التقاط CAPI:



النقاط الرئيسية:

1. يرسل العميل حزمة TCP syn.
2. يرسل العميل حزمة TCP RST.
3. تحتوي حزمة TCP syn على قيمة رقم تسلسل تساوي 4098574664.

يحتوي نفس التدفق في التقاط CAPO على:



النقاط الرئيسية:

1. يرسل العميل حزمة TCP syn. جدار الحماية العشوائية ل IS.
2. يرسل العميل حزمة TCP RST.

واستنادا إلى اللمحتين، يمكن إستنتاج ما يلي:

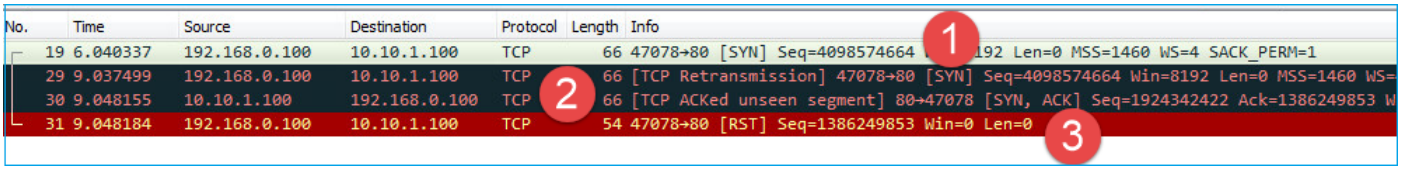
- لا توجد مصافحة TCP ثلاثية الإتجاه بين العميل والخادم.
- هناك TCP RST الذي يأتي من العميل. قيمة رقم تسلسل TCP RST في التقاط CAPI هي 1386249853.

الإجراءات الموصى بها

والغرض من الإجراءات الواردة في هذا الفرع هو زيادة تضييق نطاق هذه المسألة.

الإجراء 1. التقاط العميل.

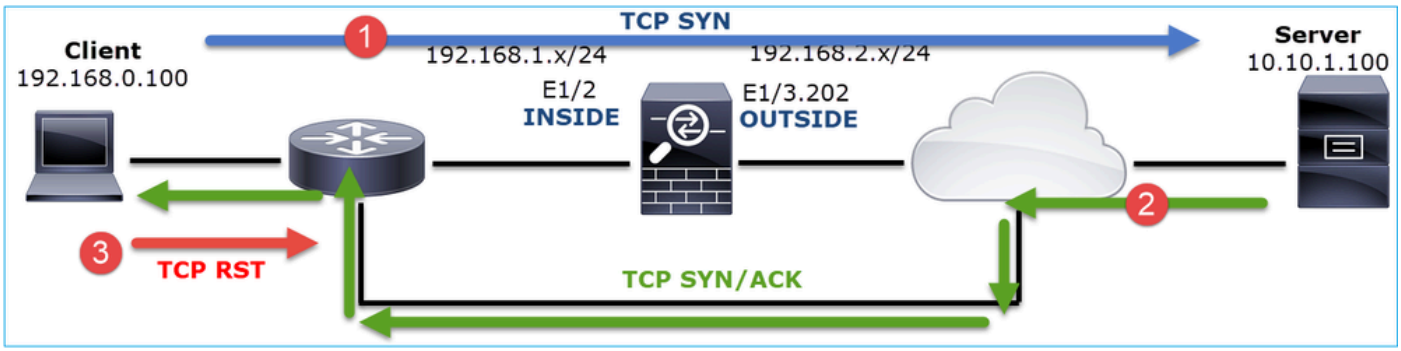
استنادا إلى عمليات الالتقاط التي تم جمعها على جدار الحماية، هناك مؤشر قوي على وجود تدفق غير متماثل. يستند هذا إلى حقيقة أن العميل يرسل TCP RST بقيمة 1386249853 (IS العشوائي):



النقاط الرئيسية:

1. يرسل العميل حزمة TCP syn. الرقم التسلسلي هو 4098574664 وهو نفسه الذي يرى على جدار الحماية في الواجهة الداخلية (CAPI)
2. يوجد TCP SYN/ACK برقم ACK 1386249853 (المتوقع أن يكون بسبب ISN randomization). لم يتم رؤية هذه الحزمة في التقاط جدار الحماية
3. يرسل العميل TCP RST منذ أن توقع SYN/ACK مع قيمة رقم ACK 4098574665، ولكنه استلم قيمة 1386249853

ويمكن تمثيل ذلك على النحو التالي:

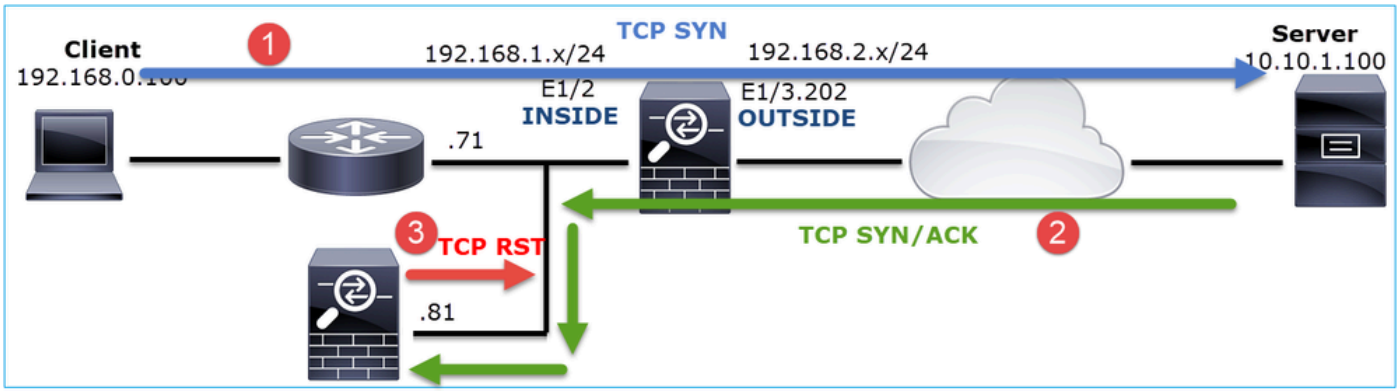


الإجراء 2. تحقق من التوجيه بين العميل وجدار الحماية.

تأكيد ما يلي:

- عناوين MAC التي تم رؤيتها في عمليات الالتقاط هي العناوين المتوقعة.
- تأكد من أن التوجيه بين جدار الحماية والعميل متماثل.

هناك سيناريوهات حيث يأتي RST من جهاز يقع بين جدار الحماية والعميل أثناء وجود توجيه غير متماثل في الشبكة الداخلية. تظهر حالة نموذجية في الصورة:



في هذه الحالة، فإن الالتقاط يحتوي على هذا المحتوى. لاحظ الفرق بين عنوان MAC المصدر لحزمة TCP syn مقابل عنوان MAC المصدر الخاص ب TCP RST وعنوان MAC الوجهة لحزمة TCP syn/ACK:

```
<#root>

firepower#

show capture CAPI detail

   1: 13:57:36.730217

 4c4e.35fc.fcd8

 00be.75f6.1dae 0x0800 Length: 66
      192.168.0.100.47740 > 10.10.1.100.80: S [tcp sum ok] 3045001876:3045001876(0) win 8192 <mss 1460,
   2: 13:57:36.981104 4c4e.35fc.fcd8 00be.75f6.1dae 0x0800 Length: 66
      192.168.0.100.47741 > 10.10.1.100.80: S [tcp sum ok] 3809380540:3809380540(0) win 8192 <mss 1460,
   3: 13:57:36.981776 00be.75f6.1dae

a023.9f92.2a4d

 0x0800 Length: 66
      10.10.1.100.80 > 192.168.0.100.47741: S [tcp sum ok] 1304153587:1304153587(0) ack 3809380541 win
```

```
   4: 13:57:36.982126

a023.9f92.2a4d

 00be.75f6.1dae 0x0800 Length: 54
      192.168.0.100.47741 > 10.10.1.100.80:

R

 [tcp sum ok] 3809380541:3809380541(0) ack 1304153588 win 8192 (ttl 255, id 48501)
...
```

الحالة 5. النقل البطيء لبروتوكول TCP (السيناريو 1)

وصف المشكلة:

نقل SFTP بين الأجهزة المضيفة 10.77.19.11 و 10.11.4.171 بطيء. على الرغم من أن الحد الأدنى لعرض النطاق الترددي (BW) بين المضيفين هو 100 ميجابت في الثانية، إلا أن سرعة النقل لا تتجاوز 5 ميجابت في الثانية.

وفي الوقت نفسه، فإن سرعة النقل بين الأجهزة المضيفة 172.25.18.134 و 10.11.2.124 أعلى من ذلك بكثير.

النظرية الأساسية:

يتم تحديد سرعة النقل القصوى لتدفق TCP واحد بواسطة منتج تأخير النطاق الترددي (BDP). يتم عرض الصيغة المستخدمة في الصورة:

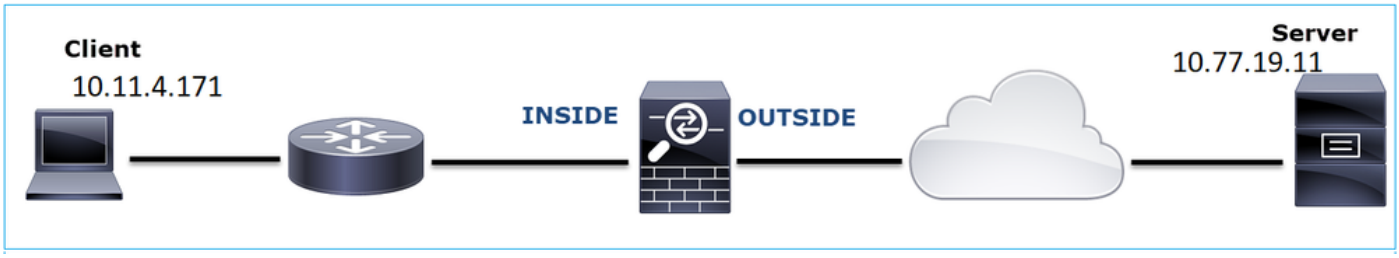
$$\text{Max Single TCP Flow Throughput [bps]} = \frac{\text{TCP Window (Bytes)}}{\text{RTT (Seconds)}} \times 8 \text{ [bits/Byte]}$$

لمزيد من التفاصيل حول BDP تحقق من الموارد هنا:

- لماذا يستخدم تطبيق 10 ميجابت في الثانية فقط حتى الارتباط 1 جيجابت في الثانية؟
- BRKSEC-3021 - متقدم - تحسين أداء جدار الحماية

السيناريو 1 - النقل البطيء

تعرض هذه الصورة المخطط:



التدفق المتأثر:

SRC IP: 10.11.4.171

بروتوكول DST IP: 10.77.19.11

البروتوكول: SFTP (FTP عبر SSH)

تحليل أسر

تمكين االلتقاط على محرك FTD LINA:

<#root>

firepower#

capture CAPI int INSIDE buffer 33554432 match ip host 10.11.4.171 host 10.77.19.11

firepower#

capture CAPO int OUTSIDE buffer 33554432 match ip host 10.11.4.171 host 10.77.19.11

تحذير: تؤثر التقاط LINA على التقاط FP1xxx و FP21xx على معدل نقل حركة المرور التي تمر عبر FTD. ال تقم بتمكين التقاط LINA على الأنظمة الأساسية FP1xxx و FP21xxx عند أستكشاف أخطاء الأداء وإصالحها (النقل البطيء عبر FTD). بدل من ذلك استعملت فسحة بين دعامتين أو HW Tap أداة باإلضافة إلى أن على قبض على المصدر وغاية مضيف. وثقت الإصدار في cisco بق id CSCvo30697.

<#root>

firepower#

capture CAPI type raw-data trace interface inside match icmp any any

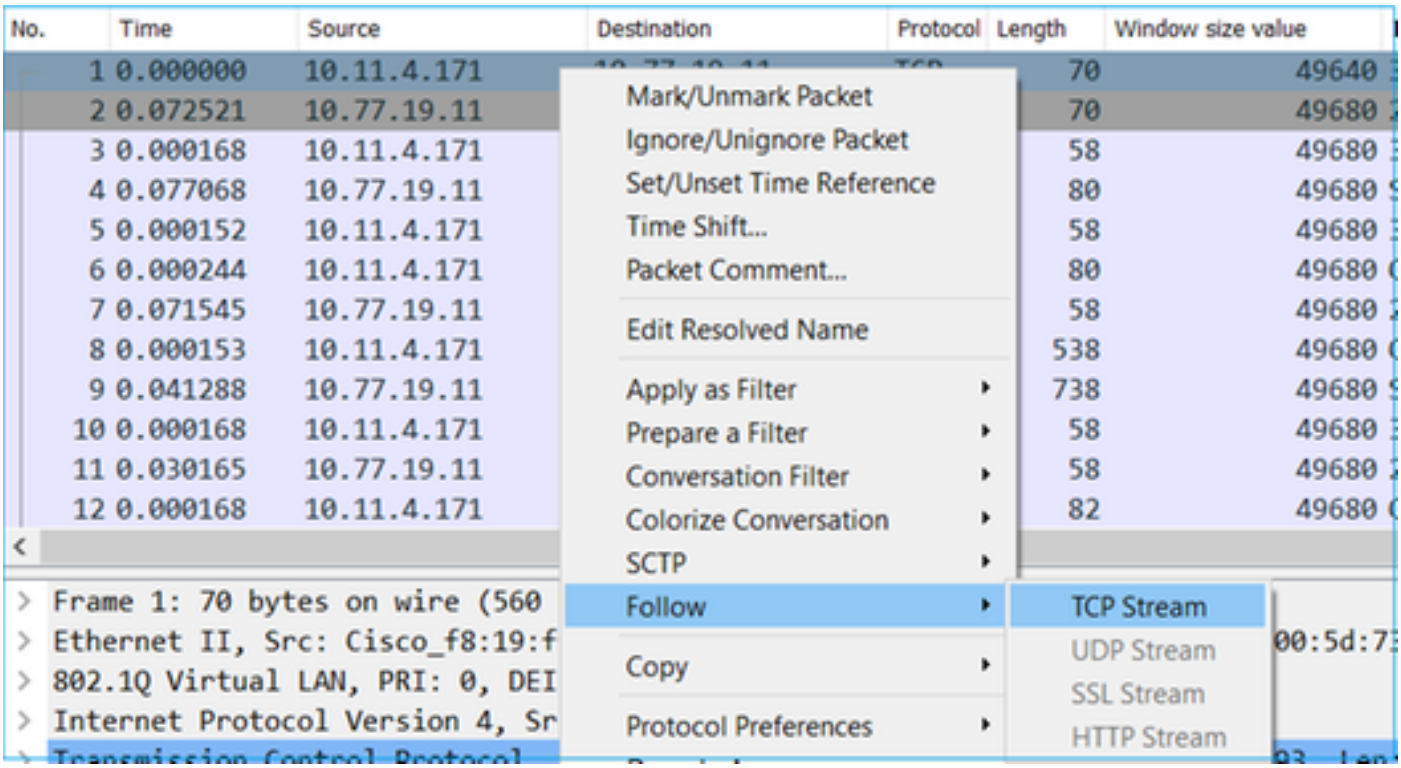
WARNING: Running packet capture can have an adverse impact on performance.

الإجراءات الموصى بها

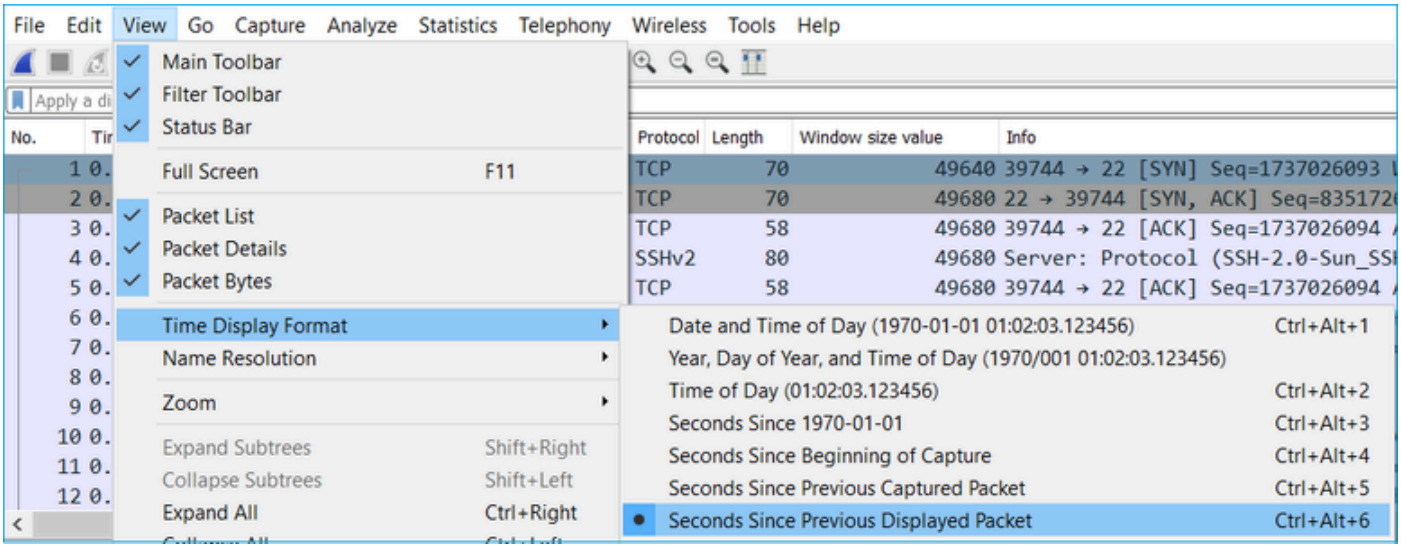
والغرض من الإجراءات الواردة في هذا القرع وه زيادة تضييق نطاق هذه المسألة.

حساب وقت الذهاب والعودة (RTT)

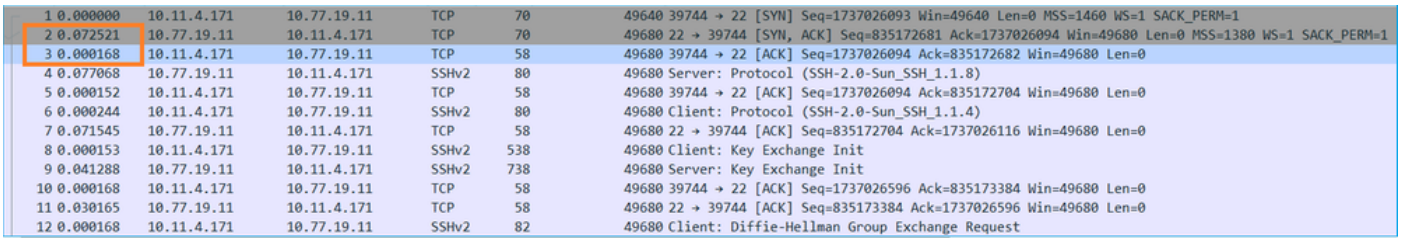
أولا، حدد تدفق النقل وتابعه:



قم بتغيير طريقة عرض Wireshark لإظهار الثواني منذ الحزمة المعروضة السابقة. وهذا من شأنه تسهيل حساب RTT:



يمكن حساب RTT من خلال إضافة قيم الوقت بين عمليتي تبادل حزم (أحدهما نحو المصدر والآخر نحو الوجهة). في هذه الحالة، تعرض الحزمة #2 RTT بين جدار الحماية والجهاز الذي أرسل حزمة SYN/ACK (الخادم). تعرض الحزمة #3 RTT بين جدار الحماية والجهاز الذي أرسل حزمة ACK (العميل). توفر إضافة الرقمين تقديرا جيدا حول RTT الشامل:

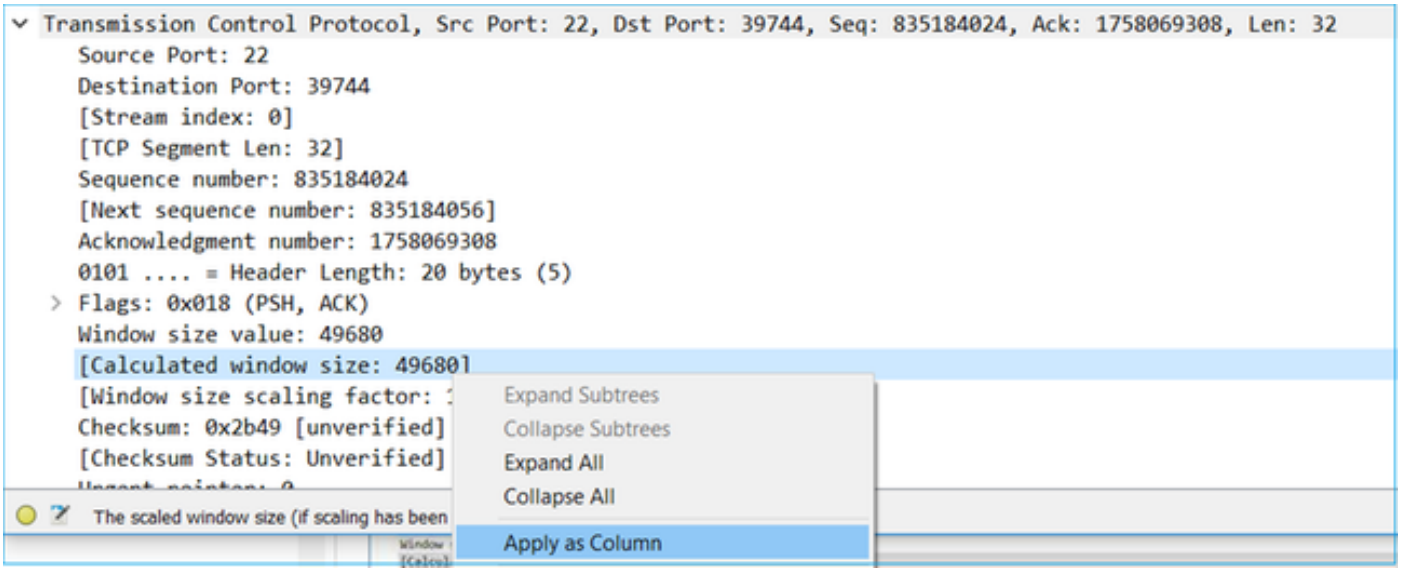


1	0.000000	10.11.4.171	10.77.19.11	TCP	70	49640 39744 → 22 [SYN] Seq=1737026093 Win=49640 Len=0 MSS=1460 WS=1 SACK_PERM=1
2	0.072521	10.77.19.11	10.11.4.171	TCP	70	49680 22 → 39744 [SYN, ACK] Seq=835172681 Ack=1737026094 Win=49680 Len=0 MSS=1380 WS=1 SACK_PERM=1
3	0.000168	10.11.4.171	10.77.19.11	TCP	58	49680 39744 → 22 [ACK] Seq=1737026094 Ack=835172682 Win=49680 Len=0
4	0.077068	10.77.19.11	10.11.4.171	SSHv2	80	49680 Server: Protocol (SSH-2.0-Sun_SSH_1.1.8)
5	0.000152	10.11.4.171	10.77.19.11	TCP	58	49680 39744 → 22 [ACK] Seq=1737026094 Ack=835172704 Win=49680 Len=0
6	0.000244	10.11.4.171	10.77.19.11	SSHv2	80	49680 Client: Protocol (SSH-2.0-Sun_SSH_1.1.4)
7	0.071545	10.77.19.11	10.11.4.171	TCP	58	49680 22 → 39744 [ACK] Seq=835172704 Ack=1737026116 Win=49680 Len=0
8	0.000153	10.11.4.171	10.77.19.11	SSHv2	538	49680 Client: Key Exchange Init
9	0.041288	10.77.19.11	10.11.4.171	SSHv2	738	49680 Server: Key Exchange Init
10	0.000168	10.11.4.171	10.77.19.11	TCP	58	49680 39744 → 22 [ACK] Seq=1737026596 Ack=835173384 Win=49680 Len=0
11	0.030165	10.77.19.11	10.11.4.171	TCP	58	49680 22 → 39744 [ACK] Seq=835173384 Ack=1737026596 Win=49680 Len=0
12	0.000168	10.11.4.171	10.77.19.11	SSHv2	82	49680 Client: Diffie-Hellman Group Exchange Request

RTT ≈ 80 ثانية

حساب حجم نافذة TCP

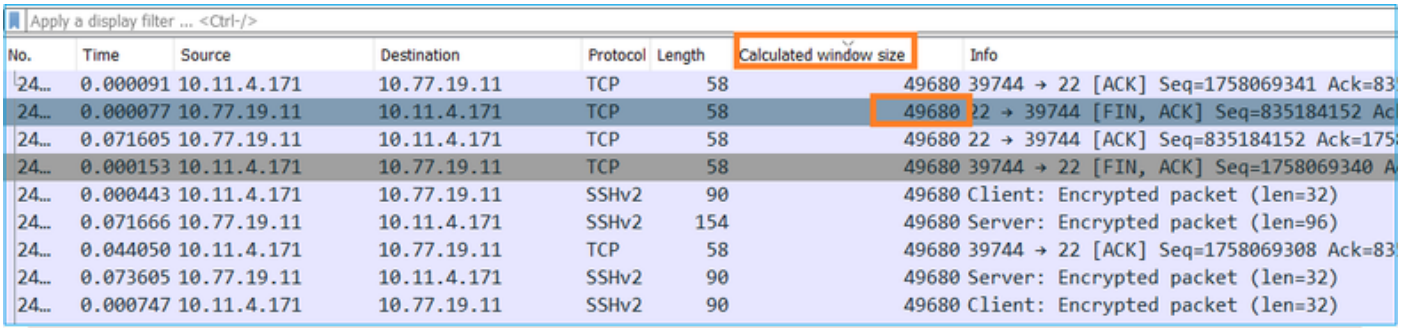
قم بتوسيع حزمة TCP، وتوسيع رأس TCP، وتحديد حجم النافذة المحسوب وحدد تطبيق كعمود:



تحقق من عمود قيمة حجم النافذة المحسوب لمعرفة ما هي قيمة الحد الأقصى لحجم النافذة أثناء جلسة عمل TCP. يمكنك أيضا تحديد اسم العمود وترتيب القيم.

إذا قمت باختبار تنزيل ملف (خادم > عميل)، فيجب عليك التحقق من القيم المعلن عنها بواسطة الخادم. تحدد القيمة القصوى لحجم النافذة المعلن عنها من قبل الخادم أقصى سرعة نقل يتم تحقيقها.

في هذه الحالة، يبلغ حجم نافذة TCP ≈ 50000 بايت



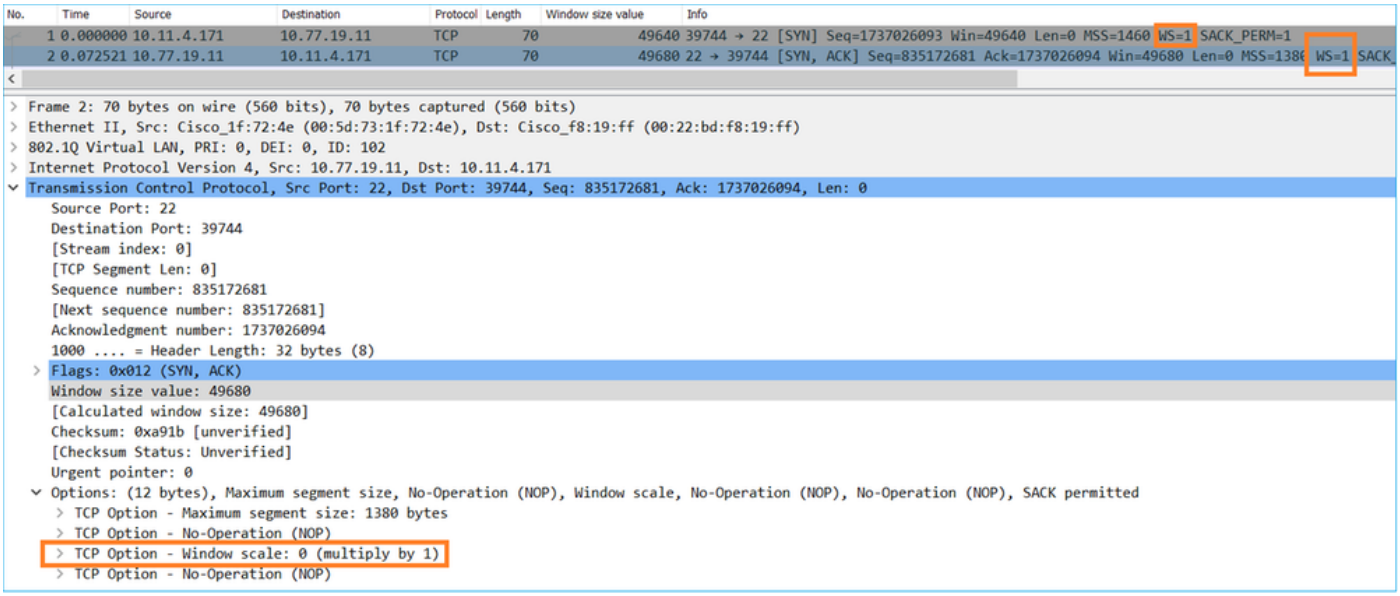
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Calculated window size	Info
24...	0.000091	10.11.4.171	10.77.19.11	TCP	58	49680	39744 → 22 [ACK] Seq=1758069341 Ack=83
24...	0.000077	10.77.19.11	10.11.4.171	TCP	58	49680	22 → 39744 [FIN, ACK] Seq=835184152 Ac
24...	0.071605	10.77.19.11	10.11.4.171	TCP	58	49680	22 → 39744 [ACK] Seq=835184152 Ack=175
24...	0.000153	10.11.4.171	10.77.19.11	TCP	58	49680	39744 → 22 [FIN, ACK] Seq=1758069340 A
24...	0.000443	10.11.4.171	10.77.19.11	SSHv2	90	49680	Client: Encrypted packet (len=32)
24...	0.071666	10.77.19.11	10.11.4.171	SSHv2	154	49680	Server: Encrypted packet (len=96)
24...	0.044050	10.11.4.171	10.77.19.11	TCP	58	49680	39744 → 22 [ACK] Seq=1758069308 Ack=83
24...	0.073605	10.77.19.11	10.11.4.171	SSHv2	90	49680	Server: Encrypted packet (len=32)
24...	0.000747	10.11.4.171	10.77.19.11	SSHv2	90	49680	Client: Encrypted packet (len=32)

استنادا إلى هذه القيم ومع إستخدام صيغة منتج تأخير النطاق الترددي ستحصل على أقصى عرض نطاق افتراضي يمكن تحقيقه في ظل هذه الظروف: 50000*8/0. 08 = 5 ميجابت في الثانية الحد الأقصى لعرض النطاق الافتراضي النظري.

وهذا يطابق ما يختبره العميل في هذه الحالة.

تحقق عن كثب من تأكيد اتصال TCP الثلاثي. يقوم كل الجانبين، والأهم من ذلك الخادم، بالإعلان عن قيمة قياس نافذة 0 والتي تعني 2^0 = 1 (لا يوجد قياس في النوافذ). ويؤثر هذا سلبا على معدل التحويل:

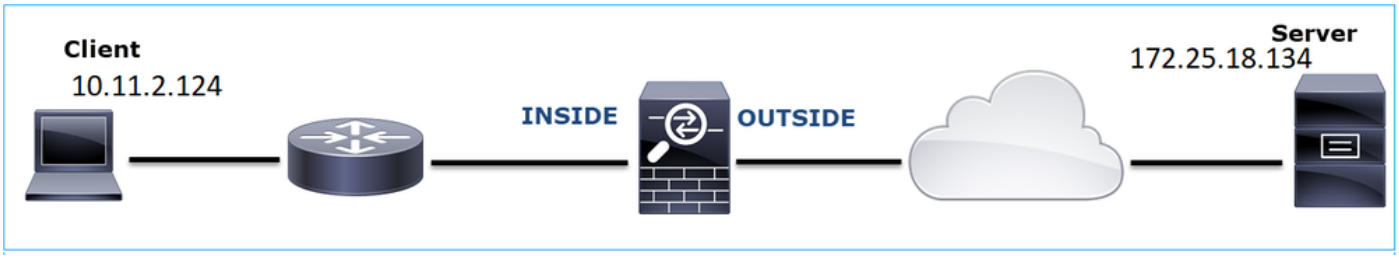


عند هذه النقطة، هناك حاجة لالتقاط صورة على الخادم، وتأكد من أنه الشخص الذي أعلن عن مقياس النافذة = 0 وأعد تكوينه (راجع وثائق الخادم لمعرفة كيفية القيام بذلك).

السيناريو 2 - النقل السريع

الآن دعنا نفحص السيناريو الجيد (النقل السريع عبر الشبكة نفسها):

المخطط:



تدفق الاهتمام:

SRC IP: 10.11.2.124

بروتوكول DST IP: 172.25.18.134

البروتوكول: SFTP (FTP عبر SSH)

تمكين التقاط على محرك FTD LINA

```
firepower#
capture CAPI int INSIDE buffer 33554432 match ip host 10.11.2.124 host 172.25.18.134
firepower#
capture CAPO int OUTSIDE buffer 33554432 match ip host 10.11.2.124 host 172.25.18.134
```

حساب وقت الذهاب والعودة (RTT): في هذه الحالة، يكون RTT 300 ≈ ثانية.

No.	Time	Source	Destination	Protocol	Length
1	0.000000	10.11.2.124	172.25.18.134	TCP	78
2	0.267006	172.25.18.134	10.11.2.124	TCP	78
3	0.000137	10.11.2.124	172.25.18.134	TCP	70
4	0.003784	10.11.2.124	172.25.18.134	SSHv2	91
5	0.266863	172.25.18.134	10.11.2.124	TCP	70
6	0.013580	172.25.18.134	10.11.2.124	SSHv2	91

حساب حجم نافذة TCP: يقوم الخادم بالإعلان عن عامل مقياس نافذة TCP رقم 7.

```
> Internet Protocol Version 4, Src: 172.25.18.134, Dst: 10.11.2.124
v Transmission Control Protocol, Src Port: 22, Dst Port: 57093, Seq: 661963571, Ack: 1770516295, Len: 0
    Source Port: 22
    Destination Port: 57093
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 661963571
    [Next sequence number: 661963571]
    Acknowledgment number: 1770516295
    1010 .... = Header Length: 40 bytes (10)
  > Flags: 0x012 (SYN, ACK)
    Window size value: 14480
    [Calculated window size: 14480]
    Checksum: 0x6497 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  v Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
    > TCP Option - Maximum segment size: 1300 bytes
    > TCP Option - SACK permitted
    > TCP Option - Timestamps: TSval 390233290, TSecr 981659424
    > TCP Option - No-Operation (NOP)
    > TCP Option - Window scale: 7 (multiply by 128)
  > [SEQ/ACK analysis]
```

حجم نافذة TCP للخادم ≈ 1600000 بايت:

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Window size value	Calculated window size	Info
23...	0.002579	172.25.18.134	10.11.2.124	TCP	70	12854	1645312	22 → 57093 [FIN, ACK]
23...	0.266847	172.25.18.134	10.11.2.124	TCP	70	12854	1645312	22 → 57093 [ACK] Seq=
23...	0.268089	172.25.18.134	10.11.2.124	SSHv2	198	12854	1645312	Server: Encrypted pac
23...	0.000076	172.25.18.134	10.11.2.124	SSHv2	118	12854	1645312	Server: Encrypted pac
23...	0.000351	172.25.18.134	10.11.2.124	SSHv2	118	12854	1645312	Server: Encrypted pac
23...	0.000092	172.25.18.134	10.11.2.124	TCP	70	12854	1645312	22 → 57093 [ACK] Seq=
23...	0.000015	172.25.18.134	10.11.2.124	TCP	70	12854	1645312	22 → 57093 [ACK] Seq=
23...	0.000091	172.25.18.134	10.11.2.124	TCP	70	12854	1645312	22 → 57093 [ACK] Seq=

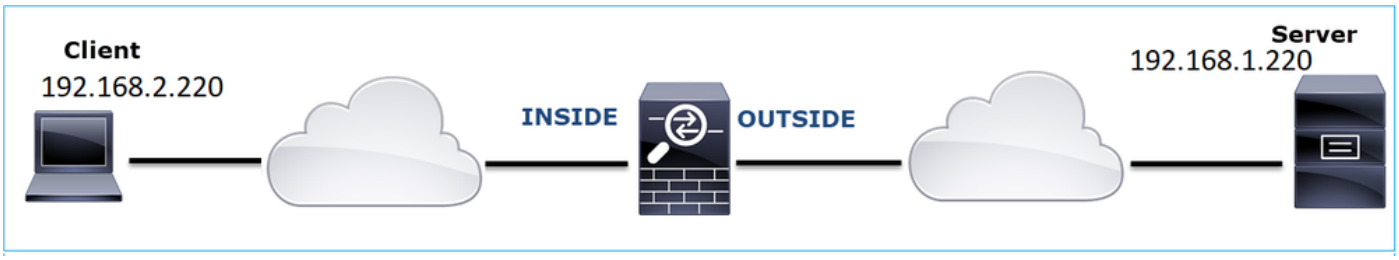
استنادا إلى هذه القيم، توفر صيغة منتجات تأخير النطاق الترددي ما يلي:

160000*8/0.3 = 43 ميجابت في الثانية الحد الأقصى لسرعة النقل النظرية

الحالة 6. النقل البطيء لبروتوكول TCP (السيناريو 2)

وصف المشكلة: نقل ملف FTP (تنزيل) عبر جدار الحماية بطيء.

تعرض هذه الصورة المخطط:



التدفق المتأثر:

SRC IP: 192.168.2.220

بروتوكول DST IP: 192.168.1.220

البروتوكول: FTP

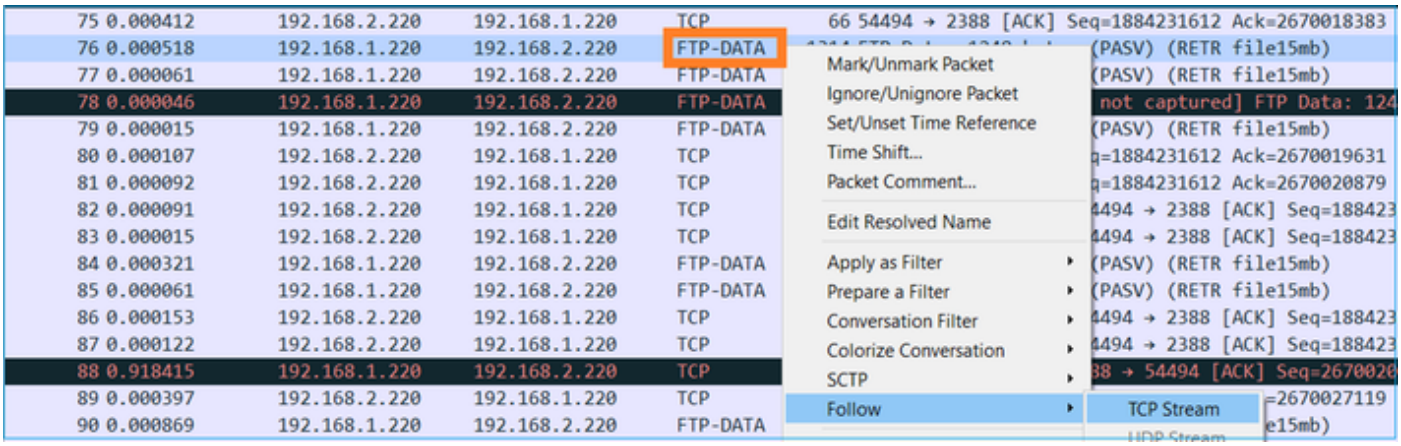
تحليل أسر

قم بتمكين عمليات الالتقاط على محرك FTD LINA.

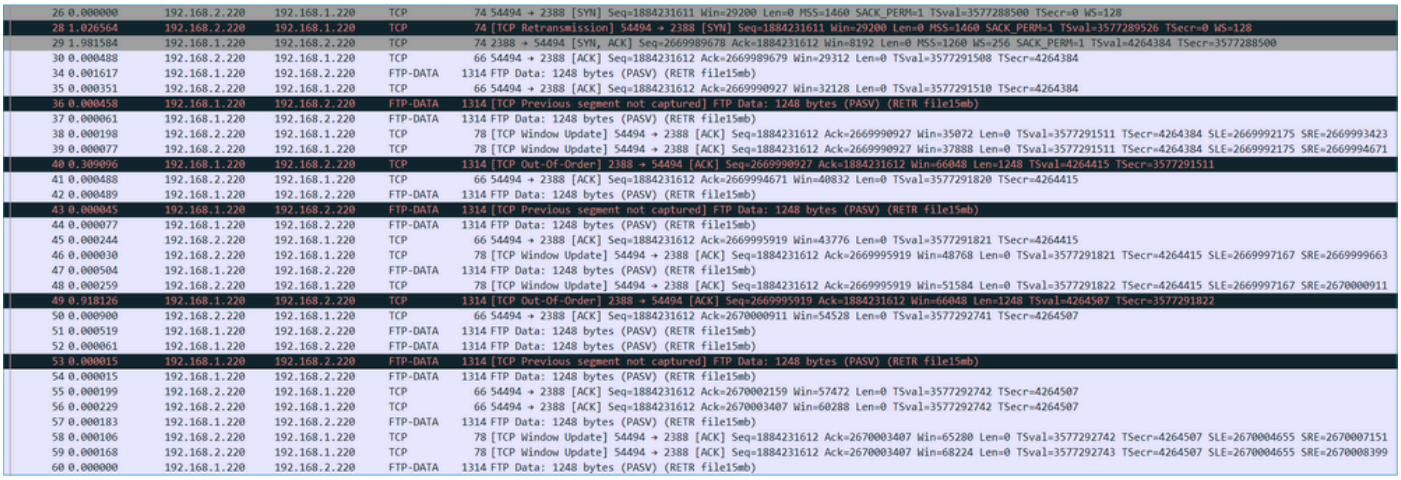
<#root>

```
firepower#
capture CAPI type raw-data buffer 33554432 interface INSIDE match tcp host 192.168.2.220 host 192.168.1.
firepower#
cap CAPO type raw-data buffer 33554432 interface OUTSIDE match tcp host 192.168.2.220 host 192.168.1.220
```

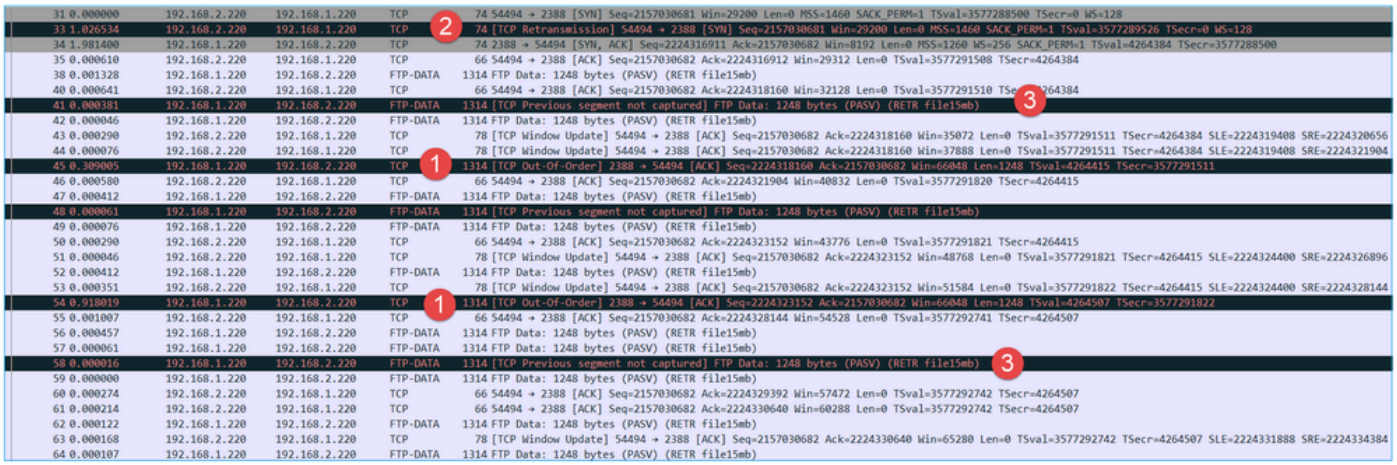
حدد حزمة FTP-Data واتبع قناة بيانات FTP على التقاط FTD Inside (CAPI):



محتوى تدفق بيانات FTP:



محتوى التقاط CAPO:

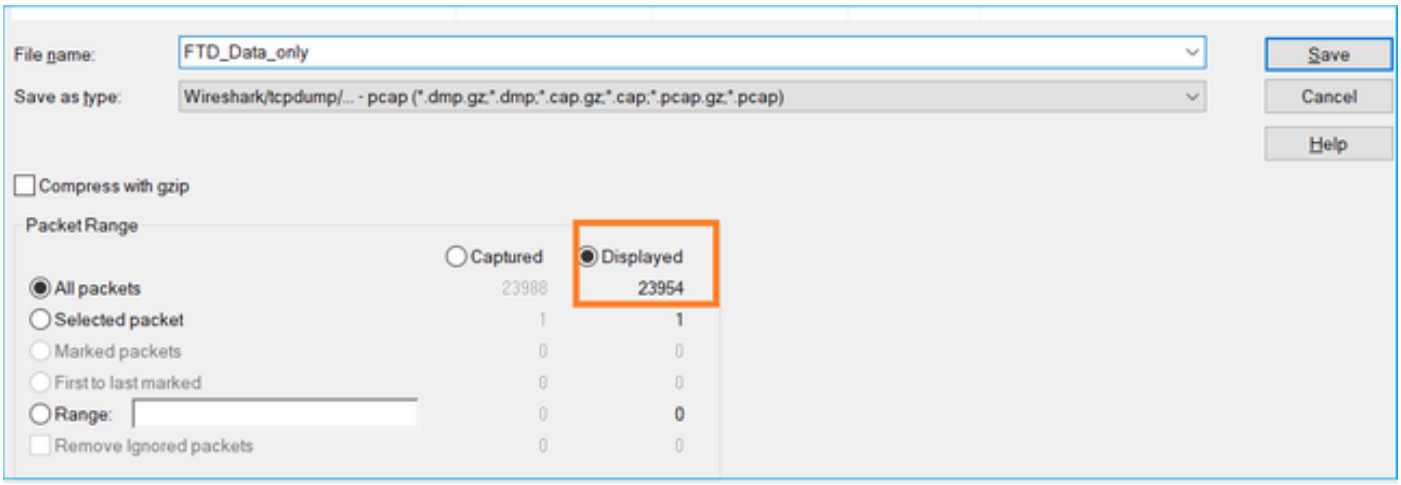


النقاط الرئيسية:

1. هناك حزم TCP خارج الترتيب (OOO).
2. هناك إعادة إرسال TCP.
3. هناك إشارة إلى فقدان حزمة (الحزم المسقطة).

تلميح: قم بحفظ الالتقاطات وأنت تتنقل إلى ملف > تصدير الحزم المحددة. ثم

احفظ فقط نطاق الحزمة المعروضة



الإجراءات الموصى بها

والغرض من الإجراءات الواردة في هذا القسم هو زيادة تضييق نطاق هذه المسألة.

الإجراء 1. تحديد موقع فقدان الحزمة.

في حالات مثل هذه، يجب عليك التقاط عمليات التقاط متزامنة واستخدام منهجية فرق الاتصال والتغلب لتحديد مقطع (مقاطع) الشبكة التي تتسبب في فقدان الحزمة. ومن وجهة نظر جدار الحماية هناك ثلاثة سيناريوهات رئيسية:

1. يرجع فقد الحزمة إلى جدار الحماية نفسه.
2. ينتج عن فقد الحزمة تدفق البيانات إلى جهاز جدار الحماية (إتجاه من الخادم إلى العميل).
3. ينتج عن فقد الحزمة تدفق إلى جهاز جدار الحماية (إتجاه من العميل إلى الخادم).

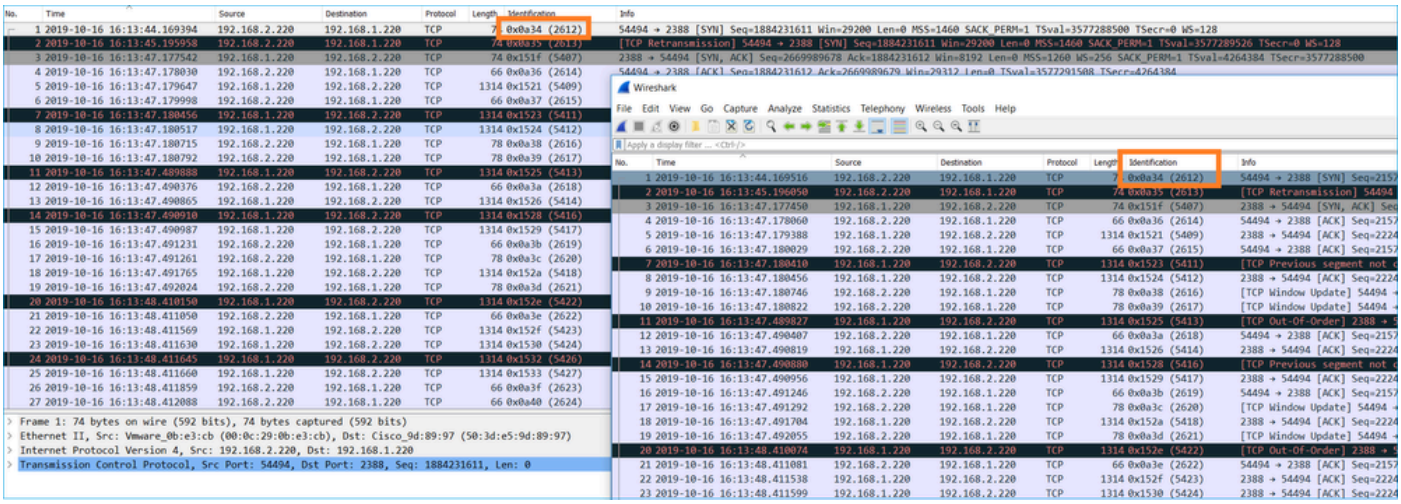
فقدان الحزمة الناجم عن جدار الحماية: in order to عينت إن الربط فقد يكون بسبب جدار حماية هناك حاجة أن يقارن المدخل التقاط إلى المخرج قبض. هناك طرق كثيرة لمقارنة طريقتين مختلفتين. يوضح هذا القسم طريقة واحدة للقيام بهذه المهمة.

إجراء مقارنة صورتين لتحديد فقدان الحزمة

الخطوة 1. تأكد من أن الملتقطات 2 تحتوي على حزم من نفس الإطار الزمني. هذا يعني أنه يجب ألا تكون هناك حزم في التقاط واحد تم التقاطه قبل أو بعد الالتقاط الآخر. وهناك عدد قليل من الطرق لتحقيق هذه الغاية:

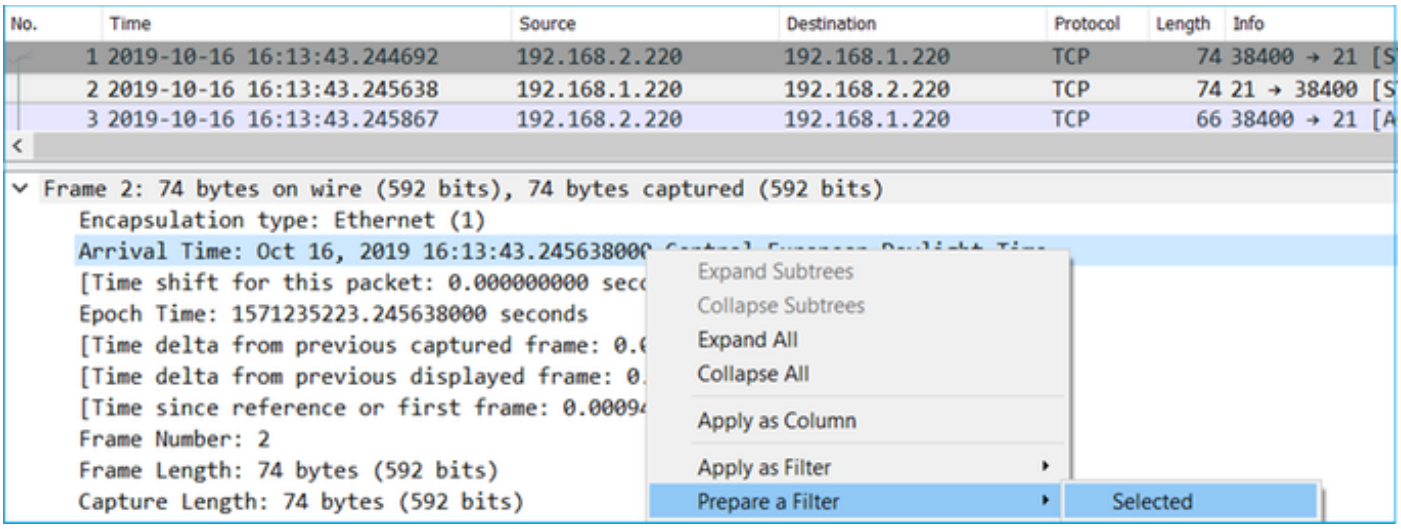
- تحقق من قيم تعريف IP (ID) الأولى والأخيرة للحزمة.
- تحقق من قيم الطابع الزمني للحزمة الأولى والأخيرة.

في هذا المثال، يمكنك أن ترى أن الحزم الأولى من كل التقاط لها نفس قيم معرف IP:



في حالة ما إذا كانوا غير متشابهين:

1. قارن الطوابع الزمنية من الحزمة الأولى من كل التقاط.
2. من الالتقاط باستخدام أحدث ختم وقت الحصول على مرشح منه تغيير مرشح ختم الوقت من == إلى >= (الحزمة الأولى) و <= (الحزمة الأخيرة)، على سبيل المثال:



(frame.time >= "16 أكتوبر 2019 16:13:43.244692000") &(frame.time <= "16 أكتوبر 2019 16:20:21.78513000")

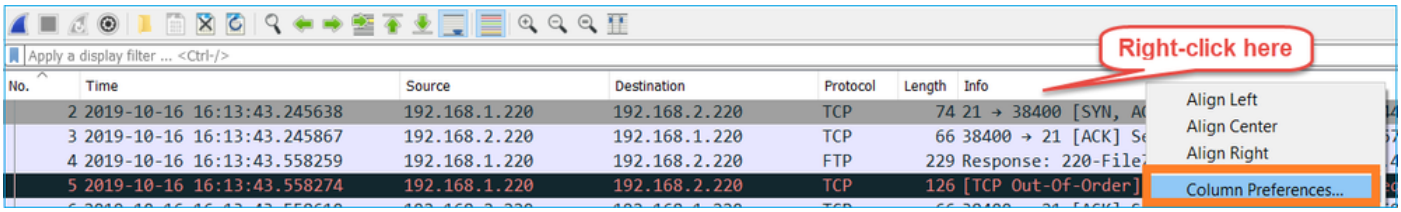
3. تصدير الحزم المحددة إلى التقاط جديد، حدد ملف > تصدير الحزم المحددة ثم احفظ الحزم المعروضة. عند هذه النقطة، يجب أن يحتوي كل الالتقاط على حزم تغطي الإطار الزمني نفسه. يمكنك الآن بدء مقارنة اللقطتين.

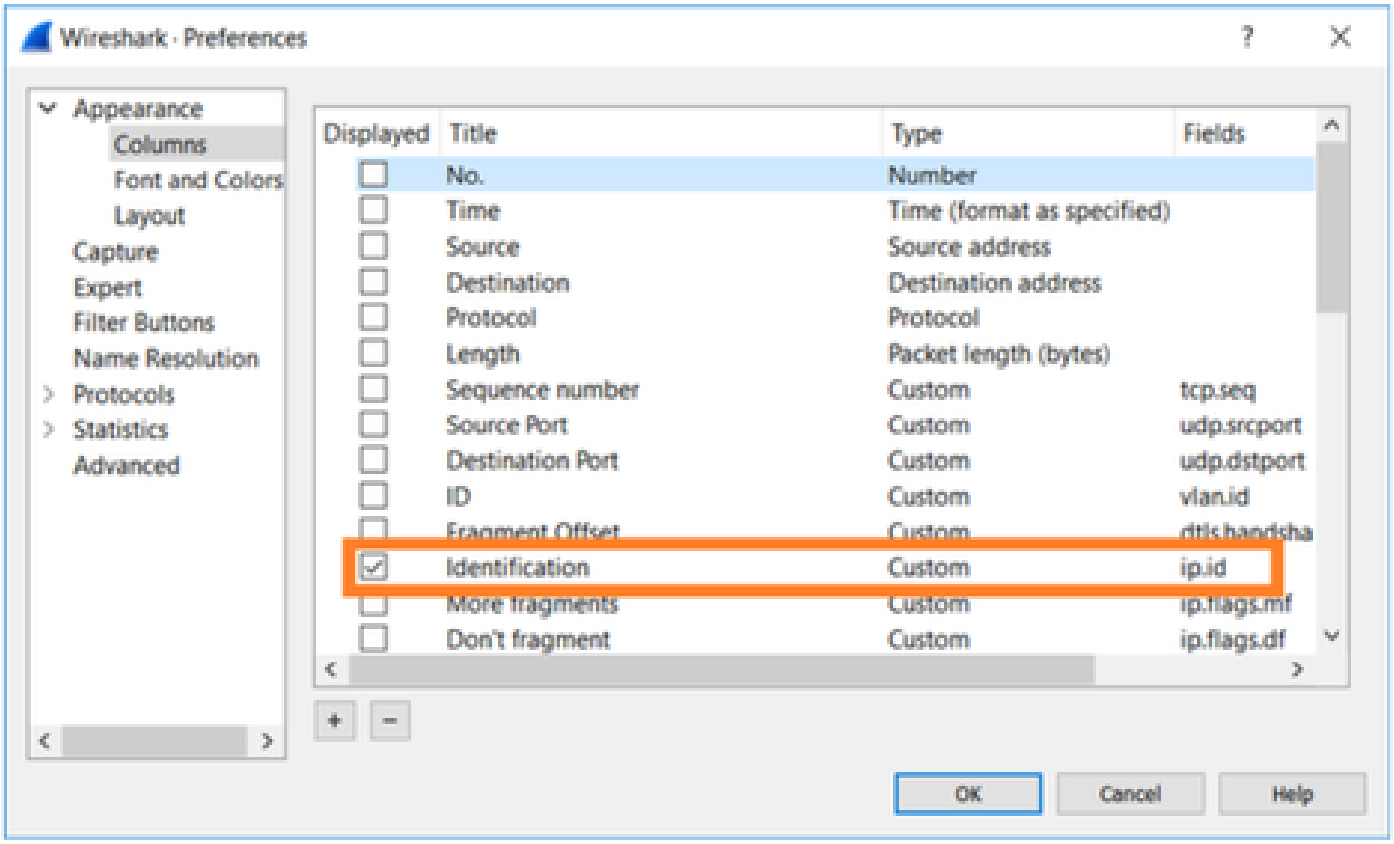
الخطوة 2. حدد حقل الحزمة الذي يتم إستخدامه للمقارنة بين الملتقيات 2. مثال الحقول التي يمكن إستخدامها:

- تعريف IP
- رقم تسلسل RTP
- الرقم التسلسلي ل ICMP

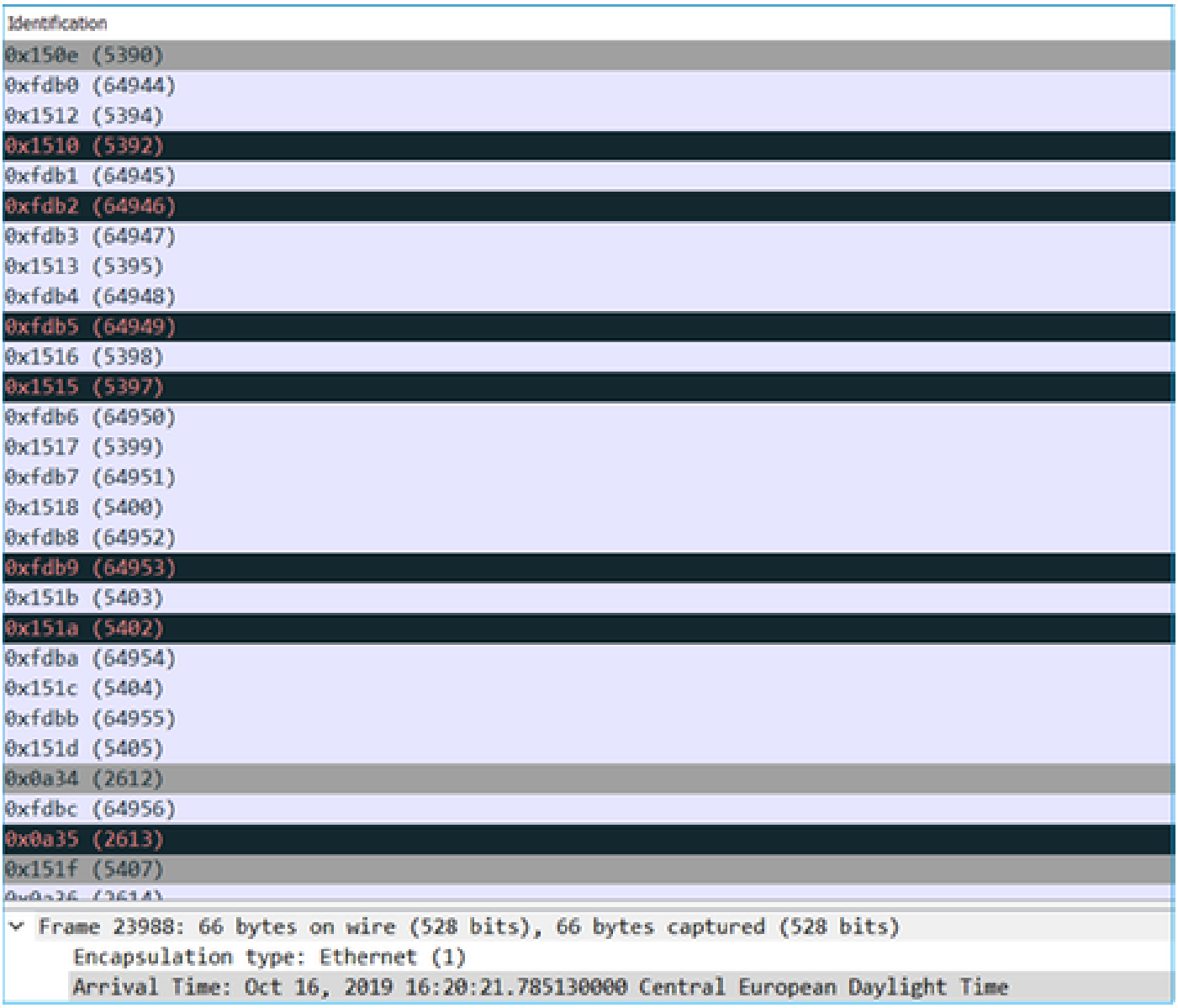
قم بإنشاء إصدار نصي من كل التقاط يحتوي على الحقل لكل حزمة تحددها في الخطوة 1. للقيام بذلك، أترك فقط عمود الاهتمام، على سبيل المثال، إذا كنت تريد مقارنة الحزم

بناء على تعريف IP ثم قم بتعديل الالتقاط كما هو موضح في الصورة.

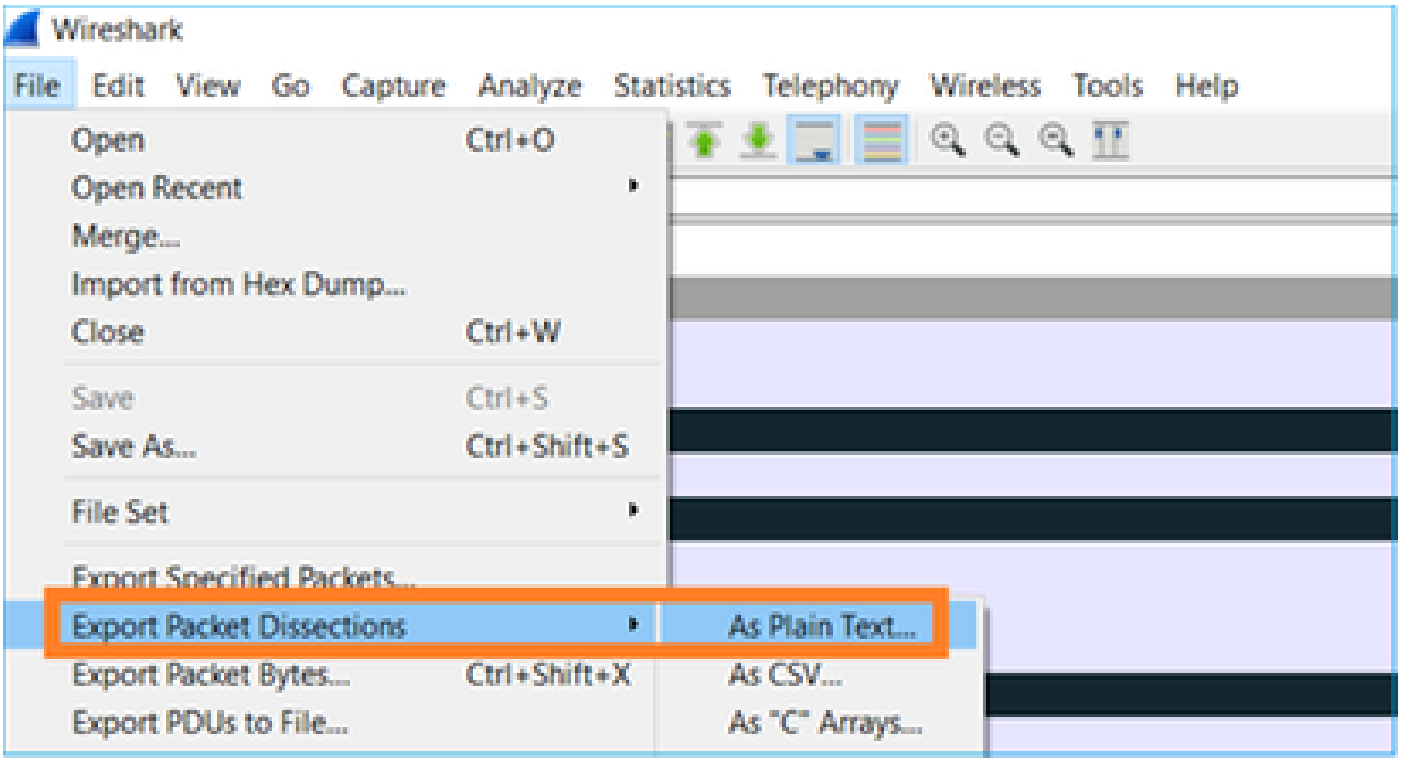




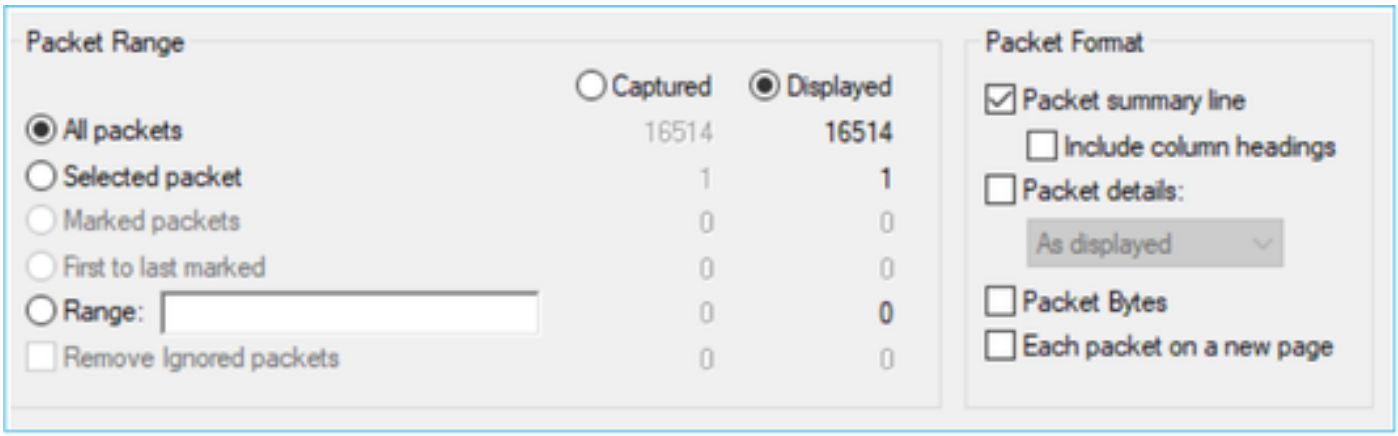
النتيجة:



الخطوة 3. قم بإنشاء إصدار نص من الالتقاط (ملف > تصدير تقسيمات الحزم > كنص عادي...)، كما هو موضح في الصورة:



قم بإلغاء تحديد خيارات تضمين رؤوس الأعمدة وتفاصيل الحزمة لتصدير قيم الحقل المعروض فقط، كما هو موضح في الصورة:



الخطوة 4. فرز الحزم في الملفات. يمكنك إستخدام أمر فرز لينوكس للقيام بذلك:

<#root>

#

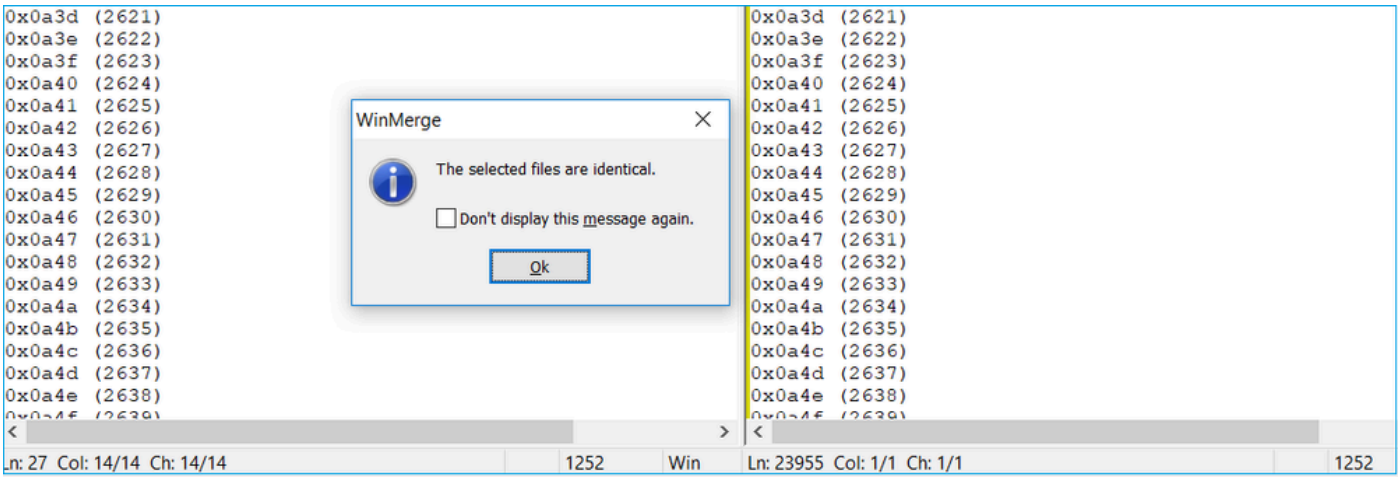
sort CAPI_IDs > file1.sorted

#

sort CAPO_IDs > file2.sorted

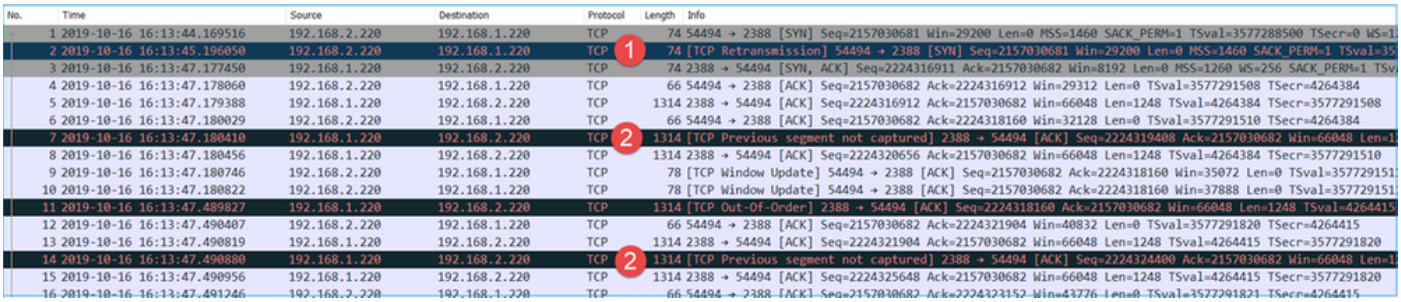
الخطوة 5. أستخدم أداة مقارنة نصوص (على سبيل المثال، WinMerge) أو أمر Linux diff للعثور

عدد الفروق بين الصور 2.



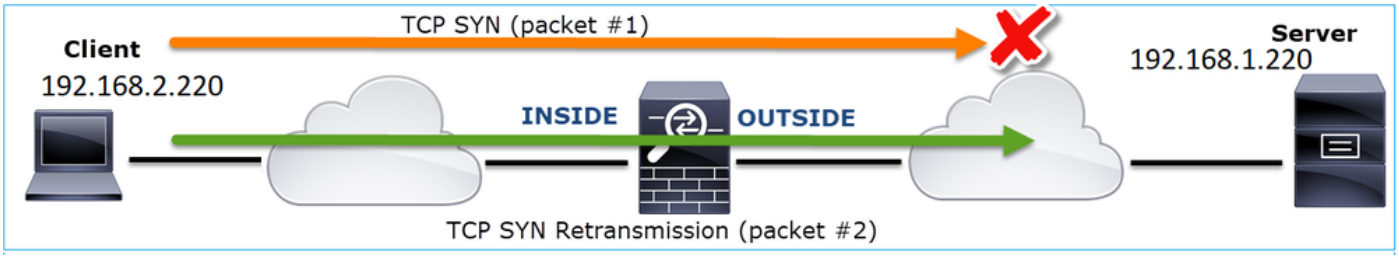
في هذه الحالة، يكون التقاط CAPI و CAPO لحركة مرور بيانات FTP متطابقين. هذا يثبت أن فقدان الحزمة لم يكن بسبب جدار الحماية.

التعرف على فقدان حزم تدفق/تدفق البيانات.

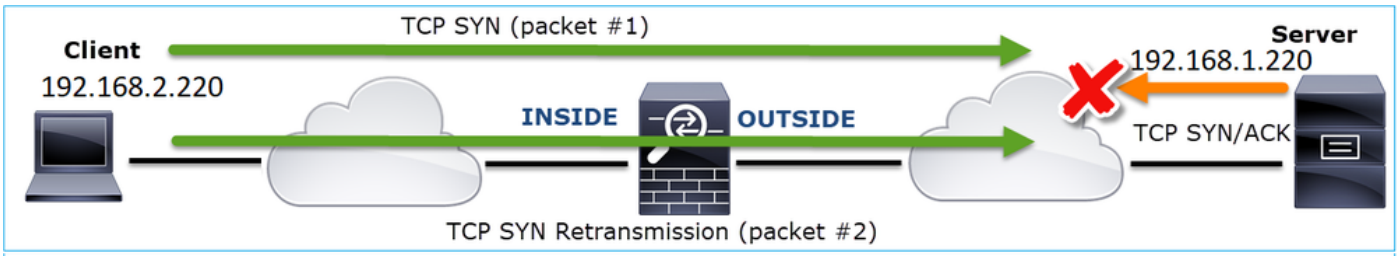


النقاط الرئيسية:

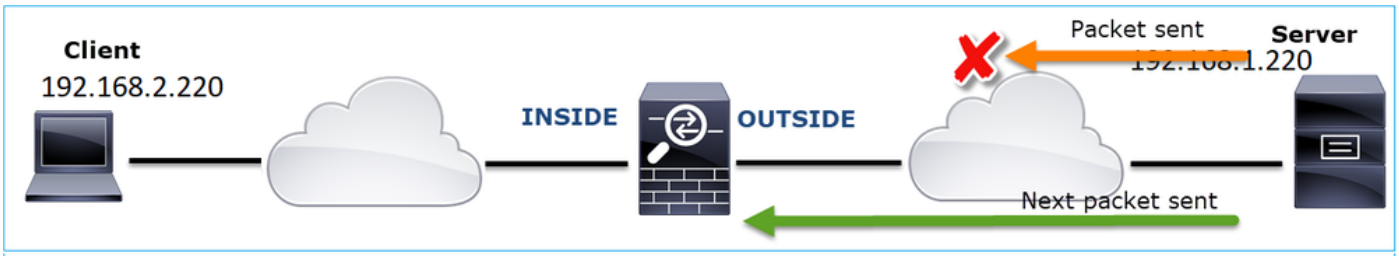
1. هذه الحزمة هي إعادة إرسال TCP. وعلى وجه الخصوص، فإنها حزمة TCP syn يتم إرسالها من العميل إلى الخادم لبيانات FTP في الوضع الخامل. بما أن العميل يعيد الربط وأنت يستطيع رأيت ال syn أولي (ربط #1) الربط فقدت نحو الخادم إلى جدار الحماية.



في هذه الحالة، هناك احتمال أن تكون حزمة SYN قد وصلت إلى الخادم، ولكن حزمة SYN/ACK قد فقدت في طريق الرجوع:



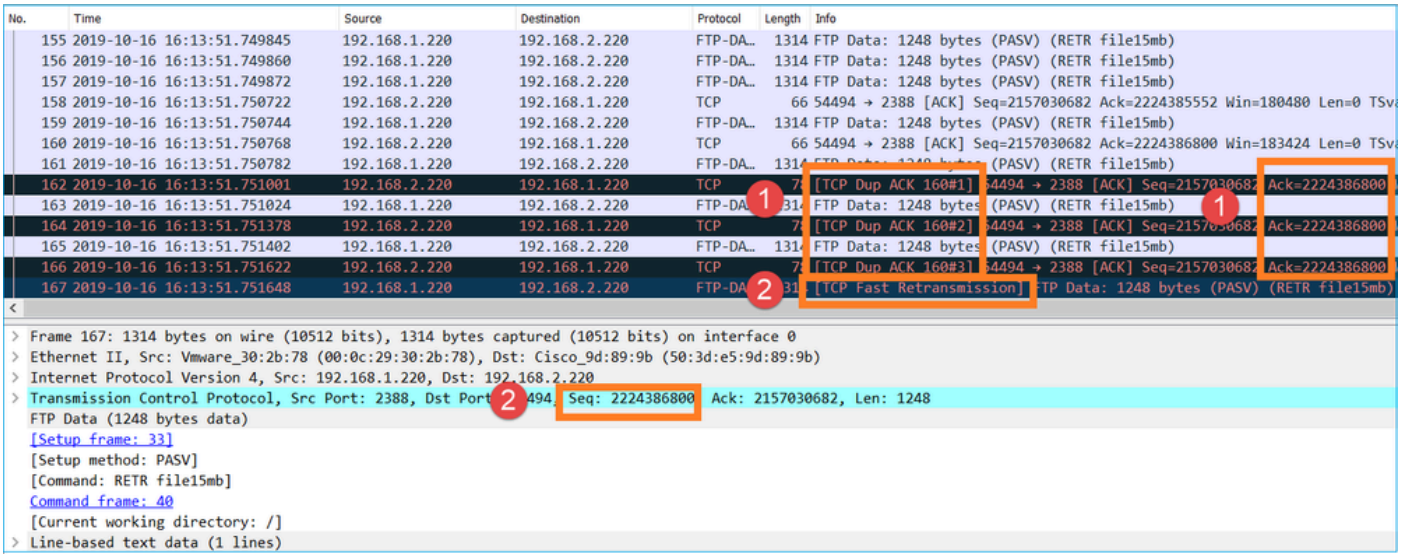
2. هناك حزمة من الخادم وتعرف Wireshark على أن المقطع السابق لم يتم عرضه/التقاطه. نظرا لأنه تم إرسال الحزمة غير الملتقطة من الخادم إلى العميل ولم يتم رؤيتها في التقاط جدار الحماية، فهذا يعني أن الحزمة قد فقدت بين الخادم وجدار الحماية.



وهذا يشير إلى وجود فقدان حزم بين خادم FTP وجدار الحماية.

الإجراء 2. التقاط صور إضافية.

قم بأخذ لقطات إضافية مع لقطات عند نقاط النهاية. حاول تطبيق طريقة التقسيم والتغلب لعزل المزيد من المقطع المثير للمشاكل الذي يسبب فقدان الحزمة.



النقاط الرئيسية:

1. يتتبع المستقبل (عميل FTP في هذه الحالة) أرقام تسلسل TCP الواردة. إذا اكتشفت أن حزمة قد تم فقدها (تم تخطي رقم تسلسل متوقع)، فإنها تقوم بإنشاء حزمة ACK برقم تسلسل متوقع تم تخطيه. في هذا المثال الـ ack=2224386800.
2. تقوم ذاكرة DUP (ACK) بتشغيل إعادة الإرسال السريع لبروتوكول TCP (إعادة الإرسال

خلال 20 ثانية بعد تلقي مكرر ACK).

ما الذي تعنيه الوجبات المكررة؟

- تشير بعض أنواع ACK المكررة ولكن لا توجد عمليات إعادة إرسال فعلية إلى أنه من الأرجح أن هناك حزم تصل خارج النظام.
- تشير رسائل ACK المكررة التي تليها عمليات إعادة الإرسال الفعلية إلى وجود قدر ما من فقدان الحزم.

الإجراء 3. حساب وقت معالجة جدار الحماية لحزم النقل.

تطبيق نفس الالتقاط على واجهتين مختلفتين:

<#root>

firepower#

capture CAPI buffer 33554432 interface INSIDE match tcp host 192.168.2.220 host 192.168.1.220

firepower#

capture CAPI interface OUTSIDE

تصدير الالتقاط تحقق من فرق الوقت بين مدخل مقابل مخرج رطب

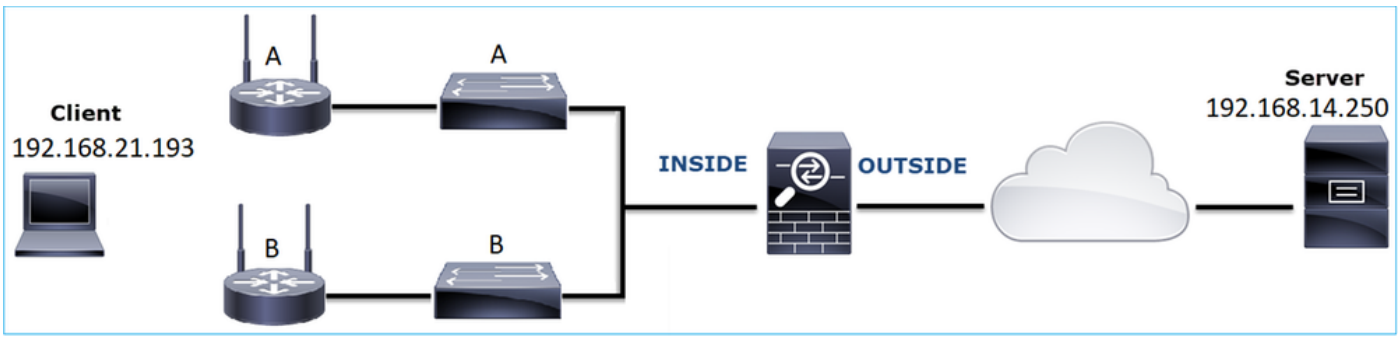
الحالة 7. مشكلة اتصال TCP (تلف الحزمة)

وصف المشكلة:

يحاول العميل السلكي (192.168.21.193) الاتصال بخادم وجهة (192.168.14.250 - HTTP) وهناك سيناريوهان مختلفان:

- عندما يتصل العميل بنقطة الوصول (AP) 'A' عندئذ لا يعمل اتصال HTTP.
- عندما يتصل العميل بنقطة الوصول (AP) 'B' عندئذ يعمل اتصال HTTP.

تعرض هذه الصورة المخطط:



التدفق المتأثر:

SRC IP: 192.168.21.193

بروتوكول DST IP: 192.168.14.250

البروتوكول: بروتوكول TCP 80

تحليل أسر

تمكين االلتقاط على محرك FTD LINA:

<#root>

```
firepower#
capture CAPI int INSIDE match ip host 192.168.21.193 host 192.168.14.250
firepower#
capture CAPO int OUTSIDE match ip host 192.168.21.193 host 192.168.14.250
```

التقاط - السيناريو الوظيفي:

كخط أساس، من المفيد جدا دائما الحصول على لقطات من سيناريو معروف جيد.

تظهر هذه الصورة التقاط واجهة NGFW Inside

No.	Time	Source	Destination	Protocol	Length	Info
1	2013-08-08 17:03:25.554582	192.168.21.193	192.168.14.250	TCP	66	1055 → 80 [SYN] Seq=1341231 Win=65535 Len=0 MSS=1460 SACK_PERM=1
2	2013-08-08 17:03:25.555238	192.168.14.250	192.168.21.193	TCP	66	80 → 1055 [SYN, ACK] Seq=1015787006 Ack=1341232 Win=64240 Len=0 MSS=1380 SACK_PERM=1
3	2013-08-08 17:03:25.579910	192.168.21.193	192.168.14.250	TCP	58	1055 → 80 [ACK] Seq=1341232 Ack=1015787007 Win=65535 Len=0
4	2013-08-08 17:03:25.841081	192.168.21.193	192.168.14.250	HTTP	370	GET /ttest.html HTTP/1.1
5	2013-08-08 17:03:25.848466	192.168.14.250	192.168.21.193	TCP	1438	80 → 1055 [ACK] Seq=1015787007 Ack=1341544 Win=63928 Len=1380 [TCP segment of a reassembled PDU]
6	2013-08-08 17:03:25.848527	192.168.14.250	192.168.21.193	HTTP	698	HTTP/1.1 404 Not Found (text/html)
7	2013-08-08 17:03:25.858445	192.168.21.193	192.168.14.250	TCP	58	1055 → 80 [ACK] Seq=1341544 Ack=1015789027 Win=65535 Len=0
8	2013-08-08 17:03:34.391749	192.168.21.193	192.168.14.250	HTTP	369	GET /test.html HTTP/1.1
9	2013-08-08 17:03:34.395487	192.168.14.250	192.168.21.193	HTTP	586	HTTP/1.1 200 OK (text/html)
10	2013-08-08 17:03:34.606352	192.168.21.193	192.168.14.250	TCP	58	1055 → 80 [ACK] Seq=1341855 Ack=1015789555 Win=65007 Len=0
11	2013-08-08 17:03:40.739601	192.168.21.193	192.168.14.250	HTTP	483	GET /test.html HTTP/1.1
12	2013-08-08 17:03:40.741538	192.168.14.250	192.168.21.193	HTTP	271	HTTP/1.1 304 Not Modified

تعرض هذه الصورة االلتقاط الذي تم على الواجهة الخارجية ل NGFW.

No.	Time	Source	Destination	Protocol	Length	Info
1	2013-08-08 17:03:25.554872	192.168.21.193	192.168.14.250	TCP	66	1055 → 80 [SYN] Seq=1839800324 Win=65535 Len=0 MSS=1380 SACK_PERM=1
2	2013-08-08 17:03:25.555177	192.168.14.250	192.168.21.193	TCP	66	80 → 1055 [SYN, ACK] Seq=521188628 Ack=1839800325 Win=64240 Len=0 MSS=1460 SACK_PERM=1
3	2013-08-08 17:03:25.579926	192.168.21.193	192.168.14.250	TCP	58	1055 → 80 [ACK] Seq=1839800325 Ack=521188629 Win=65535 Len=0
4	2013-08-08 17:03:25.841112	192.168.21.193	192.168.14.250	HTTP	370	GET /ttest.html HTTP/1.1
5	2013-08-08 17:03:25.848451	192.168.14.250	192.168.21.193	TCP	1438	80 → 1055 [ACK] Seq=521188629 Ack=1839800637 Win=63928 Len=1380 [TCP segment of a reassembled PDU]
6	2013-08-08 17:03:25.848512	192.168.14.250	192.168.21.193	HTTP	698	HTTP/1.1 404 Not Found (text/html)
7	2013-08-08 17:03:25.858476	192.168.21.193	192.168.14.250	TCP	58	1055 → 80 [ACK] Seq=1839800637 Ack=521190649 Win=65535 Len=0
8	2013-08-08 17:03:34.391779	192.168.21.193	192.168.14.250	HTTP	369	GET /test.html HTTP/1.1
9	2013-08-08 17:03:34.395456	192.168.14.250	192.168.21.193	HTTP	586	HTTP/1.1 200 OK (text/html)
10	2013-08-08 17:03:34.606368	192.168.21.193	192.168.14.250	TCP	58	1055 → 80 [ACK] Seq=1839800948 Ack=521191177 Win=65007 Len=0
11	2013-08-08 17:03:40.739646	192.168.21.193	192.168.14.250	HTTP	483	GET /test.html HTTP/1.1
12	2013-08-08 17:03:40.741523	192.168.14.250	192.168.21.193	HTTP	271	HTTP/1.1 304 Not Modified

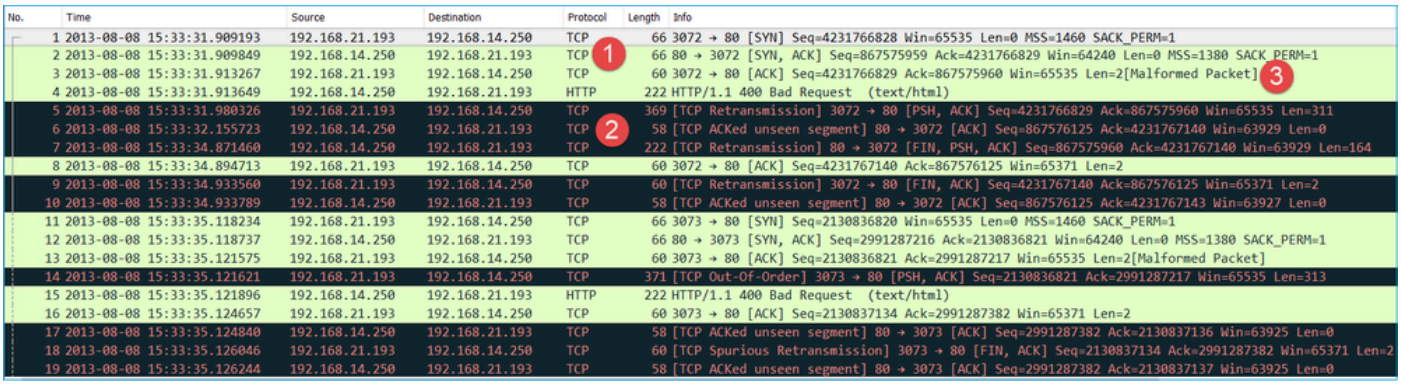
النقاط الرئيسية:

1. التقطتان متطابقتان تقريبا (تأملوا في عملية IS العشوائية).
2. ال توجد مؤشرات على فقدان الحزمة.
3. ال توجد حزم خارج الترتيب (OOO)

4. هناك 3 طلبات HTTP GET. يحصل الأول على 404 "غير موجود"، في حين يحصل الثاني على 200 "موافق"، ويحصل الثالث على رسالة إعادة توجيه "غير معدل" بحجم 304.

التقاط - السيناريو المعروف بالخطأ:

محتويات التقاط المدخل (CAPI).

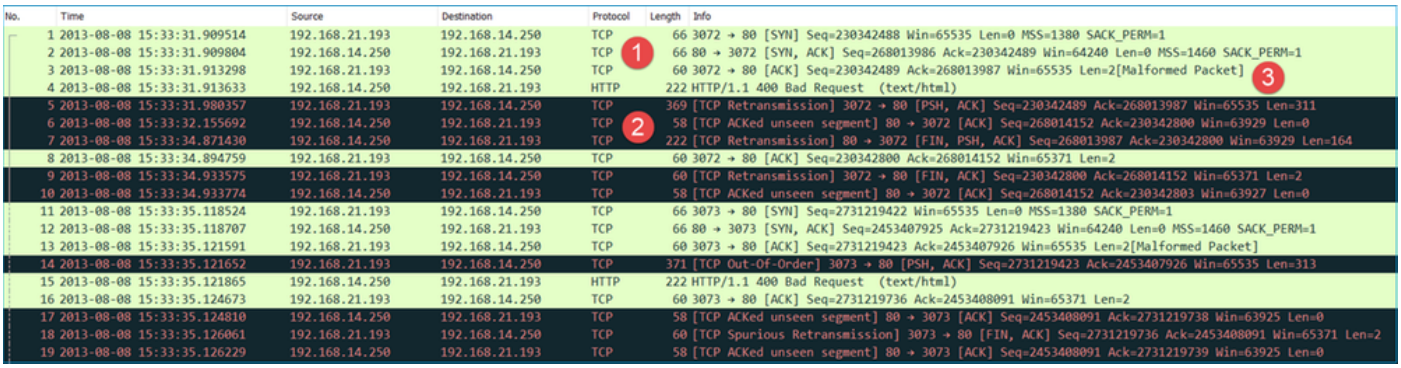


No.	Time	Source	Destination	Protocol	Length	Info
1	2013-08-08 15:33:31.909193	192.168.21.193	192.168.14.250	TCP	66	3072 → 80 [SYN] Seq=4231766828 Win=65535 Len=0 MSS=1460 SACK_PERM=1
2	2013-08-08 15:33:31.909849	192.168.14.250	192.168.21.193	TCP	66	80 → 3072 [SYN, ACK] Seq=867575959 Ack=4231766829 Win=64240 Len=0 MSS=1380 SACK_PERM=1
3	2013-08-08 15:33:31.913267	192.168.21.193	192.168.14.250	TCP	60	3072 → 80 [ACK] Seq=4231766829 Ack=867575960 Win=65535 Len=2[Malformed Packet]
4	2013-08-08 15:33:31.913649	192.168.14.250	192.168.21.193	HTTP	222	HTTP/1.1 400 Bad Request (text/html)
5	2013-08-08 15:33:31.980326	192.168.21.193	192.168.14.250	TCP	369	[TCP Retransmission] 3072 → 80 [PSH, ACK] Seq=4231766829 Ack=867575960 Win=65535 Len=311
6	2013-08-08 15:33:32.155723	192.168.14.250	192.168.21.193	TCP	58	[TCP ACKed unseen segment] 80 → 3072 [ACK] Seq=867576125 Ack=4231767140 Win=63929 Len=0
7	2013-08-08 15:33:34.871460	192.168.14.250	192.168.21.193	TCP	222	[TCP Retransmission] 80 → 3072 [FIN, PSH, ACK] Seq=867575960 Ack=4231767140 Win=63929 Len=164
8	2013-08-08 15:33:34.894713	192.168.21.193	192.168.14.250	TCP	60	3072 → 80 [ACK] Seq=4231767140 Ack=867576125 Win=65371 Len=2
9	2013-08-08 15:33:34.933560	192.168.21.193	192.168.14.250	TCP	60	[TCP Retransmission] 3072 → 80 [FIN, ACK] Seq=4231767140 Ack=867576125 Win=65371 Len=2
10	2013-08-08 15:33:34.933789	192.168.14.250	192.168.21.193	TCP	58	[TCP ACKed unseen segment] 80 → 3072 [ACK] Seq=867576125 Ack=4231767143 Win=63927 Len=0
11	2013-08-08 15:33:35.118234	192.168.21.193	192.168.14.250	TCP	66	3073 → 80 [SYN] Seq=2130836820 Win=65535 Len=0 MSS=1460 SACK_PERM=1
12	2013-08-08 15:33:35.118737	192.168.14.250	192.168.21.193	TCP	66	80 → 3073 [SYN, ACK] Seq=2991287216 Ack=2130836821 Win=64240 Len=0 MSS=1380 SACK_PERM=1
13	2013-08-08 15:33:35.121575	192.168.21.193	192.168.14.250	TCP	60	3073 → 80 [ACK] Seq=2130836821 Ack=2991287217 Win=65535 Len=2[Malformed Packet]
14	2013-08-08 15:33:35.121621	192.168.21.193	192.168.14.250	TCP	371	[TCP Out-Of-Order] 3073 → 80 [PSH, ACK] Seq=2130836821 Ack=2991287217 Win=65535 Len=313
15	2013-08-08 15:33:35.121896	192.168.14.250	192.168.21.193	HTTP	222	HTTP/1.1 400 Bad Request (text/html)
16	2013-08-08 15:33:35.124657	192.168.21.193	192.168.14.250	TCP	60	3073 → 80 [ACK] Seq=2130837134 Ack=2991287382 Win=65371 Len=2
17	2013-08-08 15:33:35.124840	192.168.14.250	192.168.21.193	TCP	58	[TCP ACKed unseen segment] 80 → 3073 [ACK] Seq=2991287382 Ack=2130837136 Win=63925 Len=0
18	2013-08-08 15:33:35.126046	192.168.21.193	192.168.14.250	TCP	60	[TCP Spurious Retransmission] 3073 → 80 [FIN, ACK] Seq=2130837134 Ack=2991287382 Win=65371 Len=2
19	2013-08-08 15:33:35.126244	192.168.14.250	192.168.21.193	TCP	58	[TCP ACKed unseen segment] 80 → 3073 [ACK] Seq=2991287382 Ack=2130837137 Win=63925 Len=0

النقاط الرئيسية:

1. هناك مصافحة TCP ثلاثية الإتجاه.
2. هناك عمليات إعادة إرسال عبر بروتوكول TCP ومؤشرات على فقدان الحزمة.
3. هناك حزمة (TCP ACK) تم تعريفها بواسطة Wireshark على أنها مشكلة بشكل غير صحيح.

تظهر هذه الصورة محتويات التقاط المخرج (CAPO).



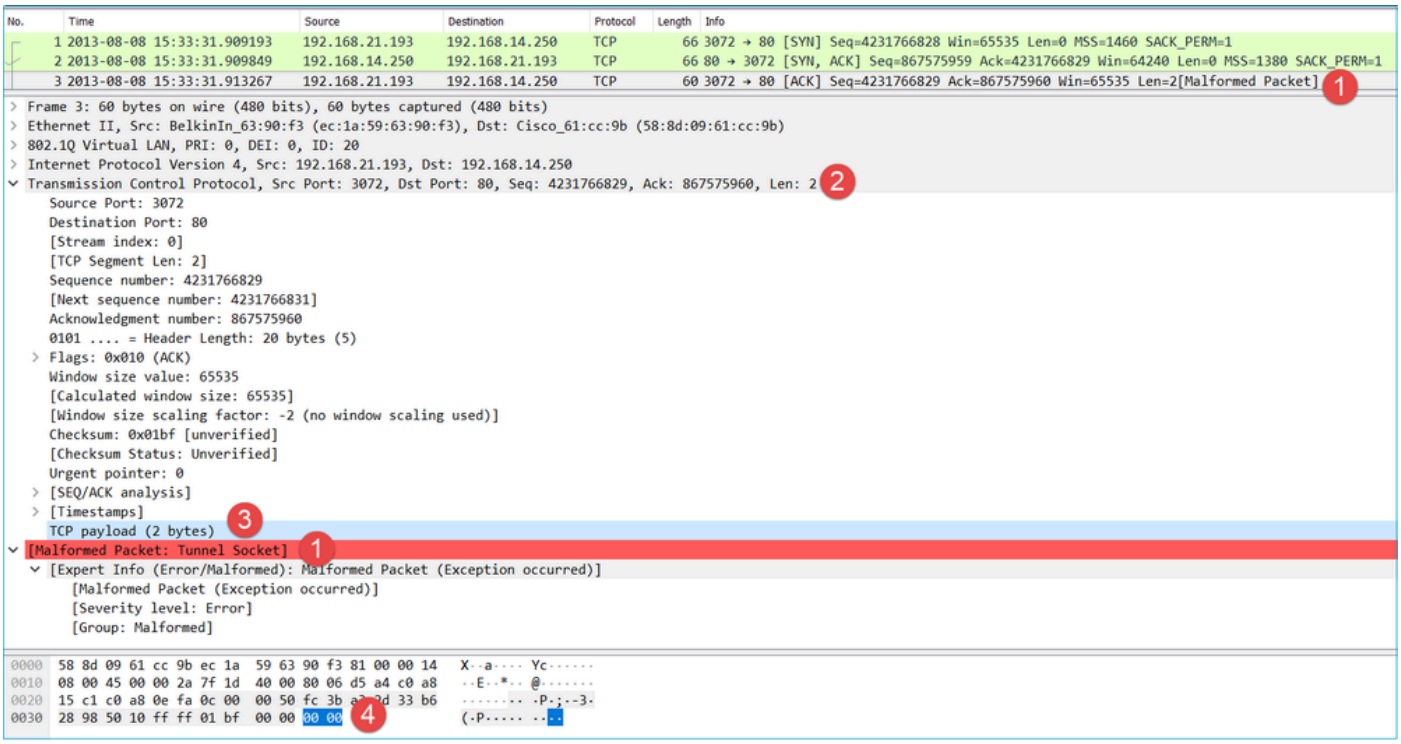
No.	Time	Source	Destination	Protocol	Length	Info
1	2013-08-08 15:33:31.909514	192.168.21.193	192.168.14.250	TCP	66	3072 → 80 [SYN] Seq=230342488 Win=65535 Len=0 MSS=1380 SACK_PERM=1
2	2013-08-08 15:33:31.909804	192.168.14.250	192.168.21.193	TCP	66	80 → 3072 [SYN, ACK] Seq=268013986 Ack=230342489 Win=64240 Len=0 MSS=1460 SACK_PERM=1
3	2013-08-08 15:33:31.913298	192.168.21.193	192.168.14.250	TCP	60	3072 → 80 [ACK] Seq=230342489 Ack=268013987 Win=65535 Len=2[Malformed Packet]
4	2013-08-08 15:33:31.913633	192.168.14.250	192.168.21.193	HTTP	222	HTTP/1.1 400 Bad Request (text/html)
5	2013-08-08 15:33:31.980357	192.168.21.193	192.168.14.250	TCP	369	[TCP Retransmission] 3072 → 80 [PSH, ACK] Seq=230342489 Ack=268013987 Win=65535 Len=311
6	2013-08-08 15:33:32.155692	192.168.14.250	192.168.21.193	TCP	58	[TCP ACKed unseen segment] 80 → 3072 [ACK] Seq=268014152 Ack=230342800 Win=63929 Len=0
7	2013-08-08 15:33:34.871430	192.168.14.250	192.168.21.193	TCP	222	[TCP Retransmission] 80 → 3072 [FIN, PSH, ACK] Seq=268013987 Ack=230342800 Win=63929 Len=164
8	2013-08-08 15:33:34.894759	192.168.21.193	192.168.14.250	TCP	60	3072 → 80 [ACK] Seq=230342800 Ack=268014152 Win=65371 Len=2
9	2013-08-08 15:33:34.933575	192.168.21.193	192.168.14.250	TCP	60	[TCP Retransmission] 3072 → 80 [FIN, ACK] Seq=230342800 Ack=268014152 Win=65371 Len=2
10	2013-08-08 15:33:34.933774	192.168.14.250	192.168.21.193	TCP	58	[TCP ACKed unseen segment] 80 → 3072 [ACK] Seq=268014152 Ack=230342803 Win=63927 Len=0
11	2013-08-08 15:33:35.118524	192.168.21.193	192.168.14.250	TCP	66	3073 → 80 [SYN] Seq=2731219422 Win=65535 Len=0 MSS=1380 SACK_PERM=1
12	2013-08-08 15:33:35.118707	192.168.14.250	192.168.21.193	TCP	66	80 → 3073 [SYN, ACK] Seq=2453407925 Ack=2731219423 Win=64240 Len=0 MSS=1460 SACK_PERM=1
13	2013-08-08 15:33:35.121591	192.168.21.193	192.168.14.250	TCP	60	3073 → 80 [ACK] Seq=2731219423 Ack=2453407926 Win=65535 Len=2[Malformed Packet]
14	2013-08-08 15:33:35.121652	192.168.21.193	192.168.14.250	TCP	371	[TCP Out-Of-Order] 3073 → 80 [PSH, ACK] Seq=2731219423 Ack=2453407926 Win=65535 Len=313
15	2013-08-08 15:33:35.121865	192.168.14.250	192.168.21.193	HTTP	222	HTTP/1.1 400 Bad Request (text/html)
16	2013-08-08 15:33:35.124673	192.168.21.193	192.168.14.250	TCP	60	3073 → 80 [ACK] Seq=2731219736 Ack=2453408091 Win=65371 Len=2
17	2013-08-08 15:33:35.124810	192.168.14.250	192.168.21.193	TCP	58	[TCP ACKed unseen segment] 80 → 3073 [ACK] Seq=2453408091 Ack=2731219738 Win=63925 Len=0
18	2013-08-08 15:33:35.126061	192.168.21.193	192.168.14.250	TCP	60	[TCP Spurious Retransmission] 3073 → 80 [FIN, ACK] Seq=2731219736 Ack=2453408091 Win=65371 Len=2
19	2013-08-08 15:33:35.126229	192.168.14.250	192.168.21.193	TCP	58	[TCP ACKed unseen segment] 80 → 3073 [ACK] Seq=2453408091 Ack=2731219739 Win=63925 Len=0

النقاط الرئيسية:

التقطتان متطابقتان تقريبا (تأملوا في عملية IS العشوائية):

1. هناك مصافحة TCP ثلاثية الإتجاه.
2. هناك عمليات إعادة إرسال عبر بروتوكول TCP ومؤشرات على فقدان الحزمة.
3. هناك حزمة (TCP ACK) تم تعريفها بواسطة Wireshark على أنها مشكلة بشكل غير صحيح.

تحقق من الحزمة ذات التكوين غير الصحيح:



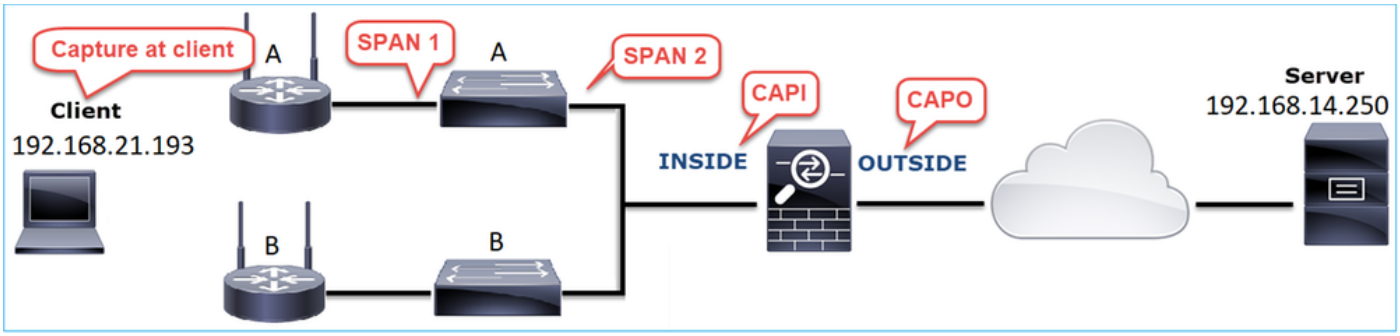
النقاط الرئيسية:

1. يتم تعريف الحزمة على أنها مشكلة بشكل غير صحيح من قبل Wireshark.
2. طول 2 بايت.
3. هناك حمولة TCP بمقدار 2 بايت.
4. الحمولة هي 4 أصفار إضافية (00 00).

الإجراءات الموصى بها

والغرض من الإجراءات الواردة في هذا القسم هو زيادة تضييق نطاق هذه المسألة.

الإجراء 1. التقاط صور إضافية. تضمنت على قبض في نقاط النهاية وإن أمكن، حاولت أن يطبق الإنقسامات وطريقطقة أن يعزل المصدر من الربط فساد، مثل:

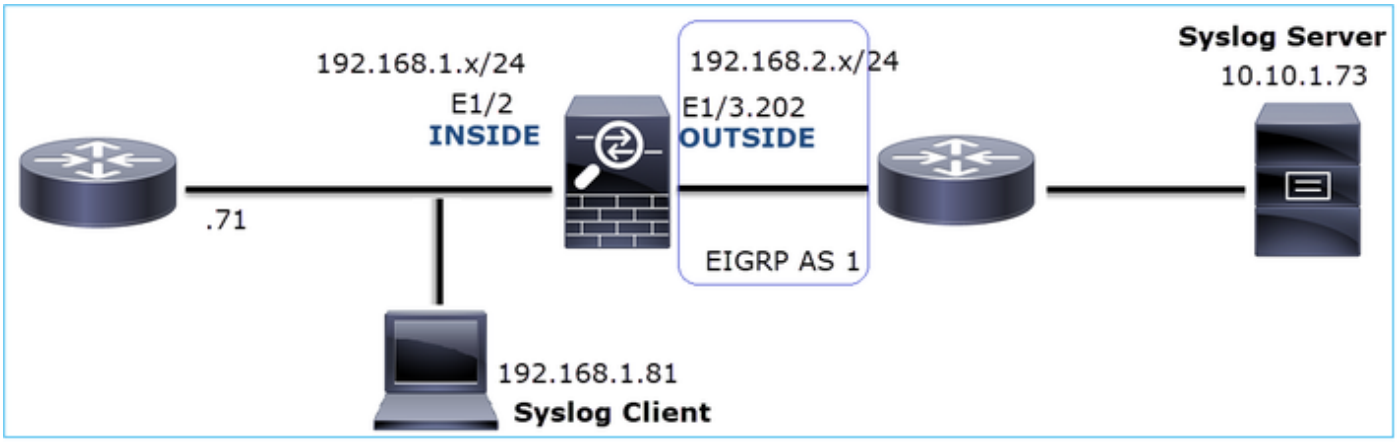


في هذه الحالة، ال 2 بايت إضافي كان أضفت بالمفتاح 'A' قارن برنامج تشغيل والحل كان أن استبدلت المفتاح أن يسبب الفساد.

الحالة 8. مشكلة اتصال UDP (الحزم المفقودة)

وصف المشكلة: لا يرى syslog (UDP 514) رسالة على الغاية syslog نادل.

تعرض هذه الصورة المخطط:



التدفق المتأثر:

SRC IP: 192.168.1.81

بروتوكول DST IP: 10.10.1.73

البروتوكول: UDP 514

تحليل أسر

تمكين االلتقاط على محرك FTD LINA:

```
<#root>

firepower#

capture CAPI int INSIDE trace match udp host 192.168.1.81 host 10.10.1.73 eq 514

firepower#

capture CAPO int OUTSIDE match udp host 192.168.1.81 host 10.10.1.73 eq 514
```

ال تظهر صور FTD أي حزم:

```
<#root>

firepower#

show capture

capture CAPI type raw-data trace interface INSIDE [Capturing - 0 bytes]
  match udp host 192.168.1.81 host 10.10.1.73 eq syslog
capture CAPO type raw-data interface OUTSIDE [Capturing - 0 bytes]
  match udp host 192.168.1.81 host 10.10.1.73 eq syslog
```

الإجراءات الموصى بها

والغرض من الإجراءات الواردة في هذا القسم هو زيادة تضييق نطاق هذه المسألة.

الإجراء 1. تحقق من جدول اتصال FTD.

للتحقق من اتصال محدد، يمكنك إستخدام هذه الصيغة:

<#root>

firepower#

show conn address 192.168.1.81 port 514

10 in use, 3627189 most used
Inspect Snort:
        preserve-connection: 6 enabled, 0 in effect, 74 most enabled, 0 most in effect

UDP

INSIDE

 10.10.1.73:514

INSIDE

 192.168.1.81:514, idle 0:00:00, bytes

480379697

, flags -

o

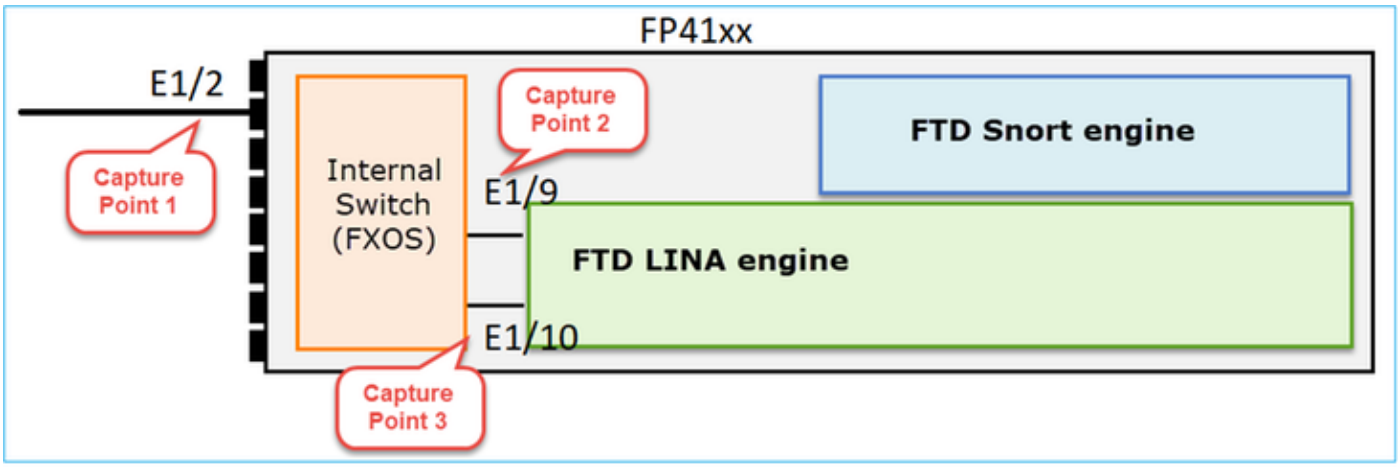
N1

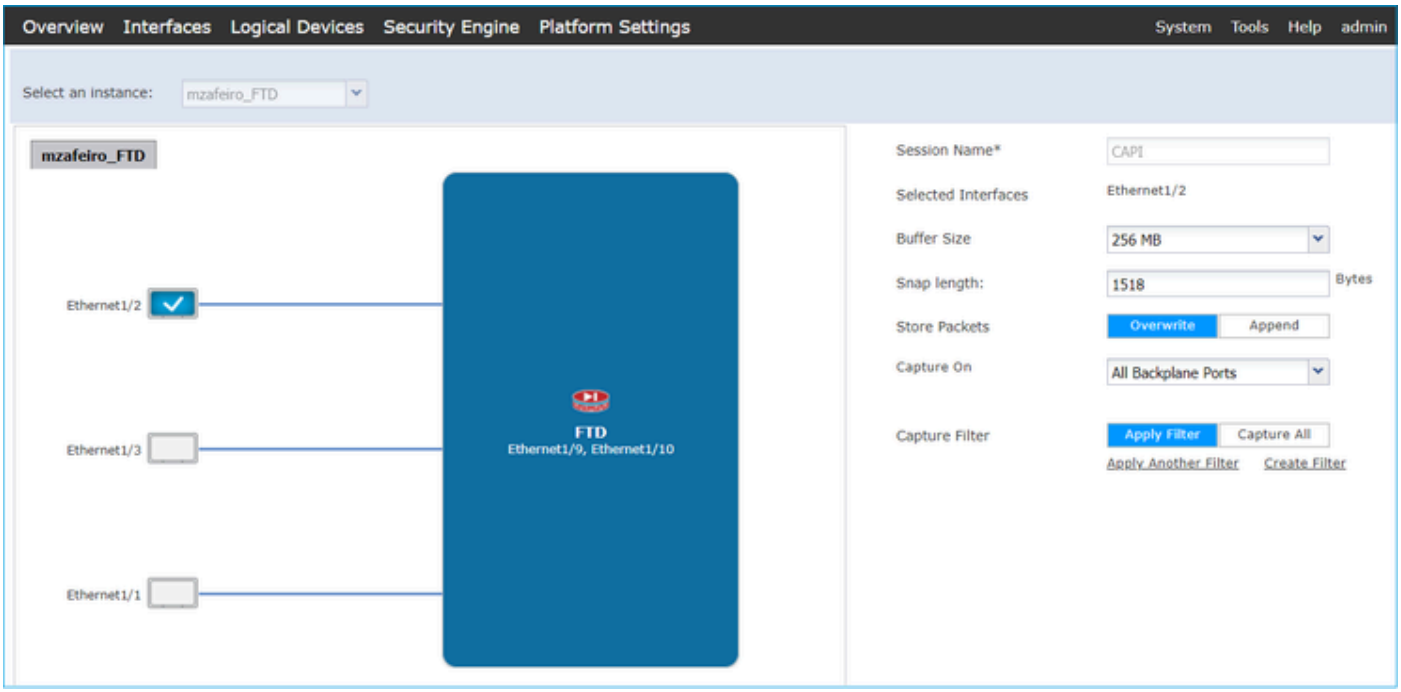
النقاط الرئيسية:

1. واجهات الدخول والخروج هي نفسها (دوران u).
2. يحتوي عدد وحدات البايت على قيمة كبيرة للغاية (~5 غيغابايت بايت).
3. تشير العلامة "o" إلى إلغاء تحميل التدفق (تدفق HW السريع). هذا هو السبب وراء عدم عرض التقاط FTD أي حزم. إلغاء تحميل التدفق مدعوم فقط على الأنظمة الأساسية 41xx و 93xx. في هذه الحالة، الجهاز هو 41xx.

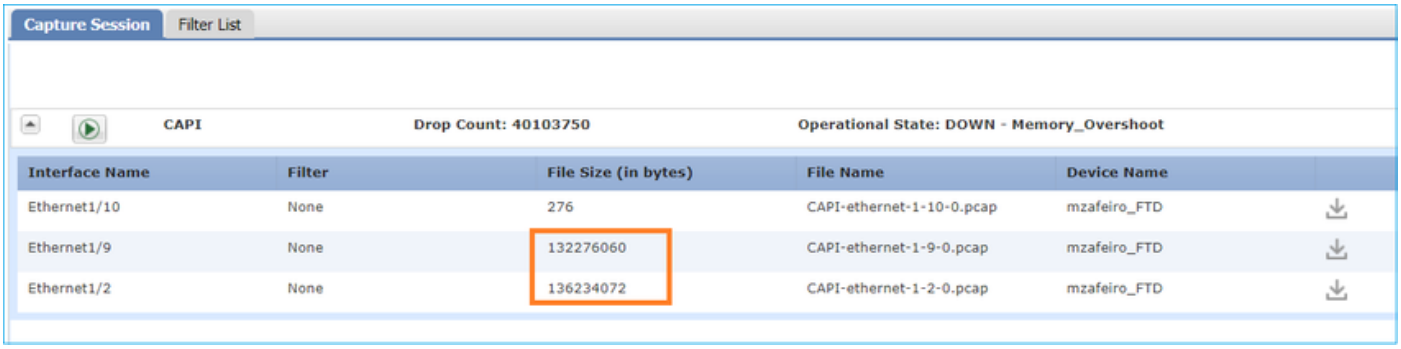
الإجراء 2. التقاط الصور على مستوى الهيكل.

قم بالاتصال بمدير هيكل FirePOWER وتمكين الالتقاط على واجهة الدخول (E1/2 في هذه الحالة) وواجهات اللوحة الخلفية (E1/9 و E1/10)، كما هو موضح في الصورة:



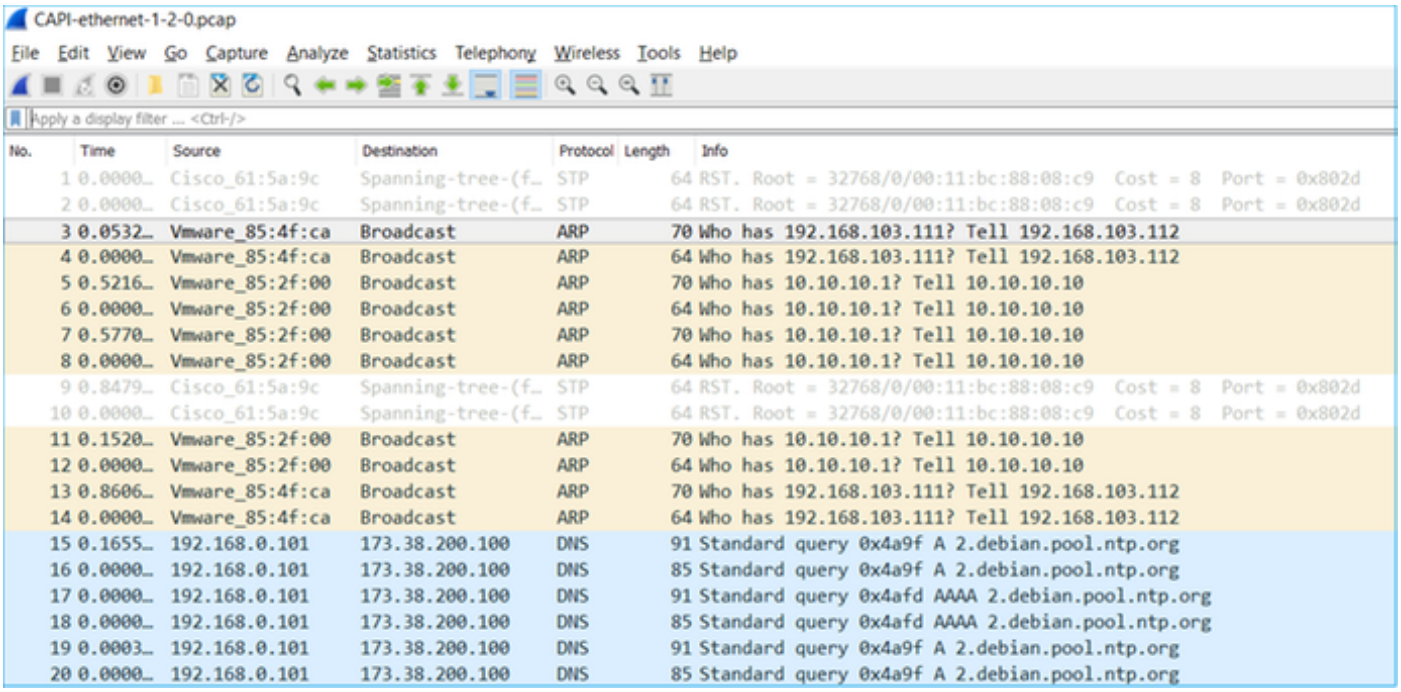


بعد بضع ثوان:

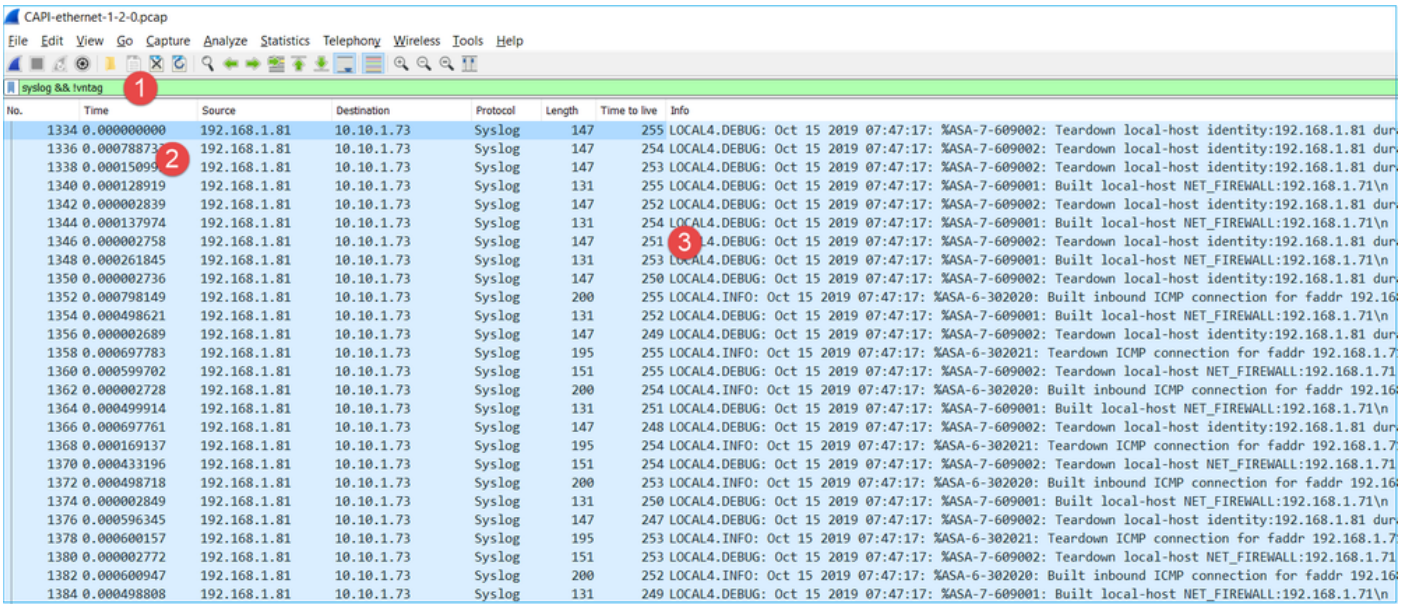


تلميح: في Wireshark استثنيت ال VN-tagged ربط أن يلغي الربط مزدوج على القارن طبيعي

قبل:

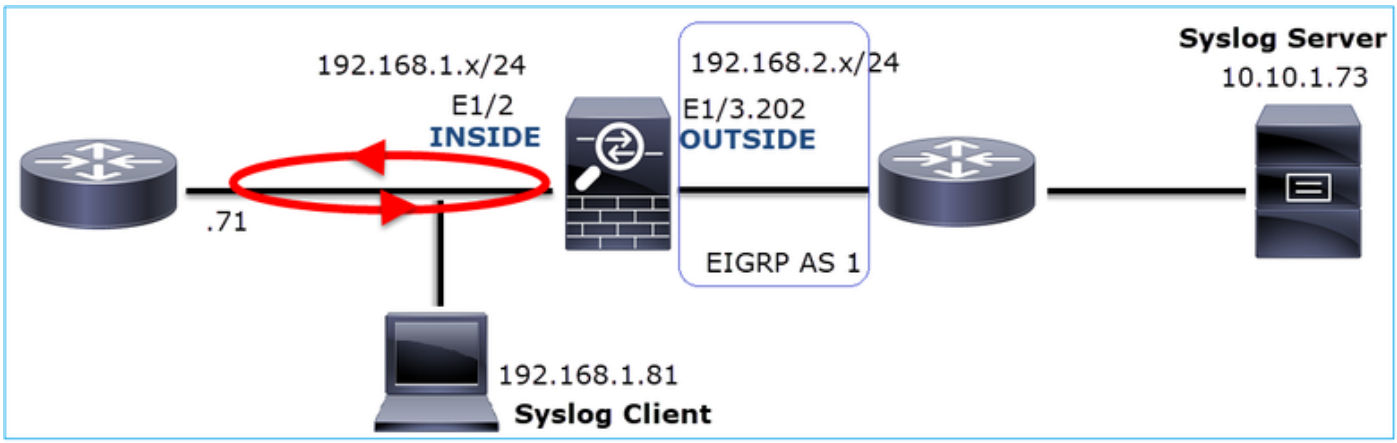


بعد:



النقاط الرئيسية:

1. يتم تطبيق عامل تصفية العرض لإزالة تكرارات الحزم وإظهار syslog فقط.
2. يكون الاختلاف بين الحزم في مستوى المايكروثانية. وهذا يشير إلى معدل حزمة مرتفع للغاية.
3. تنخفض قيمة مدة البقاء (TTL) بشكل مستمر. هذا يشير إلى حزمة أنشوطة.



الإجراء 3. إستخدام أداة تتبع الحزم.

بما أن الحزم ال تجتاز جدار الحماية LINA محرك أنت يستطيع ال يتم تتبع نشط (على قبض w/trace)، غير أن أنت يستطيع تتبعت ربط محاكي مع ربط-tracer:

```
<#root>

firepower#

packet-tracer input INSIDE udp 10.10.1.73 514 192.168.1.81 514

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 25350892, using existing flow

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

Phase: 5
```

```
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.1.81 using egress ifc  INSIDE

Phase: 6
Type: ADJACENCY-LOOKUP
Subtype: next-hop and adjacency
Result: ALLOW
Config:
Additional Information:
adjacency Active
next-hop mac address a023.9f92.2a4d hits 1 reference 1

Phase: 7
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Result:

input-interface: INSIDE

input-status: up
input-line-status: up

output-interface: INSIDE

output-status: up
output-line-status: up
Action: allow
```

الإجراء 4. تأكيد توجيه FTD.

تحقق من جدول توجيه جدار الحماية لمعرفة ما إذا كانت هناك أي مشاكل في التوجيه:

```
<#root>

firepower#

show route 10.10.1.73


Routing entry for 10.10.1.0 255.255.255.0
  Known via "eigrp 1", distance 90, metric 3072, type internal
  Redistributing via eigrp 1
  Last update from 192.168.2.72 on

OUTSIDE, 0:03:37 ago

  Routing Descriptor Blocks:
  * 192.168.2.72, from 192.168.2.72,

0:02:37 ago, via OUTSIDE

      Route metric is 3072, traffic share count is 1
```

```
      Total delay is 20 microseconds, minimum bandwidth is 1000000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 29/255, Hops 1
```

النقاط الرئيسية:

1. يشير المسار إلى واجهة الخروج الصحيحة.
2. تم تعلم الطريق قبل دقائق قليلة (0:02:37).

الإجراء 5. تأكيد وقت تشغيل الاتصال.

تحقق من وقت تشغيل الاتصال لمعرفة وقت تأسيس هذا الاتصال:

<#root>

```
firepower#
```

show conn address 192.168.1.81 port 514 detail

```
21 in use, 3627189 most used
Inspect Snort:
        preserve-connection: 19 enabled, 0 in effect, 74 most enabled, 0 most in effect
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,
       b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - initiator FIN, f - responder FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - decap tunnel, M - SMTP data, m - SIP media
       N - inspected by Snort (1 - preserve-connection enabled, 2 - preserve-connection in effect)
       n - GUP, O - responder data, o - offloaded,
       P - inside back connection, p - passenger flow
       q - SQL*Net data, R - initiator acknowledged FIN,
       R - UDP SUNRPC, r - responder acknowledged FIN,
       T - SIP, t - SIP transient, U - up,
       V - VPN orphan, v - M3UA W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow

UDP INSIDE: 10.10.1.73/514 INSIDE: 192.168.1.81/514,
    flags -oN1, idle 0s,
```

uptime 3m49s

```
, timeout 2m0s, bytes 4801148711
```

النقطة الرئيسية:

1. تم إنشاء الاتصال منذ حوالي 4 دقائق (هذا قبل تثبيت مسار EIGRP في جدول التوجيه)

الإجراء 6 - مسح الصلة القائمة.

في هذه الحالة، تتطابق الحزمة مع اتصال مؤسس ويتم توجيهها إلى واجهة مخرج خاطئة؛ هذا يسبب حلقة. يرجع السبب في ذلك إلى ترتيب عمليات جدار الحماية:

1. بحث الاتصال الذي تم إنشاؤه (أي خذ هذا الأولوية على البحث عن جدول التوجيه العام).
2. البحث عن ترجمة عنوان الشبكة (NAT) - تأخذ مرحلة UN-NAT (غاية NAT) الأولوية على PBR وبحث المسار.
3. التوجيه القائم على السياسة (PBR)
4. بحث جدول التوجيه العمومي

بما أن الاتصال ال ينتهي أبدا (يرسل عميل syslog الحزمة باستمرار بينما تكون مهلة خمول UDP هي 2 دقيقة) هناك حاجة إلى مسح الاتصال يدويا:

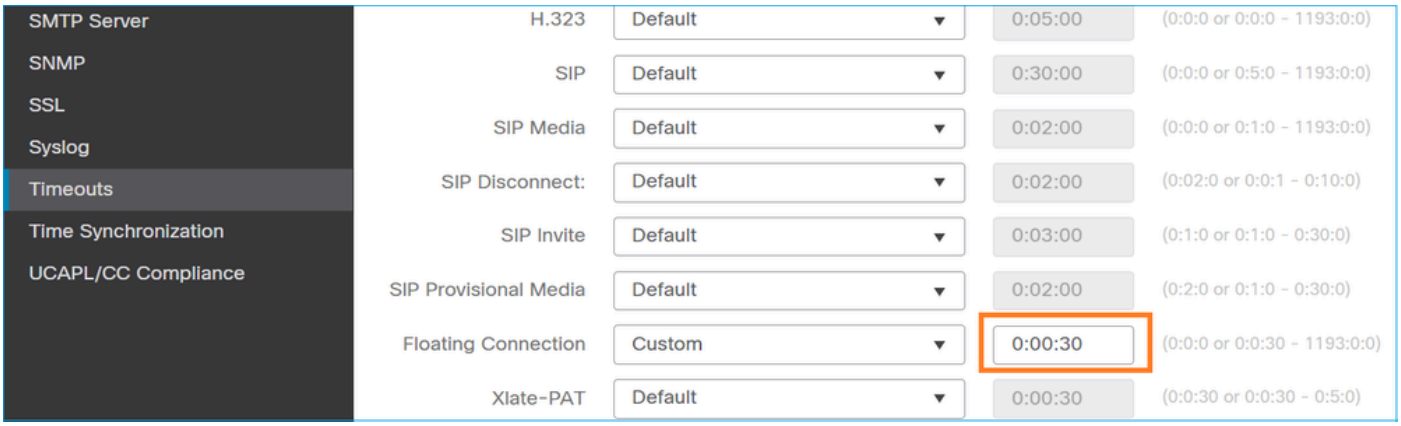
```
<#root>

firepower#

clear conn address 10.10.1.73 address 192.168.1.81 protocol udp port 514

1 connection(s) deleted.
```

تحقق من إنشاء اتصال جديد:

```
<#root>

firepower#

show conn address 192.168.1.81 port 514 detail | b 10.10.1.73.*192.168.1.81

UDP

OUTSIDE

: 10.10.1.73/514

INSIDE

: 192.168.1.81/514,
    flags -oN1, idle 1m15s, uptime 1m15s, timeout 2m0s, bytes 408
```

الإجراء 7. تكوين مهلة التداخل العائم.

هذا هو الحل المناسب لمعالجة المشكلة وتجنب التوجيه دون الأمثل، وخاصة لتدفقات UDP. انتقل إلى الأجهزة > إعدادات النظام الأساسي > مهلات وضبط القيمة:



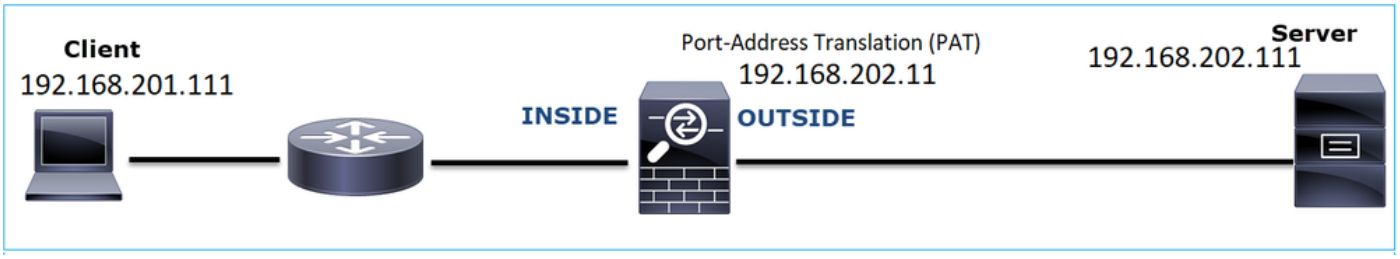
أنت يستطيع وجدت المزيد من التفاصيل حول التعويم conn مهلة في الأمر مرجع:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/T-Z/asa-command-ref-T-Z.html#pgfId-1649892

الحالة 9. مشكلة اتصال HTTPS (السيناريو 1)

وصف المشكلة: ال يمكن إنشاء اتصال HTTPS بين العميل 192.168.201.105 والخادم 192.168.202.101

تعرض هذه الصورة المخطط:



التدفق المتأثر:

SRC IP: 192.168.201.111

بروتوكول DST IP: 192.168.202.111

البروتوكول: بروتوكول TCP 443 (HTTPS)

تحليل أسر

تمكين االلتقاط على محرك FTD LINA:

ال ip يستعمل في االلتقاط الخارجي مختلف واجب إلى العنوان ترجمة تشكيل.

<#root>

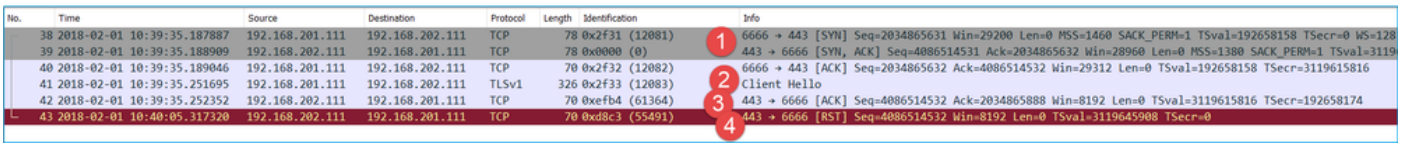
firepower#

capture CAPI int INSIDE match ip host 192.168.201.111 host 192.168.202.111

firepower#

capture CAPO int OUTSIDE match ip host 192.168.202.11 host 192.168.202.111

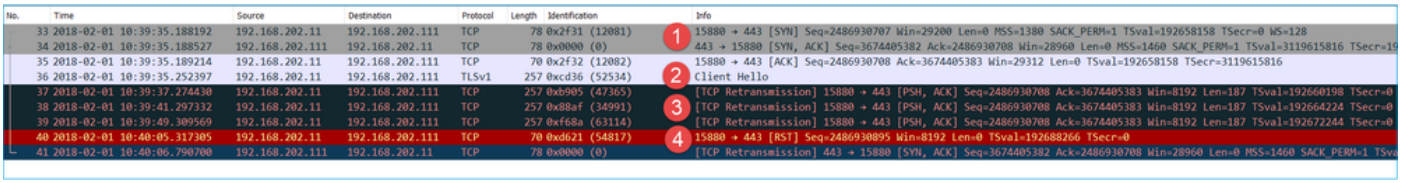
تظهر هذه الصورة الالتقاط الذي تم على واجهة NGFW Inside:



النقاط الرئيسية:

1. هناك مصافحة TCP ثلاثية الإتجاه.
2. بدء تفاوض SSL. يرسل العميل رسالة Client Hello.
3. هناك TCP ACK تم إرساله إلى العميل.
4. هناك TCP RST تم إرساله إلى العميل.

تعرض هذه الصورة الالتقاط الذي تم على الواجهة الخارجية ل NGFW.



النقاط الرئيسية:

1. هناك مصافحة TCP ثلاثية الإتجاه.
2. بدء تفاوض SSL. يرسل العميل رسالة Client Hello.
3. هناك عمليات إعادة إرسال TCP مرسلة من جدار الحماية إلى الخادم.
4. هناك TCP RST تم إرساله إلى الخادم.

الإجراءات الموصى بها

والغرض من الإجراءات الواردة في هذا القرع هو زيادة تضييق نطاق هذه المسألة.

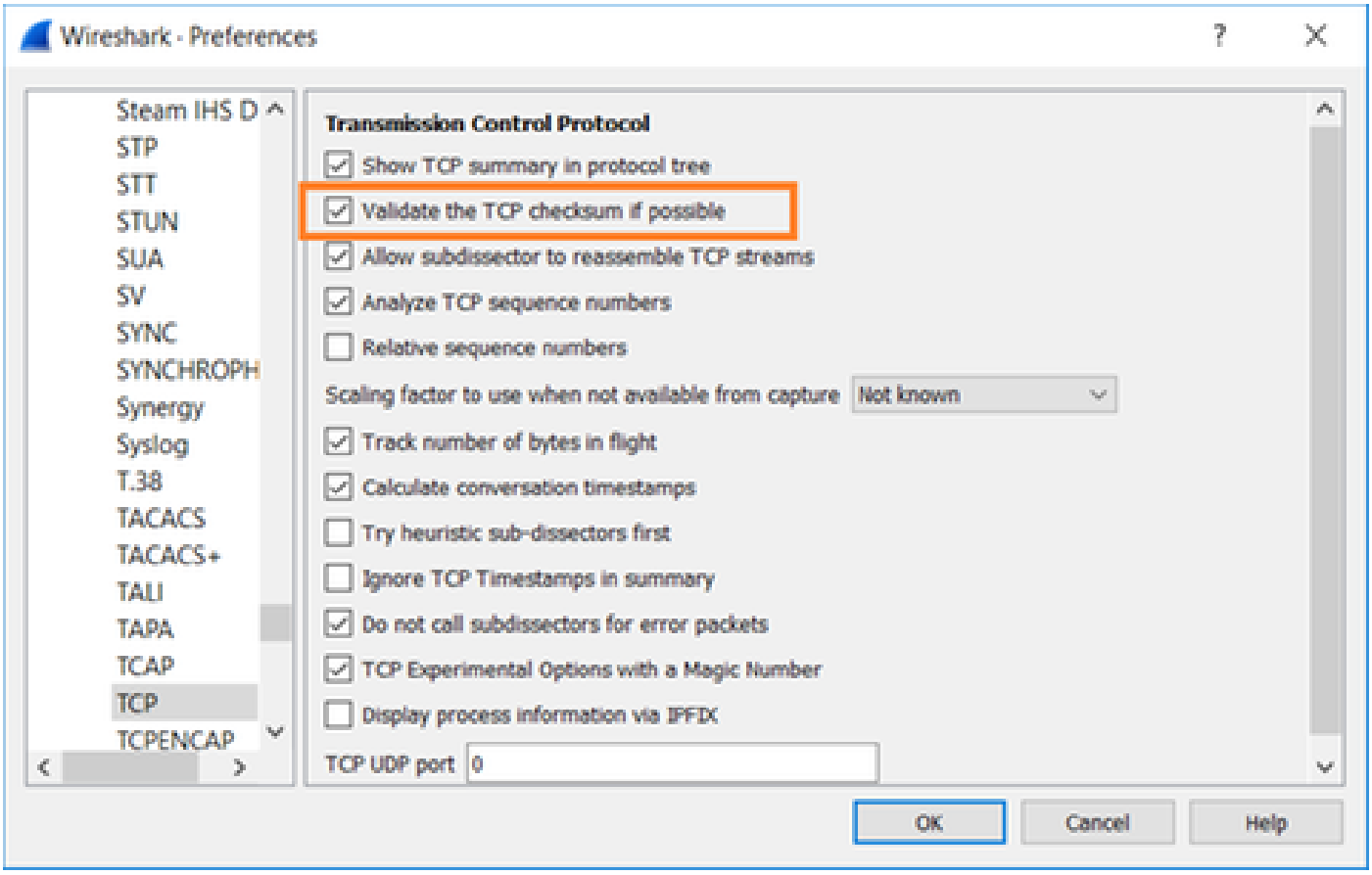
الإجراء 1. التقاط صور إضافية.

يظهر التقاط تم الالتقاط على الخادم أن الخادم استلم رمز عميل TLS مع المجموع الاختباري TCP تالف ويقوم بإسقاطه بصمت (لا يوجد TCP RST أو أي حزمة رد أخرى تجاه العميل):

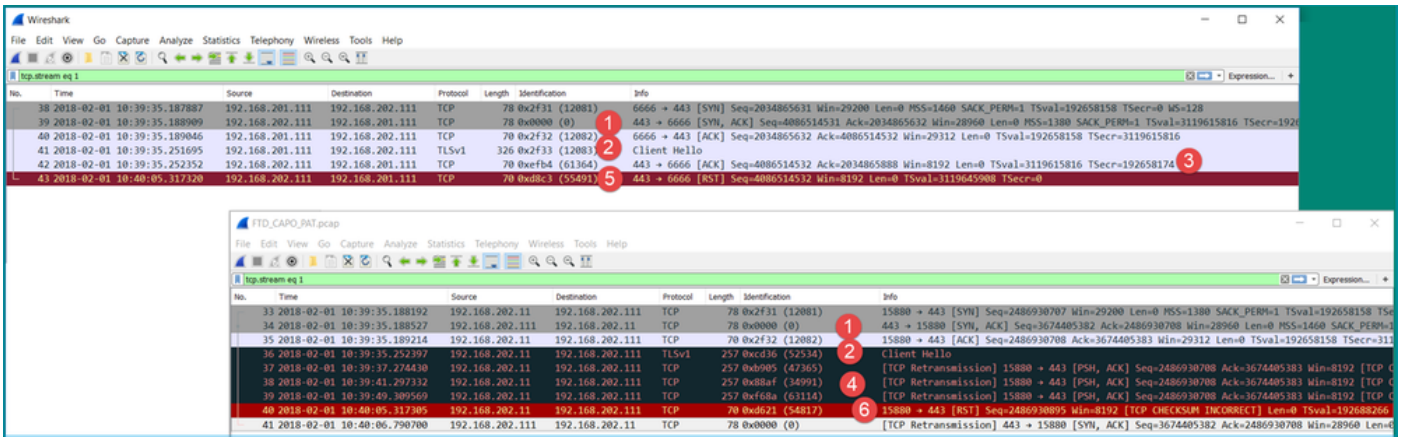
```
21:26:27.133677 IP (tos 0x0, ttl 64, id 52534, offset 0, flags [DF], proto TCP (6), length 239)
    192.168.202.11.15880 > 192.168.202.111.443: Flags [P.], cksum 0x0c65 (incorrect -> 0x3063), seq 1:188, ack 1, win 64, options [nop,nop,T
S val 192658174 ecr 3119615816], length 187
21:26:29.155652 IP (tos 0x0, ttl 64, id 47365, offset 0, flags [DF], proto TCP (6), length 239)
    192.168.202.11.15880 > 192.168.202.111.443: Flags [P.], cksum 0x4db7 (incorrect -> 0x71b5), seq 1:188, ack 1, win 64, options [nop,nop,T
S val 192660198 ecr 0], length 187
21:26:33.178142 IP (tos 0x0, ttl 64, id 34991, offset 0, flags [DF], proto TCP (6), length 239)
    192.168.202.11.15880 > 192.168.202.111.443: Flags [P.], cksum 0x3dfd (incorrect -> 0x61fb), seq 1:188, ack 1, win 64, options [nop,nop,T
S val 192664224 ecr 0], length 187
21:26:41.189640 IP (tos 0x0, ttl 64, id 63114, offset 0, flags [DF], proto TCP (6), length 239)
    192.168.202.11.15880 > 192.168.202.111.443: Flags [P.], cksum 0x1e89 (incorrect -> 0x42a7), seq 1:188, ack 1, win 64, options [nop,nop,T
S val 192672244 ecr 0], length 187
21:26:57.195947 IP (tos 0x0, ttl 64, id 54817, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.202.11.15880 > 192.168.202.111.443: Flags [R], cksum 0x9ee4 (incorrect -> 0xc2e8), seq 2486930895, win 64, options [nop,nop,TS v
al 192688266 ecr 0], length 0
21:26:58.668973 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.202.111.443 > 192.168.202.11.15880: Flags [S.], cksum 0x15fb (incorrect -> 0xffd2), seq 3674405382, ack 2486930708, win 28960, o
ptions [mss 1460,sackOK,TS val 3119647415 ecr 192658158,nop,wscale 7], length 0
^C
154 packets captured
154 packets received by filter
```

عندما تضع كل شيء معا:

في هذه الحالة، للفهم، هناك حاجة لتمكين التحقق من المجموع الاختباري ل TCP إذا كان خيار ذلك ممكنا على Wireshark. انتقل إلى تحرير > تفضيلات > بروتوكولات > TCP، كما هو موضح في الصورة.

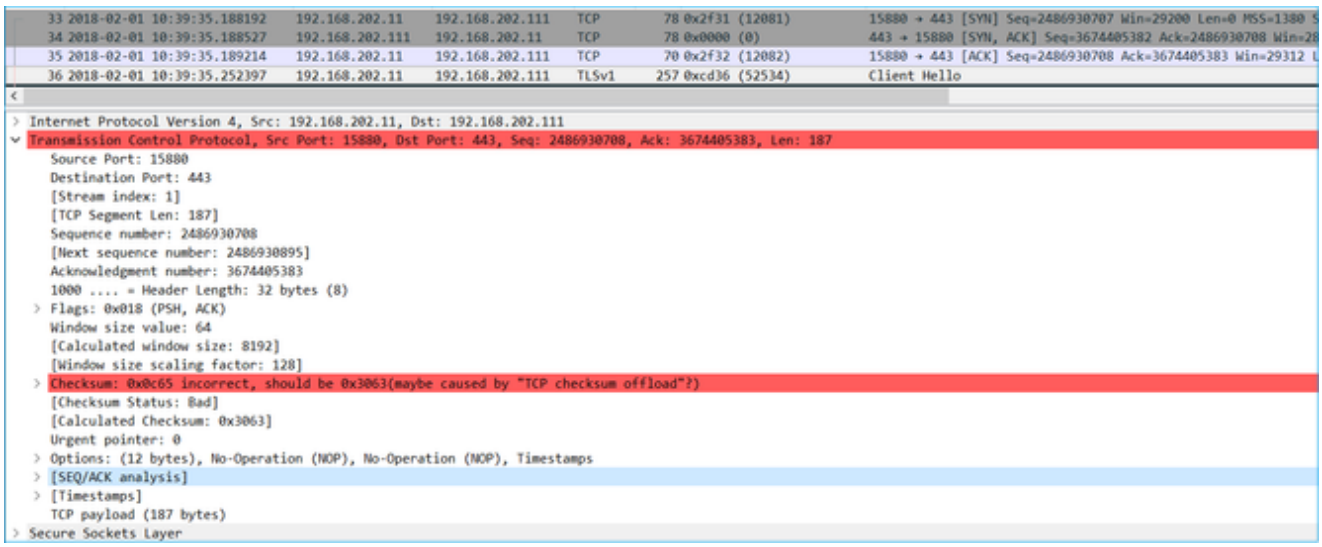


في هذه الحالة، من المفيد أن نضع إلتقاطات جنبا إلى جنب للحصول على الصورة الكاملة:



النقاط الرئيسية:

1. هناك مصافحة TCP ثلاثية الإتجاه. معرفات IP هي نفسها. وهذا يعني أن التدفق لم يتم تكويني بواسطة جدار الحماية.
2. يأتي TLS Client Hello من العميل ذي معرف IP 12083. يتم تمثيل الحزمة بواسطة جدار الحماية (تم تكويني جدار الحماية، في هذه الحالة، باستخدام سياسة فك تشفير TLS) وتم تغيير معرف IP إلى 52534. بالإضافة إلى ذلك، يتم إتلاف المجموع الاختباري للحزمة TCP (بسبب خلل في البرنامج تم إصلاحه لاحقا).
3. يوجد جدار الحماية في وضع وكيل TCP ويرسل ACK إلى العميل (الذي ينسف الخادم).



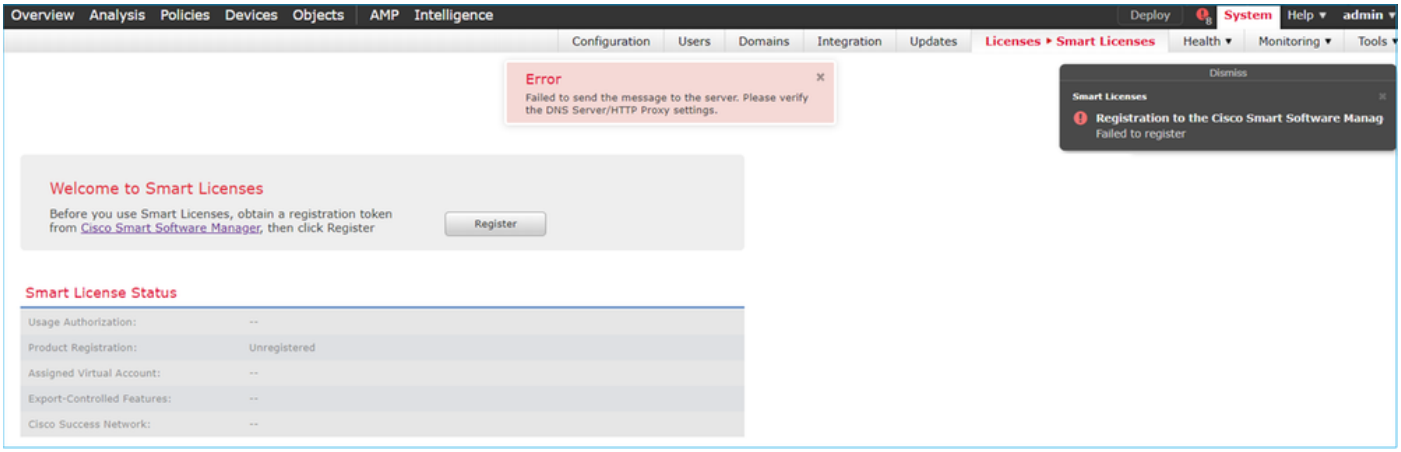
4. لا يتلقى جدار الحماية أي حزمة TCP ACK من الخادم ويعيد إرسال رسالة TLS Client Hello. مرة أخرى بسبب وضع وكيل TCP الذي قام جدار الحماية بتنشيطه.
5. بعد حوالي 30 ثانية، ينتهي جدار الحماية ويرسل TCP RST نحو العميل.
6. يرسل جدار الحماية TCP RST نحو الخادم.

للرجوع إليه:

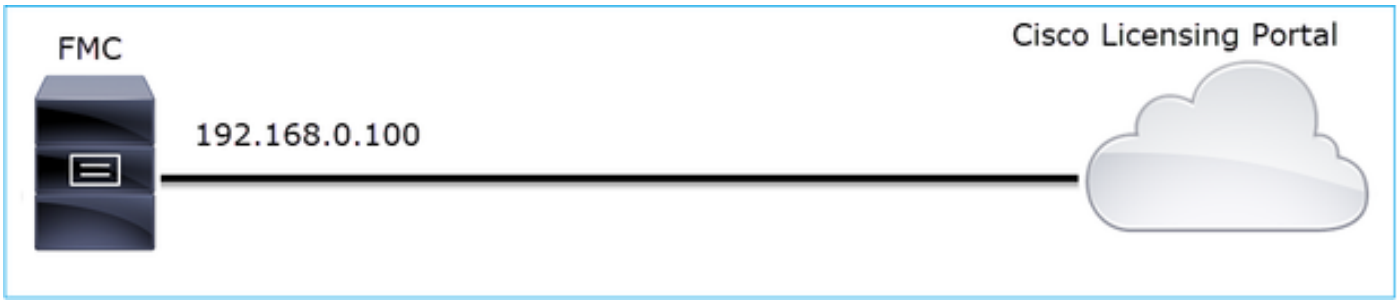
[معالجة تأكيد الاتصال Firepower TLS/SSL]

الحالة 10. مشكلة اتصال HTTPS (السيناريو 2)

وصف المشكلة: فشل تسجيل الترخيص الذكي ل FMC.



تعرض هذه الصورة المخطط:



التدفق المتأثر:

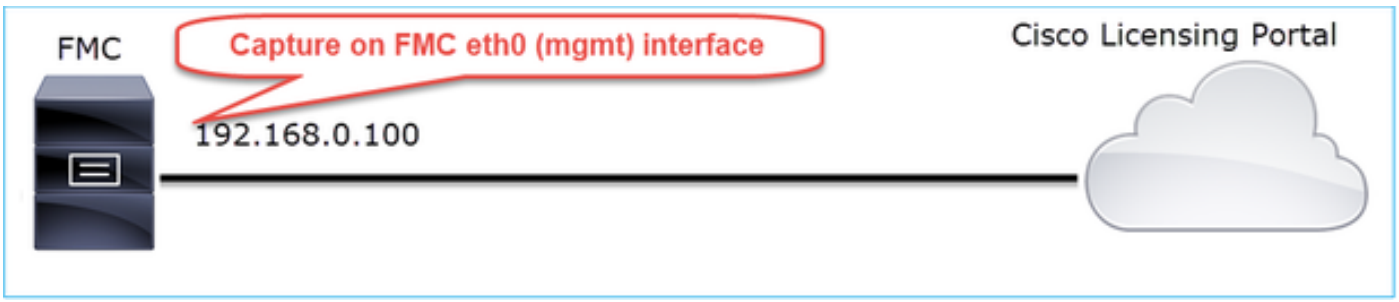
SRC IP: 192.168.0.100

DST: tools.cisco.com

البروتوكول: بروتوكول TCP 443 (HTTPS)

تحليل أسر

تمكين الالتقاط على واجهة إدارة FMC:

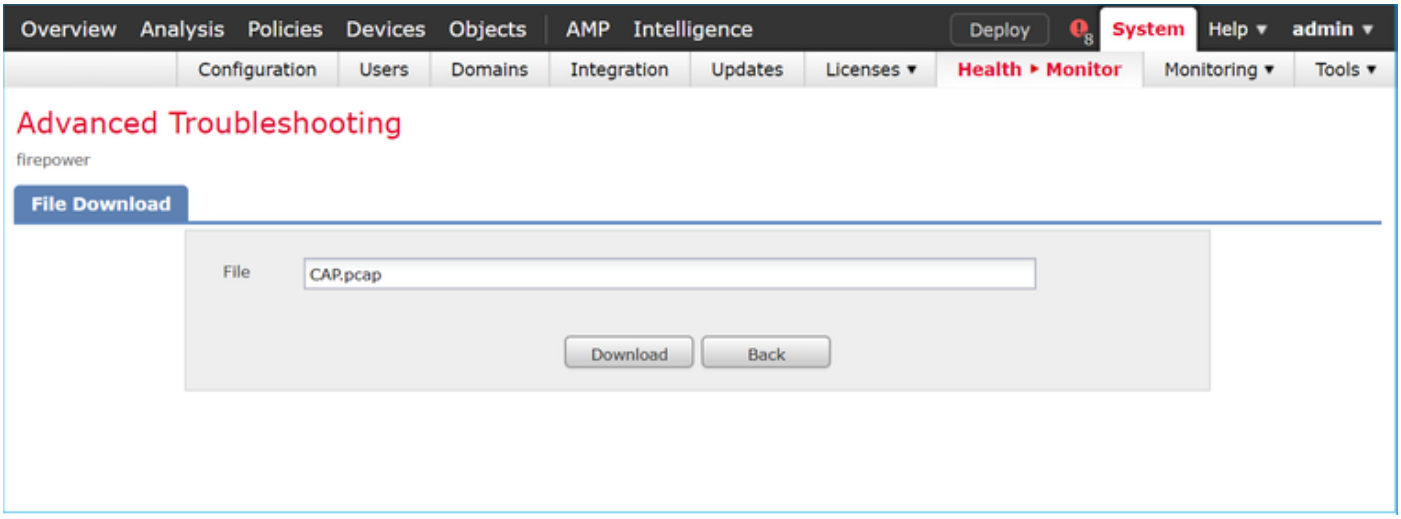


حاول التسجيل مرة أخرى. بمجرد ظهور رسالة الخطأ، اضغط على CTRL-C لإيقاف الالتقاط:

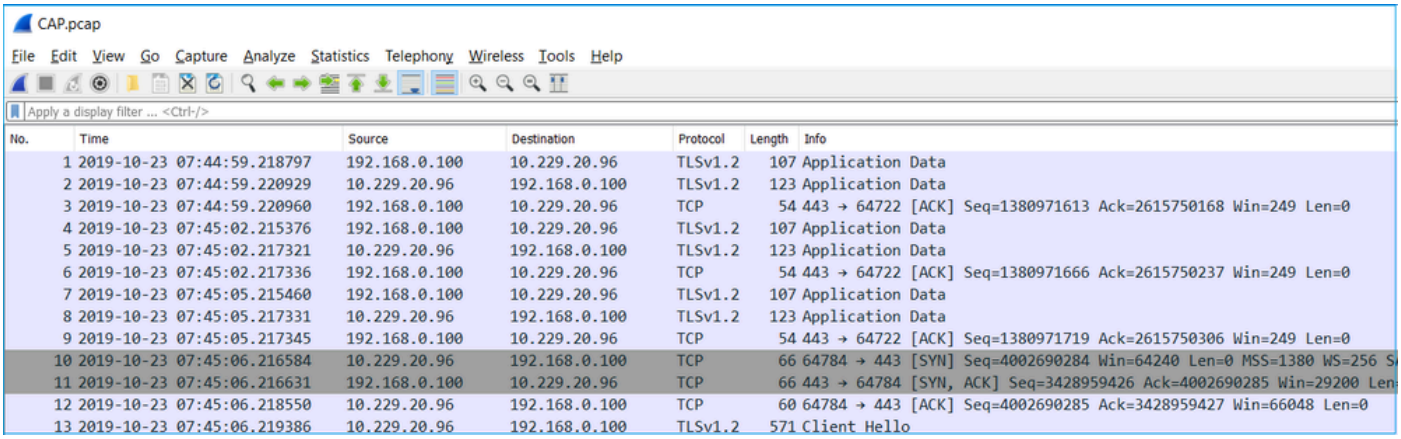
<#root>

```
root@firepower:/Volume/home/admin#

tcpdump -i eth0 port 443 -s 0 -w CAP.pcap

HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes

^C

264 packets captured

<- CTRL-C

264 packets received by filter
0 packets dropped by kernel

root@firepower:/Volume/home/admin#
```

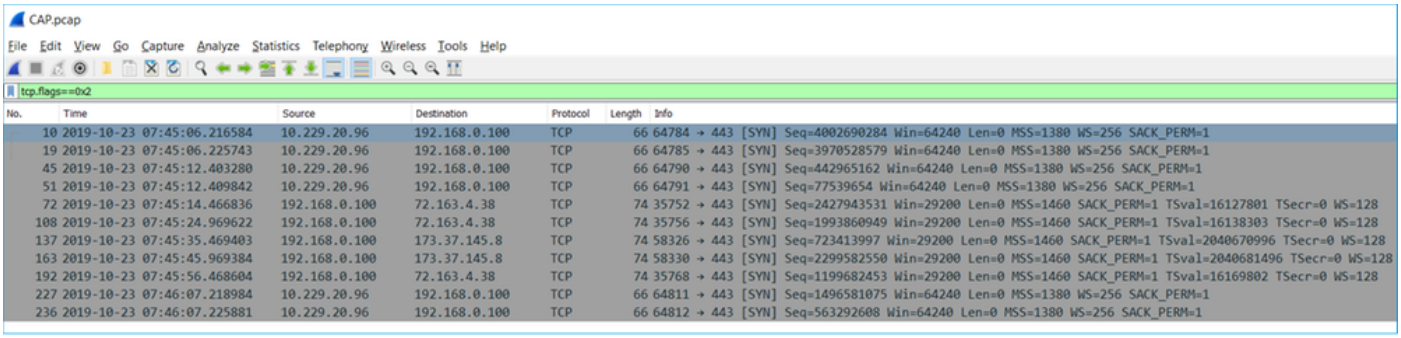
قم بجمع الالتقاط من وحدة التحكم في إدارة الهيكل (System > Health > Monitor، وحدد الجهاز وحدد أستكشاف الأخطاء وإصلاحها المتقدم)، كما هو موضح في الصورة:



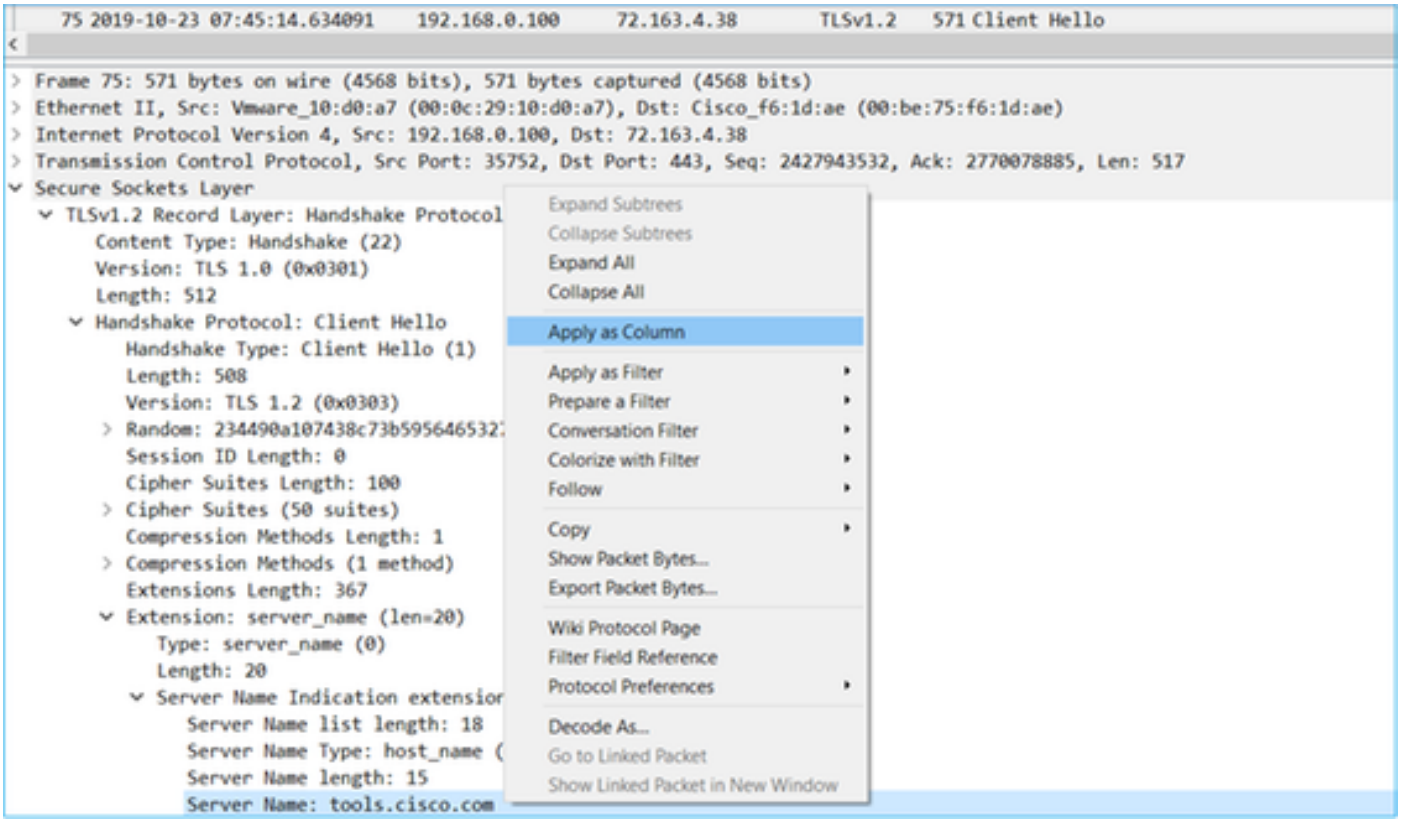
تظهر الصورة التقاط FMC على Wireshark:



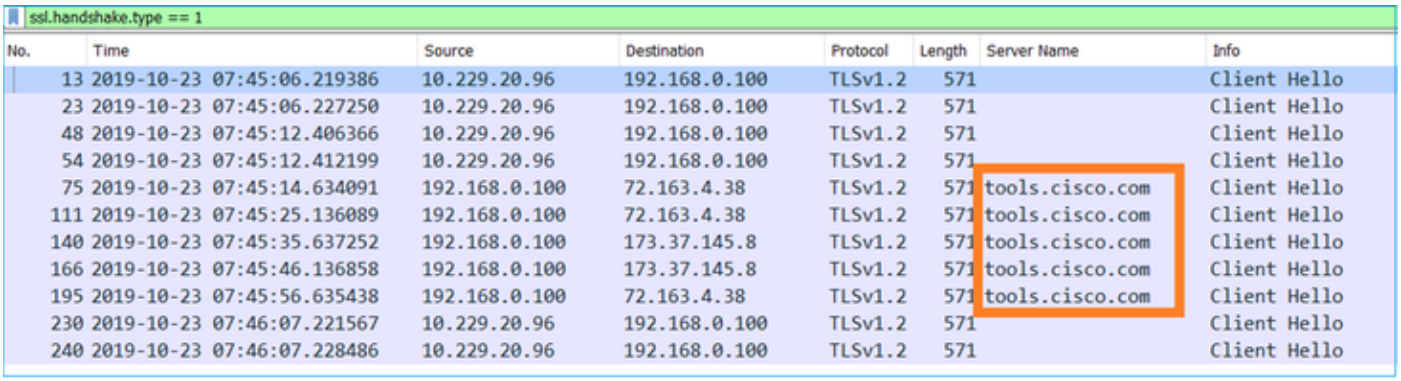
تلميح: للتحقق من جميع جلسات عمل TCP الجديدة التي تم التقاطها، أستخدم عامل تصفية عرض tcp.flags==0x2 على Wireshark. يقوم هذا بتصفية جميع حزم نظام TCP التي تم التقاطها.



تلميح: تطبيق حقل اسم الخادم من SSL Client Hello كعمود.

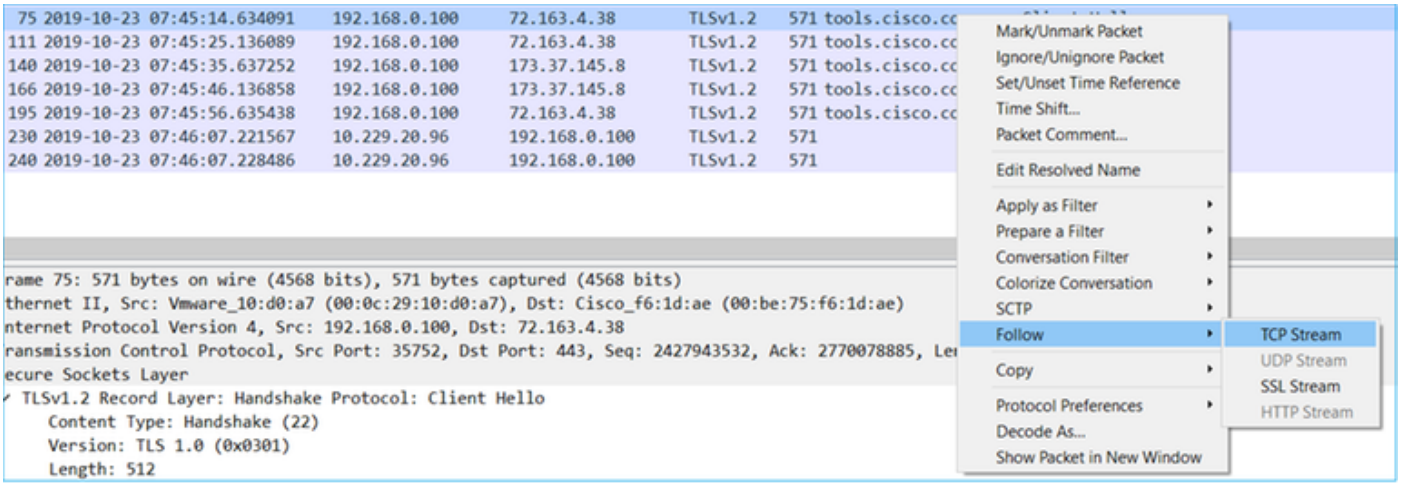


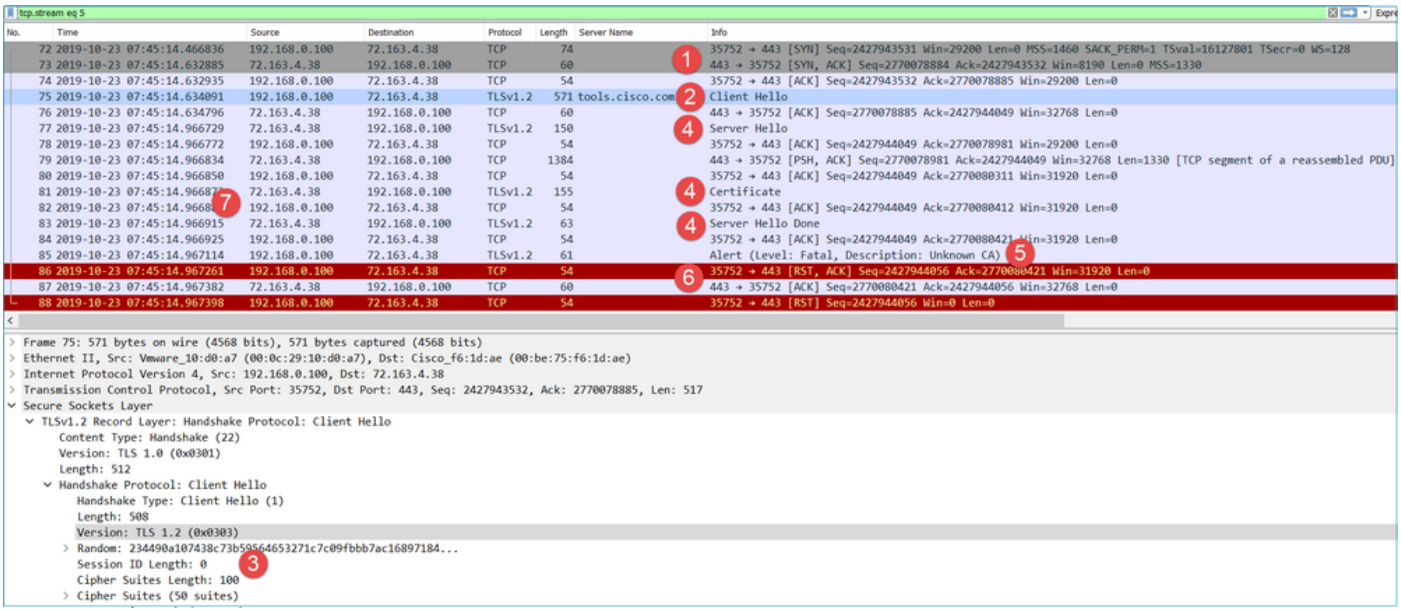
تلميح: تطبيق عامل تصفية العرض هذا لرؤية رسائل Client Hello فقط ssl.handshake.type == 1



ملاحظة: في وقت كتابة هذا التقرير، تستخدم بوابة الترخيص الذكي (tools.cisco.com) عناوين IP التالية: 72.163.4.38, 173.37.145.8

اتبع أحد تدفقات TCP (اتبع > تدفق TCP)، كما هو موضح في الصورة.



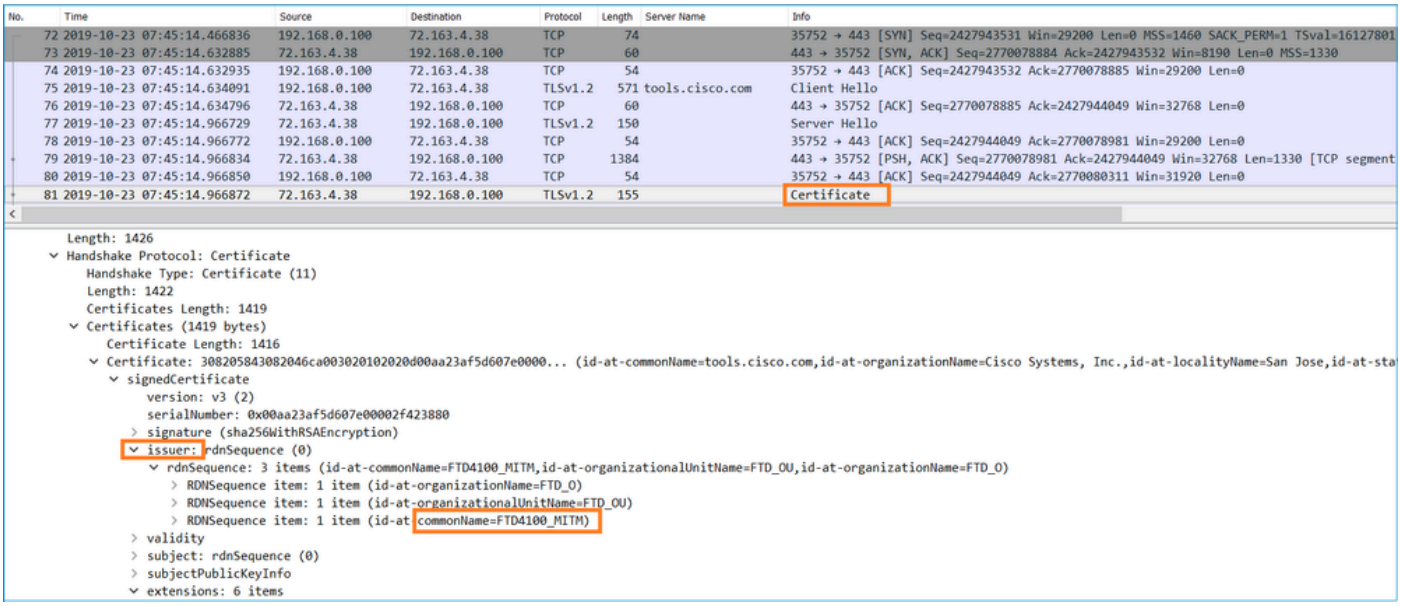


النقاط الرئيسية:

1. هناك مصافحة TCP ثلاثية الإتجاه.
2. يرسل العميل (FMC) رسالة SSL Client Hello باتجاه مدخل الترخيص الذكي.

3. معرف جلسة SSL هو 0. هذا يعني أنها ليست جلسة مستأنفة.
4. يرد الخادم الوجهة برسالة "مرحبا بك في الخادم" و"الشهادة" و"مرحبا بك في الخادم".
5. يرسل العميل تنبيه SSL مملوك والذي يتعلق ب "مرجع مصدق غير معروف".
6. يرسل العميل TCP RST لإغلاق الجلسة.
7. كانت مدة جلسة TCP بالكامل (من الإنشاء إلى الإغلاق) حوالي 0.5 ثانية.

حدد شهادة الخادم ووسع حقل المصدر لرؤية الاسم الشائع. في هذه الحالة يكشف الاسم الشائع عن جهاز يقوم بتعريف الدخيل (MITM).



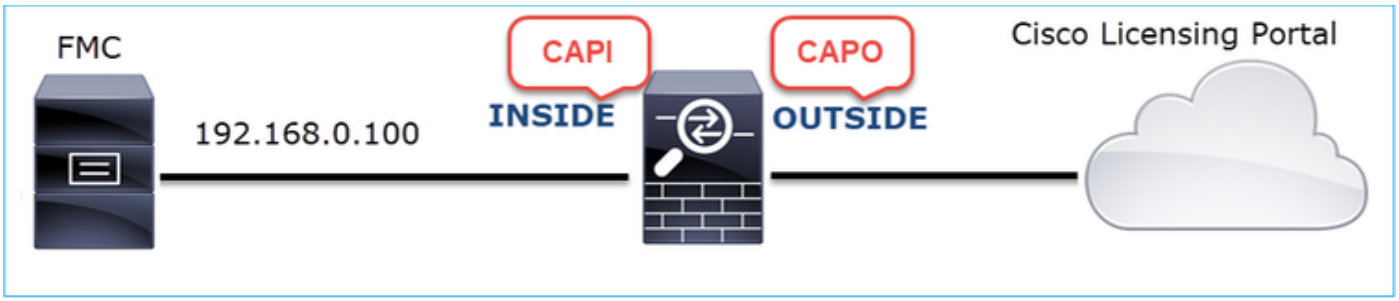
وهذا موضح في هذه الصورة:

الإجراءات الموصى بها

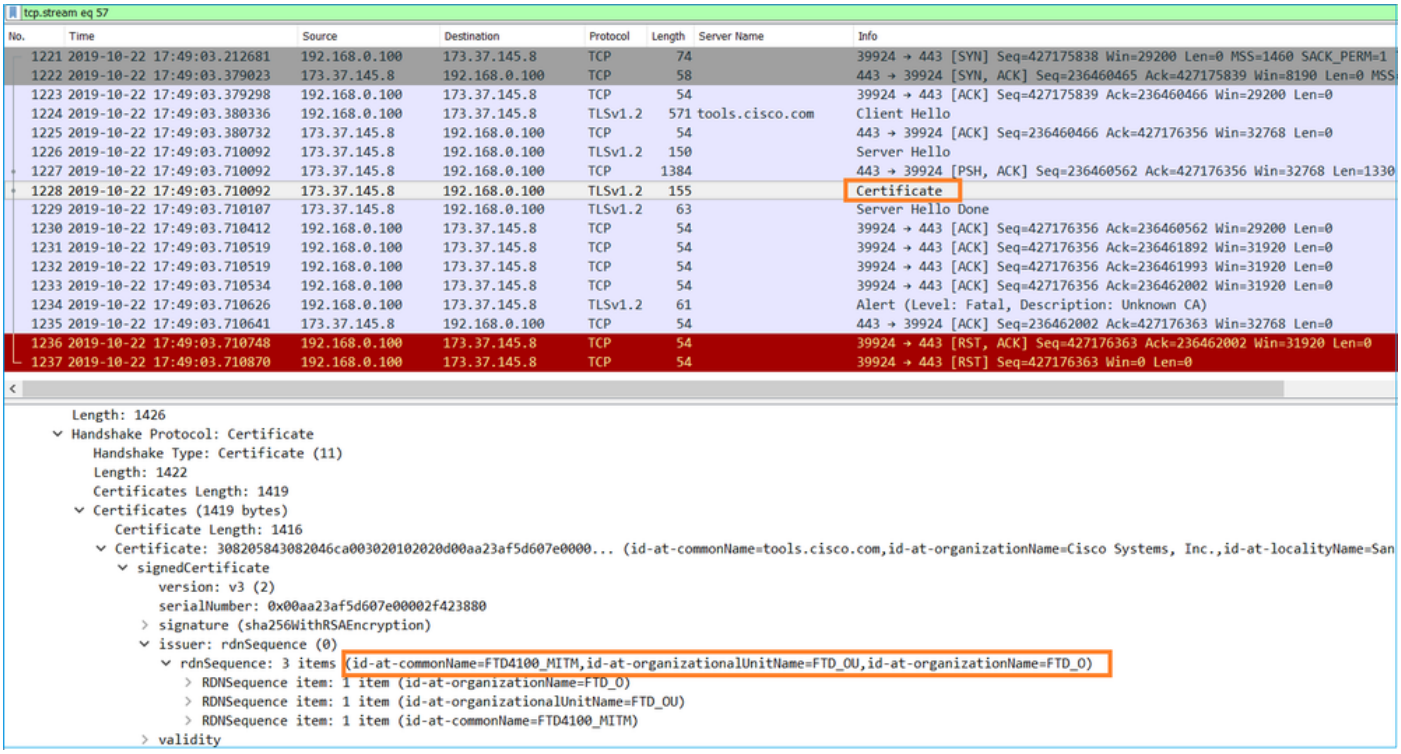
والغرض من الإجراءات الواردة في هذا القسم هو زيادة تضييق نطاق هذه المسألة.

الإجراء 1. التقاط صور إضافية.

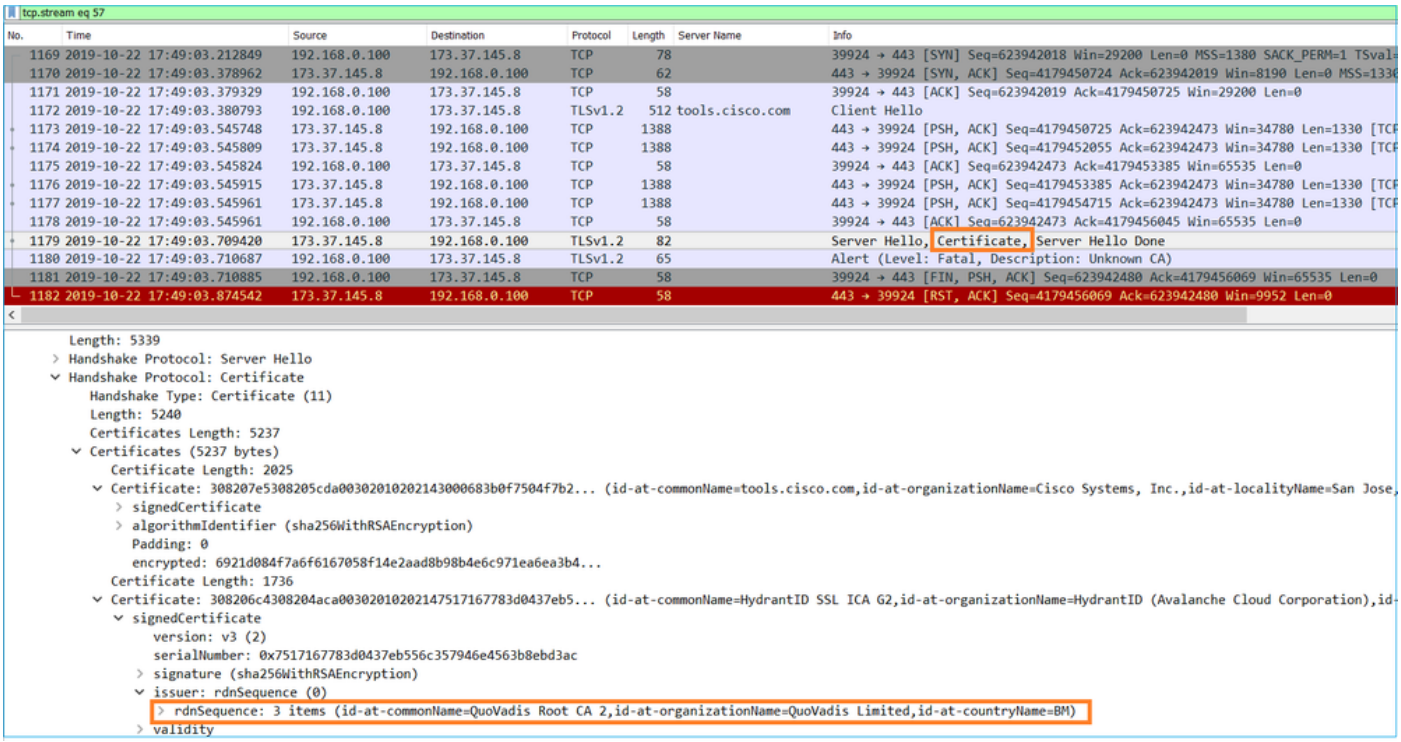
التقاط على جهاز جدار حماية النقل:



ظهر CAPI:



ظهر CAPO:



تثبت هذه المكالمة أن جدار حماية التنقل يعدل شهادة الخادم (MITM)

الإجراء 2. تحقق من سجلات الجهاز.

يمكنك تجميع حزمة FMC TS كما هو موضح في هذا المستند:

https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html

في هذه الحالة، عرض الملف /dir-archives/var-log/process_stdout.log بحثًا عن:

<#root>

SOUT: 10-23 05:45:14 2019-10-23 05:45:36 sla[10068]: *Wed .967 UTC: CH-LIB-ERROR: ch_pf_curl_send_msg[4

failed to perform, err code 60, err string "SSL peer certificate or SSH remote key was not OK"

...

SOUT: 10-23 05:45:14 2019-10-23 05:45:36 sla[10068]: *Wed .967 UTC: CH-LIB-TRACE: ch_pf_curl_is_cert_is

cert issue checking, ret 60, url "https://tools.cisco.com/its/

الحل الموصى به

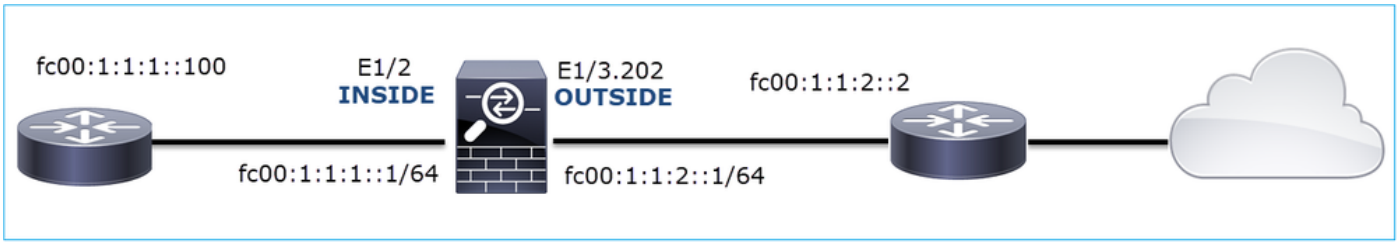
قم بتعطيل MITM للتدفق المحدد حتى يمكن لـ FMC التسجيل بنجاح إلى سحابة الترخيص الذكي.

الحالة 11. مشكلة في اتصال IPv6

وصف المشكلة: لا يمكن للمضيفين الداخليين (الموجودين خلف واجهة جدار الحماية الداخلية) الاتصال بالمضيفين الخارجيين (البيئات المضيفة الموجودة خلف واجهة جدار

الحماية الخارجية).

تعرض هذه الصورة المخطط:



التدفق المتأثر:

SRC IP: القناة الليفية 00:1:1:1::100

بروتوكول DST IP: القناة الليفية 00:1:1:2::2

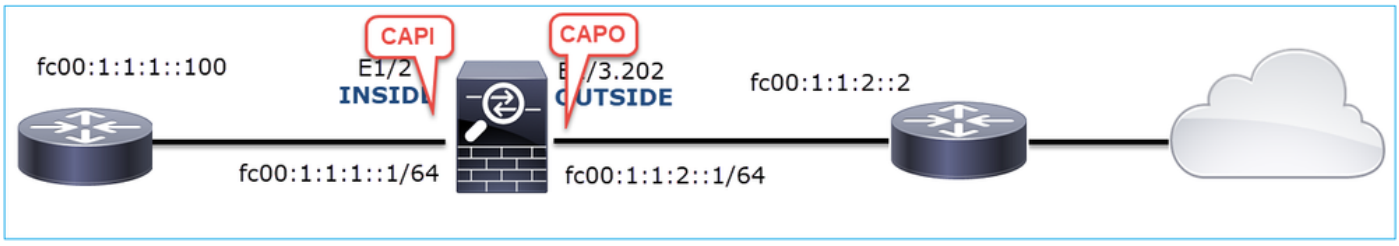
البروتوكول: أي

تحليل أسر

قم بتمكين عمليات الالتقاط على محرك FTD LINA.

<#root>

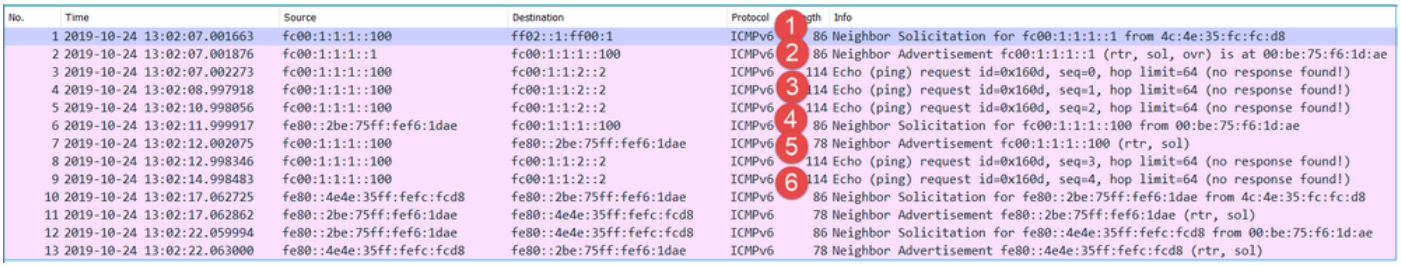
```
firepower#
capture CAPI int INSIDE match ip any6 any6
firepower#
capture CAPO int OUTSIDE match ip any6 any6
```



التقاط - سيناريو لا يعمل

تم أخذ هذه الالتقاط بالتوازي مع إختبار اتصال ICMP من IP FC00:1:1:1::100 (داخل الموجه) إلى IP FC00:1:1:2::2 (موجه من الخادم).

يحتوي واجهة Capture on Firewall INSIDE على:

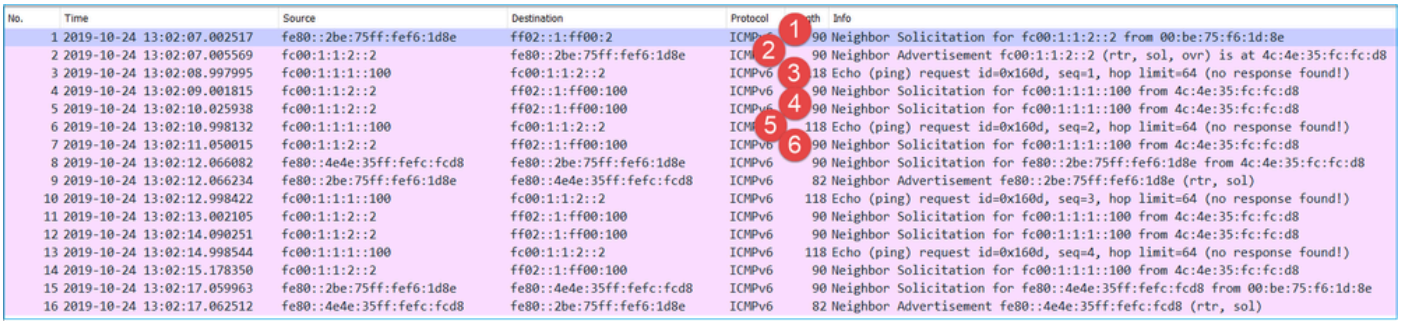


No.	Time	Source	Destination	Protocol	Length	Info
1	2019-10-24 13:02:07.001663	fc00:1:1:1::100	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation for fc00:1:1:1::1 from 4c:4e:35:fc:fc:d8
2	2019-10-24 13:02:07.001876	fc00:1:1:1::1	fc00:1:1:1::100	ICMPv6	86	Neighbor Advertisement fc00:1:1:1::1 (rtr, sol, ovr) is at 00:be:75:f6:1d:ae
3	2019-10-24 13:02:07.002273	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	114	Echo (ping) request id=0x160d, seq=0, hop limit=64 (no response found!)
4	2019-10-24 13:02:08.997918	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	114	Echo (ping) request id=0x160d, seq=1, hop limit=64 (no response found!)
5	2019-10-24 13:02:10.998056	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	114	Echo (ping) request id=0x160d, seq=2, hop limit=64 (no response found!)
6	2019-10-24 13:02:11.999917	fe80::2be:75ff:fef6:1dae	fc00:1:1:1::100	ICMPv6	86	Neighbor Solicitation for fc00:1:1:1::100 from 00:be:75:f6:1d:ae
7	2019-10-24 13:02:12.002075	fc00:1:1:1::100	fe80::2be:75ff:fef6:1dae	ICMPv6	78	Neighbor Advertisement fc00:1:1:1::100 (rtr, sol)
8	2019-10-24 13:02:12.998346	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	114	Echo (ping) request id=0x160d, seq=3, hop limit=64 (no response found!)
9	2019-10-24 13:02:14.998483	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	114	Echo (ping) request id=0x160d, seq=4, hop limit=64 (no response found!)
10	2019-10-24 13:02:17.062725	fe80::4e4e:35ff:fefc:fcd8	fe80::2be:75ff:fef6:1dae	ICMPv6	86	Neighbor Solicitation for fe80::2be:75ff:fef6:1dae from 4c:4e:35:fc:fc:d8
11	2019-10-24 13:02:17.062862	fe80::2be:75ff:fef6:1dae	fe80::4e4e:35ff:fefc:fcd8	ICMPv6	78	Neighbor Advertisement fe80::2be:75ff:fef6:1dae (rtr, sol)
12	2019-10-24 13:02:22.059994	fe80::2be:75ff:fef6:1dae	fe80::4e4e:35ff:fefc:fcd8	ICMPv6	86	Neighbor Solicitation for fe80::4e4e:35ff:fefc:fcd8 from 00:be:75:f6:1d:ae
13	2019-10-24 13:02:22.063000	fe80::4e4e:35ff:fefc:fcd8	fe80::2be:75ff:fef6:1dae	ICMPv6	78	Neighbor Advertisement fe80::4e4e:35ff:fefc:fcd8 (rtr, sol)

النقاط الرئيسية:

1. يرسل الموجه رسالة طلب طلب مجاورة ل IPv6 ويطلب عنوان MAC الخاص بجهاز البث (IP FC00:1:1::1).
2. ردود جدار الحماية باستخدام إعلان جار IPv6.
3. يرسل الموجه طلب ICMP Echo.
4. يرسل جدار الحماية رسالة طلب مجاورة ل IPv6 ويطلب عنوان MAC الخاص بجهاز تدفق البيانات من الخادم (fc00:1:1::100).
5. يرد الموجه باستخدام إعلان جار IPv6.
6. يرسل الموجه طلبات ICMP إضافية لصدى IPv6.

يحتوي الالتقاط على جدار الحماية الموجود خارج الواجهة على:



No.	Time	Source	Destination	Protocol	Length	Info
1	2019-10-24 13:02:07.002517	fe80::2be:75ff:fef6:1d8e	ff02::1:ff00:2	ICMPv6	90	Neighbor Solicitation for fc00:1:1:2::2 from 00:be:75:f6:1d:8e
2	2019-10-24 13:02:07.005569	fc00:1:1:2::2	fe80::2be:75ff:fef6:1d8e	ICMPv6	90	Neighbor Advertisement fc00:1:1:2::2 (rtr, sol, ovr) is at 4c:4e:35:fc:fc:d8
3	2019-10-24 13:02:08.997995	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	118	Echo (ping) request id=0x160d, seq=1, hop limit=64 (no response found!)
4	2019-10-24 13:02:09.001815	fc00:1:1:2::2	ff02::1:ff00:100	ICMPv6	90	Neighbor Solicitation for fc00:1:1:1::100 from 4c:4e:35:fc:fc:d8
5	2019-10-24 13:02:10.025938	fc00:1:1:2::2	ff02::1:ff00:100	ICMPv6	90	Neighbor Solicitation for fc00:1:1:1::100 from 4c:4e:35:fc:fc:d8
6	2019-10-24 13:02:10.998132	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	118	Echo (ping) request id=0x160d, seq=2, hop limit=64 (no response found!)
7	2019-10-24 13:02:11.050015	fc00:1:1:2::2	ff02::1:ff00:100	ICMPv6	90	Neighbor Solicitation for fc00:1:1:1::100 from 4c:4e:35:fc:fc:d8
8	2019-10-24 13:02:12.066082	fe80::4e4e:35ff:fefc:fcd8	fe80::2be:75ff:fef6:1d8e	ICMPv6	90	Neighbor Solicitation for fe80::2be:75ff:fef6:1d8e from 4c:4e:35:fc:fc:d8
9	2019-10-24 13:02:12.066234	fe80::2be:75ff:fef6:1d8e	fe80::4e4e:35ff:fefc:fcd8	ICMPv6	82	Neighbor Advertisement fe80::2be:75ff:fef6:1d8e (rtr, sol)
10	2019-10-24 13:02:12.998422	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	118	Echo (ping) request id=0x160d, seq=3, hop limit=64 (no response found!)
11	2019-10-24 13:02:13.002105	fc00:1:1:2::2	ff02::1:ff00:100	ICMPv6	90	Neighbor Solicitation for fc00:1:1:1::100 from 4c:4e:35:fc:fc:d8
12	2019-10-24 13:02:14.090251	fc00:1:1:2::2	ff02::1:ff00:100	ICMPv6	90	Neighbor Solicitation for fc00:1:1:1::100 from 4c:4e:35:fc:fc:d8
13	2019-10-24 13:02:14.998544	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	118	Echo (ping) request id=0x160d, seq=4, hop limit=64 (no response found!)
14	2019-10-24 13:02:15.178350	fc00:1:1:2::2	ff02::1:ff00:100	ICMPv6	90	Neighbor Solicitation for fc00:1:1:1::100 from 4c:4e:35:fc:fc:d8
15	2019-10-24 13:02:17.059963	fe80::2be:75ff:fef6:1d8e	fe80::4e4e:35ff:fefc:fcd8	ICMPv6	90	Neighbor Solicitation for fe80::4e4e:35ff:fefc:fcd8 from 00:be:75:f6:1d:8e
16	2019-10-24 13:02:17.062512	fe80::4e4e:35ff:fefc:fcd8	fe80::2be:75ff:fef6:1d8e	ICMPv6	82	Neighbor Advertisement fe80::4e4e:35ff:fefc:fcd8 (rtr, sol)

النقاط الرئيسية:

1. يرسل جدار الحماية رسالة طلب مجاورة IPv6 التي تطلب عنوان MAC لجهاز البث (IP FC00:1:1:2::2).
2. يرد الموجه باستخدام إعلان جار IPv6.
3. يرسل جدار الحماية طلب صدى ICMP ل IPv6.
4. يرسل جهاز تدفق البيانات (الموجه FC00:1:1:2::2) رسالة طلب طلب جوار IPv6 التي تطلب عنوان MAC لعنوان IPv6 fc00:1:1:1::100.
5. يرسل جدار الحماية طلب صدى ICMP إضافي IPv6.
6. يرسل موجه البث رسالة طلب طلب مجاورة ل IPv6 التي تطلب عنوان MAC لعنوان IPv6 fc00:1:1:1::100.

النقطة 4 مثيرة جدا للاهتمام. عادة ما يطلب موجه البث عنوان MAC الخاص بجدار الحماية الخارجي (FC00:1:1:2::2)، ولكن بدلا من ذلك، يطلب وضع FC00:1:1:1:100. هذا يشير إلى تكوين غير صحيح.

الإجراءات الموصى بها

والغرض من الإجراءات الواردة في هذا القرع هو زيادة تضييق نطاق هذه المسألة.

الإجراء 1. تحقق من الجدول المجاور ل IPv6.

الجدول المجاور لجدار الحماية IPv6 مع أب بشكل صحيح.

<#root>

```
firepower#

show ipv6 neighbor | i fc00

fc00:1:1:2::2                            58 4c4e.35fc.fcd8  STALE OUTSIDE
fc00:1:1:1::100                          58 4c4e.35fc.fcd8  STALE INSIDE
```

الإجراء 2. تحقق من تكوين IPv6.

هذا هو تكوين جدار الحماية.

<#root>

```
firewall#

show run int e1/2

!
interface Ethernet1/2
 nameif INSIDE
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 192.168.0.1 255.255.255.0
 ipv6 address

fc00:1:1:1::1/64

 ipv6 enable

firewall#

show run int e1/3.202

!
interface Ethernet1/3.202
 vlan 202
 nameif OUTSIDE
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 192.168.103.96 255.255.255.0
 ipv6 address

fc00:1:1:2::1/64

 ipv6 enable
```

يكشف ال up أداة تشكيل ال misconfiguration:

<#root>

Router#

show run interface g0/0.202

!
interface GigabitEthernet0/0.202
 encapsulation dot1Q 202
 vrf forwarding VRF202
 ip address 192.168.2.72 255.255.255.0
 ipv6 address FC00:1:1:2::2

/48

التقاط - سيناريو وظيفي

أصلح تغيير قناع الشبكة الفرعية (من /48 إلى /64) المشكلة. هذا هو التقاط CAPI في السيناريو الوظيفي.

No.	Time	Source	Destination	Protocol	Length	Info
1	2019-10-24 15:17:20.677775	fc00:1:1:1::100	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation for fc00:1:1:1::1 from 4c:4e:35:fc:fc:d8
2	2019-10-24 15:17:20.677989	fc00:1:1:1::1	fc00:1:1:1::100	ICMPv6	86	Neighbor Advertisement fc00:1:1:1::1 (rtr, sol, ovr) is at 00:be:75:f6:1d:ae
3	2019-10-24 15:17:20.678401	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	114	Echo (ping) request id=0x097e, seq=0, hop limit=64 (no response found!)
4	2019-10-24 15:17:22.674281	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	114	Echo (ping) request id=0x097e, seq=1, hop limit=64 (no response found!)
5	2019-10-24 15:17:24.674403	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	114	Echo (ping) request id=0x097e, seq=2, hop limit=64 (reply in 6)
6	2019-10-24 15:17:24.674815	fc00:1:1:2::2	fc00:1:1:1::100	ICMPv6	114	Echo (ping) reply id=0x097e, seq=2, hop limit=64 (request in 5)
7	2019-10-24 15:17:24.675242	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	114	Echo (ping) request id=0x097e, seq=3, hop limit=64 (reply in 8)
8	2019-10-24 15:17:24.675731	fc00:1:1:2::2	fc00:1:1:1::100	ICMPv6	114	Echo (ping) reply id=0x097e, seq=3, hop limit=64 (request in 7)
9	2019-10-24 15:17:24.676356	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	114	Echo (ping) request id=0x097e, seq=4, hop limit=64 (reply in 10)
10	2019-10-24 15:17:24.676753	fc00:1:1:2::2	fc00:1:1:1::100	ICMPv6	114	Echo (ping) reply id=0x097e, seq=4, hop limit=64 (request in 9)

النقطة الرئيسية:

1. يرسل الموجه رسالة طلب طلب مجاورة IPv6 التي تطلب عنوان MAC لجهاز البث (IP FC00:1:1::1).
2. ردود جدار الحماية باستخدام إعلان جار IPv6.
3. يرسل الموجه طلبات ICMP ECHO ويحصل على ردود ECHO.

محتويات CAPO:

No.	Time	Source	Destination	Protocol	Length	Info
1	2019-10-24 15:17:20.678645	fe80::2be:75ff:fe…	ff02::1:ff00:2	ICMPv6	90	Neighbor Solicitation for fc00:1:1:2::2 from 00:be:75:f6:1d:8e
2	2019-10-24 15:17:20.681818	fc00:1:1:2::2	fe80::2be:75ff:fe…	ICMPv6	90	Neighbor Advertisement fc00:1:1:2::2 (rtr, sol, ovr) is at 4c:4e:35:fc:fc:d8
3	2019-10-24 15:17:22.674342	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	118	Echo (ping) request id=0x097e, seq=1, hop limit=64 (reply in 6)
4	2019-10-24 15:17:22.677943	fc00:1:1:2::2	ff02::1:ff00:1	ICMPv6	90	Neighbor Solicitation for fc00:1:1:2::1 from 4c:4e:35:fc:fc:d8
5	2019-10-24 15:17:22.678096	fc00:1:1:2::1	fc00:1:1:2::2	ICMPv6	90	Neighbor Advertisement fc00:1:1:2::1 (rtr, sol, ovr) is at 00:be:75:f6:1d:8e
6	2019-10-24 15:17:22.678462	fc00:1:1:2::2	fc00:1:1:1::100	ICMPv6	118	Echo (ping) reply id=0x097e, seq=1, hop limit=64 (request in 3)
7	2019-10-24 15:17:24.674449	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	118	Echo (ping) request id=0x097e, seq=2, hop limit=64 (reply in 8)
8	2019-10-24 15:17:24.674785	fc00:1:1:2::2	fc00:1:1:1::100	ICMPv6	118	Echo (ping) reply id=0x097e, seq=2, hop limit=64 (request in 7)
9	2019-10-24 15:17:24.675395	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	118	Echo (ping) request id=0x097e, seq=3, hop limit=64 (reply in 10)
10	2019-10-24 15:17:24.675700	fc00:1:1:2::2	fc00:1:1:1::100	ICMPv6	118	Echo (ping) reply id=0x097e, seq=3, hop limit=64 (request in 9)
11	2019-10-24 15:17:24.676448	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	118	Echo (ping) request id=0x097e, seq=4, hop limit=64 (reply in 12)
12	2019-10-24 15:17:24.676738	fc00:1:1:2::2	fc00:1:1:1::100	ICMPv6	118	Echo (ping) reply id=0x097e, seq=4, hop limit=64 (request in 11)

النقاط الرئيسية:

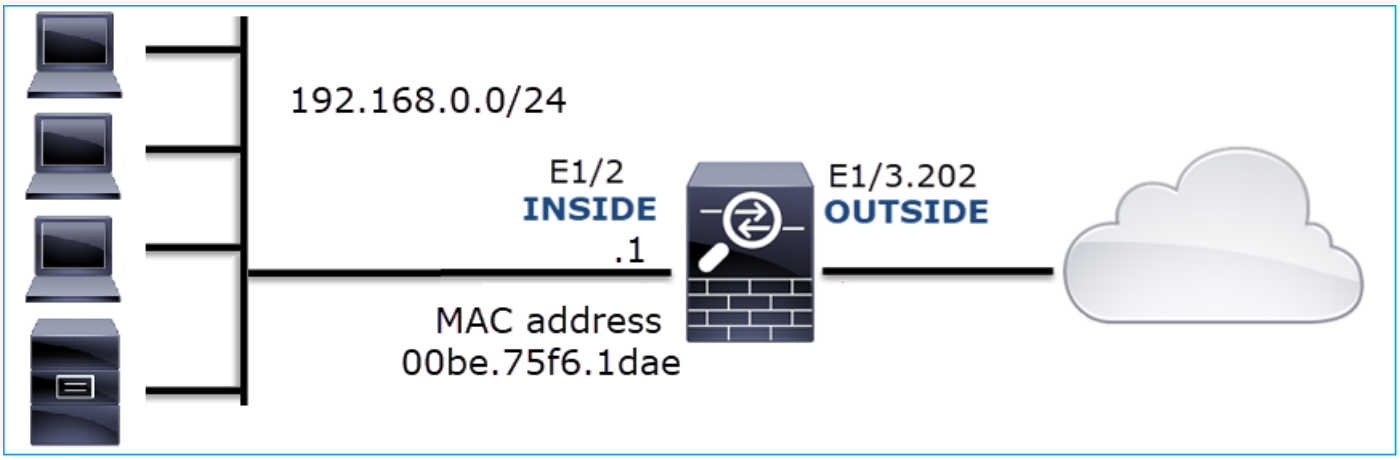
1. يرسل جدار الحماية رسالة طلب مجاورة IPv6 التي تطلب عنوان MAC لجهاز البث (IP FC00:1:1:2::2).

2. ردود جدار الحماية باستخدام إعلان جار IPv6.
3. يرسل جدار الحماية طلب ICMP Echo.
4. يرسل الموجه رسالة طلب طلب مجاورة IPv6 التي تطلب عنوان MAC لجهاز تدفق البيانات من الخادم (IP FC00:1:1::1).
5. ردود جدار الحماية باستخدام إعلان جار IPv6.
6. يرسل جدار الحماية طلبات ICMP ECHO ويحصل على ردود ECHO.

الحالة 12. مشكلة التوصيل المتقطع (تسميم ARP)

وصف المشكلة: تواجه الأجهزة المضيفة الداخلية (192.168.0.x/24) مشاكل اتصال متقطعة مع الأجهزة المضيفة في الشبكة الفرعية نفسها

تعرض هذه الصورة المخطط:



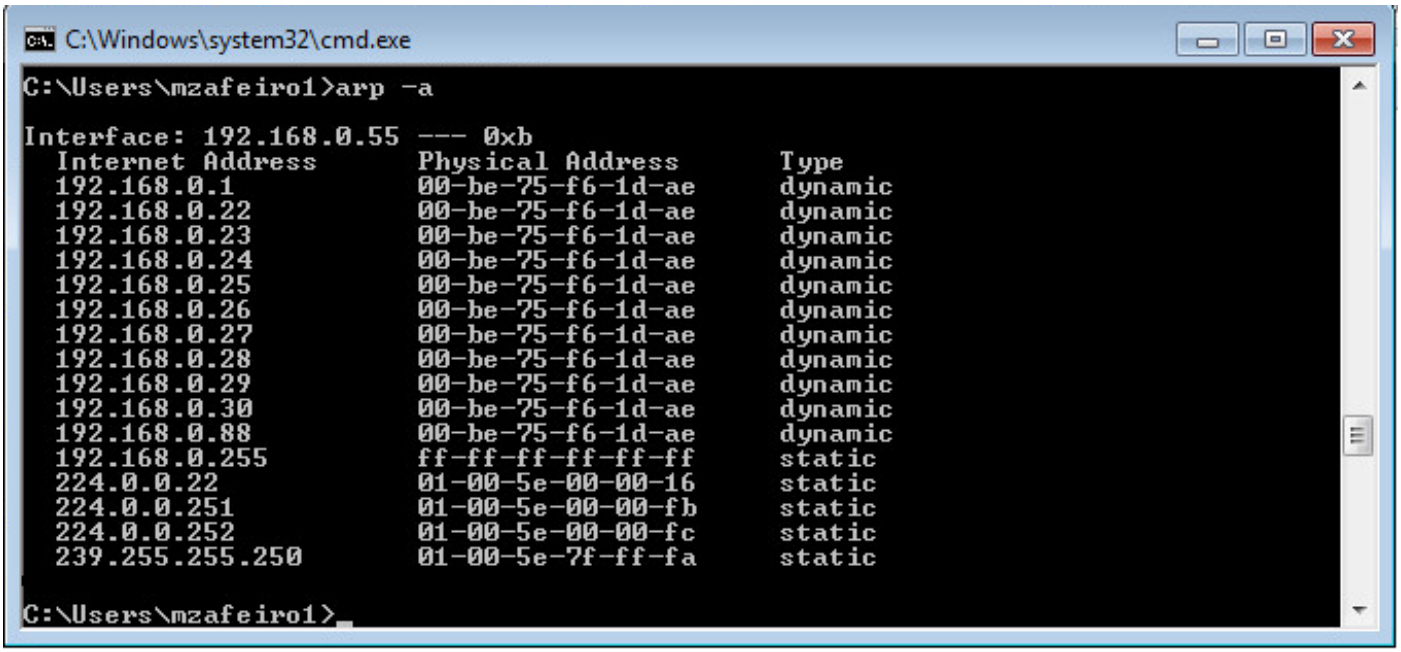
التدفق المتأثر:

SRC IP: 192,168,0,x/24

بروتوكول DST IP: 192,168,0,x/24

البروتوكول: أي

يبدو أن ذاكرة تخزين ARP المؤقت لمضيف داخلي قد تم تسميمها:



تحليل أسر

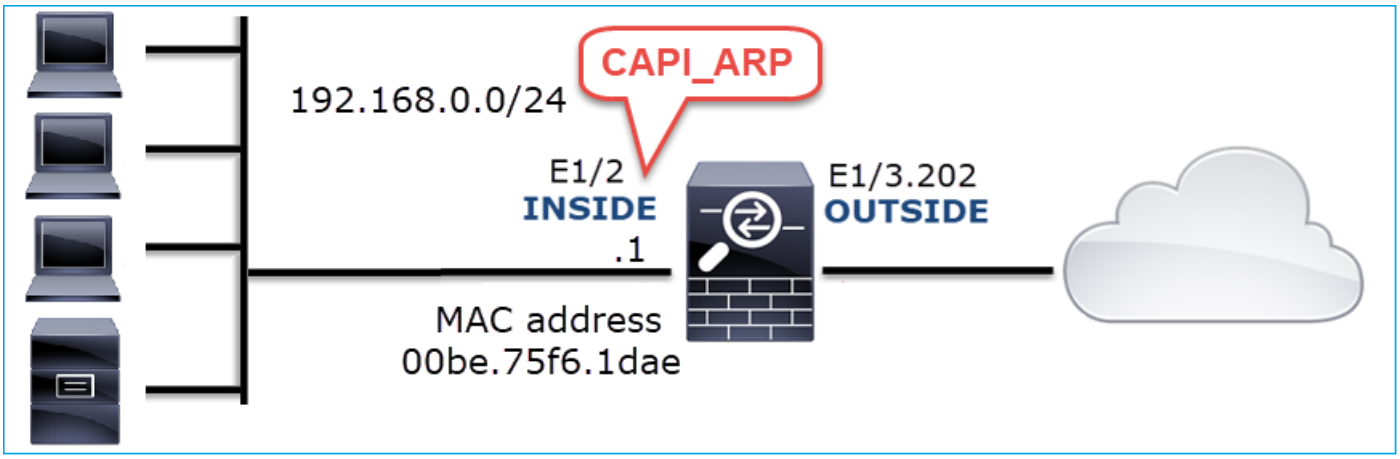
تمكين التقاط عل محرك FTD LINA

عل قبض هذا التقاط حزم ARP فقط عل الواجهة الداخلية:

<#root>

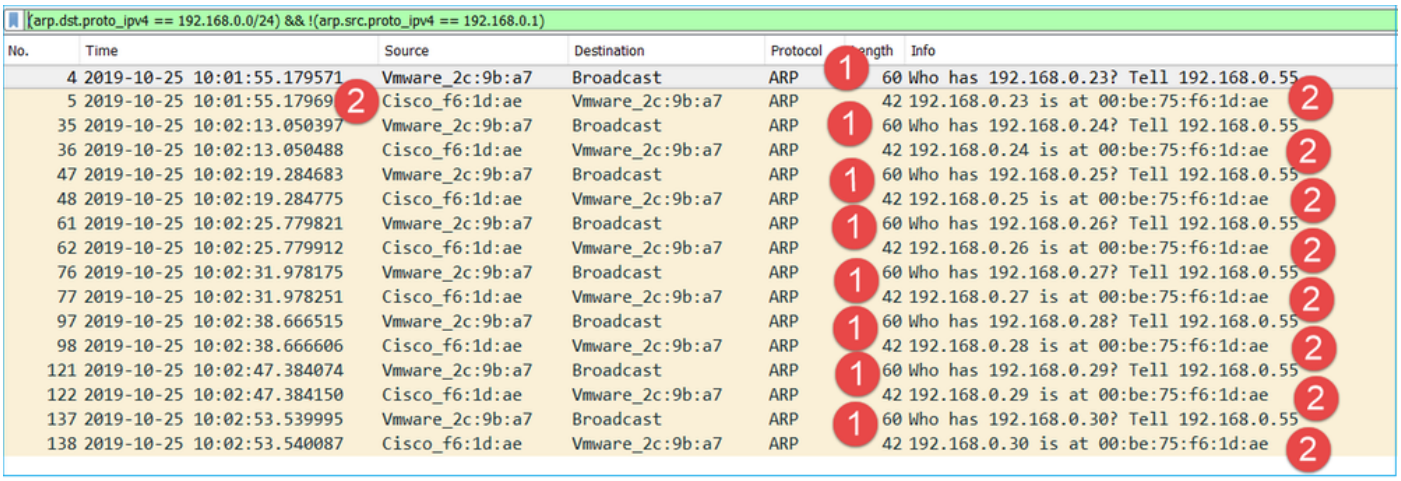
firepower#

capture CAPI_ARP interface INSIDE ethernet-type arp



التقاط - سيناريو ال يعمل:

يحتوي االلتقاط عل واجهة جدار الحماية INSIDE.



النقاط الرئيسية:

1. يتلقى جدار الحماية طلبات ARP مختلفة من أجل IPs ضمن شبكة 192.168.0.x/24
2. يستجيب جدار الحماية إلى كل هذه العناوين (proxy-arp) باستخدام عنوان MAC الخاص به

الإجراءات الموصى بها

والغرض من الإجراءات الواردة في هذا القسم هو زيادة تضييق نطاق هذه المسألة.

إجراء 1. تحقق من تكوين NAT.

فيما يتعلق بتكوين NAT، هناك حالات يمكن فيها للكلمة الأساسية no-proxy-arp منع السلوك السابق:

```
<#root>

firepower#

show run nat

nat (INSIDE,OUTSIDE) source static NET_1.1.1.0 NET_2.2.2.0 destination static NET_192.168.0.0 NET_4.4.4

no-proxy-arp
```

الإجراء 2. تعطيل وظيفة ARP للوكيل على واجهة جدار الحماية.

إذا لم تحل الكلمة الأساسية "no-proxy-arp" المشكلة، فحاول تعطيل ARP للوكيل على الواجهة نفسها. في حالة وجود FTD، يجب عليك في وقت هذه الكتابة إستخدام FlexConfig ونشر الأمر (تحديد اسم الواجهة المناسب).

```
sysopt noproxyarp INSIDE
```

الحالة 13. التعرف على معرفات كائن SNMP (OIDs) التي تتسبب في ظهور وحدة المعالجة المركزية (CPU) أخطاء

توضح هذه الحالة كيفية تحديد بعض معرفات SNMP لعملية التحقق من الذاكرة على أنها السبب الرئيسي لأخطاء وحدة المعالجة المركزية (إصدار الأداة) استنادا إلى تحليل مجموعات SNMP الإصدار 3 (SNMPv3).

وصف المشكلة: زيادة التجاوزات على واجهات البيانات بشكل مستمر. كما كشفت أبحاث أخرى عن وجود أيضا أخطاء وحدة المعالجة المركزية (الناجمة عن عملية SNMP) التي تعد السبب الرئيسي لتجاوزات الواجهة.

كانت الخطوة التالية في عملية أستكشاف الأخطاء وإصلاحها هي تحديد السبب الجذري لأخطاء وحدة المعالجة المركزية (CPU) التي تتسبب فيها عملية SNMP، وعلى وجه الخصوص، تضييق نطاق المشكلة لتحديد معرفات كائن SNMP (OID) التي يمكن أن ينتج عنها، عندما يتم استقطابها، أخطاء وحدة المعالجة المركزية.

حاليا، لا يوفر محرك FTD LINA أمر "show" لمعرفة SNMP OIDs الذي يتم تلقيحه في الوقت الفعلي.

يمكن إستيراد قائمة SNMP OIDs الخاصة بالقارئ من أداة مراقبة SNMP، ومع ذلك، في هذه الحالة، كانت هناك هذه العوامل الوقائية:

- لم يتمكن مسؤول FTD من الوصول إلى أداة مراقبة SNMP
- تم تكوين الإصدار 3 من SNMP مع المصادقة وتشفير البيانات للخصوصية على FTD

تحليل أسر

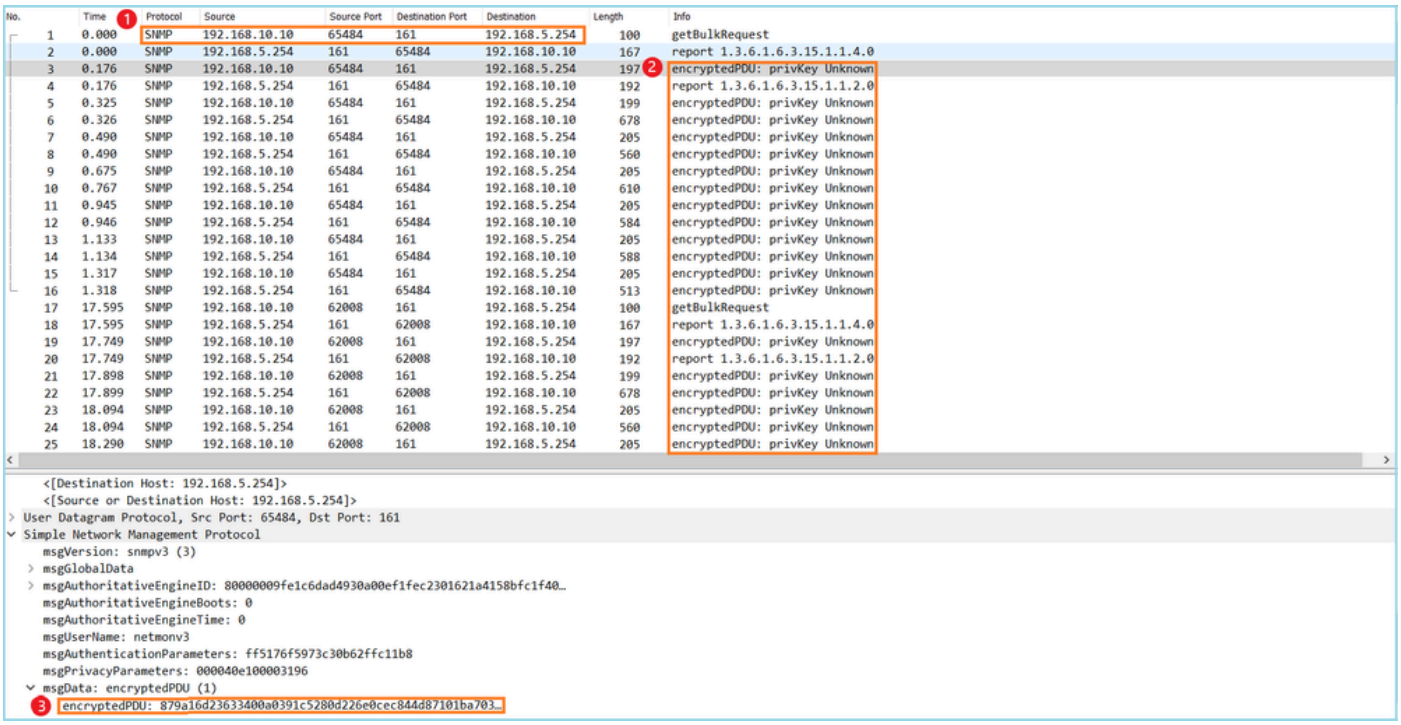
بما أن مسؤول FTD كان لديه بيانات اعتماد لمصادقة SNMP الإصدار 3 وتشفير البيانات، تم اقتراح خطة العمل هذه:

1. التقاط حزم SNMP
2. احفظ الالتقاط واستخدم تفضيلات بروتوكول SNMP الخاص ب Wireshark لتحديد بيانات اعتماد الإصدار 3 من SNMP لفك تشفير حزم SNMP الإصدار 3. يتم إستخدام عمليات الالتقاط التي تم فك تشفيرها لتحليل معرفات SNMP المادية واسترجاعها

تكوين التقاط حزم SNMP على الواجهة التي يتم إستخدامها في تكوين مضيف خادم snmp:

```
<#root>

firepower#

show run snmp-server  | include host

snmp-server host management 192.168.10.10 version 3 netmonv3


firepower#

show ip address management
```

```
System IP Address:
Interface                  Name                 IP address      Subnet mask      Method
Management0/0              management           192.168.5.254   255.255.255.0    CONFIG
Current IP Address:
Interface                  Name                 IP address      Subnet mask      Method
Management0/0              management           192.168.5.254   255.255.255.0    CONFIG

firepower#

capture capsnmp interface management buffer 10000000 match udp host 192.168.10.10  host 192.168.5.254 eq

firepower#

show capture capsnmp

capture capsnmp type raw-data buffer 10000000 interface outside [Capturing -

9512

 bytes]
  match udp host 192.168.10.10  host 192.168.5.254 eq snmp
```



النقاط الرئيسية:

1. منفذ/عنوان مصدر SNMP والوجهة.
2. تعذر فك ترميز وحدة بيانات بروتوكول SNMP لأن privKey غير معروف لـ Wireshark.
3. قيمة EncryptedPDU الأولية.

الإجراءات الموصى بها

والغرض من الإجراءات الواردة في هذا القرع هو زيادة تضييق نطاق هذه المسألة.

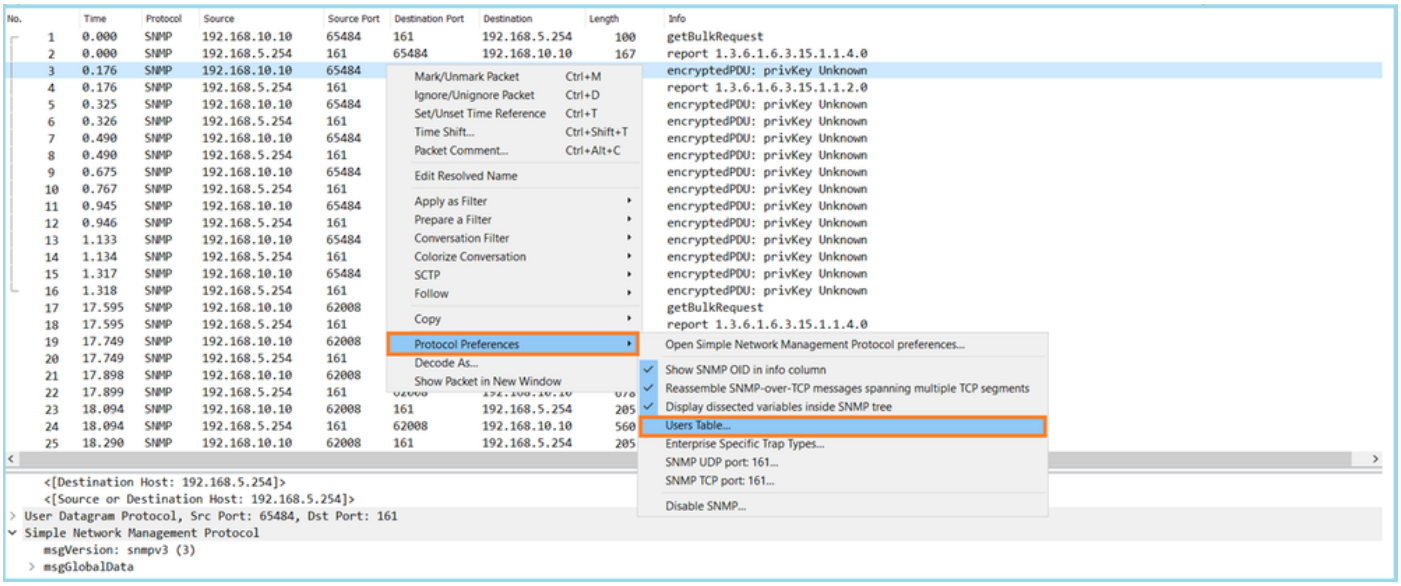
الإجراء 1. فك تشفير التقاط SNMP.

احفظ الالتقاط وحرر تفضيلات بروتوكول SNMP الخاص ب Wireshark لتحديد بيانات اعتماد الإصدار 3 من SNMP لفك تشفير الحزم.

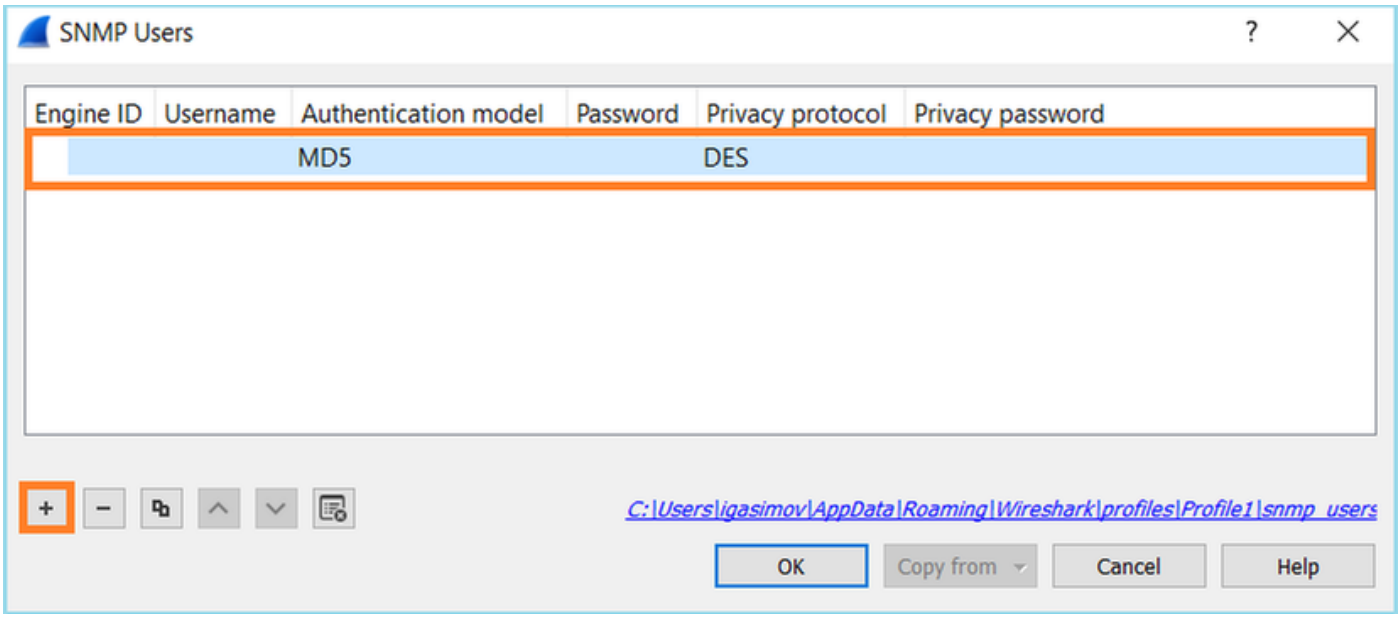
<#root>

```
firepower#

copy /pcap capture: tftp:


Source capture name [capsnmp]?

Address or name of remote host []? 192.168.10.253

Destination filename [capsnmp]? capsnmp.pcap

!!!!!!
64 packets copied in 0.40 secs
```

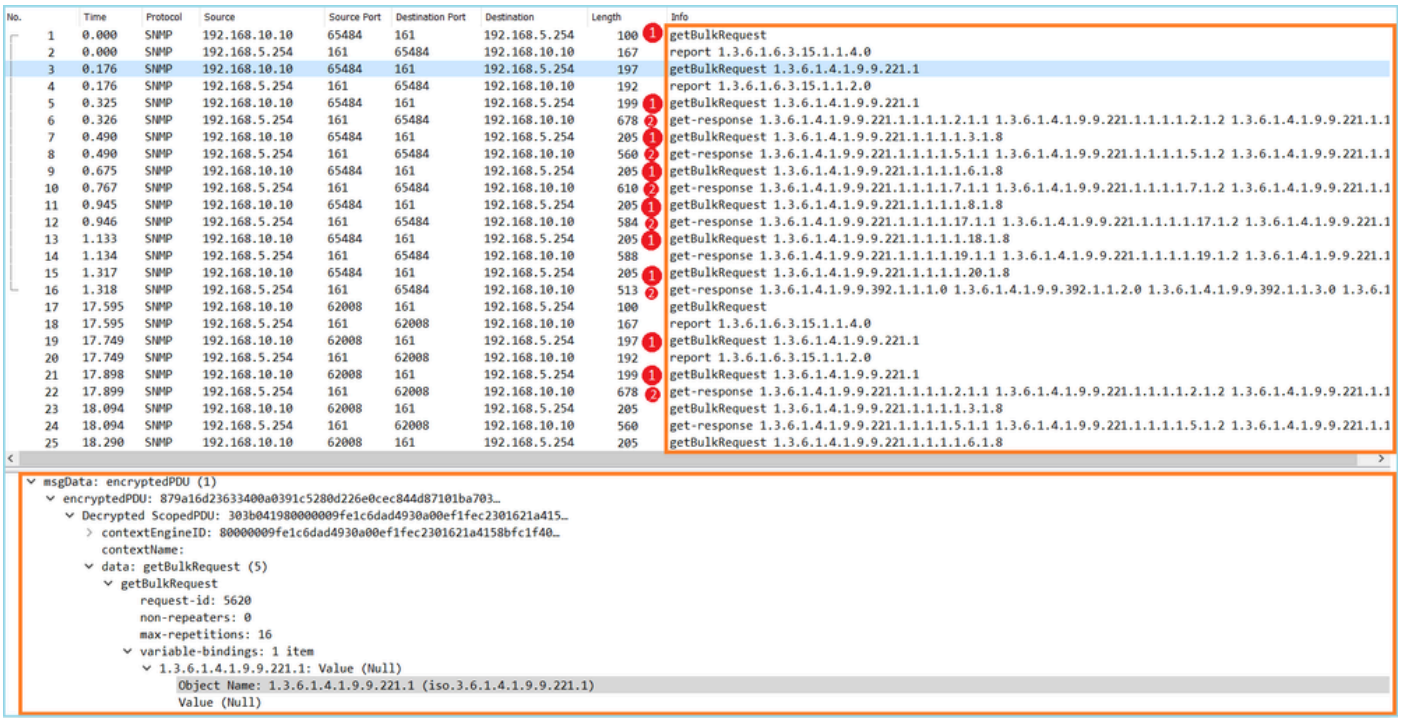
افتح ملف الالتقاط على Wireshark، حدد حزمة SNMP وتصفح إلى تفضيلات البروتوكول > جدول المستخدمين، كما هو موضح في الصورة:



في جدول مستخدمي SNMP، تم تحديد اسم مستخدم الإصدار 3 من SNMP ونموذج المصادقة وكلمة مرور المصادقة وبروتوكول الخصوصية وكلمة مرور الخصوصية (لا يتم عرض بيانات الاعتماد الفعلية أدناه):



بمجرد تطبيق إعدادات مستخدمي SNMP، قام Wireshark بعرض وحدات بيانات بروتوكول SNMP (PDU) التي تم فك تشفيرها:

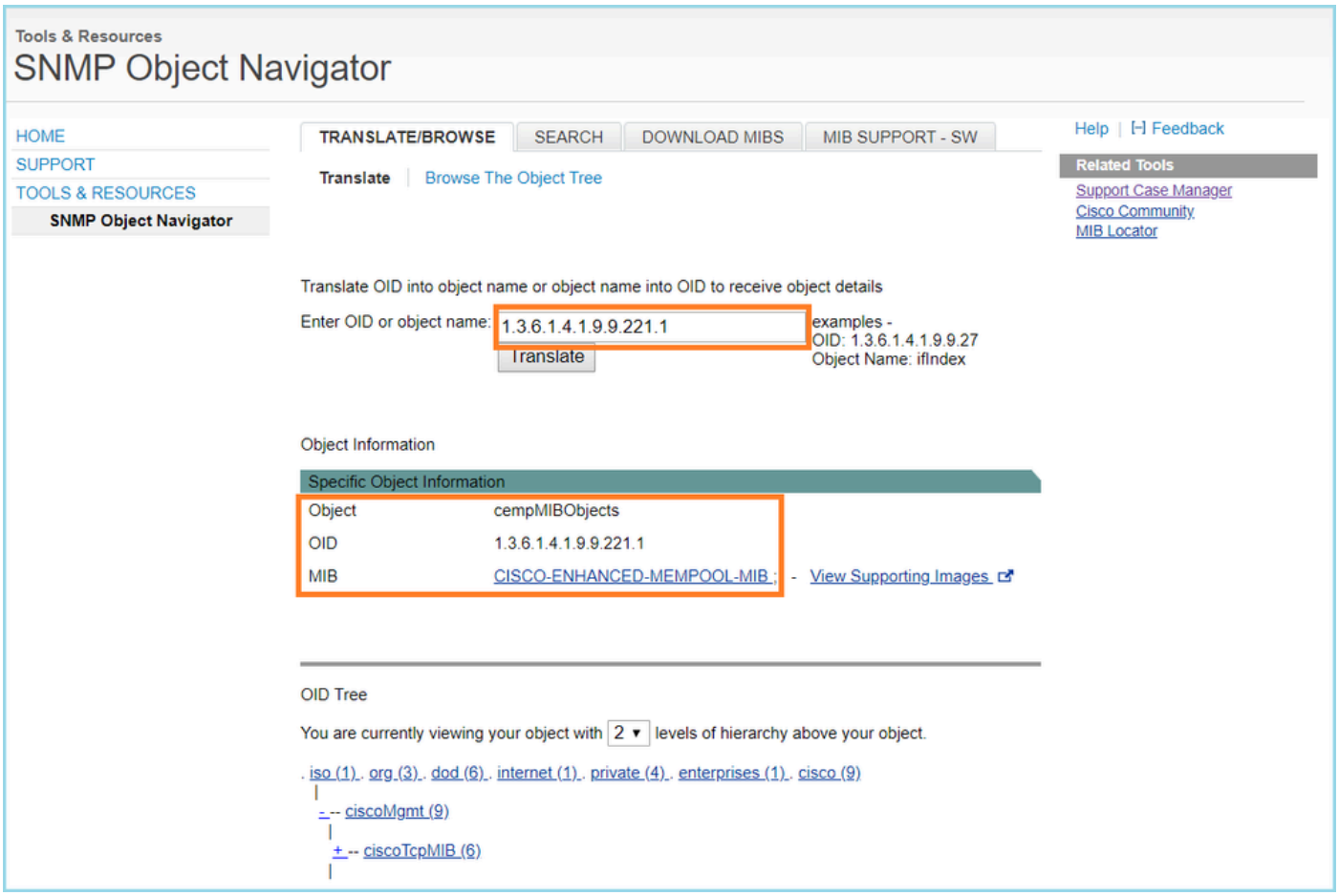


النقاط الرئيسية:

1. تستخدم أدوات مراقبة SNMP SNMP GetBulkRequest للاستعلام والتنقل عبر OID الأصل 1.3.6.1.4.1.9.9.221.1 ومعرفات OID ذات الصلة.
2. استجاب FTD لكل GetBulkRequest مع get-response الذي يحتوي على OIDs المتعلقة ب 1.3.6.1.4.1.9.9.221.1.

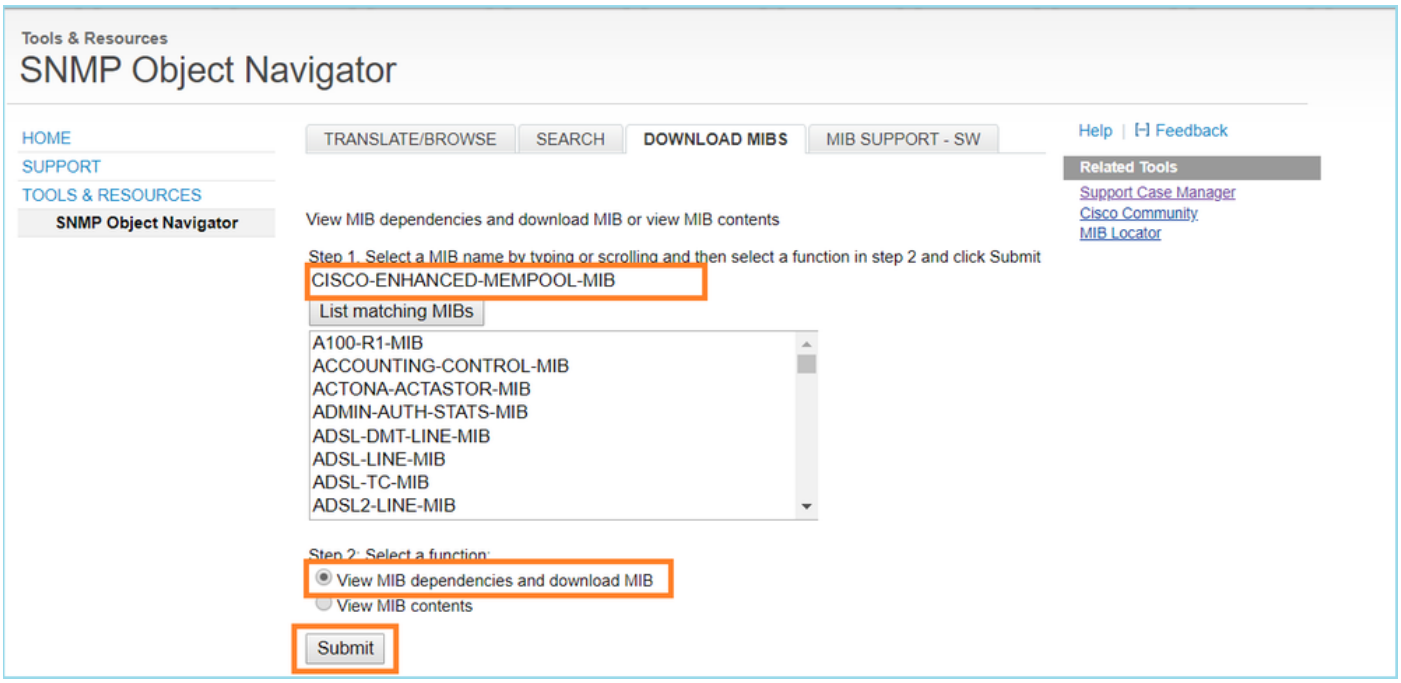
الإجراء 2. التعرف على معرفات SNMP OIDs.

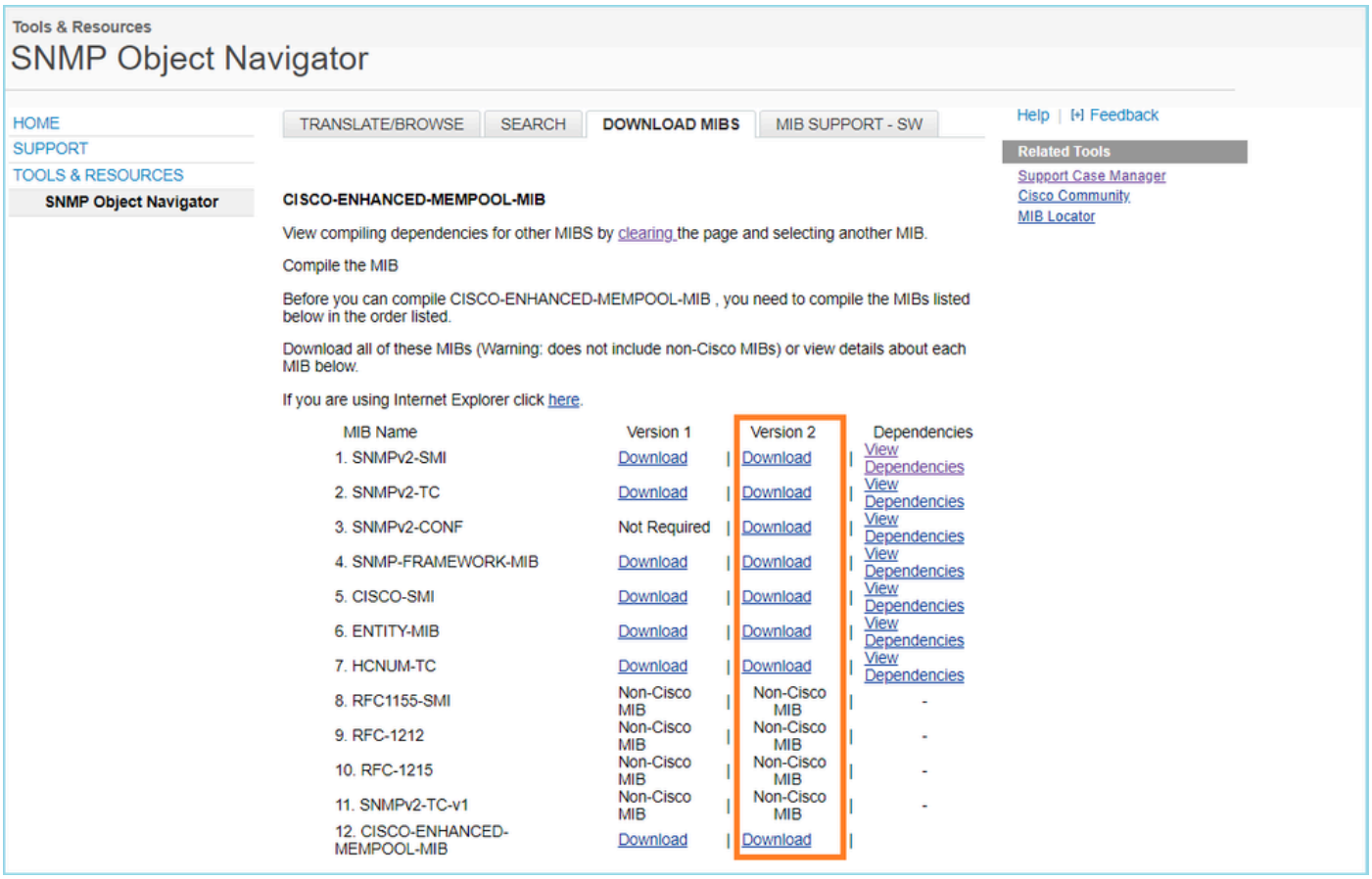
أظهر متصفح كائن SNMP أن OID 1.3.6.1.4.1.9.221.1 ينتمي إلى قاعدة معلومات الإدارة (MIB) المسماة Cisco-Enhanced-MEMPOOL-MIB، كما هو موضح في الصورة:



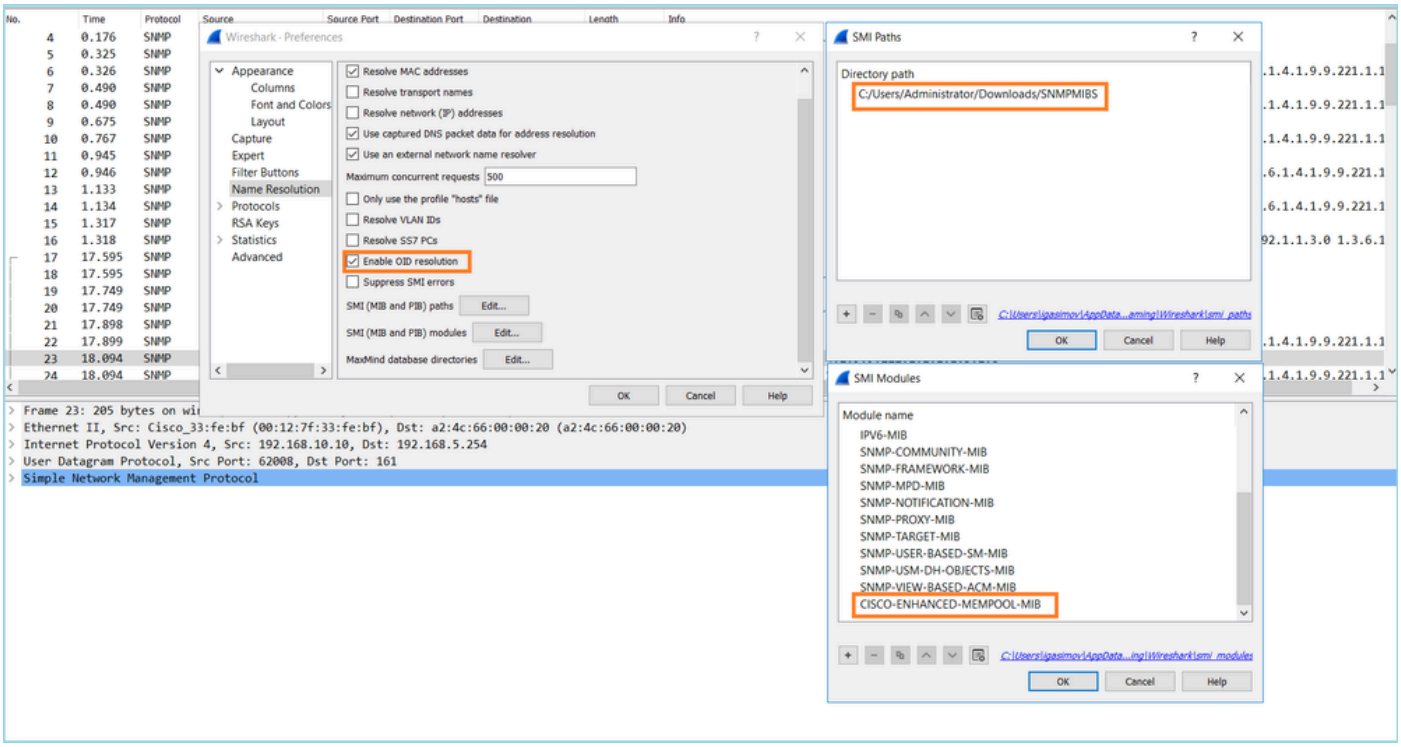
لعرض OIDs بتنسيق يمكن قراءته من قبل الإنسان في Wireshark:

1. تنزيل قاعدة معلومات الإدارة (MIB) من Cisco-Enhanced-Mempool-MIB وتبعياتها، كما هو موضح في الصورة:

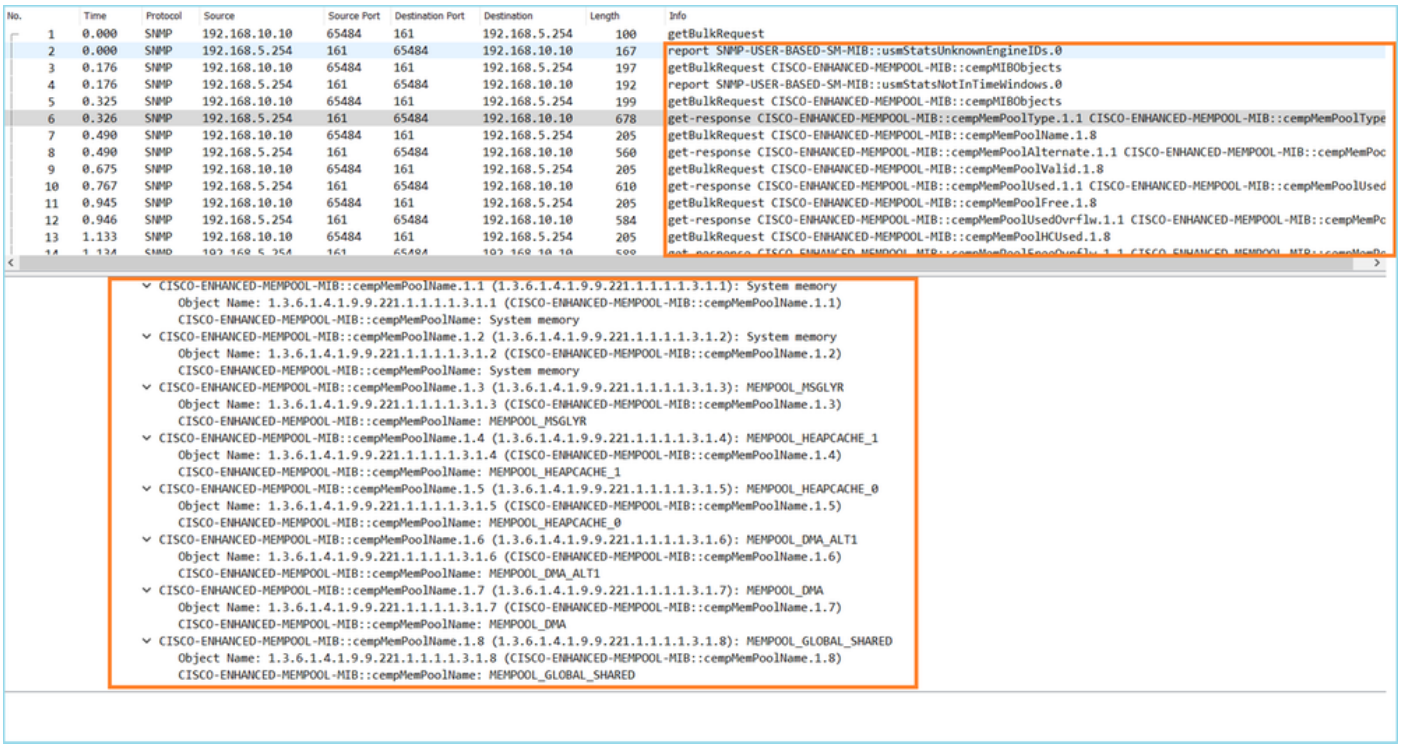




2. في Wireshark في Edit (تحرير) > Preferences > Name Resolution (تحليل الاسم) نافذة تمكين دقة OID يتم تحديدها. في SMI (مسارات MIB و PIB) يحدد الإطار المجلد باستخدام قواعد معلومات الإدارة (MIB) التي تم تنزيلها وفي SMI (وحدات MIB و PIB). تتم إضافة Cisco-Enhanced-Mempool-MIB تلقائيا إلى قائمة الوحدات النمطية:



3. بمجرد إعادة تشغيل Wireshark، يتم تنشيط دقة OID:



استنادا إلى الإخراج الذي تم فك تشفيره لملف الالتقاط، كانت أداة مراقبة SNMP تقوم بشكل دوري (افصل 10 ثوان) بفحص بيانات إستخدام تجمعات الذاكرة على FTD. كما هو موضح في مقالة TechNote [قارنة ASA SNMP للإحصائيات المتعلقة بالذاكرة](#)، ومسح إستخدام التجمع المشترك العالمي (GSP) باستخدام SNMP ينتج عنه إستخدام وحدة المعالجة المركزية (CPU) بشكل كبير. في هذه الحالة من Capture (التقاط)، كان من الواضح أن قد تم فحص إستخدام "التجمع المشترك العالمي" بشكل دوري كجزء من GetBulkRequest الأولي ل SNMP.

من أجل تقليل أخطاء وحدة المعالجة المركزية (CPU) التي تتسبب فيها عملية SNMP، تمت التوصية باتباع خطوات التخفيف لأخطاء وحدة المعالجة المركزية لبروتوكول SNMP المشار إليها في المقالة وتجنب إستطلاع معرفات العمالء المرتبطة بنظام GSP. بدون إستطلاع عبر بروتوكول SNMP لمعرف فئة المورد (OIDs) المرتبط بمعيار GSP، لم يتم مالحظة أية أخطاء لوحدة المعالجة المركزية الناتجة عن عملية بروتوكول SNMP، كما انخفض معدل التجاوز بشكل ملحوظ.

معلومات ذات صلة

- [أدلة تكوين مركز إدارة FireSIGHT التابع لشركة Cisco](#)
- [توضيح إجراءات قواعد سياسة التحكم في الوصول إلى برنامج Firepower Threat Defense](#)
- [العمل مع مجموعات الدفاع ضد تهديد FirePOWER وتتبع الحزم](#)
- [تعلم Wireshark](#)

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).