إستخدام ASDM لإدارة وحدة FirePOWER النمطية على ASA

المحتويات

المقدمة

يوضح هذا المستند كيفية اتصال برنامج ASDM بجهاز الأمان القابل للتكيف (ASA) ووحدة برنامج FirePOWER مثبتة عليه.

معلومات أساسية

يمكن إدارة وحدة FirePOWER التي تم تثبيتها على ASA إما:

- مركز إدارة Firepower (FMC) - هذا هو حل الإدارة بمجرد إخراجه من عبوته.
- مدير أجهزة حلول الأمان المعدلة (ASDM) - هذا هو حل الإدارة المتوفر في المربع.

المتطلبات الأساسية

المتطلبات

تكوين ASA لتمكين إدارة ASDM:

```
<#root>

ASA5525(config)#

interface GigabitEthernet0/0
```

```
ASA5525(config-if)#
nameif INSIDE
ASA5525(config-if)#
security-level 100
ASA5525(config-if)#
ip address 192.168.75.23 255.255.255.0
ASA5525(config-if)#
no shutdown
ASA5525(config)#
ASA5525(config)#
http server enable
ASA5525(config)#
http 192.168.75.0 255.255.255.0 INSIDE
ASA5525(config)#
asdm image disk0:/asdm-762150.bin
ASA5525(config)#
ASA5525(config)#
 aaa authentication http console LOCAL
ASA5525(config)#
 username cisco password cisco
```

تحقق من التوافق بين وحدة ASA/SFR النمطية، وإلا فلن يتم عرض علامات تبويب FirePOWER.

بالإضافة إلى ذلك، يجب تمكين ترخيص 3DES/AES في ASA:

```
<#root>
ASA5525#
show version | in 3DES
Encryption-3DES-AES
                :
Enabled
 perpetual
```

تأكد من أن نظام عميل ASDM لإصدار مدعوم من Java JRE.

المكونات المستخدمة

- جهاز مضيف لنظام التشغيل Microsoft Windows 7
- ASA5525-X الذي يشغل ASA، الإصدار 9.6(2.3)
- ASDM، الإصدار 7.6.2.150
- وحدة برنامج FirePOWER 6.1.0-330

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.

عامة

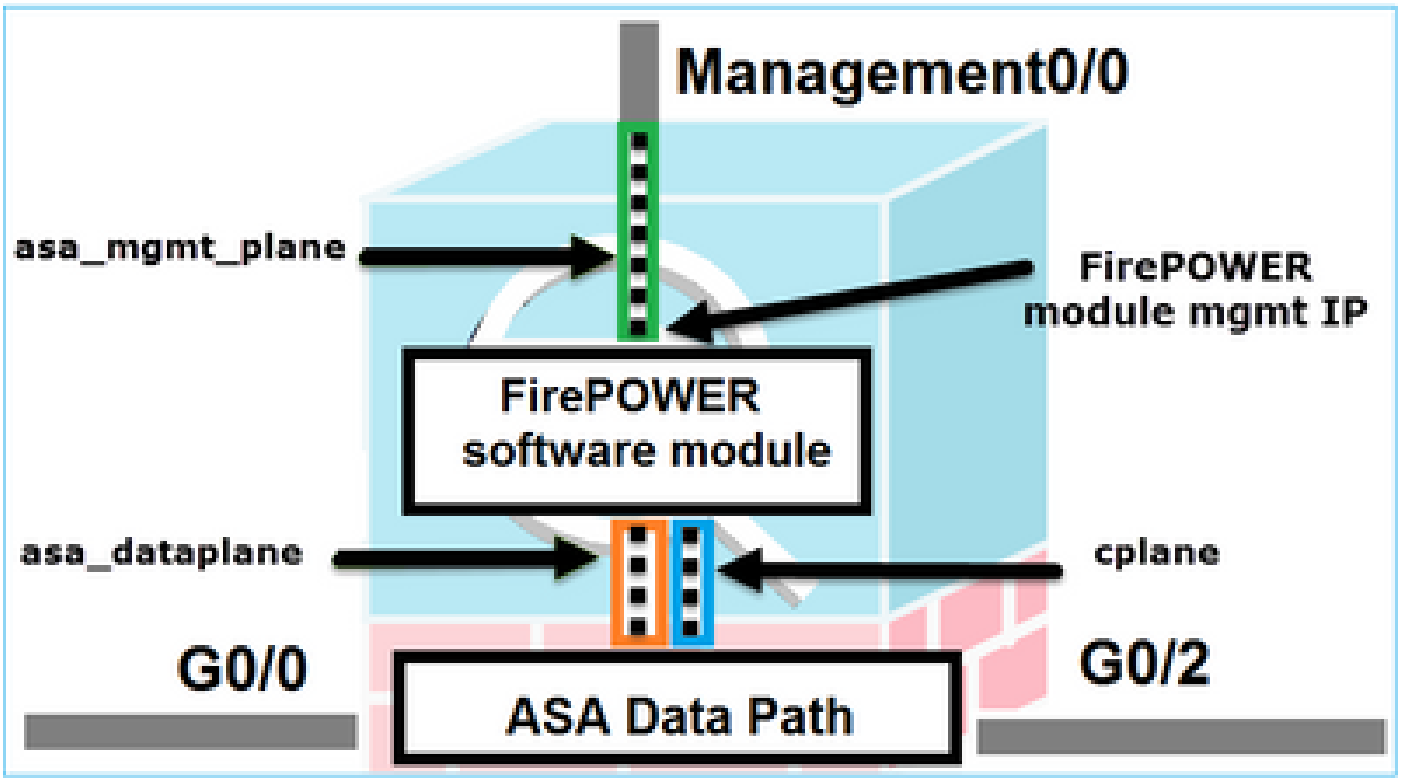
يحتوي ASA على ثلاث واجهات داخلية:

- ASA_DATAPLANE - يتم إستخدامه لإعادة توجيه الحزم من مسار بيانات ASA إلى الوحدة النمطية لبرنامج FirePOWER.
- asa_mgmt_plane - يتم إستخدامه للسماح لواجهة إدارة FirePOWER بالاتصال بالشبكة.
- cplane - واجهة مستوى التحكم التي يتم إستخدامها لنقل رسائل keepalive بين ASA والوحدة النمطية FirePOWER.

أنت يستطيع على قبض حركة مرور في كل قارن داخلي:

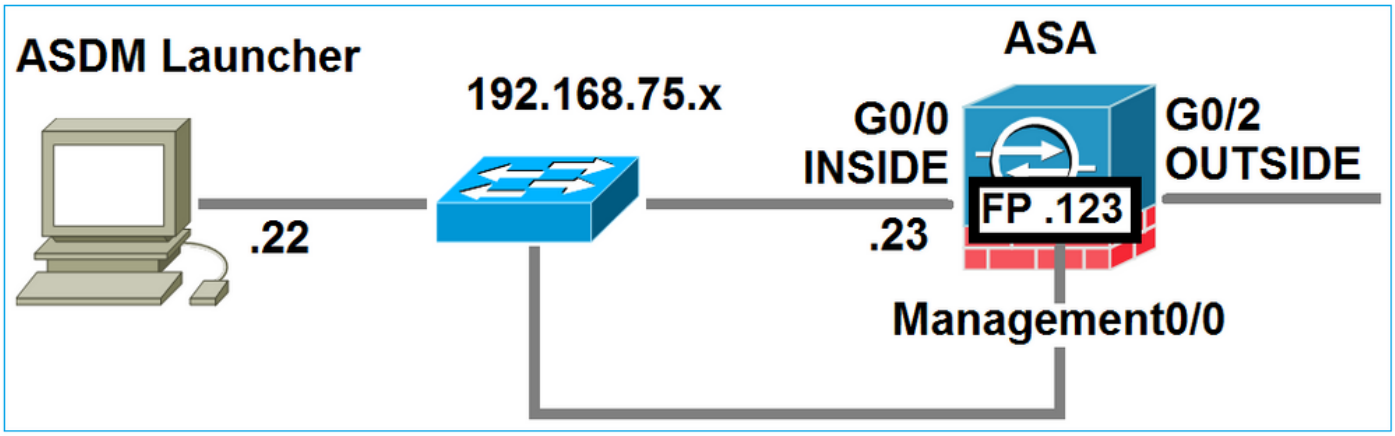
```
<#root>

ASA5525#

capture CAP interface ?


  asa_dataplane   Capture packets on dataplane interface
  asa_mgmt_plane  Capture packets on managementplane interface
  cplane          Capture packets on controlplane interface
```

ويمكن تصور ذلك على النحو التالي:



عملية في الخلفية عند اتصال مستخدم ب ASA عبر ASDM

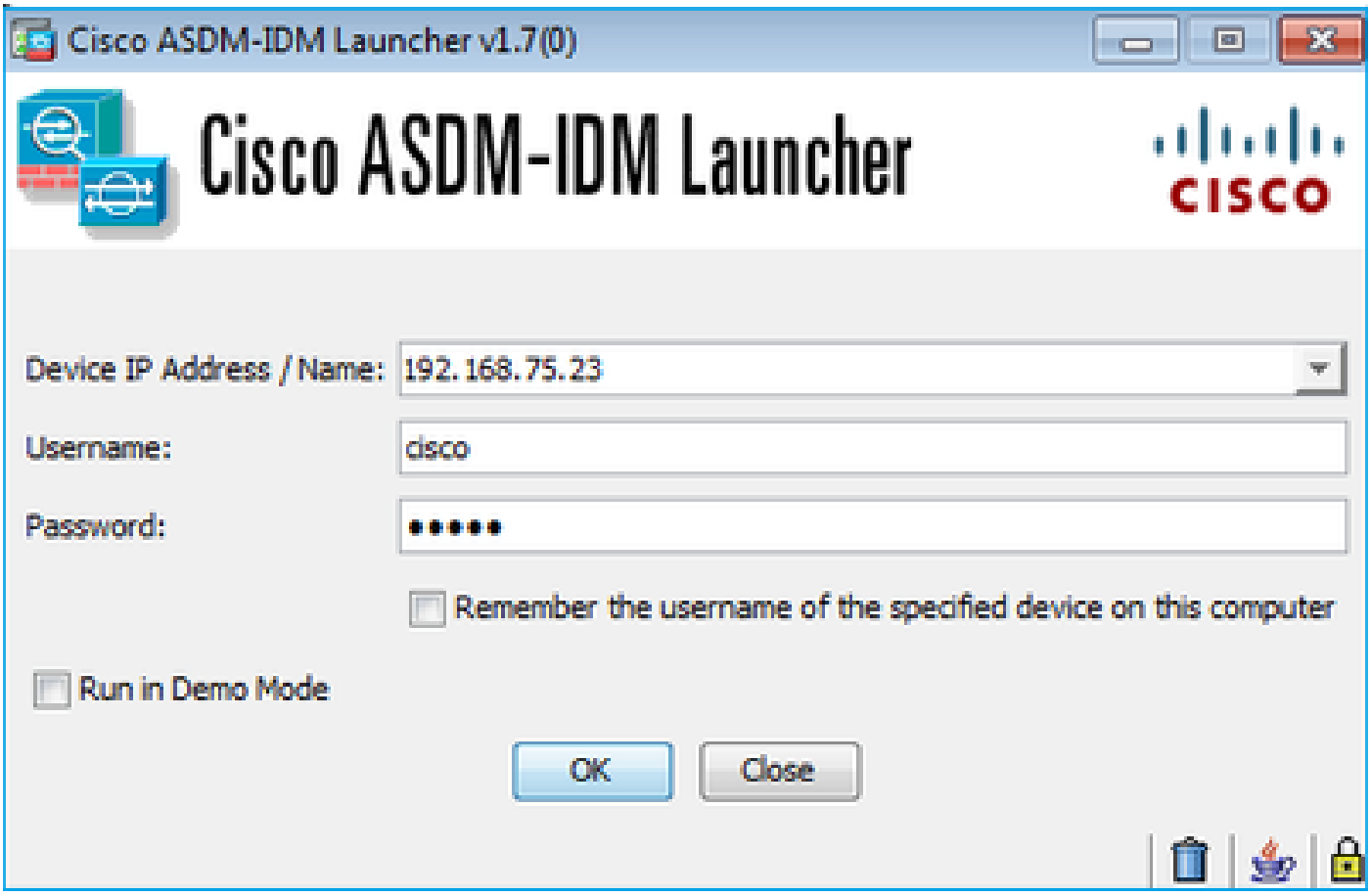
خذ بعين الاعتبار هذا الهيكل:



عندما يقوم المستخدم بتهيئة اتصال ASDM ب ASA، تحدث هذه الأحداث:

الخطوة 1 - يبدأ المستخدم اتصال ASDM

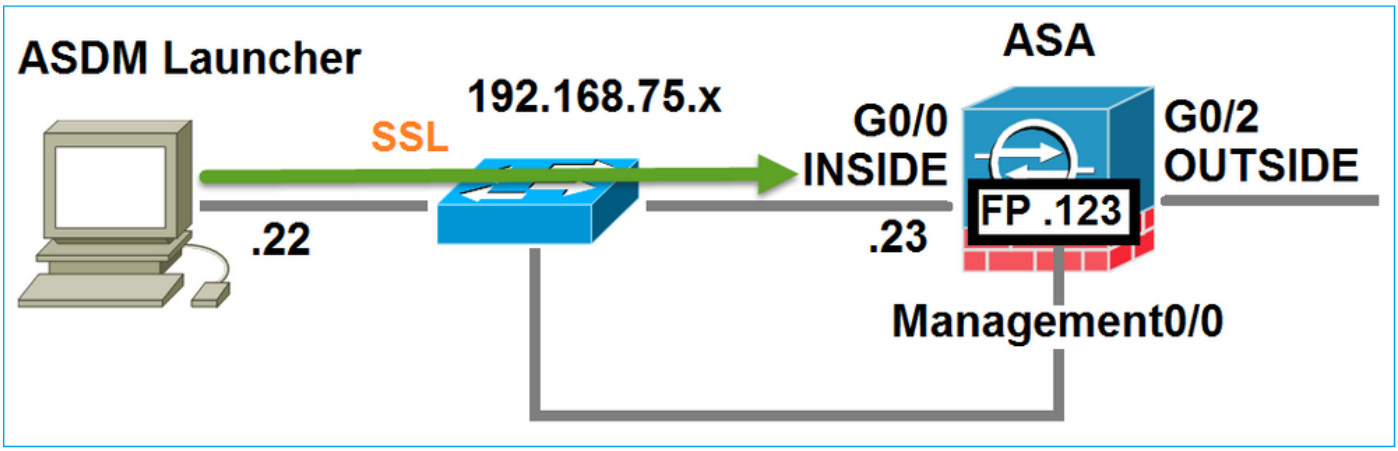
يحدد المستخدم عنوان ASA IP المستخدم لإدارة HTTP، ويدخل بيانات الاعتماد، ويبدأ التوصيل نحو ASA:



في الخلفية، يتم إنشاء نفق SSL بين ASDM و ASA:

Source	Destination	Protocol	Length	Data	Info
192.168.75.22	192.168.75.23	TLSv1.2	252		Client Hello

ويمكن تصور ذلك على النحو التالي:



الخطوة 2 - يكتشف ASDM تكوين ASA وعنوان IP لوحدة FirePOWER النمطية

أدخل الأمر debug http 255 على ASA لعرض جميع التحققات التي يتم إجراؤها في الخلفية عند اتصال ASDM ب ASA:

```
<#root>
ASA5525#

debug http 255

…
HTTP: processing ASDM request [/admin/exec/

show+module

] with cookie-based authentication
HTTP: processing GET URL '/admin/exec/show+module' from host 192.168.75.22
HTTP: processing ASDM request [/admin/exec/show+cluster+interface-mode] with cookie-based authenticatio
HTTP: processing GET URL '/admin/exec/show+cluster+interface-mode' from host 192.168.75.22
HTTP: processing ASDM request [/admin/exec/show+cluster+info] with cookie-based authentication
HTTP: processing GET URL '/admin/exec/show+cluster+info' from host 192.168.75.22
HTTP: processing ASDM request [/admin/exec/s

how+module+sfr+details

] with cookie-based authentication
HTTP: processing GET URL '/admin/exec/show+module+sfr+details' from host 192.168.75.22
```

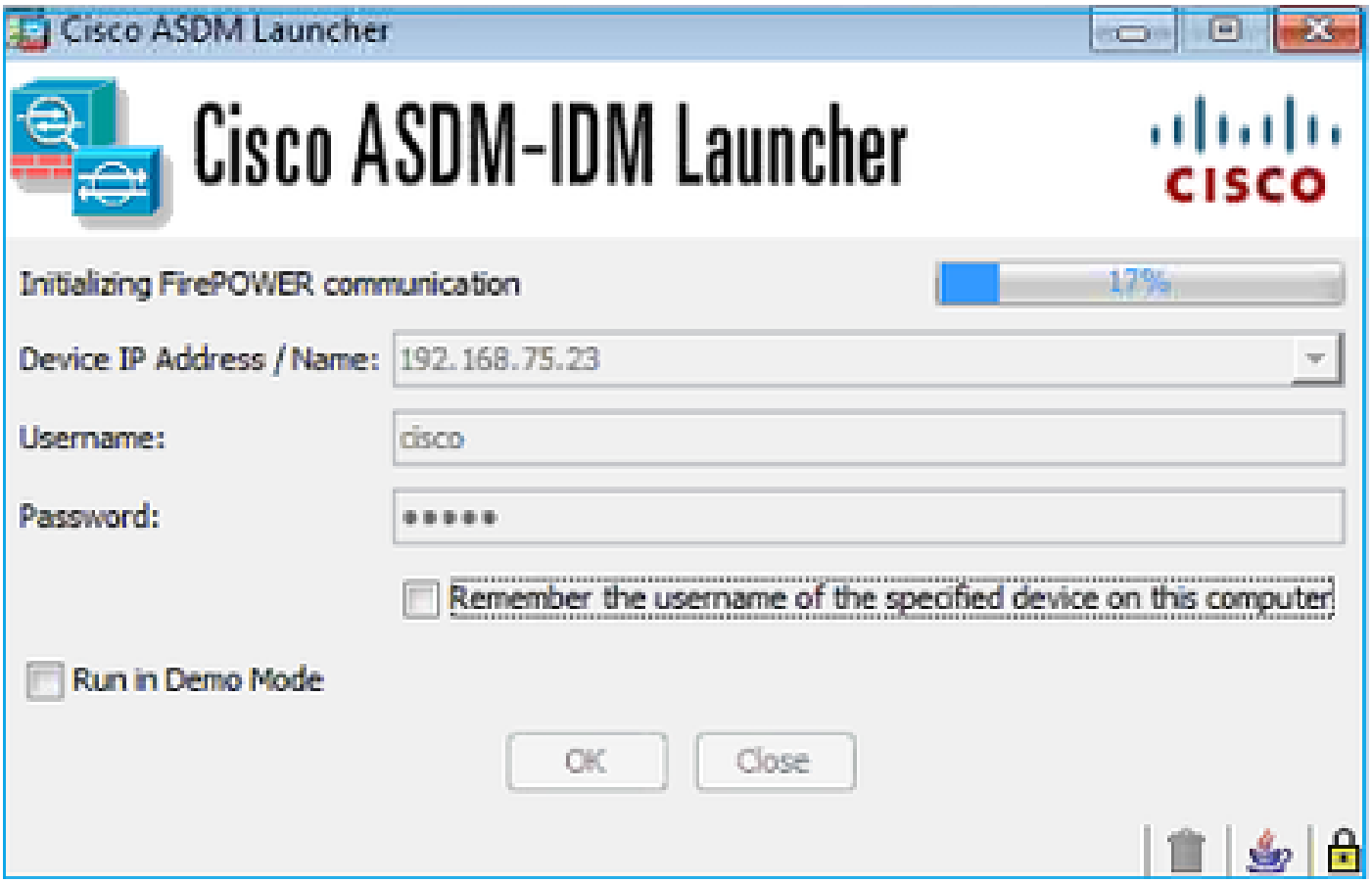
- show module - يكتشف ASDM وحدات ASA النمطية.
- show module sfr details - يكتشف ASDM تفاصيل الوحدة النمطية، والتي تتضمن عنوان IP الخاص بإدارة FirePOWER.

وتتم ملاحظة ذلك في الخلفية كسلسلة من إتصالات SSL من الكمبيوتر الشخصي نحو عنوان IP ل ASA:

Source	Destination	Protocol	Length	Data	Info
192.168.75.22	192.168.75.23	TLSv1.2	252		Client Hello
192.168.75.22	192.168.75.23	TLSv1.2	284		Client Hello
192.168.75.22	192.168.75.23	TLSv1.2	284		Client Hello
192.168.75.22	192.168.75.23	TLSv1.2	284		Client Hello
192.168.75.22	192.168.75.23	TLSv1.2	284		Client Hello
192.168.75.22	192.168.75.23	TLSv1.2	284		Client Hello
192.168.75.22	192.168.75.23	TLSv1.2	284		Client Hello
192.168.75.22	192.168.75.23	TLSv1.2	284		Client Hello
192.168.75.22	192.168.75.23	TLSv1.2	284		Client Hello
192.168.75.22	192.168.75.23	TLSv1.2	284		Client Hello
192.168.75.22	192.168.75.23	TLSv1.2	284		Client Hello
192.168.75.22	192.168.75.23	TLSv1.2	284		Client Hello
192.168.75.22	192.168.75.123	TLSv1.2	252		Client Hello
192.168.75.22	192.168.75.23	TLSv1.2	284		Client Hello
192.168.75.22	192.168.75.123	TLSv1.2	220		Client Hello
192.168.75.22	192.168.75.23	TLSv1.2	284		Client Hello

الخطوة 3 - يقوم ASDM ببدء الاتصال نحو الوحدة النمطية FirePOWER

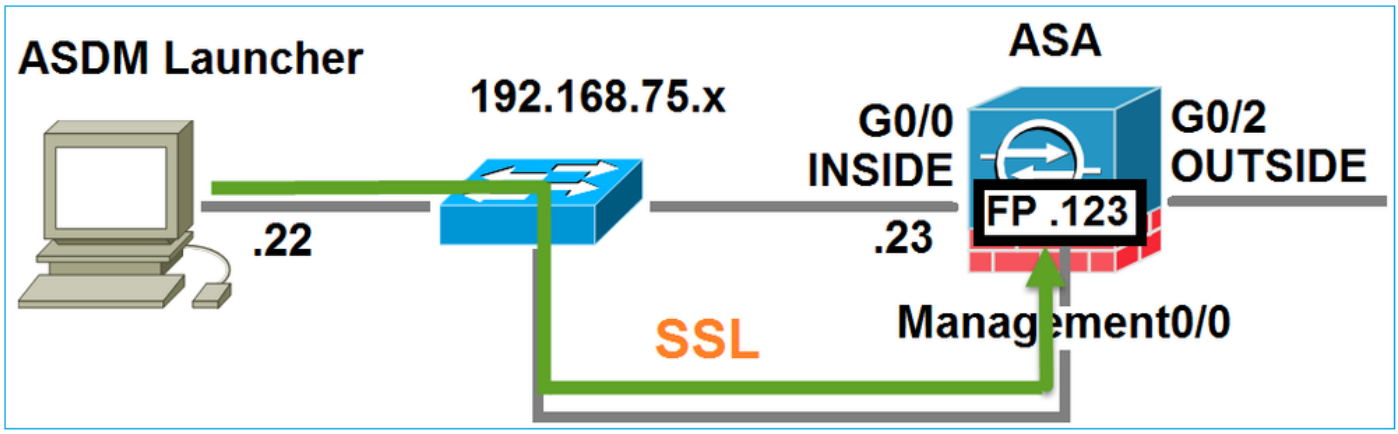
بما أن ASDM يعرف عنوان FirePOWER Management IP، فإنه يبدأ جلسات SSL تجاه الوحدة النمطية:



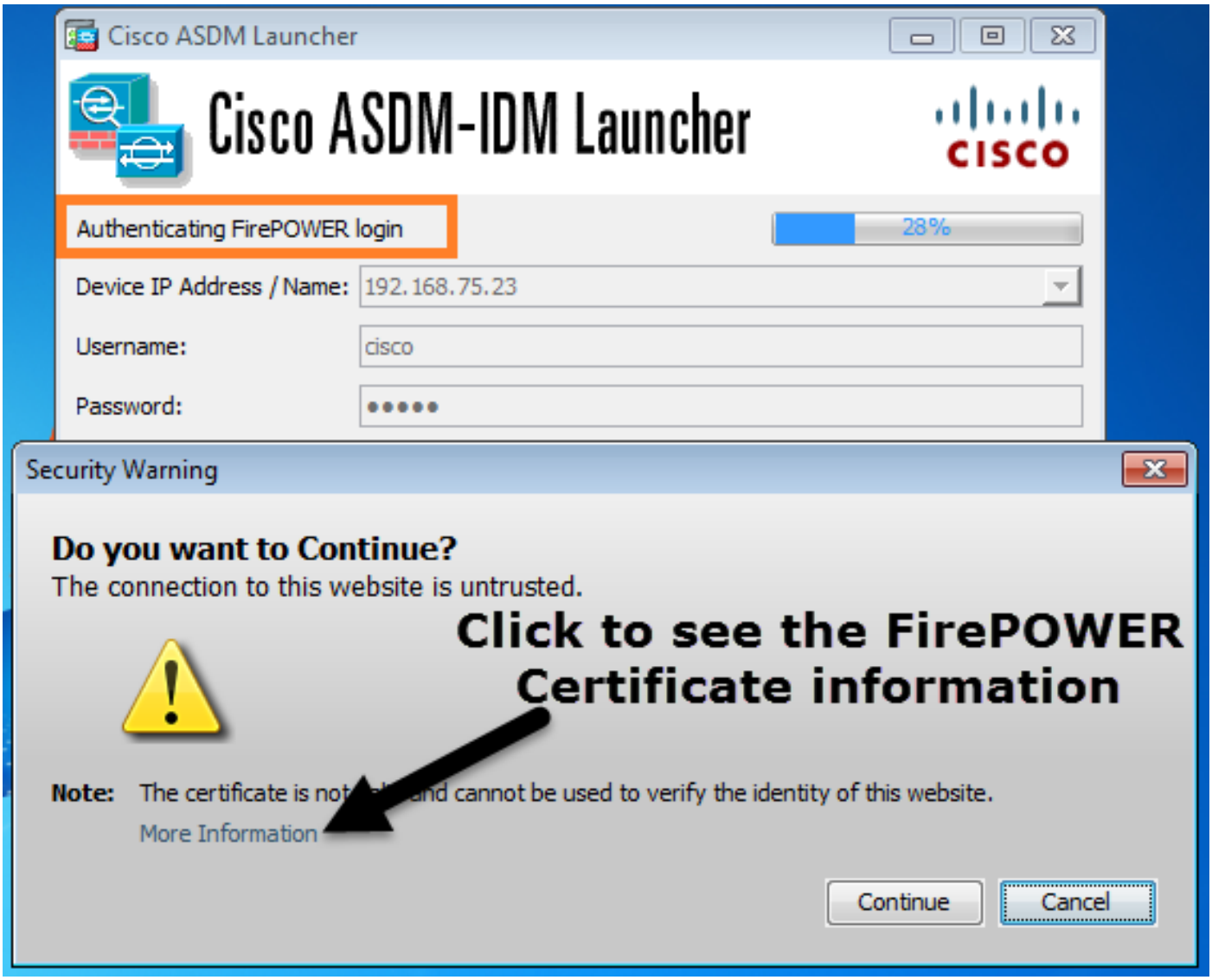
ويلاحظ هذا في الخلفية على أنه إتصالات SSL من مضيف ASDM إلى عنوان IP الخاص بإدارة FirePOWER:

Source	Destination	Protocol	Length	Data	Info
192.168.75.22	192.168.75.123	TLSv1.2	252		Client Hello
192.168.75.22	192.168.75.123	TLSv1.2	220		Client Hello

ويمكن تصور ذلك على النحو التالي:

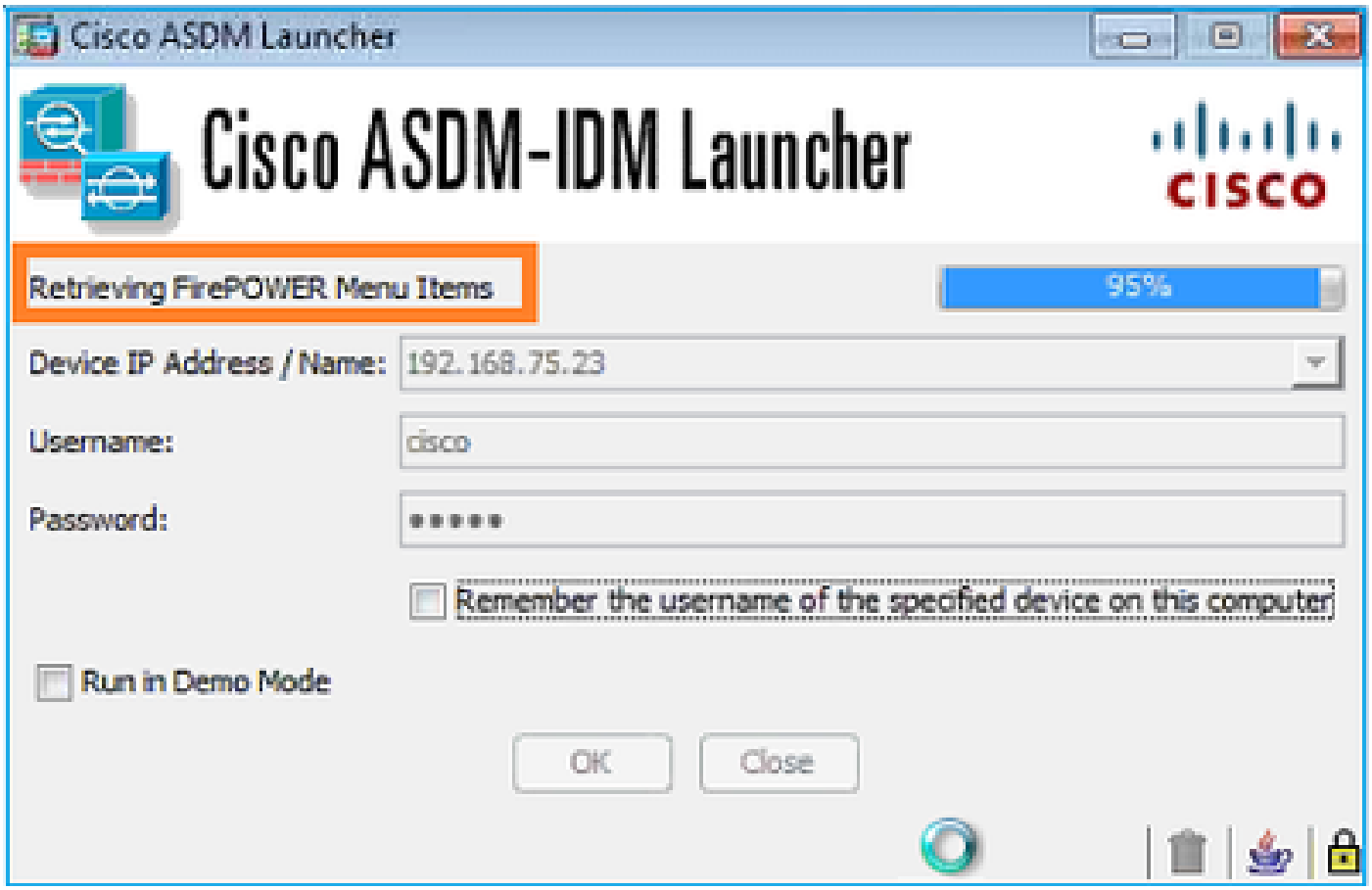


يصادق ASDM FirePOWER ويظهر تحذير أمان لأن شهادة FirePOWER موقعة ذاتيا:

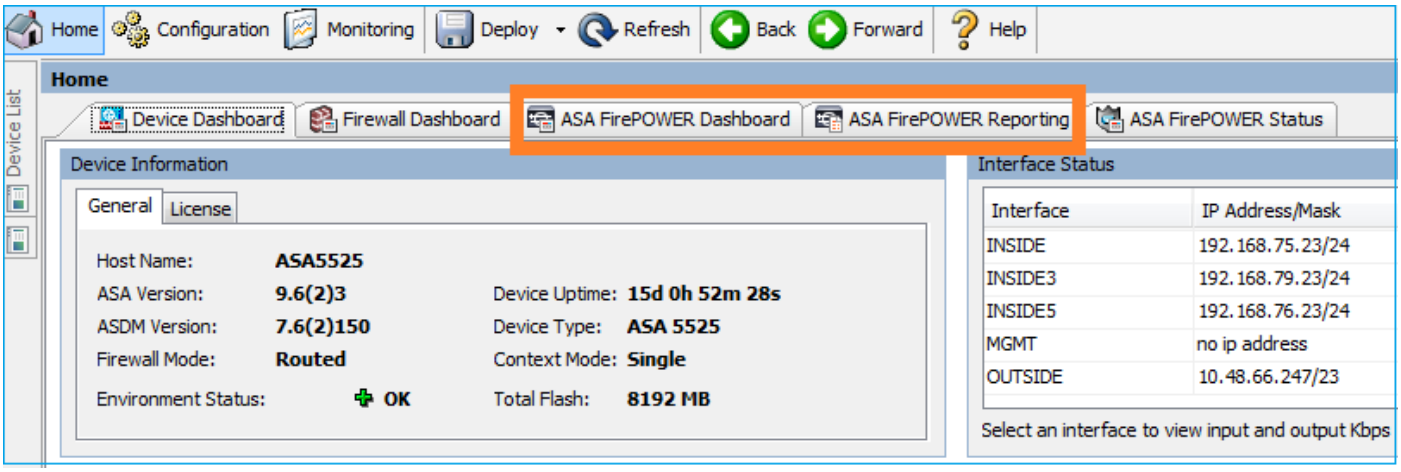


الخطوة 4 - يسترجع ASDM عناصر قائمة FirePOWER

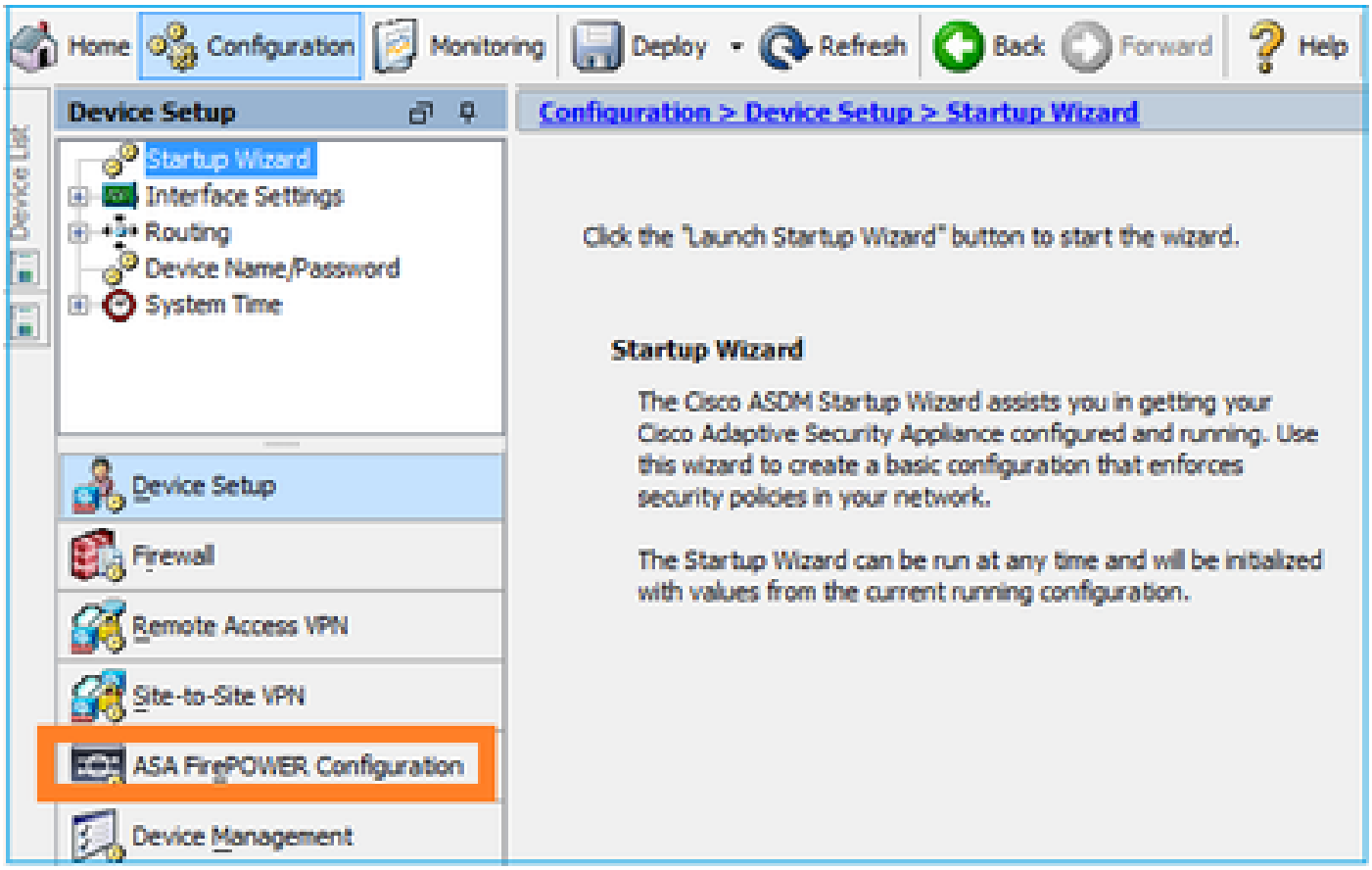
بعد المصادقة الناجحة، يسترجع ASDM عناصر القائمة من جهاز FirePOWER:



تظهر علامات التبويب التي تم إستردادها في هذا المثال:

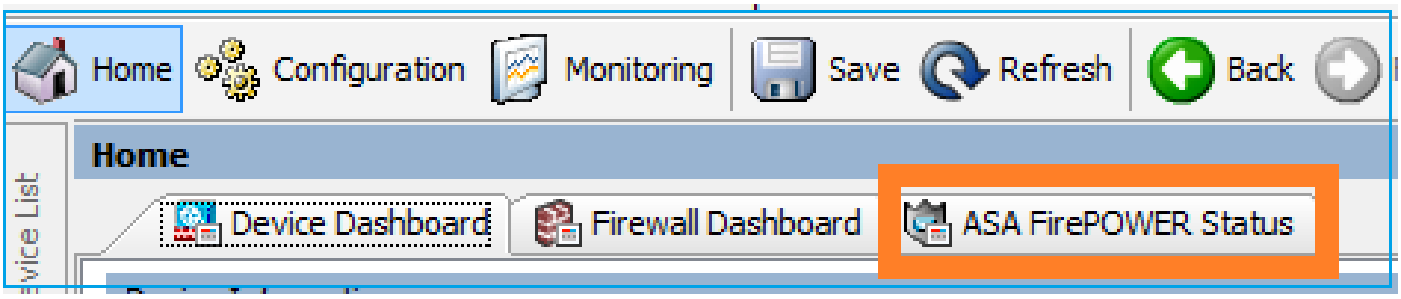


كما أنه يسترجع عنصر قائمة تكوين ASA FirePOWER:

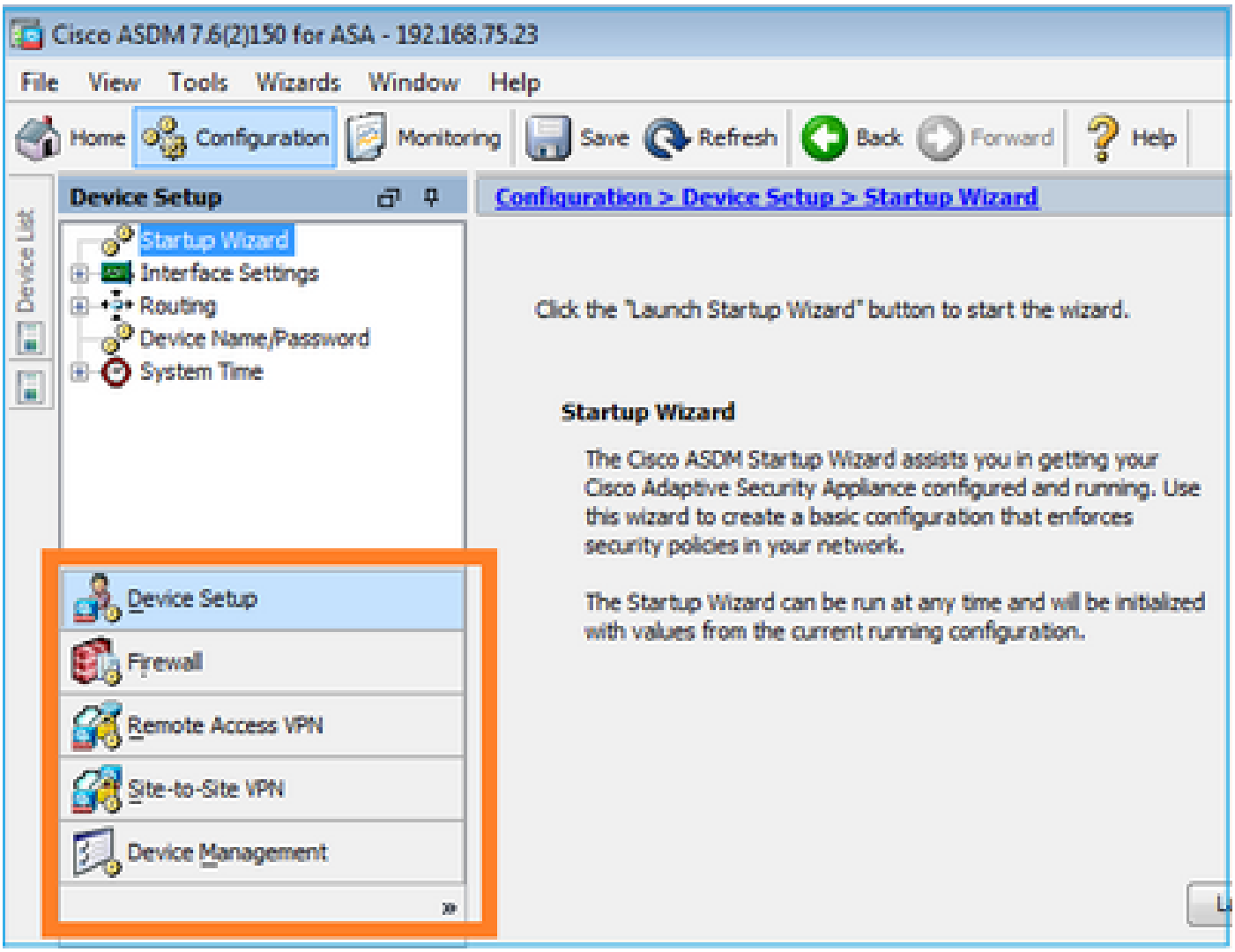


استكشاف الأخطاء وإصلاحها

في حالة عدم قدرة ASDM على إنشاء نفق SSL بعنوان IP الخاص بإدارة FirePOWER، فإنها تقوم فقط بتحميل عنصر قائمة FirePOWER هذا:



عنصر التكوين ASA FirePOWER مفقود أيضا:



التحقق 1

تأكدت أن ال ASA إدارة قارن up وال switchport يربط إلى وه في ال VLAN منا سب:

<#root>

ASA5525#

show interface ip brief | include Interface|Management0/0

Interface IP-Address OK? Method Status Protocol
Management0/0 unassigned YES unset

up up

موصى باستكشاف الأخطاء وإصلاحها

- ثبتت ال VLAN منا سب.
- جلب الميناء up (فحصت الكبل، فحصت ال switchport تشكيل (speed/duplex/shutdown).

التحقق 2

تأكد من تهيئة وحدة FirePOWER النمطية بالكامل وتشغيلها وصيانتها:

<#root>

ASA5525#

show module sfr details

Getting details from the Service Module, please wait...

Card Type: FirePOWER Services Software Module
Model: ASA5525
Hardware version: N/A
Serial Number: FCH1719J54R
Firmware version: N/A
Software version: 6.1.0-330
MAC Address Range: 6c41.6aa1.2bf2 to 6c41.6aa1.2bf2
App. name: ASA FirePOWER

App. Status: Up

App. Status Desc: Normal Operation

App. version: 6.1.0-330

Data Plane Status: Up

Console session: Ready

Status: Up

DC addr: No DC Configured
Mgmt IP addr: 192.168.75.123
Mgmt Network mask: 255.255.255.0
Mgmt Gateway: 192.168.75.23
Mgmt web ports: 443
Mgmt TLS enabled: true

<#root>

A5525#

session sfr console

Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.
>

show version

--------------------[FP5525-3]--------------------
Model : ASA5525 (72) Version 6.1.0 (Build 330)
UUID : 71fd1be4-7641-11e6-87e4-d6ca846264e3
Rules update version : 2016-03-28-001-vrt
VDB version : 270

>

موصى باستكشاف الأخطاء وإصلاحها

- فحصت الإنتاج من العرض وحدة نمطية sfr log وحدة طرفية للتحكم أمر للخطأ أو الفشل.

التحقق 3

تحقق من الاتصال الأساسي بين ضيف ASDM و FirePOWER module إدارة IP باستخدام أوامر مثل ping وtracert/traceroute:

```
C:\Users\cisco>ping 192.168.75.123

Pinging 192.168.75.123 with 32 bytes of data:
Reply from 192.168.75.123: bytes=32 time=3ms TTL=64
Reply from 192.168.75.123: bytes=32 time<1ms TTL=64
Reply from 192.168.75.123: bytes=32 time<1ms TTL=64
Reply from 192.168.75.123: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.75.123:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms

C:\Users\cisco>tracert 192.168.75.123

Tracing route to 192.168.75.123 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  192.168.75.123

Trace complete.
```

موصى باستكشاف الأخطاء وإصلاحها

- تحقق من التوجيه عبر المسار.
- تحقق من عدم وجود أجهزة في المسار تمنع حركة المرور.

التحقق 4

إذا كان ضيف ASDM وعنوان IP الخاص بإدارة FirePOWER في شبكة الطبقة 3 نفسها، فتحقق من جدول بروتوكول تحليل العنوان (ARP) على ضيف ASDM:

```
C:\Users\cisco>arp -a

Interface: 192.168.75.22 --- 0xb
  Internet Address      Physical Address      Type
  192.168.75.23         6c-41-6a-a1-2b-f9     dynamic
  192.168.75.123        6c-41-6a-a1-2b-f2     dynamic
  192.168.75.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

موصى باستكشاف الأخطاء وإصلاحها

- إذا لم توجد إدخالات ARP، أستخدم Wireshark للتحقق من اتصال ARP. تأكد من صحة عناوين MAC الخاصة بالحزم.
- إذا كانت هناك إدخالات ARP، فتأكد من صحتها.

التحقق 5

قم بتمكين الالتقاط على جهاز ASDM أثناء إتصالك عبر ASDM لمعرفة ما إذا كان هناك اتصال TCP صحيح بين المضيف ووحدة FirePOWER النمطية. على أقل تقدير، ترى:

- مصافحة TCP 3-way بين مضيف ASDM و ASA.
- نفق SSL المنشأ بين مضيف ASDM و ASA.
- مصافحة TCP 3-way بين مضيف ASDM وعنوان IP لإدارة وحدة FirePOWER النمطية.
- نفق SSL الذي تم إنشاؤه بين مضيف ASDM وعنوان IP لإدارة وحدة FirePOWER النمطية.

موصى باستكشاف الأخطاء وإصلاحها

- إذا فشل مصافحة TCP 3-way، فتأكد من عدم وجود حركة مرور غير متماثلة أو أجهزة في المسار التي تمنع حزم TCP.
- إذا فشل SSL، فتحقق مما إذا كان لا يوجد جهاز في المسار يقوم بالتوسط (MITM) (يعطي مصدر شهادة الخادم تلميحا لهذا).

التحقق 6

للتحقق من حركة المرور من وحدة FirePOWER وإليها، قم بتمكين الالتقاط على واجهة asa_mgmt_plane. في عملية الالتقاط، يمكنك أن ترى:

- طلب ARP من مضيف ASDM (الحزمة 42).
- رد ARP من الوحدة النمطية FirePOWER (الحزمة 43).
- مصافحة TCP 3-way بين مضيف ASDM والوحدة النمطية FirePOWER (الحزم 44-46).

ASA5525# **capture FP_MGMT interface asa_mgmt_plane**

ASA5525# **show capture FP_MGMT | i 192.168.75.123**

…

42: 20:27:28.532076 arp who-has 192.168.75.123 tell 192.168.75.22

43: 20:27:28.532153 **arp reply** 192.168.75.123 is-at 6c:41:6a:a1:2b:f2

44: 20:27:28.532473 192.168.75.22.48391 > 192.168.75.123.443: **S** 2861923942:2861923942(0) win 8192

45: 20:27:28.532549 192.168.75.123.443 > 192.168.75.22.48391:

S 1324352332:1324352332(0)

ack 2861923943 win 14600

46: 20:27:28.532839 192.168.75.22.48391 > 192.168.75.123.443: .

ack 1324352333 win 16695

موصى باستكشاف الأخطاء وإصلاحها

- نفس الموجود في التحقق 5.

التحقق 7

دقق أن ال ASDM مستعمل يتلقى امتياز مستوى 15. تتمثل إحدى طرق تأكيد هذا الأمر في إدخال الأمر debug http 255 أثناء إتصاله عبر ASDM:

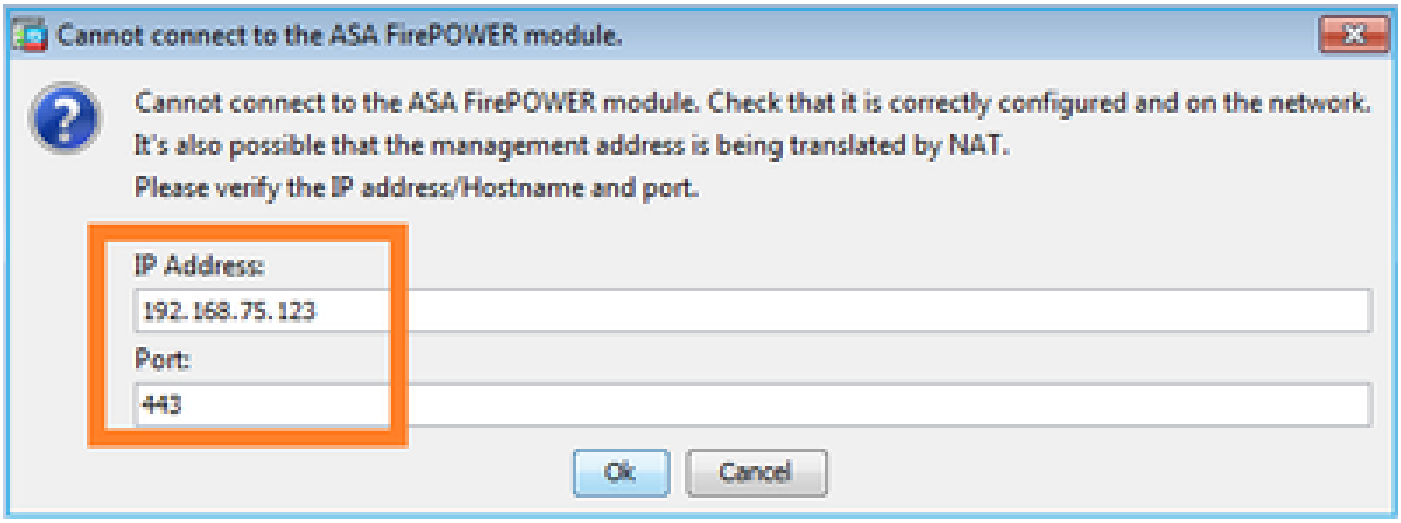
```
<#root>

ASA5525#

debug http 255

debug http enabled at level 255.
HTTP: processing ASDM request [/admin/asdm_banner] with cookie-based authentication (aware_webvpn_conf.
HTTP: check admin session. Cookie index [2][c8a06c50]
HTTP: Admin session cookie [A27614B@20480@78CF@58989AACB80CE5159544A1B3EE62661F99D475DC]
HTTP: Admin session idle-timeout reset
HTTP: admin session verified =  [1]
HTTP: username = [user1],

privilege = [14]
```

موصى باستكشاف الأخطاء وإصلاحها

- إذا لم يكن مستوى الامتياز 15، فحاول مع مستخدم لديه المستوى 15.

التحقق 8

إن بيني مضيف ASDM ووحدة FirePOWER هناك شبكة عنوان ترجمة (NAT) لعنوان FirePOWER إدارة، بعد ذلك أنت تحتاج أن يعين ال NATed عنوان:



موصى باستكشاف الأخطاء وإصلاحها

- تؤكد الالتقاط عند نقاط النهاية (ASA/SFR والمضيف النهائي) هذا.

التحقق 9

تأكد من أن وحدة FirePOWER النمطية ال تتم إدارتها بالفعل بواسطة FMC، لأنه في هذه الحالة تكون عالمات التبويب FirePOWER في ASDM مفقودة:

```
<#root>

ASA5525#

session sfr console

Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.
>

show managers

Managed locally.


>
```

وهناك طريقة أخرى باستخدام أمر show module sfr details:

```
<#root>

ASA5525#

show module sfr details

Getting details from the Service Module, please wait...

Card Type:          FirePOWER Services Software Module
Model:              ASA5525
Hardware version:   N/A
Serial Number:      FCH1719J54R
Firmware version:   N/A
Software version:   6.1.0-330
MAC Address Range:  6c41.6aa1.2bf2 to 6c41.6aa1.2bf2
App. name:          ASA FirePOWER
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       6.1.0-330
Data Plane Status:  Up
Console session:    Ready
Status:             Up

DC addr:            No DC Configured

Mgmt IP addr:       192.168.75.123
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.168.75.23
Mgmt web ports:     443
Mgmt TLS enabled:   true
```

موصى باستكشاف الأخطاء وإصلاحها

- إذا كان الجهاز تتم إدارته بالفعل، فأنت بحاجة إلى إلغاء تسجيله قبل إدارته من ASM. رأيت دليل تكوين مركز إدارة firepower لـ.

التحقق 10

تحقق من التقاط Wireshark لضمان اتصال عميل ASDM بإصدار TLS صحيح (على سبيل المثال، TLSv1.2).

موصى باستكشاف الأخطاء وإصلاحها

- قم بضبط إعدادات SSL للمستعرض.
- حاول باستخدام مستعرض آخر.
- حاول من مضيف نهائي آخر.

التحقق 11

تحقق من توافق صور ASA في دليل توافق Cisco ASA أن تكون صور ASA/ASDM متوافقة.

موصى باستكشاف الأخطاء وإصلاحها

- إستخدام صورة ASDM متوافقة.

التحقق 12

تحقق في دليل توافق Cisco ASA من أن جهاز FirePOWER متوافق مع إصدار ASDM.

موصى باستكشاف الأخطاء وإصلاحها

- إستخدام صورة ASDM متوافقة.

معلومات ذات صلة

- دليل البدء السريع للوحدة النمطية Cisco ASA FirePOWER Module
- دليل تكوين الإدارة المحلية لخدمات FirePOWER، الإصدار 6.1.0 مع ASA
- دليل مستخدم وحدة ASA FirePOWER النمطية لـ ASA5506-X، ASA5506H-X، ASA5506W-X، ASA5508-X، و ASA5516-X، الإصدار 5.4.1
- الدعم التقني والمستندات - Cisco Systems

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