使用ASDM管理ASA上的FirePOWER模組

目錄

簡介

本文檔介紹ASDM軟體如何與自適應安全裝置(ASA)和安裝在其上的FirePOWER軟體模組通訊。

背景資訊

ASA上安裝的FirePOWER模組可通過以下任一方式進行管理：

- Firepower管理中心(FMC) — 這是開箱即用的管理解決方案。
- 自適應安全裝置管理器(ASDM) — 這是機上管理解決方案。

必要條件

需求

用於啟用ASDM管理的ASA配置：

<#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
```

檢查ASA/SFR模組之間的相容性，否則無法看到FirePOWER頁籤。

此外，在ASA上，必須啟用3DES/AES許可證：

```
<#root>

ASA5525#

show version | in 3DES

Encryption-3DES-AES

                :

Enabled

 perpetual
```

確保ASDM客戶端系統運行支援的Java JRE版本。

採用元件

- Microsoft Windows 7主機
- 執行ASA 9.6(2.3)版的ASA5525-X
- ASDM版本7.6.2.150
- FirePOWER軟體模組6.1.0-330

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

架構

ASA有三個內部介面：

- asa_dataPlane — 用於將資料包從ASA資料路徑重定向到FirePOWER軟體模組。
- asa_mgmt_plane — 用於允許FirePOWER管理介面與網路通訊。
- cplane — 控制平面介面，用於在ASA和FirePOWER模組之間傳輸keepalive。

您可以在所有內部介面中捕獲流量：

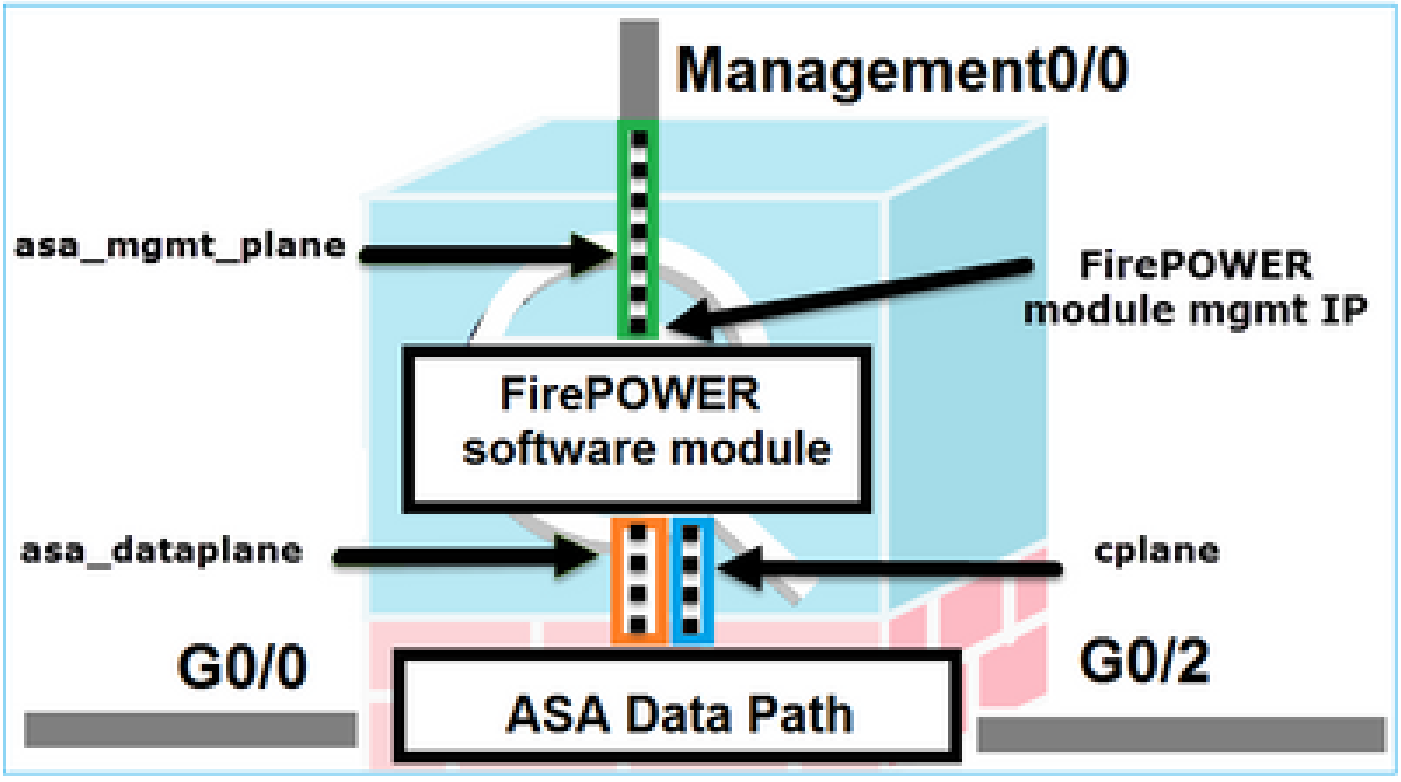
<#root>

ASA5525#

capture CAP interface ?

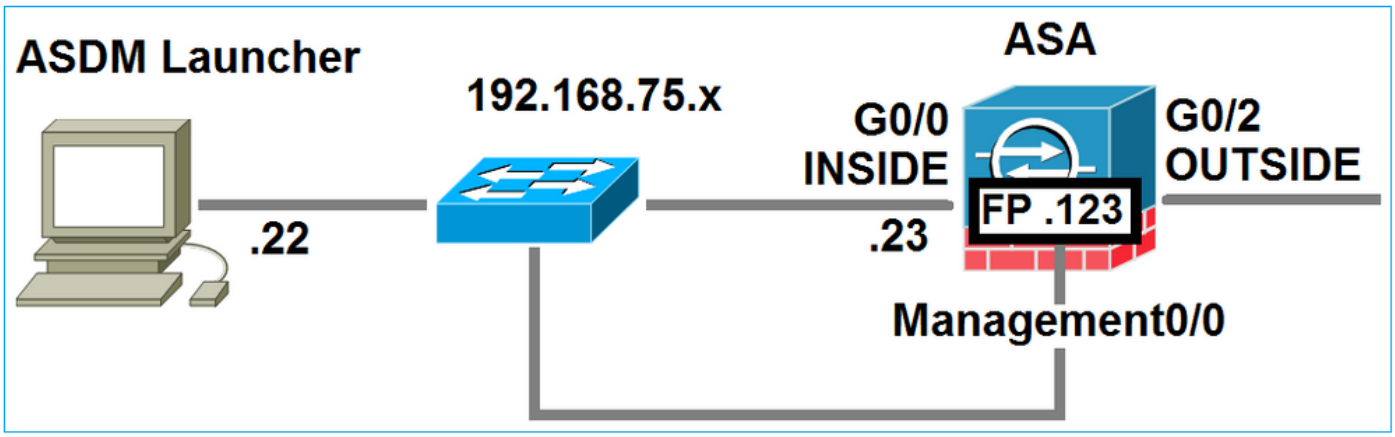
```
  asa_dataplane   Capture packets on dataplane interface
  asa_mgmt_plane  Capture packets on managementplane interface
  cplane          Capture packets on controlplane interface
```

視覺化的方式如下：



使用者通過ASDM連線到ASA時的後台操作

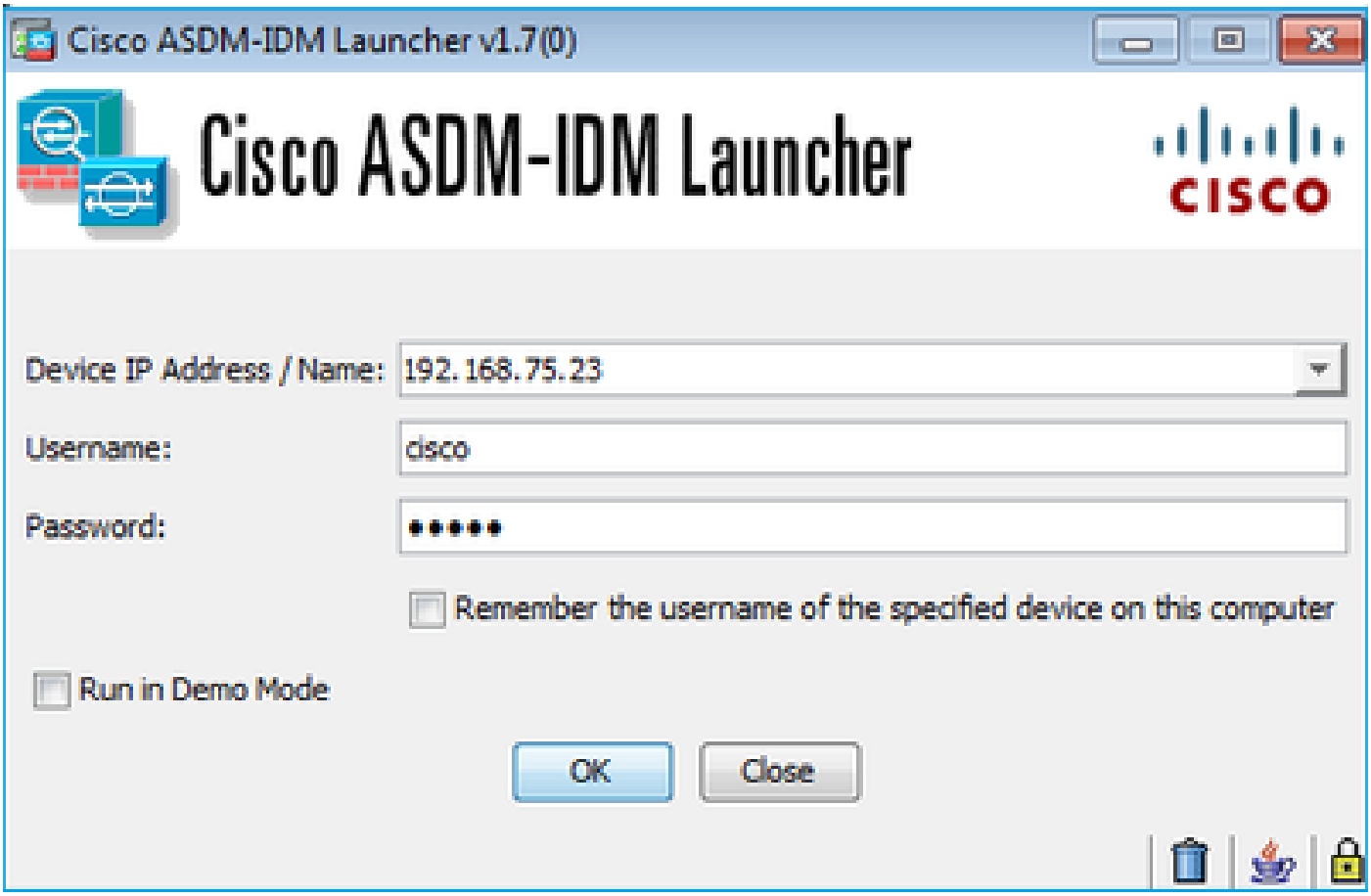
請考慮使用此拓樸：



當使用者啟動與ASA的ASDM連線時，會發生以下事件：

第1步 — 使用者發起ASDM連線

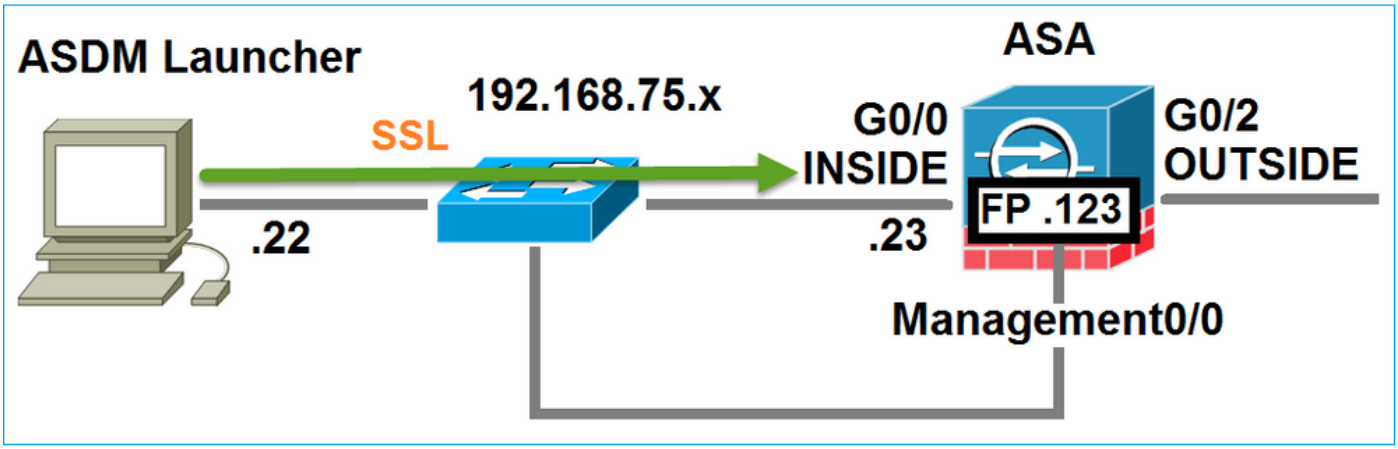
使用者指定用於HTTP管理的ASA IP地址，輸入憑證，並啟動與ASA的連線：



在後台，在ASDM和ASA之間建立SSL隧道：

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

視覺化的方式如下：



第2步 — ASDM發現ASA配置和FirePOWER模組IP地址

在ASA上輸入debug http 255命令，以顯示ASDM連線到ASA時在後台執行的所有檢查：

```
<#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 authentication
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
```

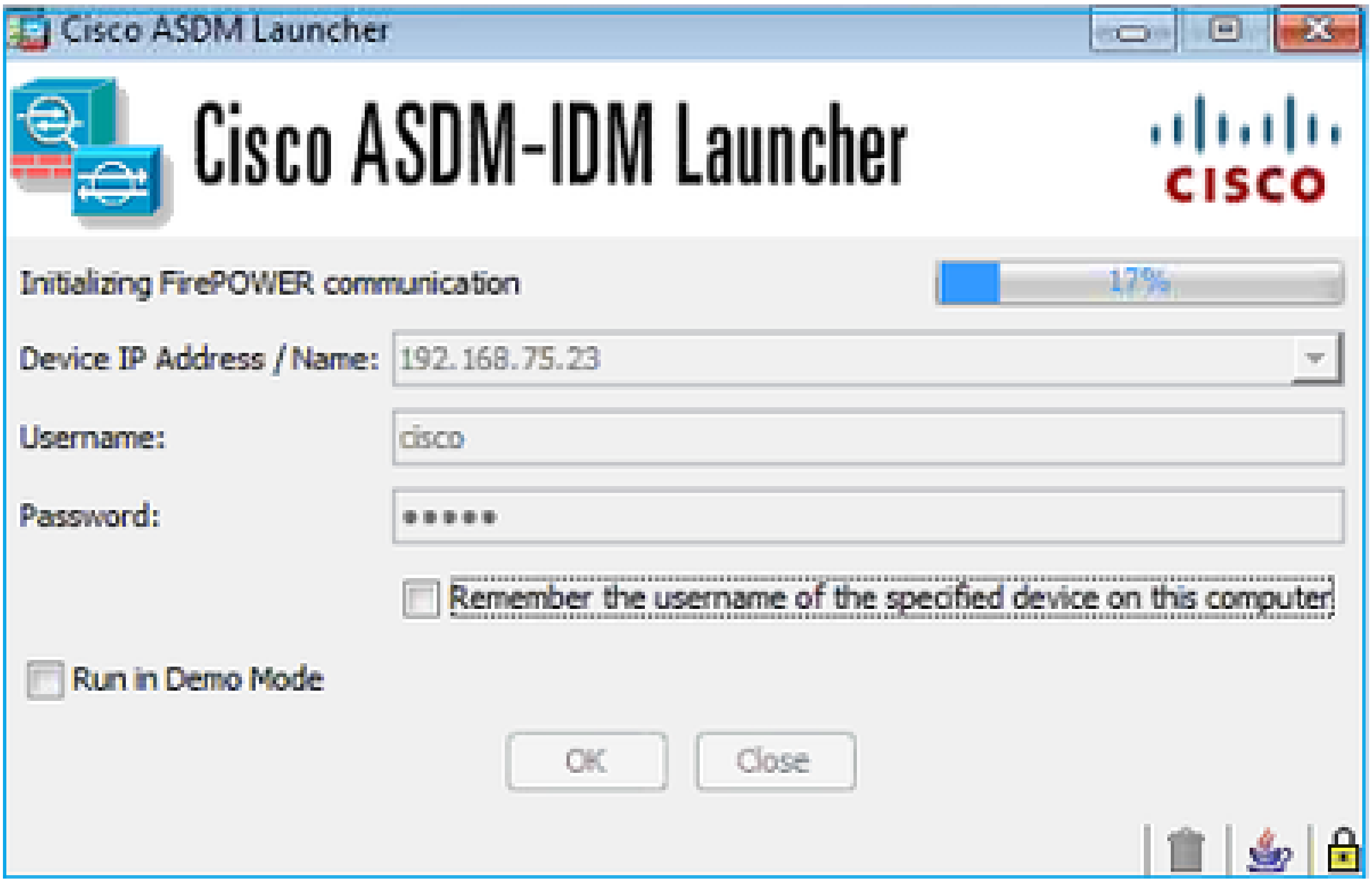
- show module - ASDM發現ASA模組。
- show module sfr details - ASDM發現模組詳細資訊，包括FirePOWER管理IP地址。

在後台可以看到從PC到ASA IP地址的一系列的SSL連線：

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

第3步 — ASDM啟動與FirePOWER模組的通訊

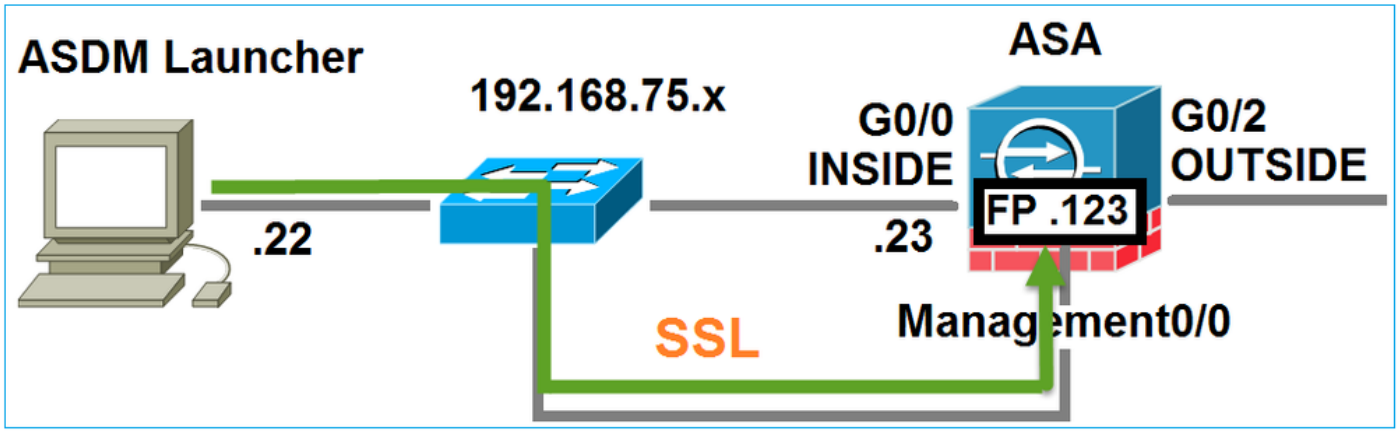
由於ASDM知道FirePOWER管理IP地址，因此它會向模組發起SSL會話：



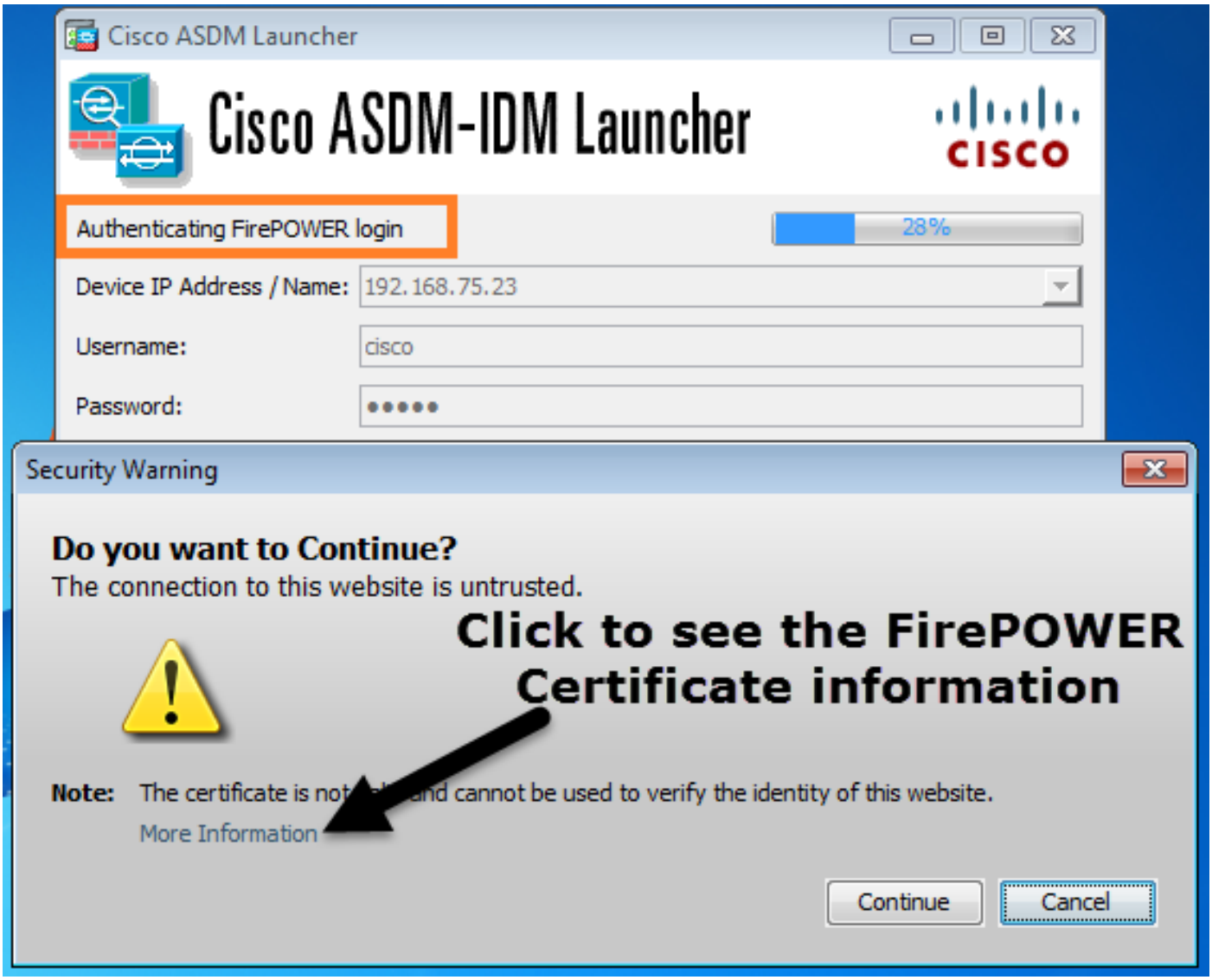
在後台將這視為從ASDM主機到FirePOWER管理IP地址的SSL連線：

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

視覺化的方式如下：

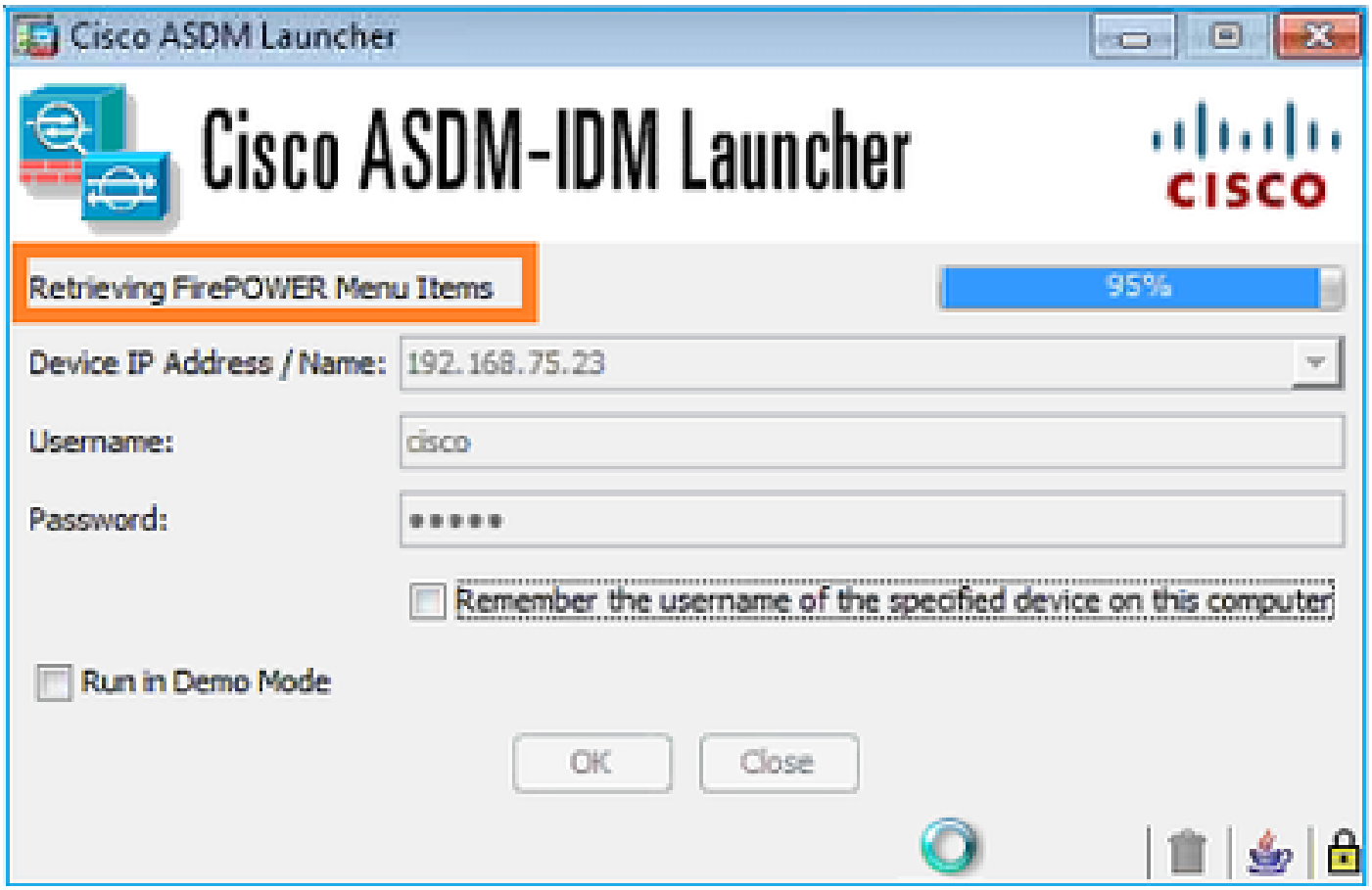


ASDM對FirePOWER進行身份驗證，並顯示FirePOWER證書自簽名後的安全警告：

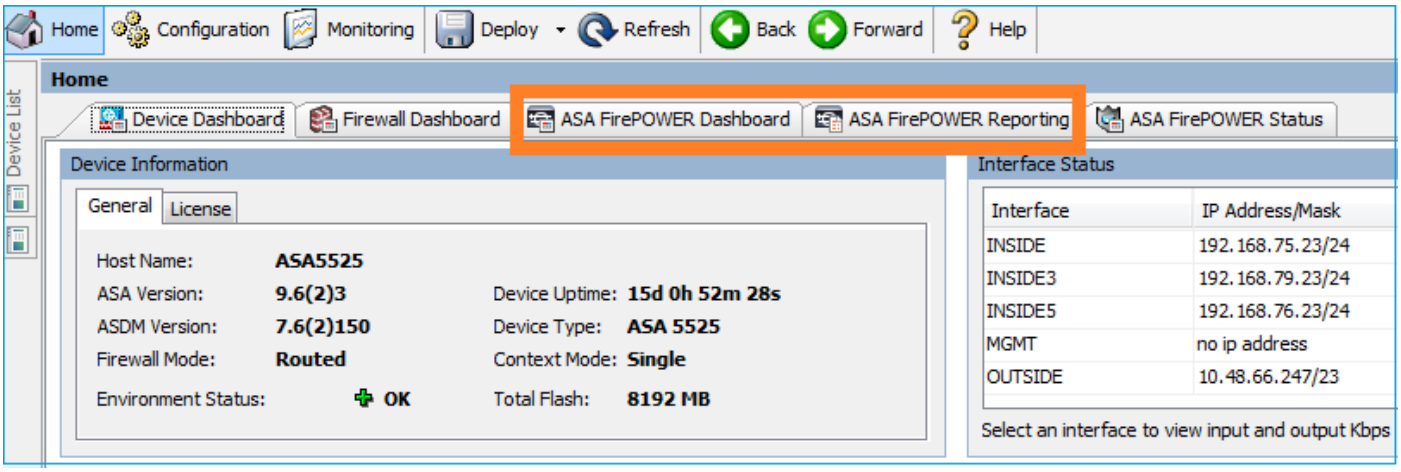


第4步 — ASDM檢索FirePOWER選單項

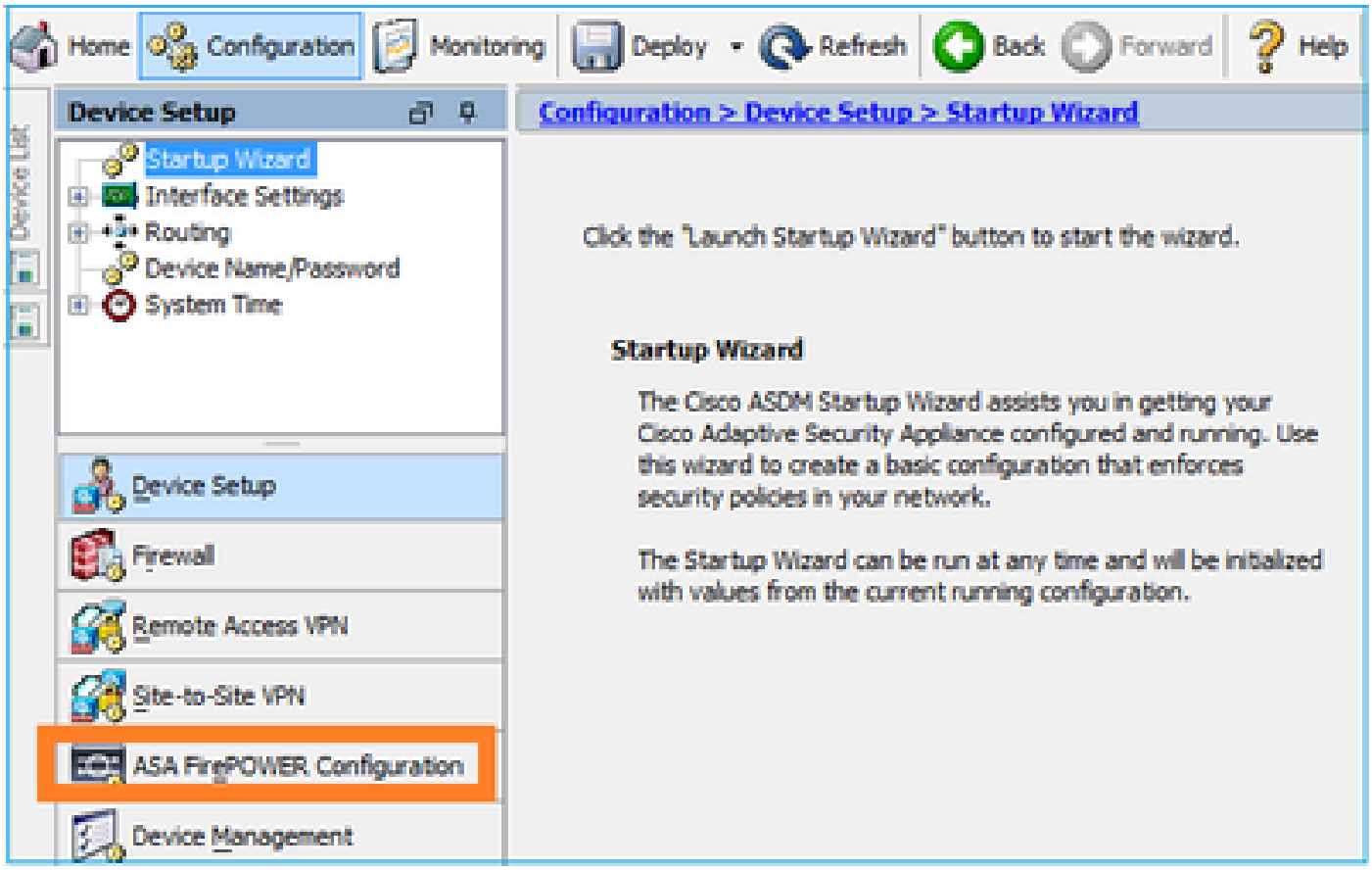
身份驗證成功後，ASDM從FirePOWER裝置檢索選單項：



檢索到的頁籤如下例所示：

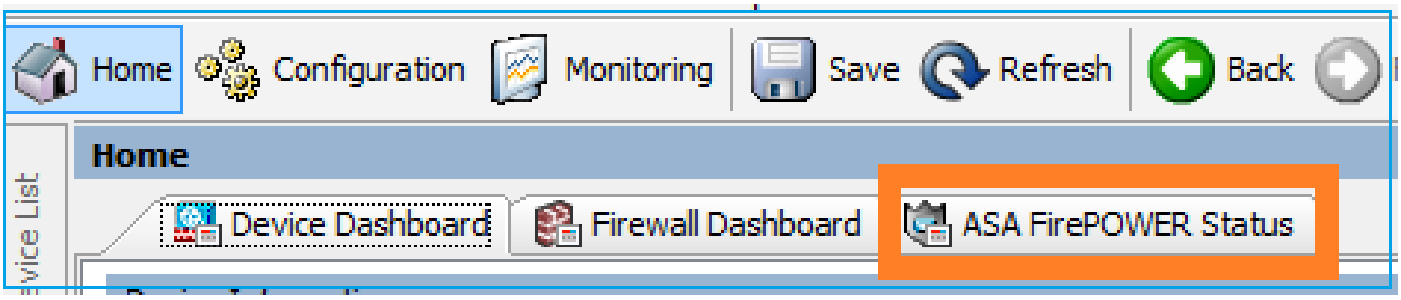


它還檢索ASA FirePOWER配置選單項：

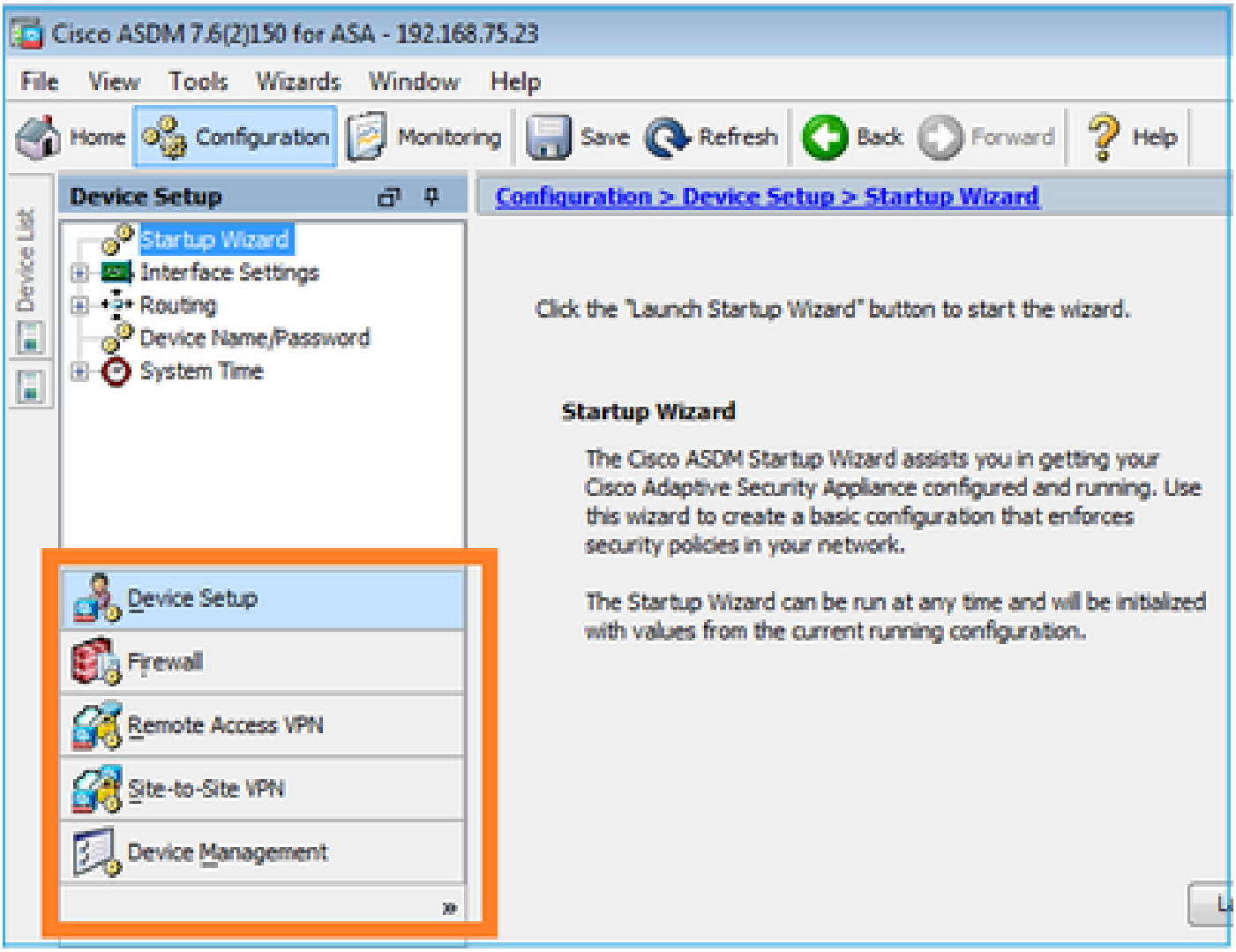


疑難排解

如果ASDM無法使用FirePOWER管理IP地址建立SSL隧道，則僅載入此FirePOWER選單項：



ASA FirePOWER配置項也丟失：



驗證 1

確保ASA管理介面為UP狀態，並且與其連線的switchport位於正確的VLAN中：

<#root>

ASA5525#

show interface ip brief | include Interface|Management0/0

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

up up

建議的疑難排解

- 設定正確的VLAN。
- 使埠開啟(檢查電纜，檢查交換機埠配置（速度/雙工/關閉））。

驗證 2

確保FirePOWER模組完全初始化、UP並正在運行：

<#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
----------------------------------------------------

>
```

建議的疑難排解

- 檢查show module sfr log console命令的輸出中是否存在錯誤或故障。

驗證 3

使用ping和tracert/traceroute等命令檢查ASDM主機和FirePOWER模組管理IP之間的基本連通性：

```
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.
```

建議的疑難排解

- 檢查路徑沿途的路由。
- 驗證路徑中是否有裝置阻止流量。

驗證 4

如果ASDM主機和FirePOWER管理IP地址位於同一第3層網路中，請檢查ASDM主機上的地址解析協定(ARP)表：

```
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
```

建議的疑難排解

- 如果沒有ARP條目，請使用Wireshark檢查ARP通訊。確保資料包的MAC地址正確。
- 如果有ARP條目，請確保它們正確。

驗證 5

當您通過ASDM連線時，在ASDM裝置上啟用捕獲，以檢視主機和FirePOWER模組之間是否存在正確的TCP通訊。您至少會看到：

- ASDM主機和ASA之間的TCP三次握手。
- 在ASDM主機和ASA之間建立SSL隧道。
- ASDM主機和FirePOWER模組管理IP地址之間的TCP三次握手。
- 在ASDM主機和FirePOWER模組管理IP地址之間建立SSL隧道。

建議的疑難排解

- 如果TCP三次握手失敗，請確保路徑中不存在阻塞TCP資料包的非對稱流量或裝置。
- 如果SSL失敗，請檢查路徑中是否沒有任何裝置進行中間人(MITM)（伺服器證書頒發機構會對此給出提示）。

驗證 6

為了檢查往返於FirePOWER模組的流量，請在asa_mgmt_plane介面上啟用捕獲。在捕獲中，您可以看到：

- 來自ASDM主機的ARP請求（資料包42）。
- FirePOWER模組的ARP應答（資料包43）。
- ASDM主機和FirePOWER模組之間的TCP三次握手（資料包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

建議的疑難排解

- 與驗證5中的相同。

驗證 7

驗證ASDM使用者的許可權級別為15。確認此情況的方法之一是在它透過ASDM連線時輸入debug http 255命令：

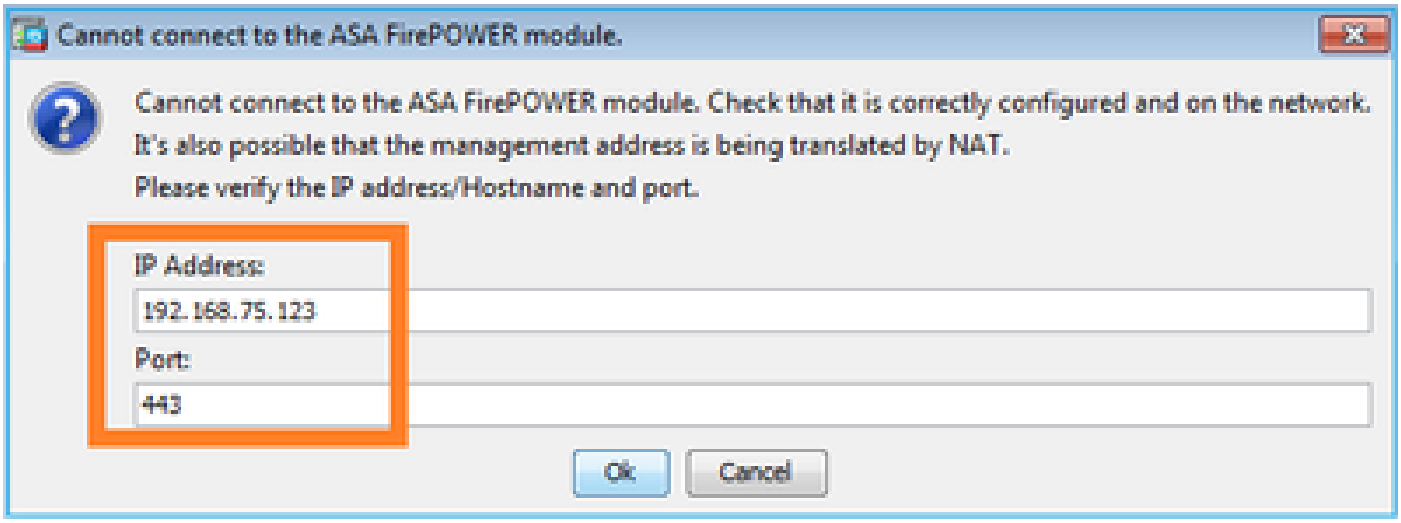
```
<#root>

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]
```

建議的疑難排解

- 如果許可權級別不是15，請嘗試使用級別為15的使用者。

驗證 8

如果在ASDM主機和FirePOWER模組之間存在FirePOWER管理IP地址的網路地址轉換(NAT)，則需要指定NATed IP地址：



建議的疑難排解

- 在終端（ASA/SFR和終端主機）捕獲可確認這一點。

驗證 9

確保FirePOWER模組尚未由FMC管理，因為在這種情況下，ASDM中缺少FirePOWER頁籤：

```
<#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.


>
```

另一種方法是使用show module sfr details命令：

```
<#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
```

建議的疑難排解

- 如果裝置已經受管，您需要先將其註銷，然後才能從ASDM對其進行管理。請參閱

Firepower管理中心配置指南。

驗證 10

檢查wireshark捕獲以確保ASDM客戶端使用正確的TLS版本（例如TLSv1.2）連線。

建議的疑難排解

- 調整瀏覽器SSL設定。
- 嘗試使用其他瀏覽器。
- 從另一個終端主機嘗試。

驗證 11

在Cisco ASA相容性指南中驗證ASA/ASDM映像是否相容。

建議的疑難排解

- 使用相容的ASDM映像。

驗證 12

在Cisco ASA相容性指南中驗證FirePOWER裝置是否與ASDM版本相容。

建議的疑難排解

- 使用相容的ASDM映像。

相關資訊

- Cisco ASA FirePOWER模組快速入門手冊
- 具備FirePOWER服務的ASA本地管理配置指南6.1.0版
- 適用於ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X和ASA5516-X版本5.4.1的ASA FirePOWER模組使用手冊
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。