使用管理的ASDM在ASA的一个FirePOWER模块

目录

[简介](#)
[使用的组件](#)
[先决条件](#)
[体系结构](#)
[背景操作，当用户连接对ASA通过ASDM](#)
[Step1 –用户首次ASDM连接](#)
[步骤2 – ASDM发现ASA配置和FirePOWER模块IP](#)
[步骤3 – ASDM启动往FirePOWER模块的通信](#)
[步骤4 – ASDM获取FirePOWER菜单项](#)
[排除故障](#)
[推荐的操作](#)
[相关文档](#)

简介

在ASA安装的FirePOWER模块可以由管理：

- Firepower管理中心(FMC) –这是箱外管理解决方案
- 可适应安全设备管理器(ADSM) –这是在箱上管理解决方案

本文目标是解释ASDM软件如何与对此和FirePOWER软件模块联络安装的ASA。

使用的组件

- Windows 7主机
- 运行ASA 9.6.2-3代码的ASA5525-X
- ASDM软件7.6.2.150
- FirePOWER软件模块6.1.0-330

先决条件

启用ASDM管理的ASA配置：

```
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
```

另外，在ASA应该启用3DES/AES许可证：

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

体系结构

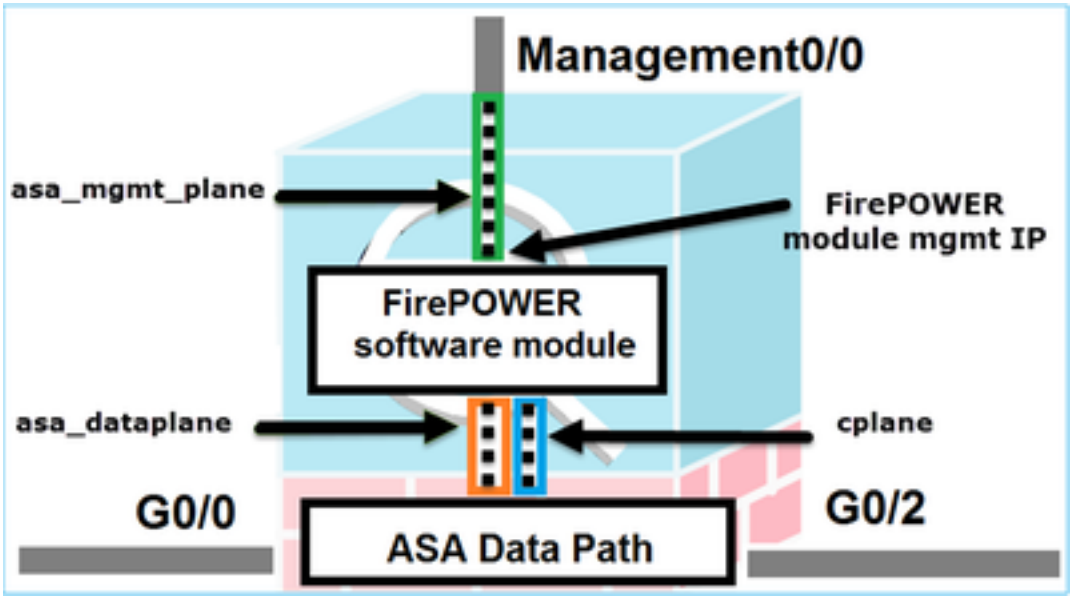
ASA有3个内部接口：

- **asa_dataplane** =它用于重定向从ASA数据路径的数据包到FirePOWER软件模块
- **asa_mgmt_plane** =它用于允许FirePOWER管理接口与网络联络
- **cplane** =使用转接Keepalive在ASA和FirePOWER模块之间的控制层面接口

您能捕获在所有内部接口的流量：

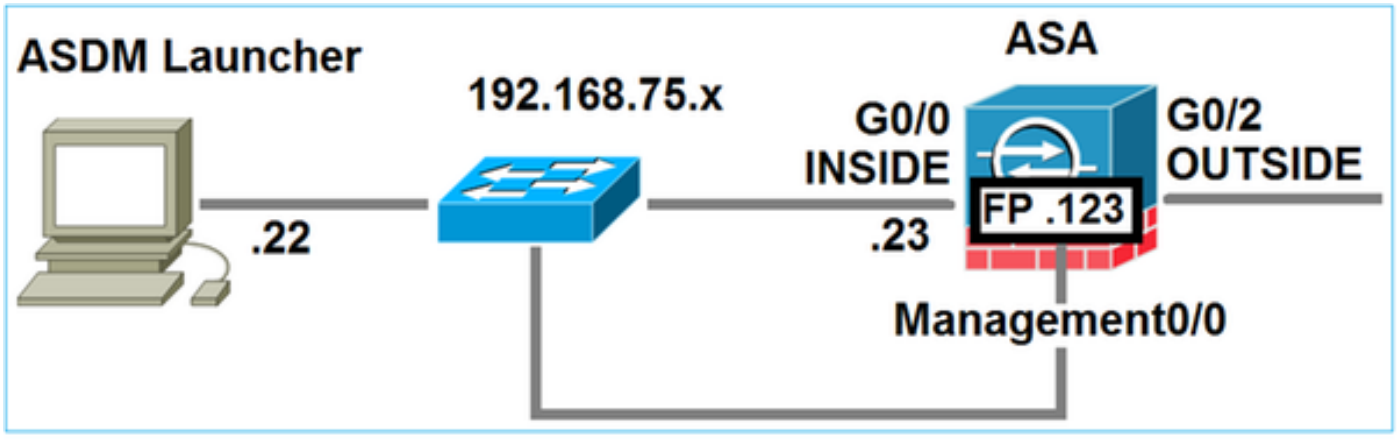
```
ASA5525# capture CAP interface ? asa_dataplane Capture packets on dataplane interface
asa_mgmt_plane Capture packets on managementplane interface cplane Capture packets on
controlplane interface
```

以上可以形象化如下：



背景操作，当用户连接对ASA通过ASDM

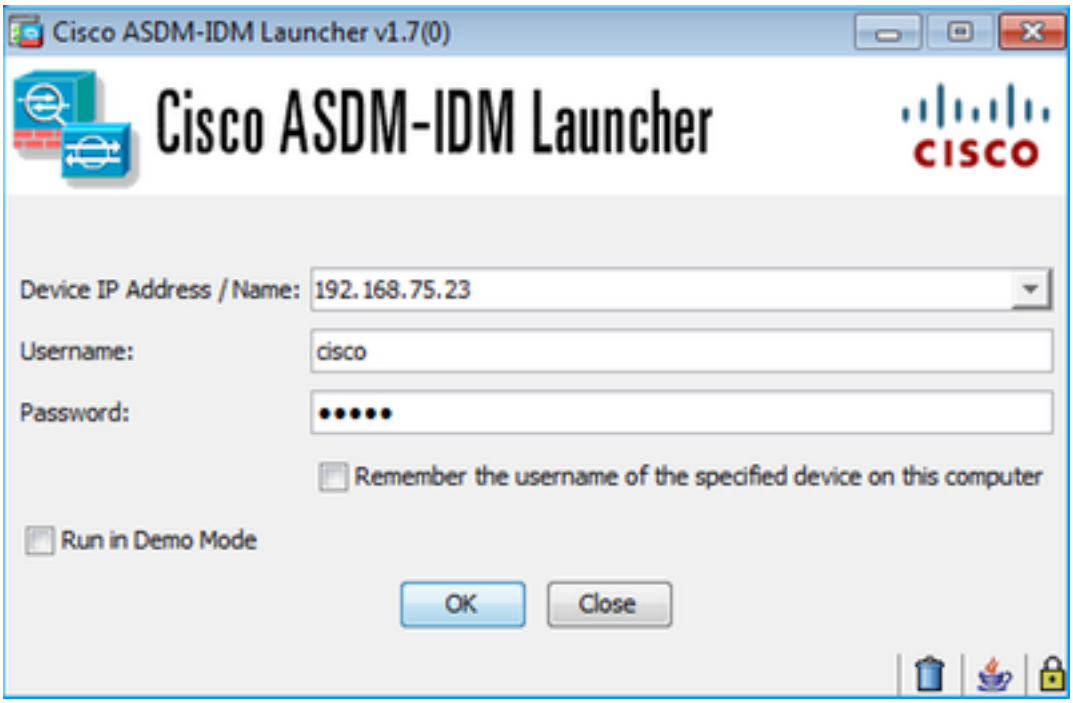
考虑以下拓扑



当用户首次对ASA的ASDM连接以下事件将发生：

Step1 –用户首次ASDM连接

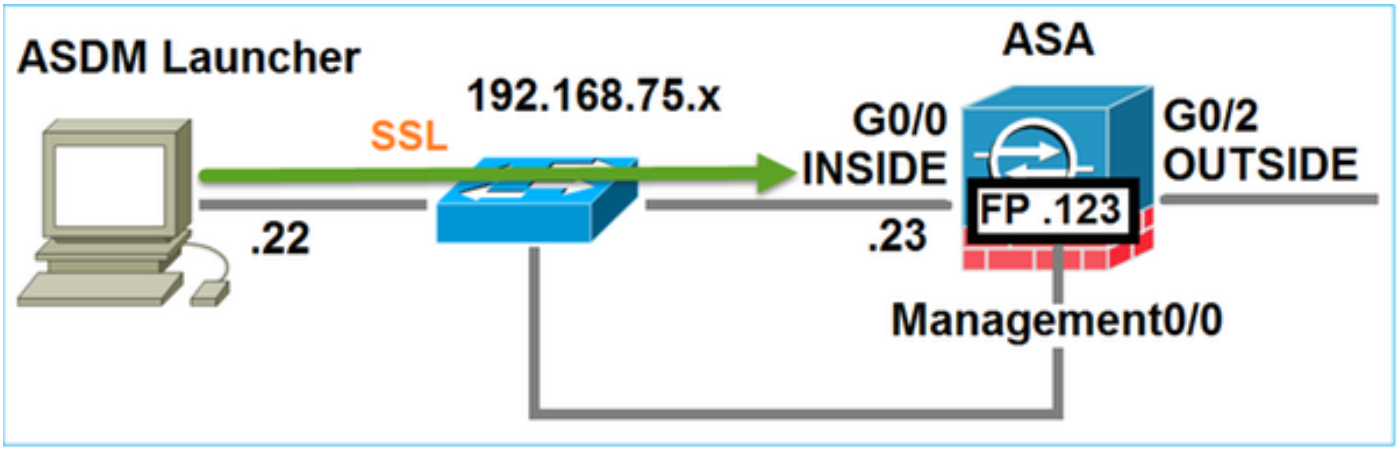
用户指定用于HTTP管理的ASA IP，输入凭证并且首次往ASA的连接：



在背景在ASDM和ASA之间的一个SSL通道设立：

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

这可以形象化如下：



步骤2 – ASDM发现ASA配置和FirePOWER模块IP

启用在ASA的**调试http 255将**显示在背景进行的所有检查，当ASDM连接对ASA ：

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

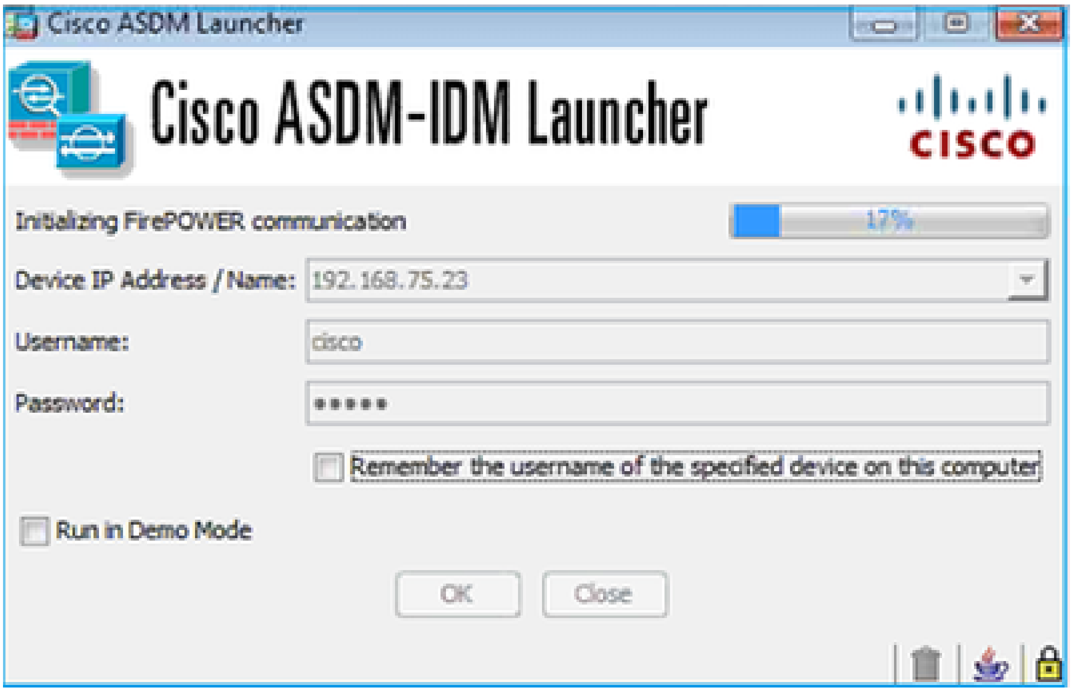
- show module = ASDM发现ASA模块
- show module sfr详细信息= ASDM发现模块详细信息包括FirePOWER管理IP

以上在背景将被看到作为从PC的一系列的SSL连接往ASA IP:

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

步骤3 – ASDM启动往FirePOWER模块的通信

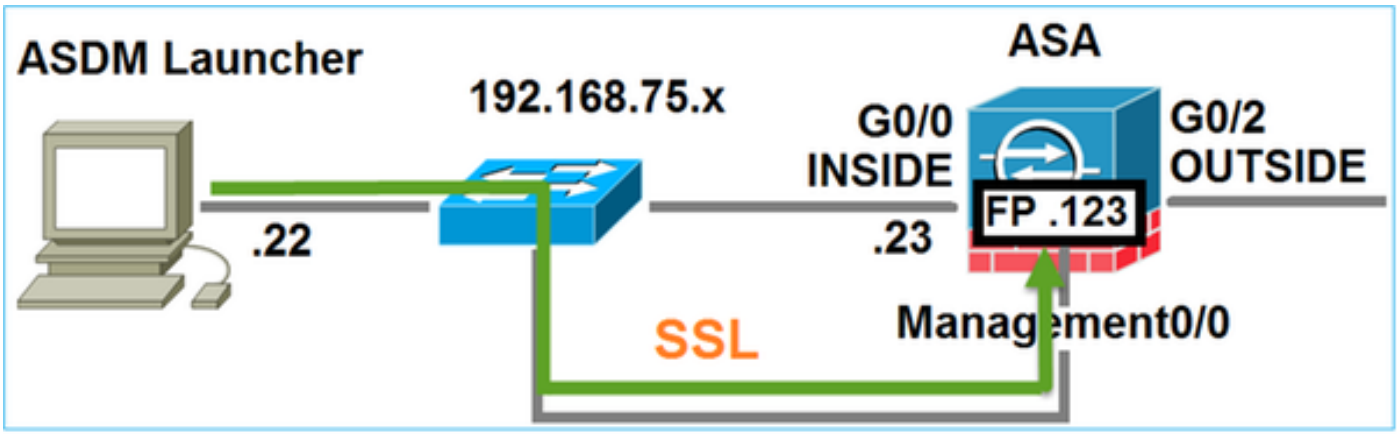
因为ASDM认识FirePOWER管理IP启动往模块的SSL会话：



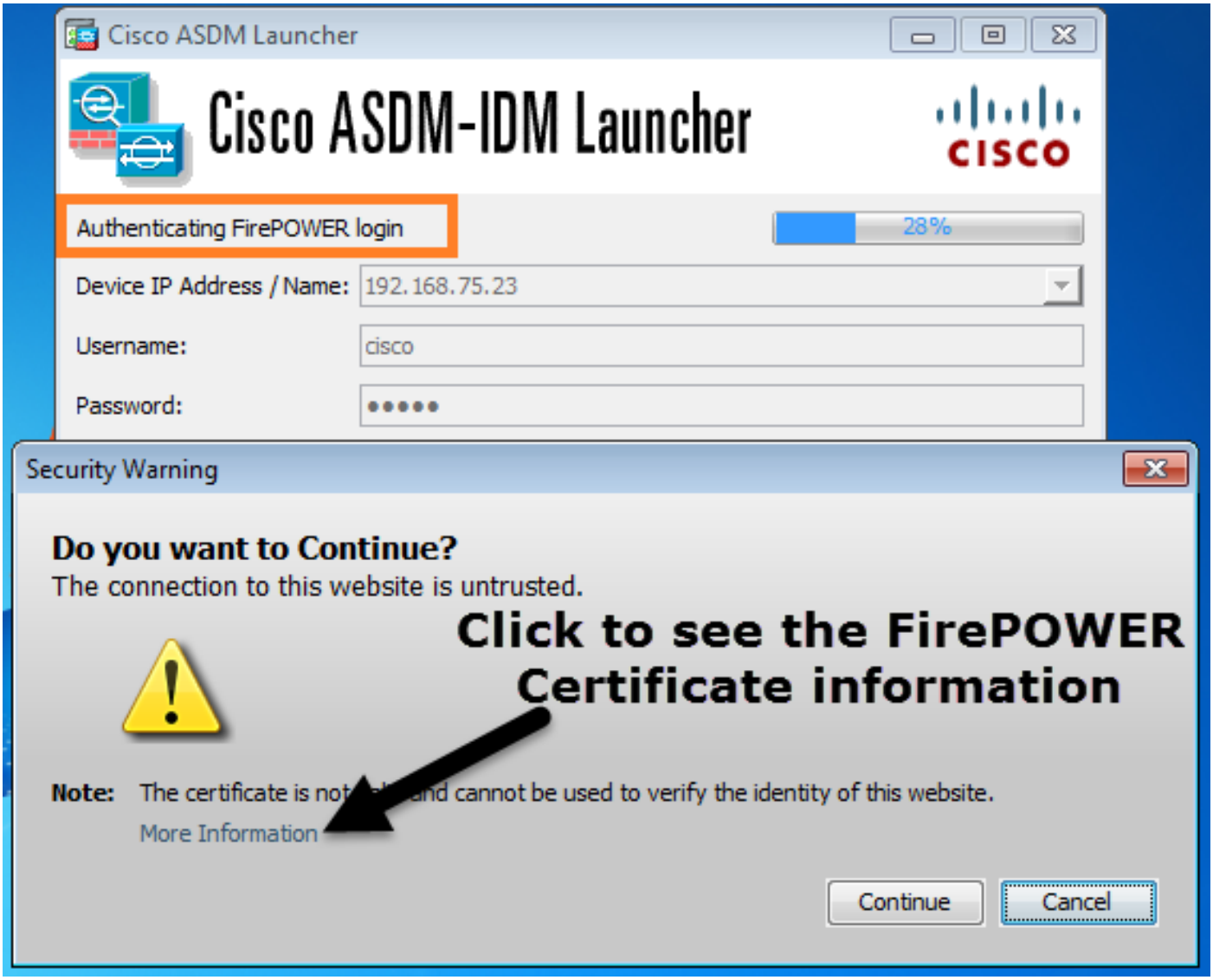
以上在背景将被看到，从ASDM主机的SSL连接往FirePOWER管理IP ：

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

这可以形象化如下：

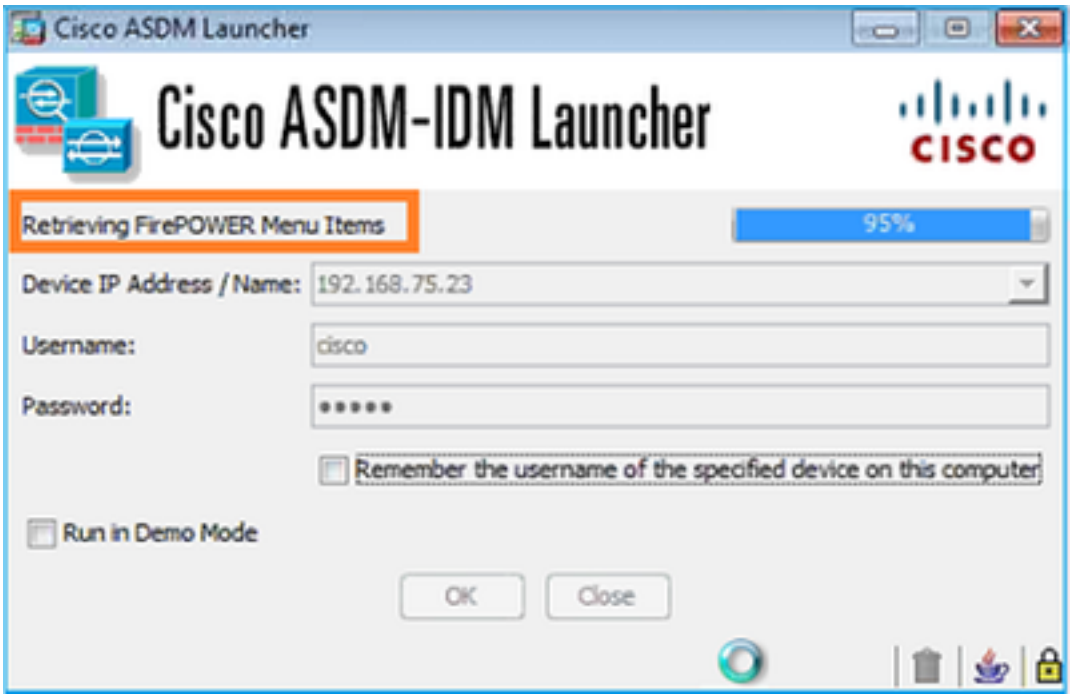


ASDM验证FirePOWER，并且安全亚里桑显示，因为FirePOWER证书自已签署的：

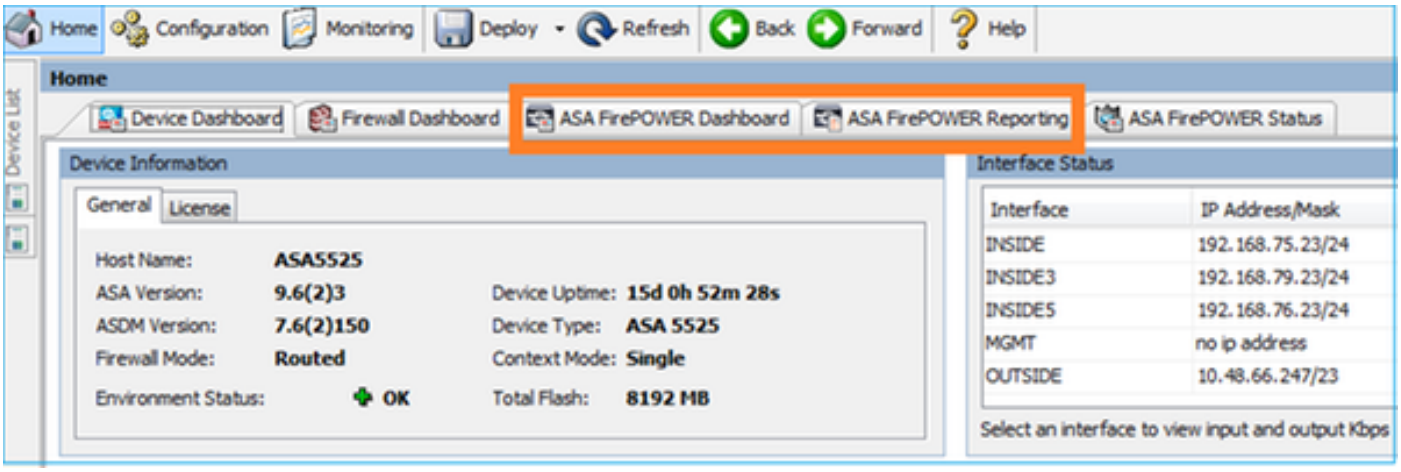


步骤4 – ASDM获取FirePOWER菜单项

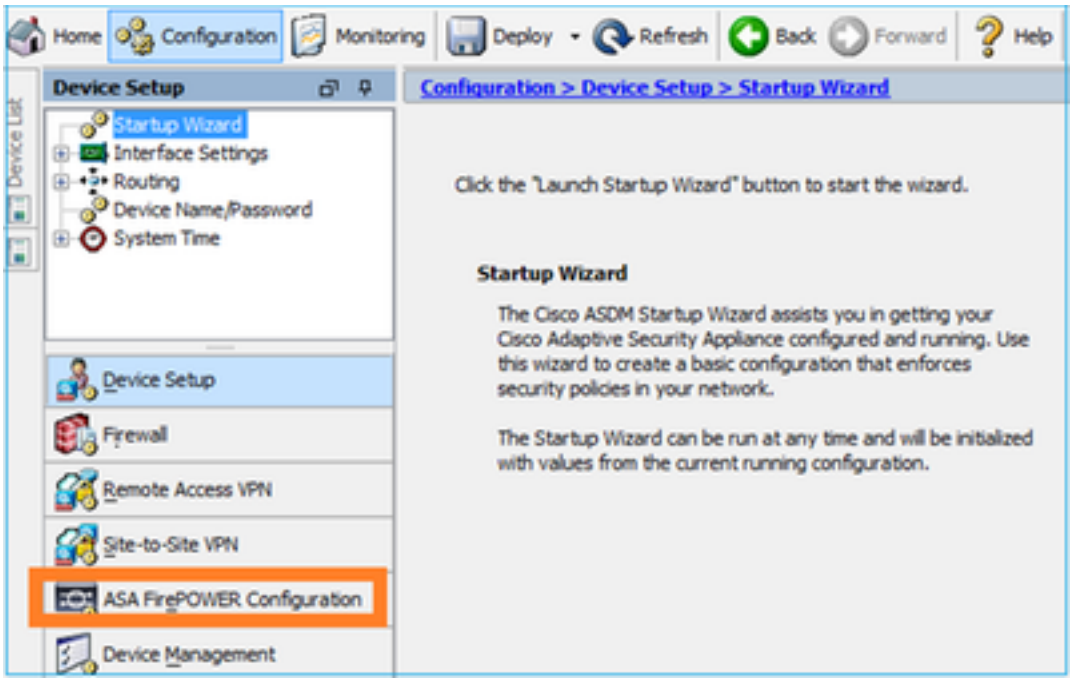
在成功认证以后ASDM从FirePOWER获取菜单项：



获取的选项卡：

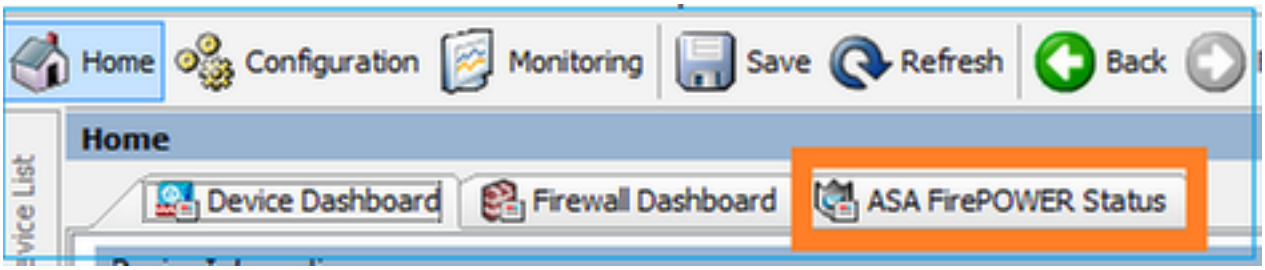


它也获取ASA FirePOWER配置菜单项目：

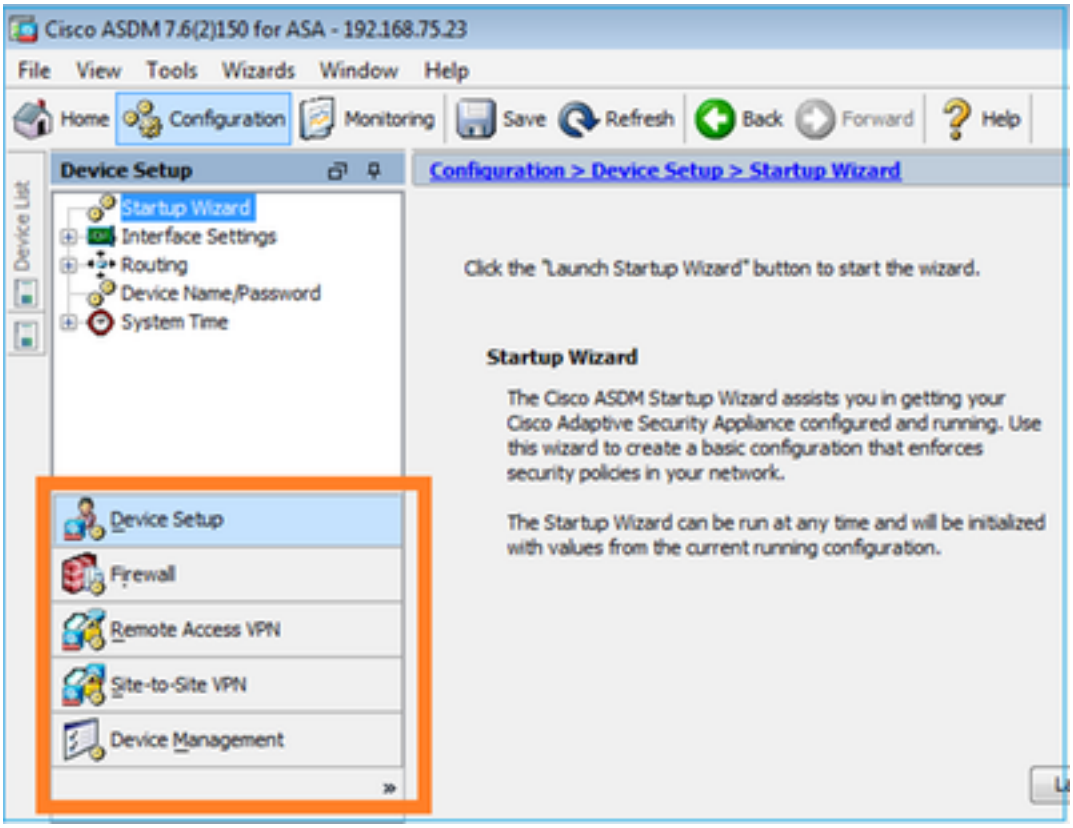


排除故障

万一ASDM不能设立有FP管理IP的一个SSL通道然后只将装载以下FirePOWER菜单项：



ASA FirePOWER配置项未命中：



推荐的操作

验证1

确保ASA管理接口启用，并且switchport连接对它在适当的VLAN ：

```
ASA5525# show interface ip brief | include Interface|Management0/0 Interface IP-Address OK?
Method Status Protocol Management0/0 unassigned YES unset up up
```

验证2

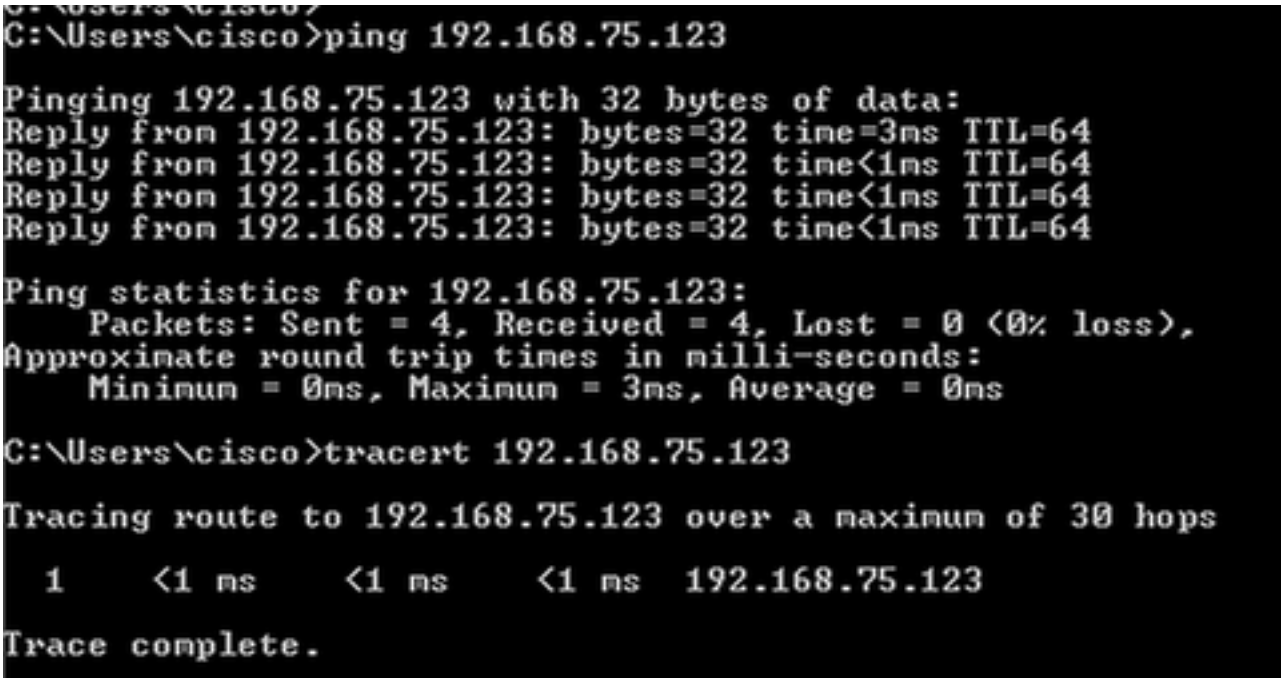
确保FirePOWER模块充分地初始化，正在运行：

```
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 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 ------------------------------------------------- >
```

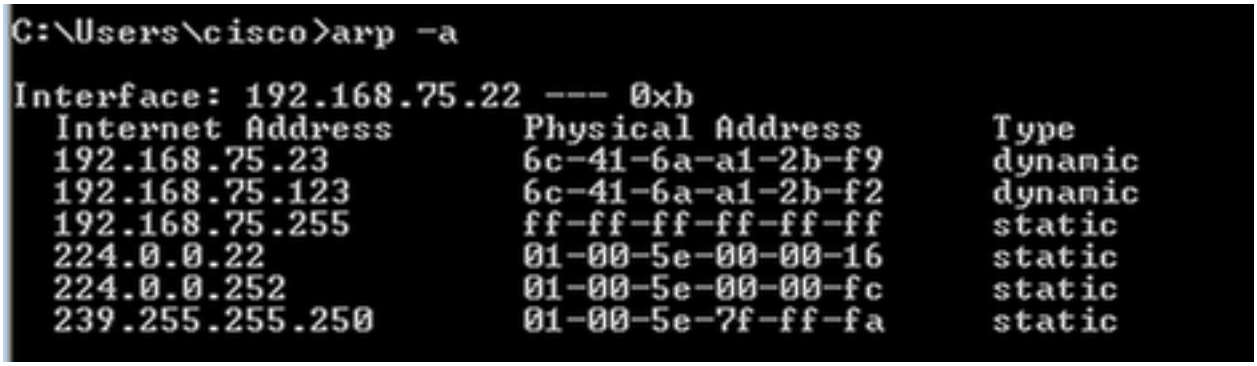
验证3

检查ASDM主机和FirePOWER模块管理IP通过使用工具类似ping和tracert/traceroute之间的基本连通性：



验证4

如果ASDM主机和FirePOWER管理IP是在同一L3网络检查ARP表在ASDM主机：



验证5

在ASDM设备的Enable (event)捕获，当您通过ASDM连接发现时是否有主机和FirePOWER模块之间的适当的TCP通信。在最低您应该看到：

- 在ASDM主机和ASA之间的TCP三通的握手
- SSL通道设立在ASDM主机和ASA之间
- 在ASDM主机和FirePOWER模块管理IP之间的TCP三通的握手
- SSL通道设立在ASDM主机和FirePOWER模块管理IP之间

验证6

到/从FirePOWER模块要检查流量您能启用在asa_mgmt_plane接口的捕获。在捕获在它之下能被看到：

- 从ASDM主机(数据包42)的ARP请求
- 从FirePOWER模块(数据包43)的ARP应答
- 在ASDM主机和FirePOWER模块(数据包之间的TCP三通的握手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 <mss
1260,nop,wscale 2,nop,nop,sackOK> 45: 20:27:28.532549 192.168.75.123.443 > 192.168.75.22.48391:
S 1324352332:1324352332(0) ack 2861923943 win 14600 <mss 1460,nop,nop,sackOK,nop,wscale 7> 46:
20:27:28.532839 192.168.75.22.48391 > 192.168.75.123.443: . ack 1324352333 win 16695
```

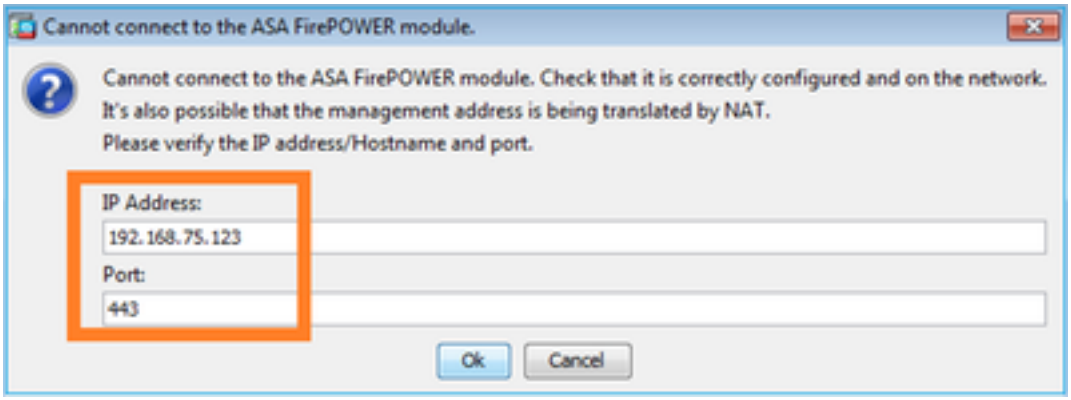
验证7

验证ASDM用户有权限级别15。一种方式确认此是通过运行**调试http 255**，当连接通过ASDM时：

```
ASA5525# debug http 255 debug http enabled at level 255. HTTP: processing ASDM request
[/admin/asdm_banner] with cookie-based authentication (aware_webvpn_conf.re2c:444) 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]
```

验证8

如果在ASDM主机和FirePOWER模块之间有Firepower管理IP的NAT然后您需要指定NAT的IP:



验证9

确保FirePOWER模块没有由Firepower管理中心(FMC)已经管理，因为在那种情况下在ASDM的FirePOWER选项卡未命中：

```
ASA5525# session sfr console Opening console session with module sfr. Connected to module sfr.
Escape character sequence is 'CTRL-^X'. > show managers Managed locally. >
```

另一个方式：

```
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
```

验证10

验证在ASA/ASDM镜像兼容的ASA兼容性指南：

http://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asamatrx.html

验证11

验证在Firepower兼容性指南FirePOWER设备是与ASDM版本兼容：

http://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html

相关文档

思科ASA FirePOWER模块快速入门指南

ASA用FirePOWER服务本地管理配置指南，版本6.1.0

ASA FirePOWER ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X和ASA5516-X的模块用户指南，版本5.4.1