使用ASDM管理ASA上的FirePOWER模块

目录

简介

背景信息

先决条件

- 要求
- 使用的组件

架构

用户通过ASDM连接到ASA时的后台操作

- 第1步-用户启动ASDM连接
- 第2步- ASDM发现ASA配置和FirePOWER模块IP地址
- 第3步- ASDM启动与FirePOWER模块的通信
- 第4步- ASDM检索FirePOWER菜单项

故障排除

相关信息

简介

本文档介绍ASDM软件如何与自适应安全设备(ASA)及其上安装的FirePOWER软件模块通信。

背景信息

ASA上安装的FirePOWER模块可通过以下方式之一进行管理：

- Firepower管理中心(FMC) -这是机下管理解决方案。
- 自适应安全设备管理器(ASDM) -这是机上管理解决方案。

先决条件

要求

启用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
```

检查ASA/SFR模块之间的兼容性，否则无法看到FirePOWER选项卡。

此外，在ASA上，必须启用3DES/AES许可证：

```
<#root>

ASA5525#

show version | in 3DES

Encryption-3DES-AES

                :

Enabled

 perpetual
```

确保ASDM客户端系统运行受支持的Java JRE版本。

使用的组件

- Microsoft Windows 7主机
- 运行ASA版本9.6(2.3)的ASA5525-X
- ASDM 版本 7.6.2.150
- FirePOWER软件模块6.1.0-330

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

架构

ASA有三个内部接口：

- asa_dataplane -用于将数据包从ASA数据路径重定向到FirePOWER软件模块。
- asa_mgmt_plane -用于允许FirePOWER管理接口与网络通信。
- cplane -控制平面接口，用于在ASA和FirePOWER模块之间传输keepalive数据包。

可以捕获所有内部接口中的流量：

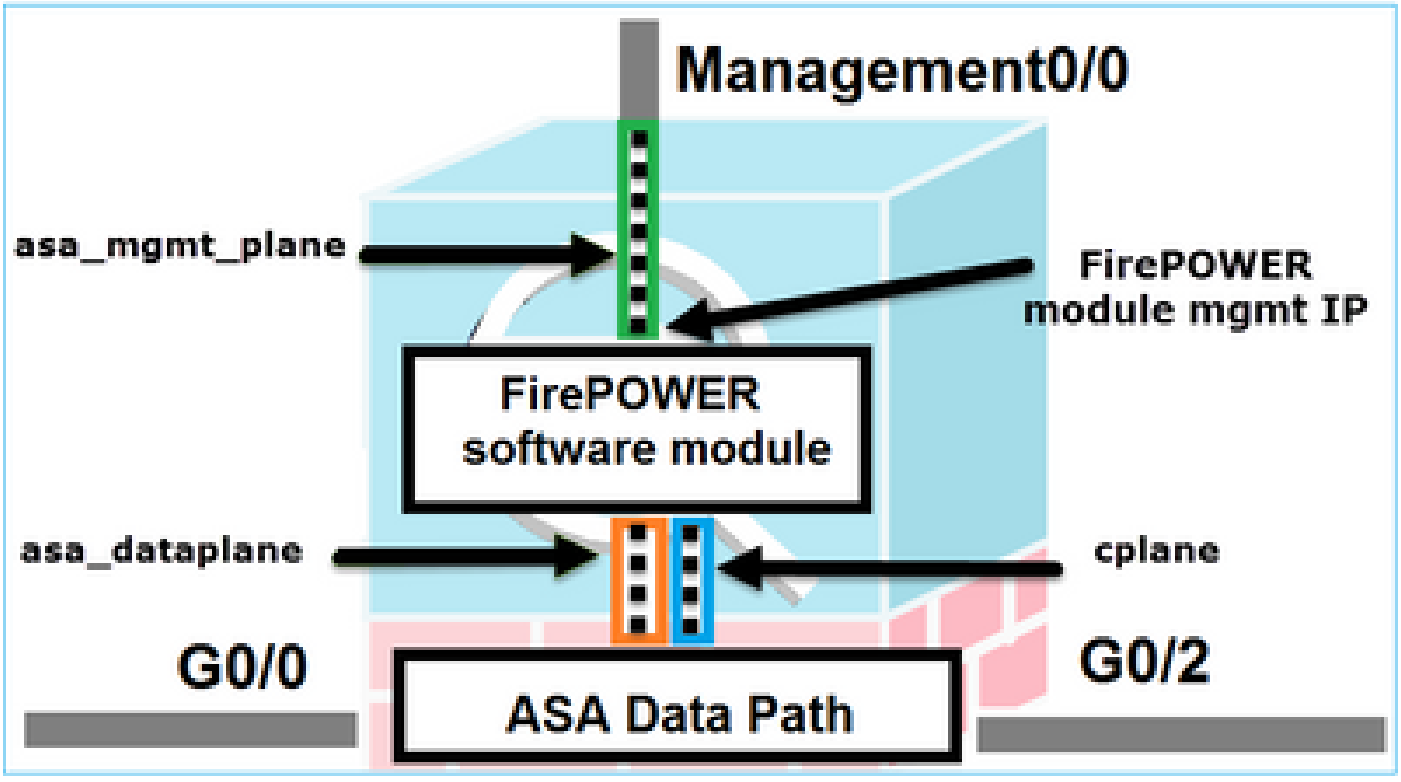
```
<#root>

ASA5525#

capture CAP interface ?

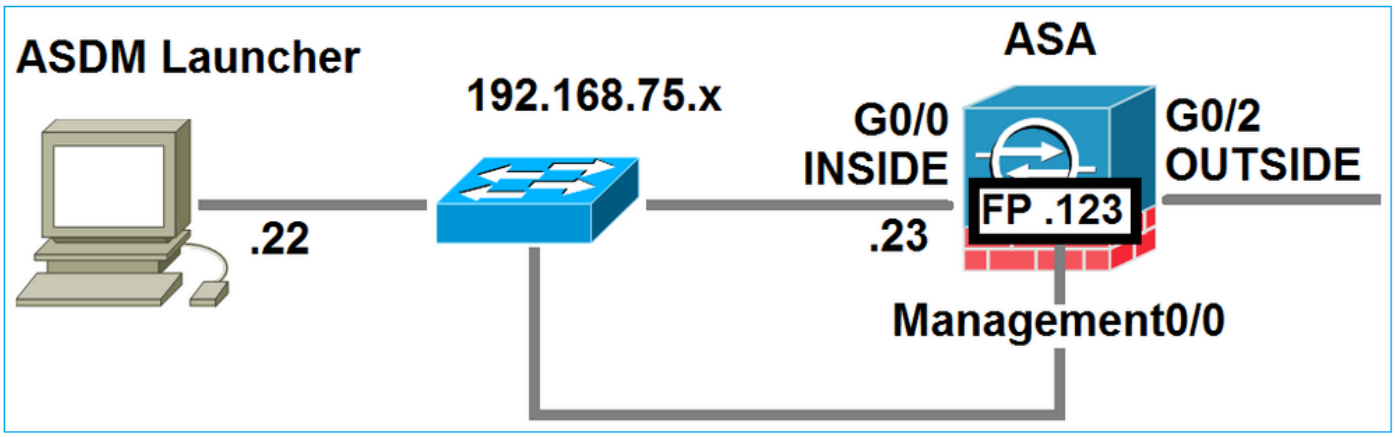

  asa_dataplane   Capture packets on dataplane interface
  asa_mgmt_plane  Capture packets on managementplane interface
  cplane          Capture packets on controlplane interface
```

可以直观地看到以下内容：



用户通过ASDM连接到ASA时的后台操作

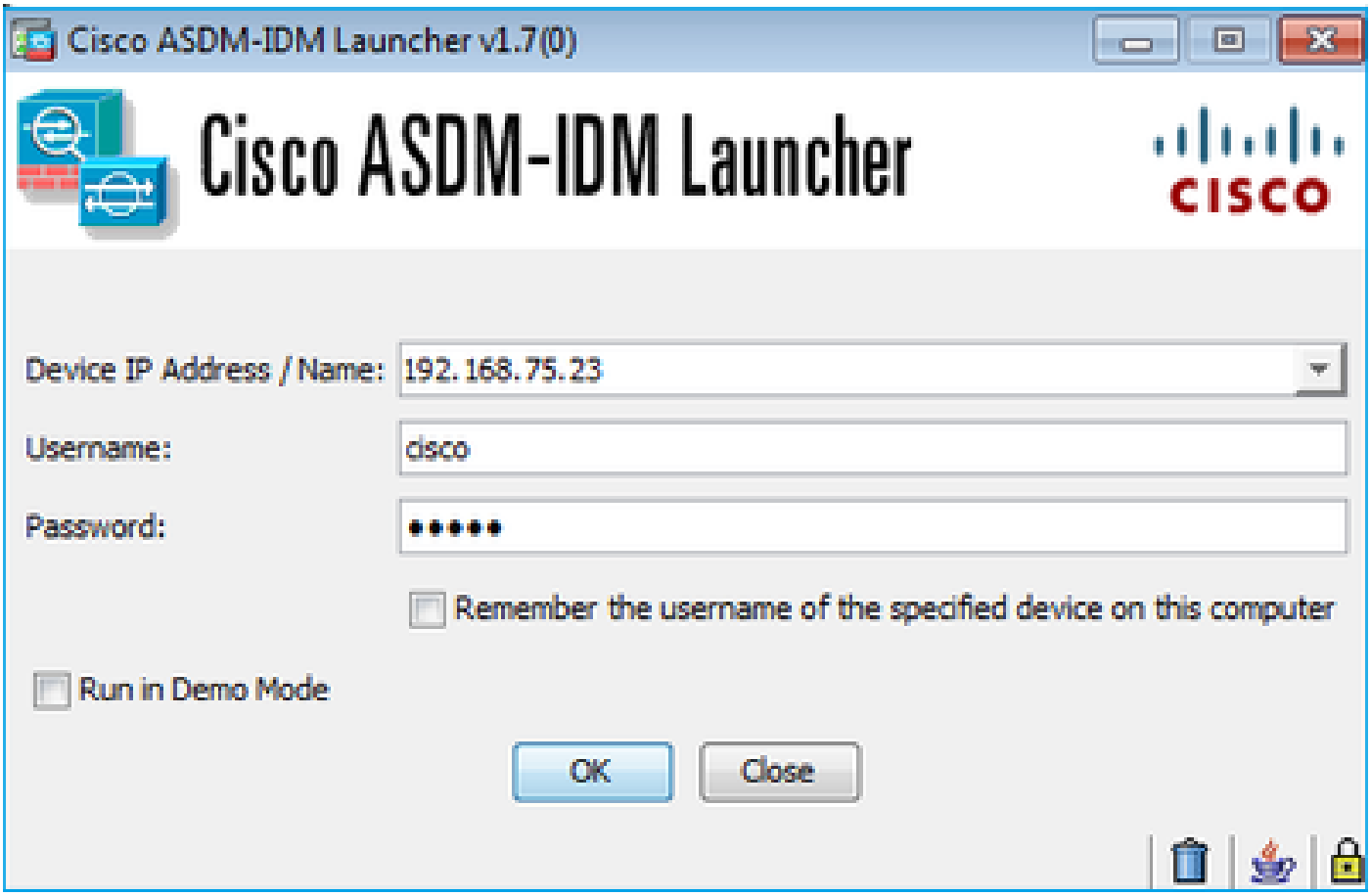
请思考以下拓扑：



当用户发起到ASA的ASDM连接时，会发生以下事件：

第1步-用户启动ASDM连接

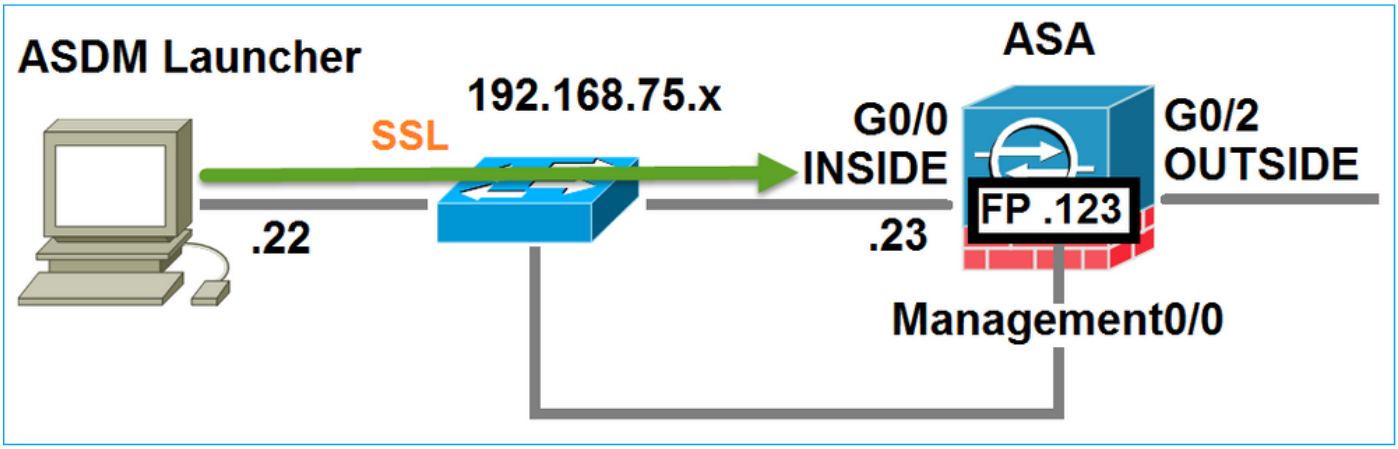
用户指定用于HTTP管理的ASA IP地址，输入凭证，然后发起与ASA的连接：



在后台，在ASDM和ASA之间建立SSL隧道：

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

可以直观地看到以下内容：



第2步- ASDM发现ASA配置和FirePOWER模块IP地址

在ASA上输入debug http 255命令，以显示ASDM连接到ASA时在后台执行的所有检查：

```
<#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
```

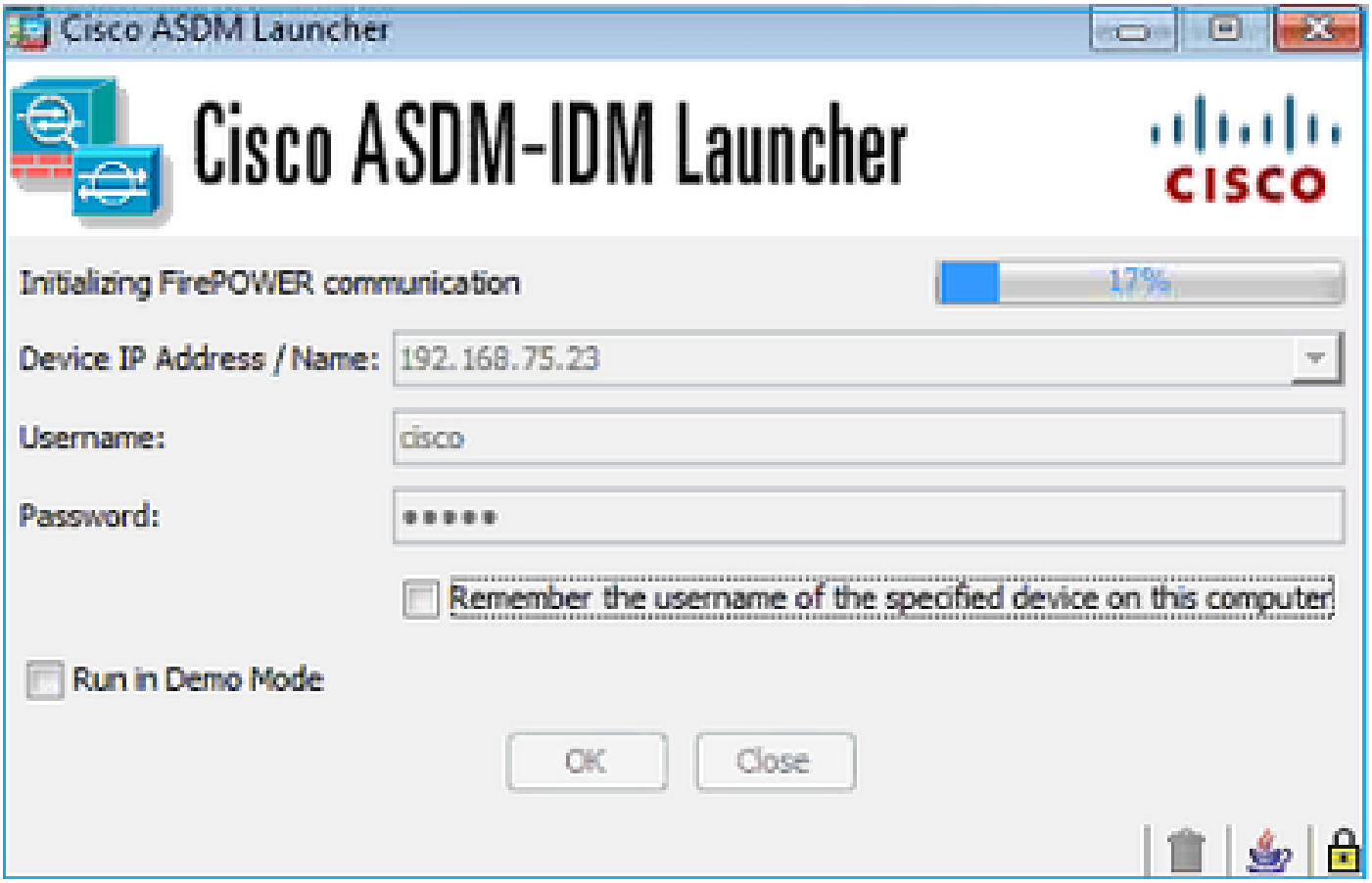
- show module - ASDM发现ASA模块。
- show module sfr details - ASDM发现模块详细信息，包括FirePOWER管理IP地址。

这些在后台显示为从PC到ASA IP地址的一系列SSL连接：

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	192.168.75.23	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启动与FirePOWER模块的通信

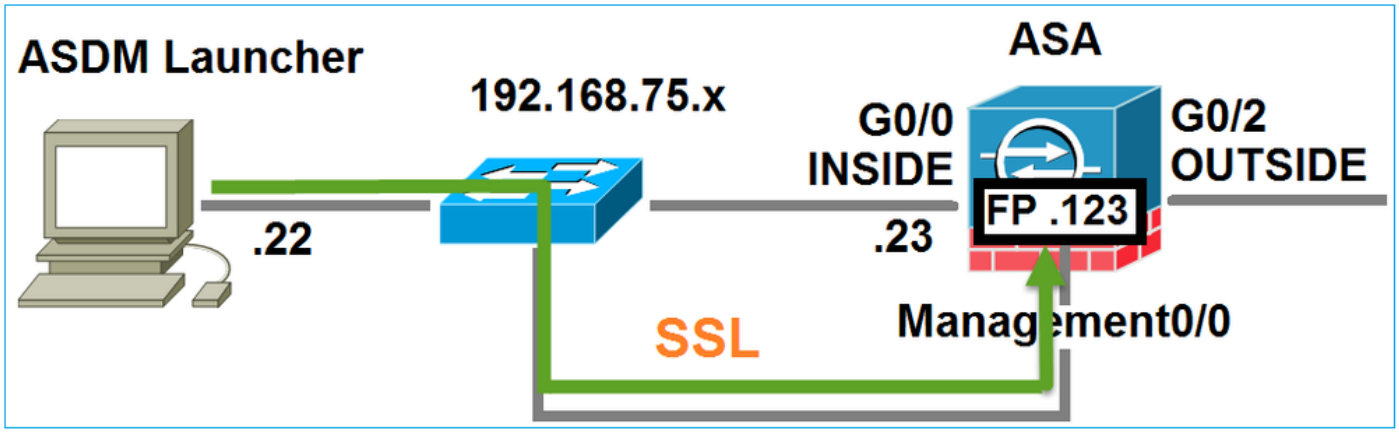
由于ASDM知道FirePOWER管理IP地址，因此它会向模块发起SSL会话：



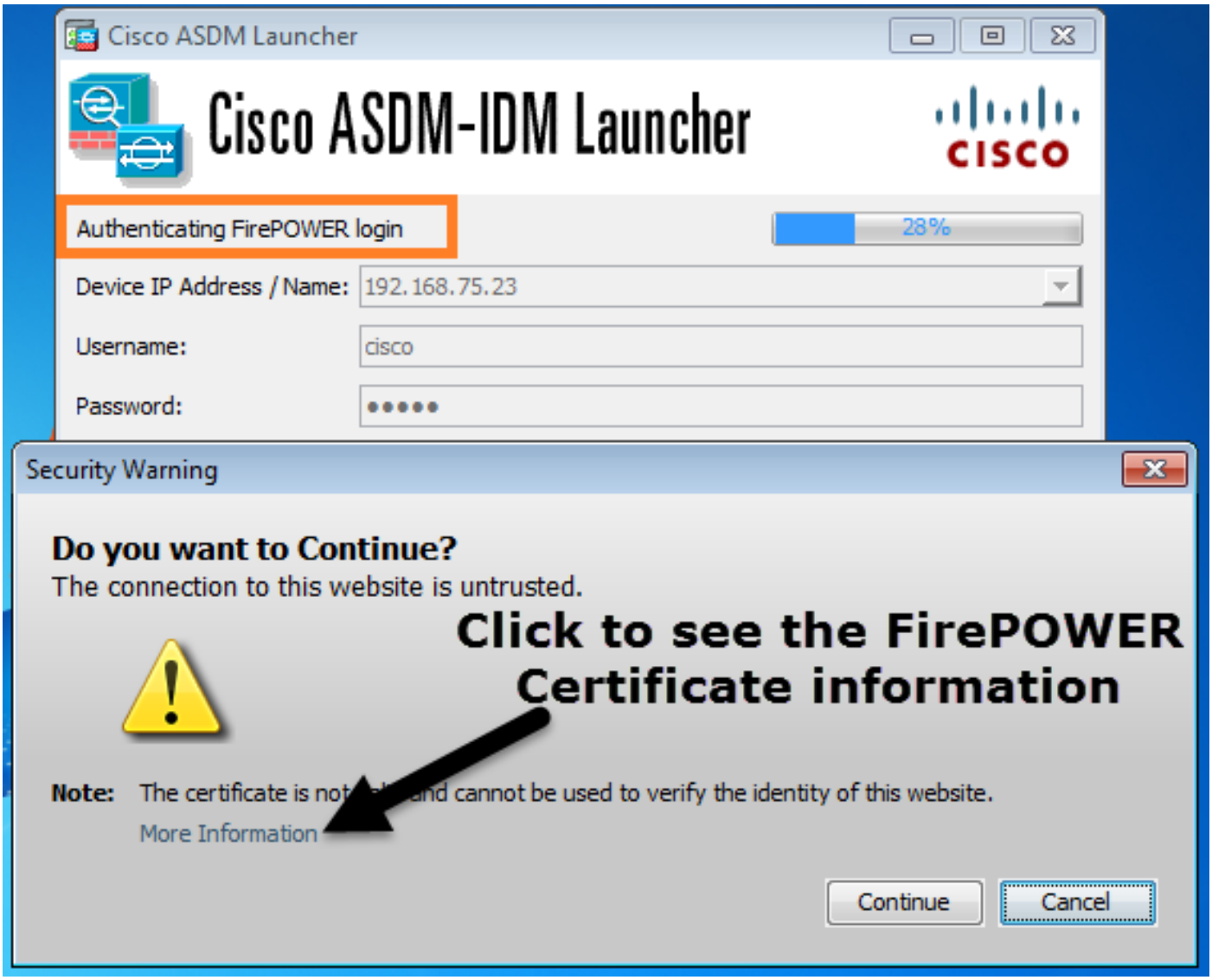
这在后台显示为从ASDM主机到FirePOWER管理IP地址的SSL连接：

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

可以直观地看到以下内容：

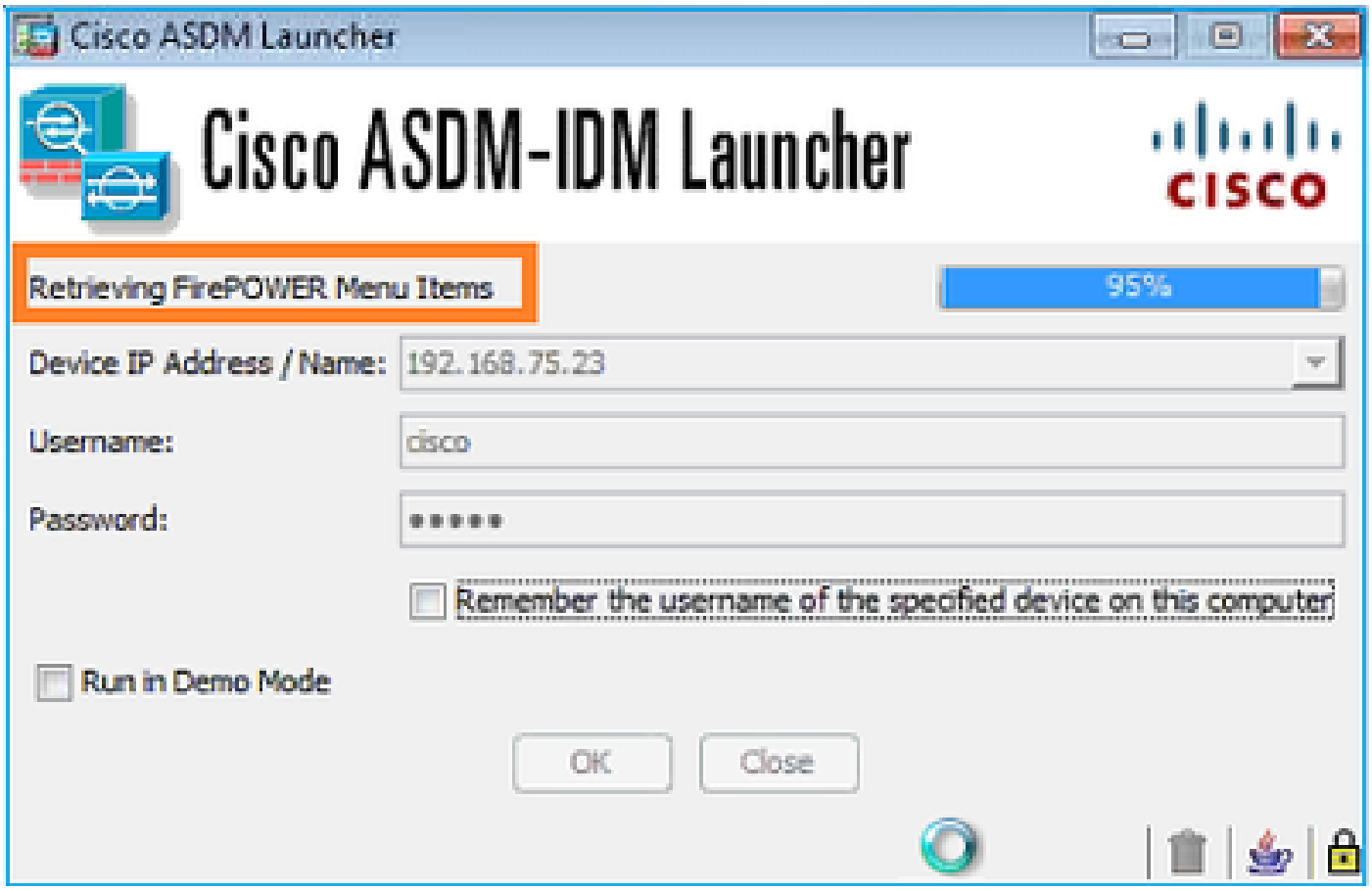


ASDM对FirePOWER进行身份验证，由于FirePOWER证书是自签名证书，因此显示安全警告：

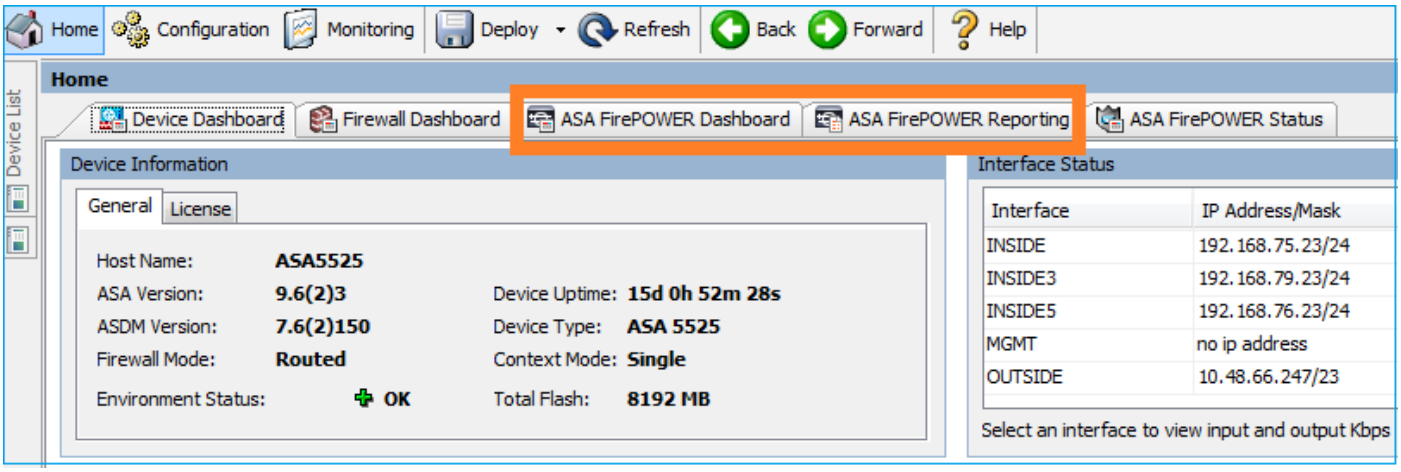


第4步- ASDM检索FirePOWER菜单项

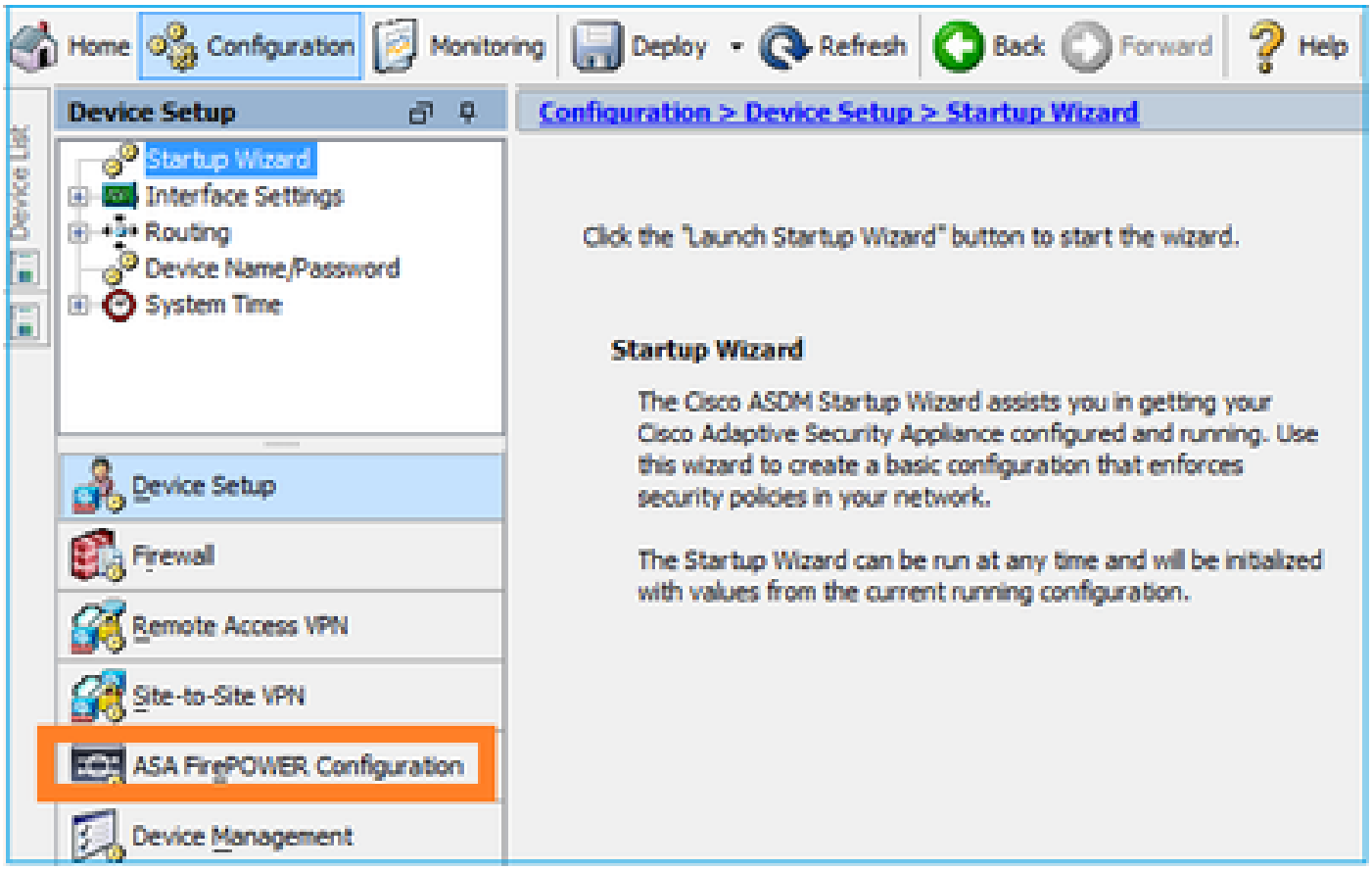
身份验证成功后，ASDM从FirePOWER设备检索菜单项：



检索到的选项卡如下例所示：

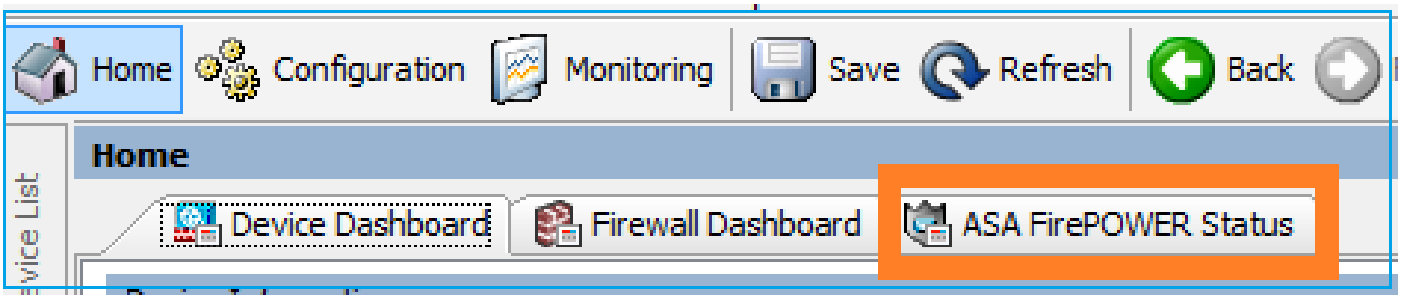


它还检索ASA FirePOWER配置菜单项：

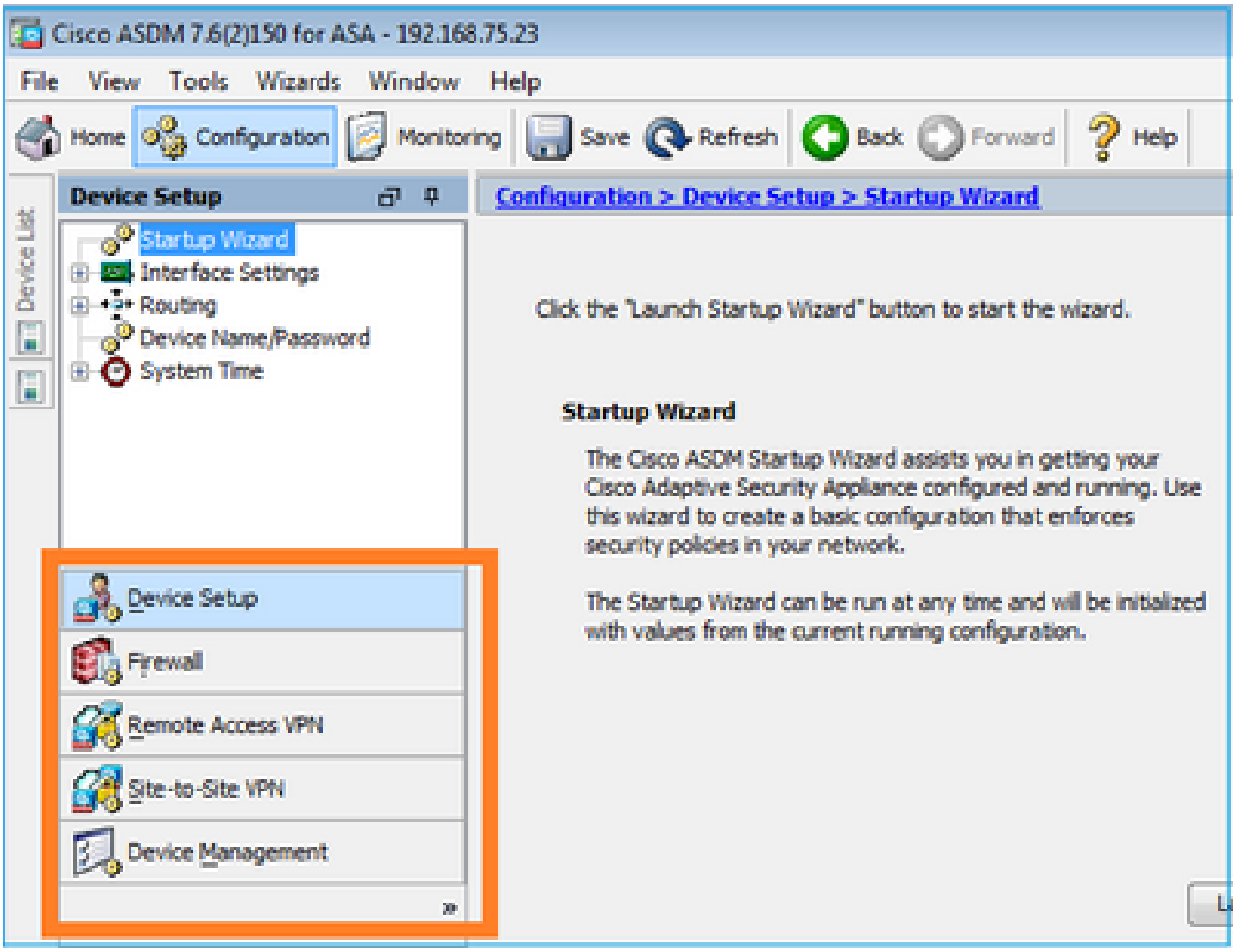


故障排除

如果ASDM无法使用FirePOWER管理IP地址建立SSL隧道，则仅加载此FirePOWER菜单项：



还缺少ASA FirePOWER配置项：



验证1

确保ASA管理接口已启动，并且连接到该接口的交换机端口位于正确的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
```

故障排除建议

- 设置正确的VLAN。
- 打开端口(检查电缆，检查交换机端口配置（速度/双工/关闭））。

验证2

确保FirePOWER模块完全初始化、已启动且正在运行：

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

>
```

故障排除建议

- 检查show module sfr log console命令的输出中是否存在错误或故障。

验证3

使用ping 和tracert/traceroute 等命令检查ASDM主机和FirePOWER模块管理IP之间的基本连接：

```
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.
```

故障排除建议

- 检查路径沿途的路由。
- 验证路径中没有阻止流量的设备。

验证4

如果ASDM主机和FirePOWER管理IP地址位于同一第3层网络中，请检查ASDM主机上的地址解析协议(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
```

故障排除建议

- 如果没有ARP条目，请使用Wireshark检查ARP通信。确保数据包的MAC地址正确。
- 如果有ARP条目，请确保它们正确。

验证5

当您通过ASDM连接时，在ASDM设备上启用捕获，以查看主机与FirePOWER模块之间是否存在正确的TCP通信。然后，您至少会看到：

- ASDM主机和ASA之间的TCP三次握手。
- 在ASDM主机和ASA之间建立SSL隧道。
- ASDM主机和FirePOWER模块管理IP地址之间的TCP三次握手。
- 在ASDM主机和FirePOWER模块管理IP地址之间建立SSL隧道。

故障排除建议

- 如果TCP三次握手失败，请确保路径中没有阻塞TCP数据包的非对称流量或设备。
- 如果SSL失败，请检查路径中是否没有设备执行中间人(MITM)（服务器证书颁发者对此提供了提示）。

验证6

要检查进出FirePOWER模块的流量，请在asa_mgmt_plane接口上启用捕获。在捕获中，您可以看到：

- ASDM主机的ARP请求（数据包42）。
- FirePOWER模块的ARP应答（数据包43）。
- ASDM主机和FirePOWER模块之间的TCP三次握手（数据包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 <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

故障排除建议

- 与验证5中的相同。

验证7

验证ASDM用户的权限级别为15。确认这一点的一种方法是在通过ASDM连接时输入**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],
```

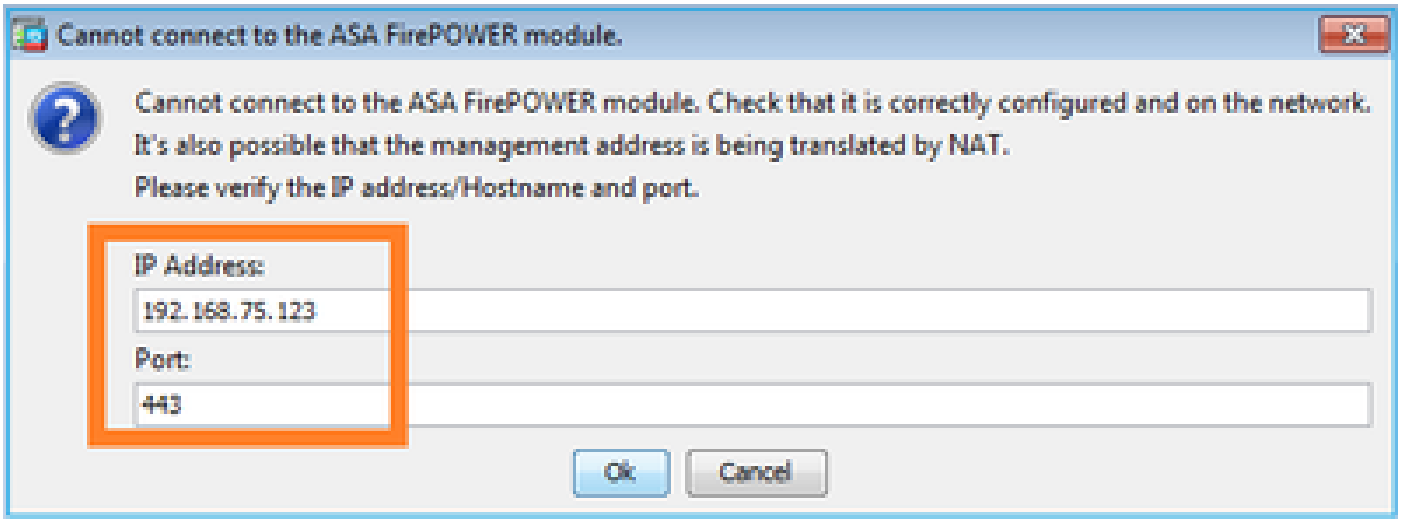
privilege = [14]

故障排除建议

- 如果权限级别不是15，请尝试使用级别为15的用户。

验证8

如果ASDM主机和FirePOWER模块之间存在FirePOWER管理IP地址的网络地址转换(NAT)，则需要指定NATed IP地址：



故障排除建议

- 终端（ASA/SFR和终端主机）的捕获信息可确认这一点。

验证9

确保FirePOWER模块未由FMC管理，因为在这种情况下，ASDM中缺少FirePOWER选项卡：

<#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.


>
```

另一个方法是**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
```

故障排除建议

- 如果设备已经受管，您需要先取消注册它，然后才能从ASDM对其进行管理。请参阅Firepower管理中心配置指南。

验证10

检查Wireshark捕获以确保ASDM客户端使用正确的TLS版本（例如TLSv1.2）连接。

故障排除建议

- 调整浏览器SSL设置。
- 尝试使用其他浏览器。
- 从其他终端主机尝试。

验证11

在思科ASA兼容性指南中验证ASA/ASDM映像是否兼容。

故障排除建议

- 使用兼容的ASDM映像。

验证12

在思科ASA兼容性指南中验证FirePOWER设备是否与ASDM版本兼容。

故障排除建议

- 使用兼容的ASDM映像。

相关信息

- **Cisco ASA FirePOWER模块快速入门指南**
- **具备FirePOWER服务的ASA的本地管理配置指南，版本6.1.0**
- **适用于ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X和ASA5516-X版本5.4.1的ASA FirePOWER模块用户指南**
- **技术支持和文档 - Cisco Systems**

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。