Use ASDM to Manage a FirePOWER Module on an ASA

Contents

Introduction

This document describes how ASDM software communicates with the Adaptive Security Appliance (ASA) and a FirePOWER software module installed on it.

Background information

A FirePOWER module that is installed on an ASA can be managed by either:

- Firepower Management Center (FMC) - This is the off-box management solution.
- Adaptive Security Device Manager (ASDM) - This is the on-box management solution.

Prerequisites

Requirements

An ASA configuration to enable ASDM management:

<#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
```

Check the compatibility between the ASA/SFR module, otherwise the FirePOWER tabs are not seen.

Additionally, on the ASA the 3DES/AES license must be enabled:

<#root>

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

```
perpetual
```

Ensure the ASDM client system runs a supported version of Java JRE.

Components Used

- A Microsoft Windows 7 host
- ASA5525-X that runs ASA Version 9.6(2.3)
- ASDM Version 7.6.2.150
- FirePOWER software module 6.1.0-330

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Architecture

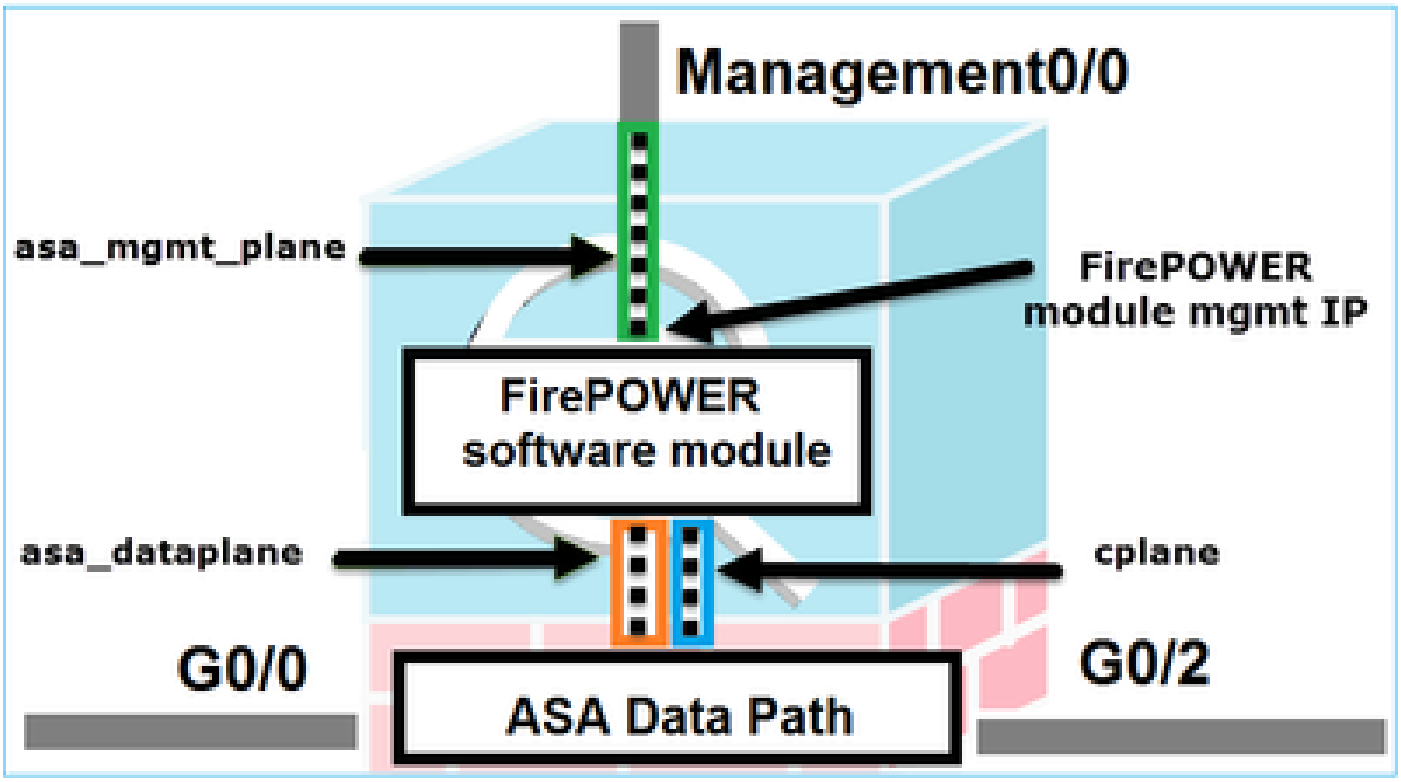
The ASA has three internal interfaces:

- asa_dataplane - It is used to redirect packets from the ASA Data Path to the FirePOWER software module.
- asa_mgmt_plane - It is used to allow the FirePOWER management interface to communicate with the network.
- cplane - Control Plane interface that is used to transfer keepalives between the ASA and the FirePOWER module.

You can capture traffic in all internal interfaces:

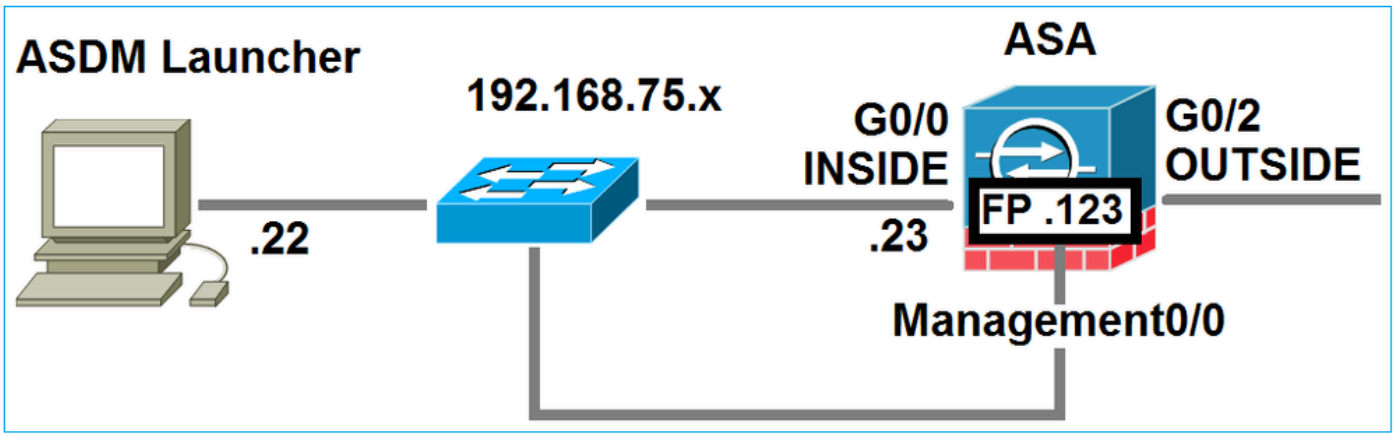
```
<#root>

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
```

This can be visualized as follows:



Background Operation When a User Connects to an ASA via ASDM

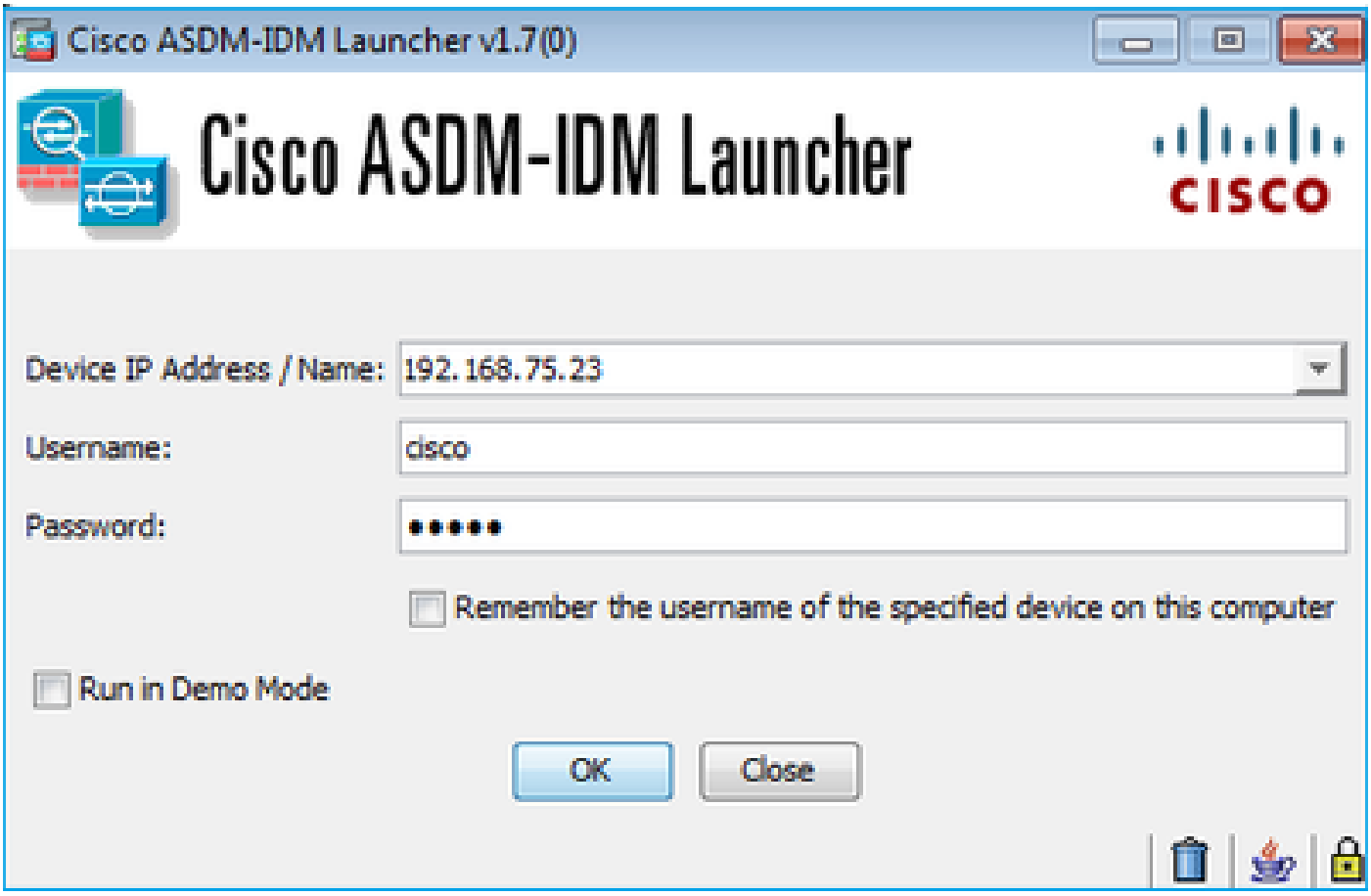
Consider this topology:



When a user initiates an ASDM connection to the ASA, these events occur:

Step 1 - The User Initiates the ASDM Connection

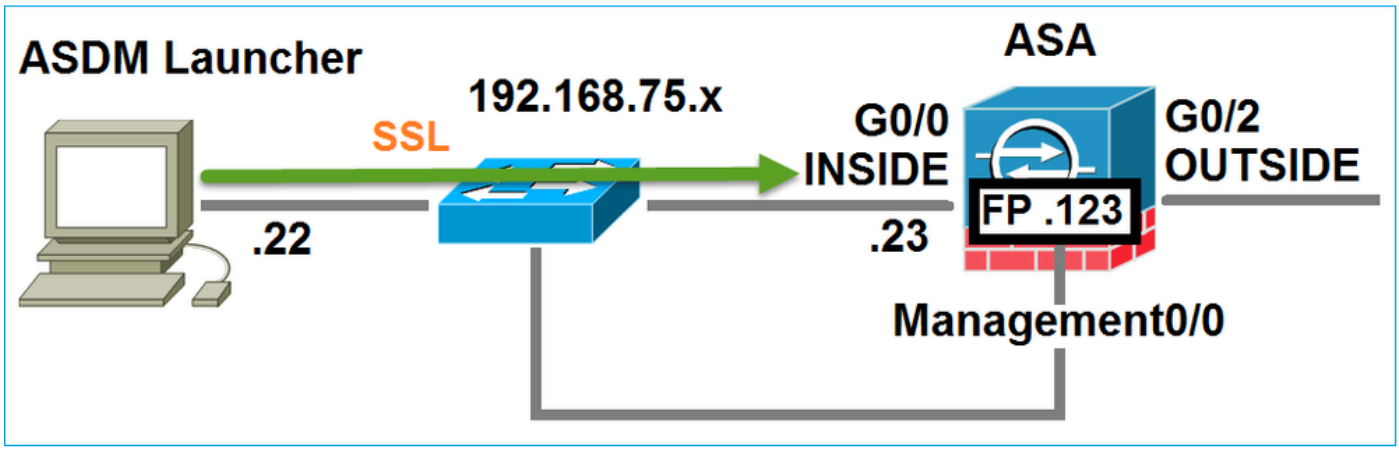
The user specifies the ASA IP address used for HTTP management, enters the credentials, and initiates a connection towards the ASA:



In the background, an SSL tunnel between the ASDM and the ASA is established:

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

This can be visualized as follows:



Step 2 - The ASDM Discovers the ASA Configuration and the FirePOWER Module IP Address

Enter the **debug http 255** command on the ASA in order to show all the checks that are done in the background when the ASDM connects to the 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
```

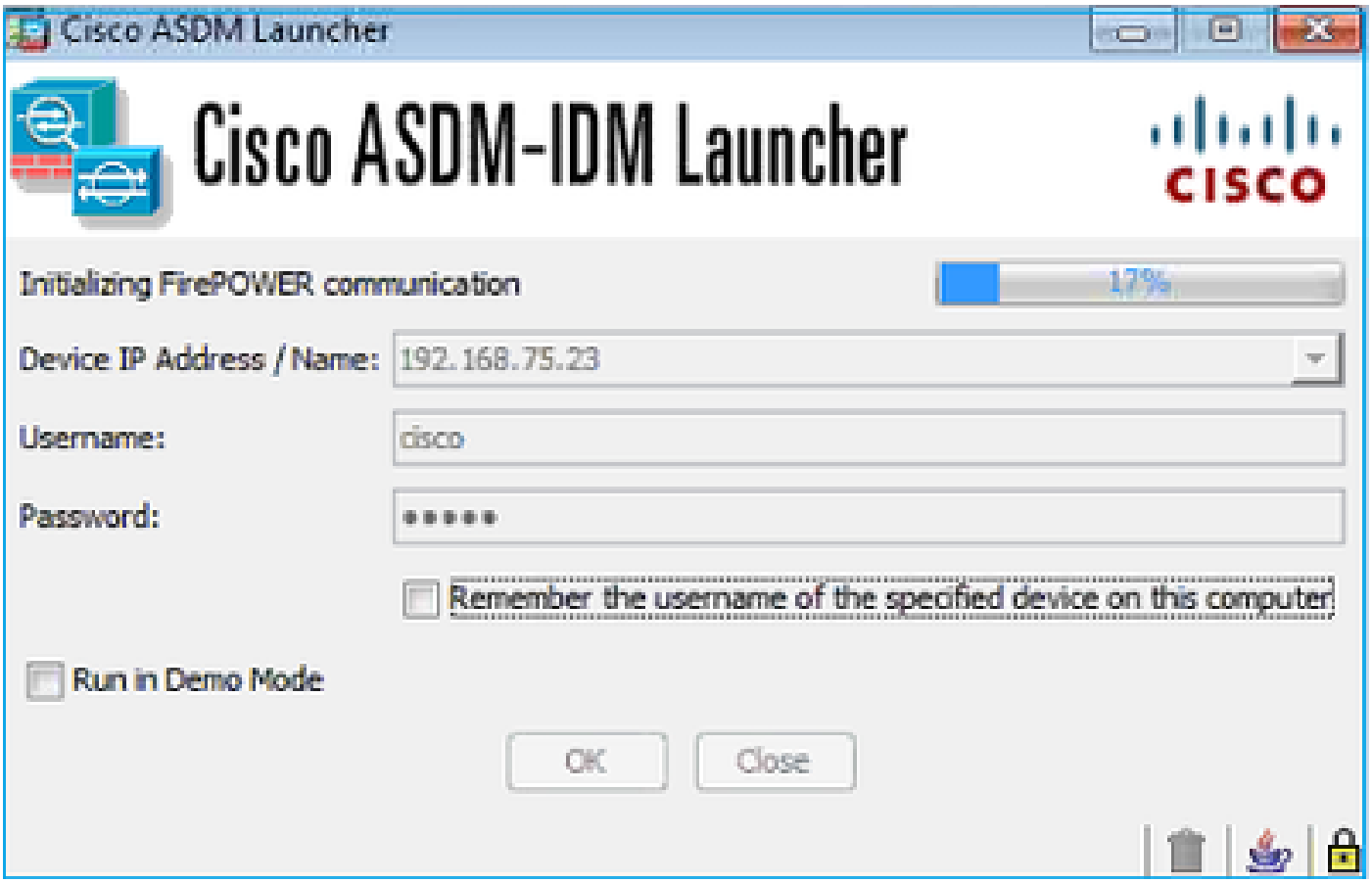
- show module - The ASDM discovers the ASA modules.
- show module sfr details - The ASDM discovers the module details, which include the FirePOWER management IP address.

These are seen in the background as a series of SSL connections from the PC towards the ASA IP address:

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

Step 3 - The ASDM Initiates Communication Towards the FirePOWER Module

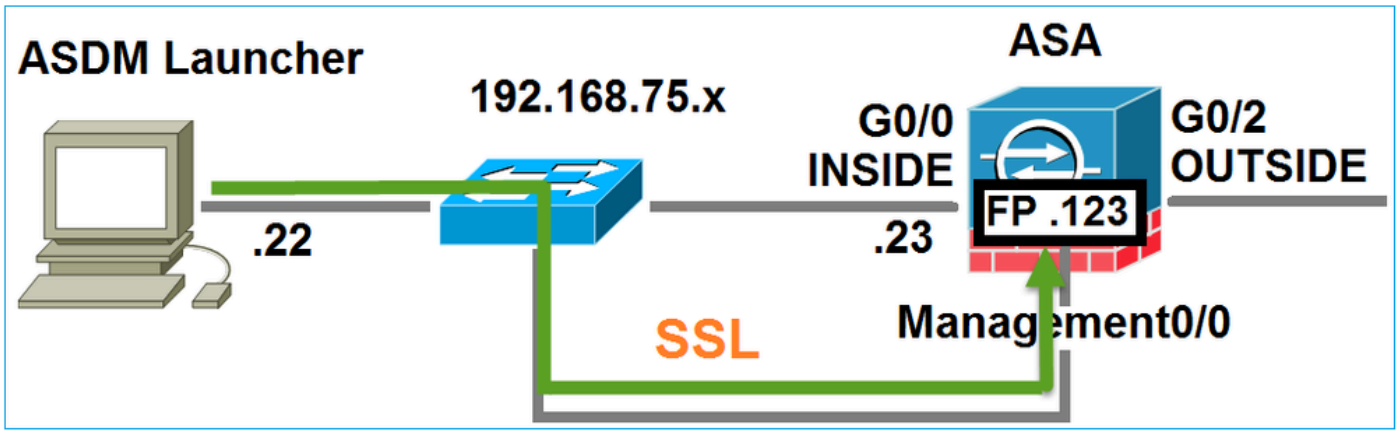
Since the ASDM knows the FirePOWER management IP address, it initiates SSL sessions towards the module:



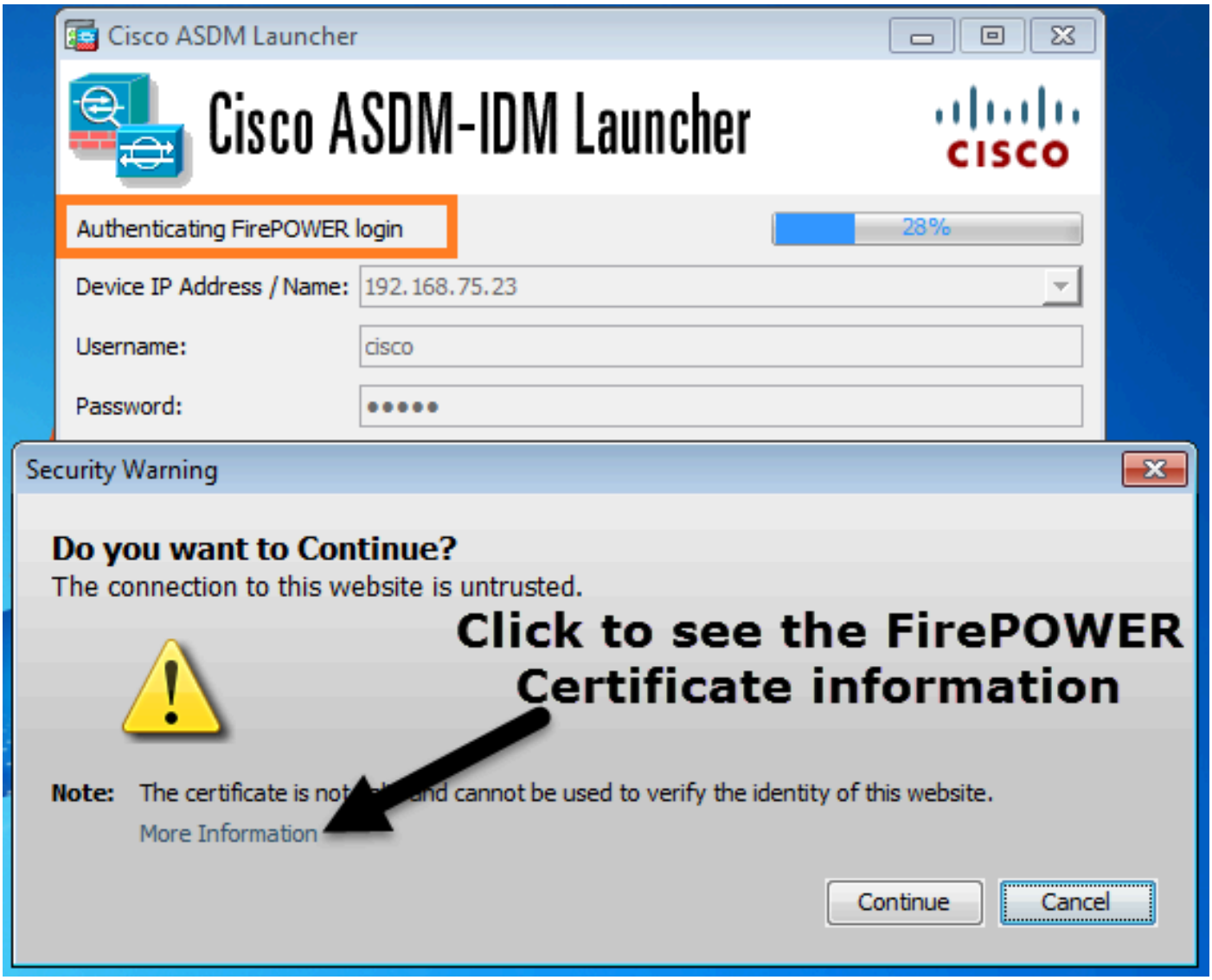
This is seen in the background as SSL connections from the ASDM host towards the FirePOWER management IP address:

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

This can be visualized as follows:

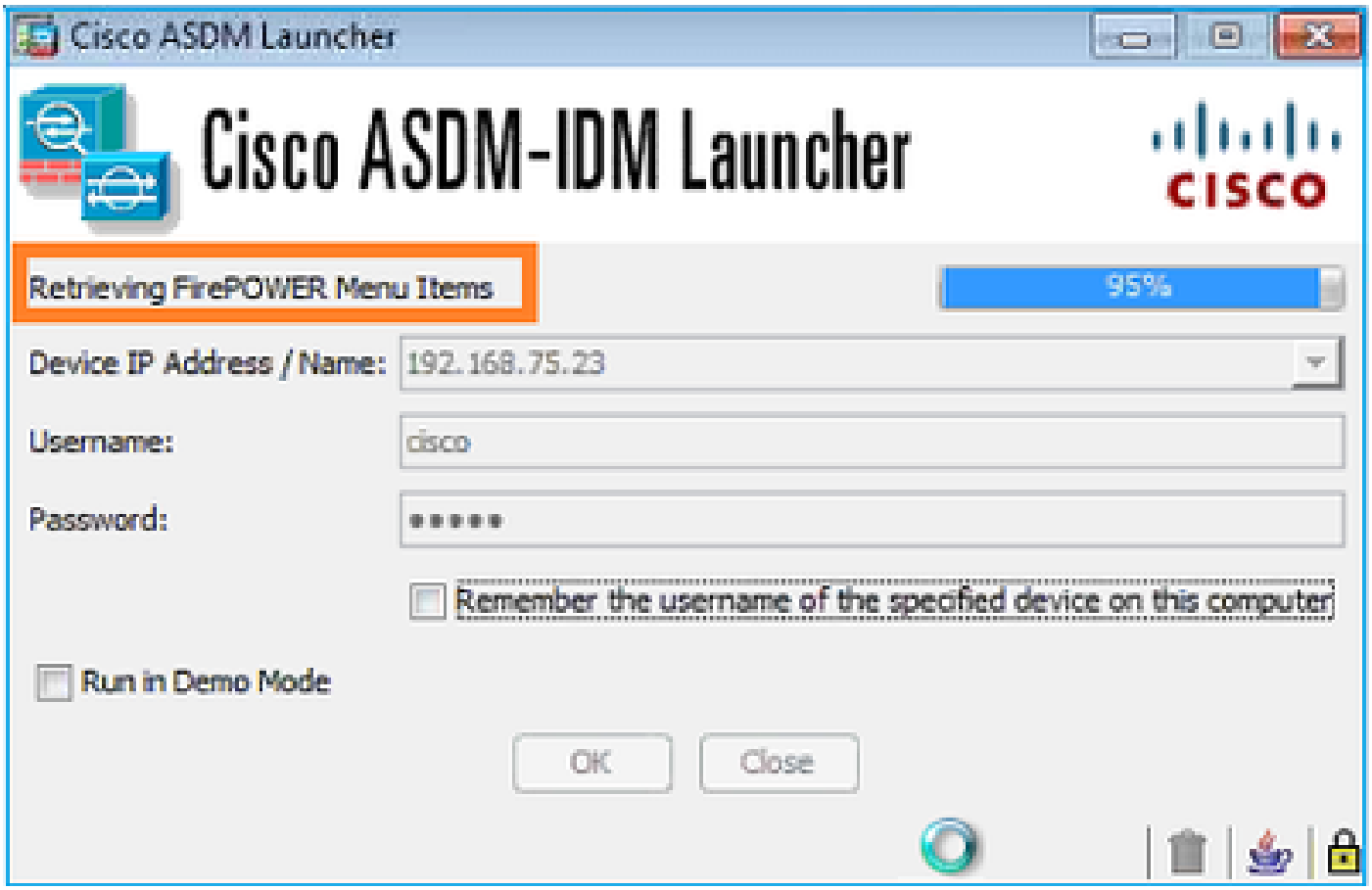


The ASDM authenticates the FirePOWER and a security warning is shown since the FirePOWER Certificate is self-signed:

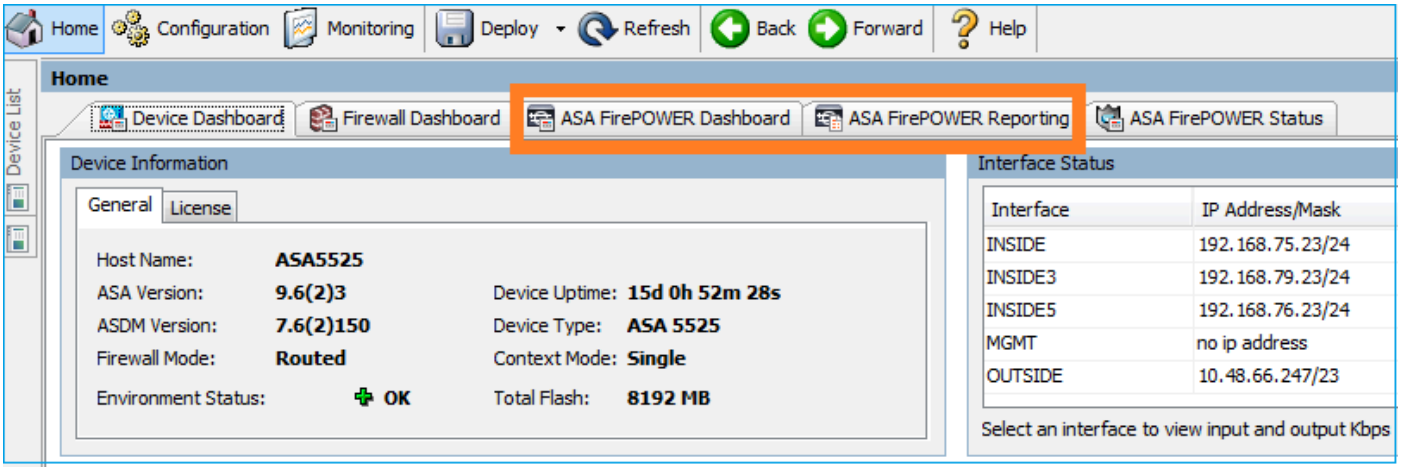


Step 4 - The ASDM Retrieves the FirePOWER Menu Items

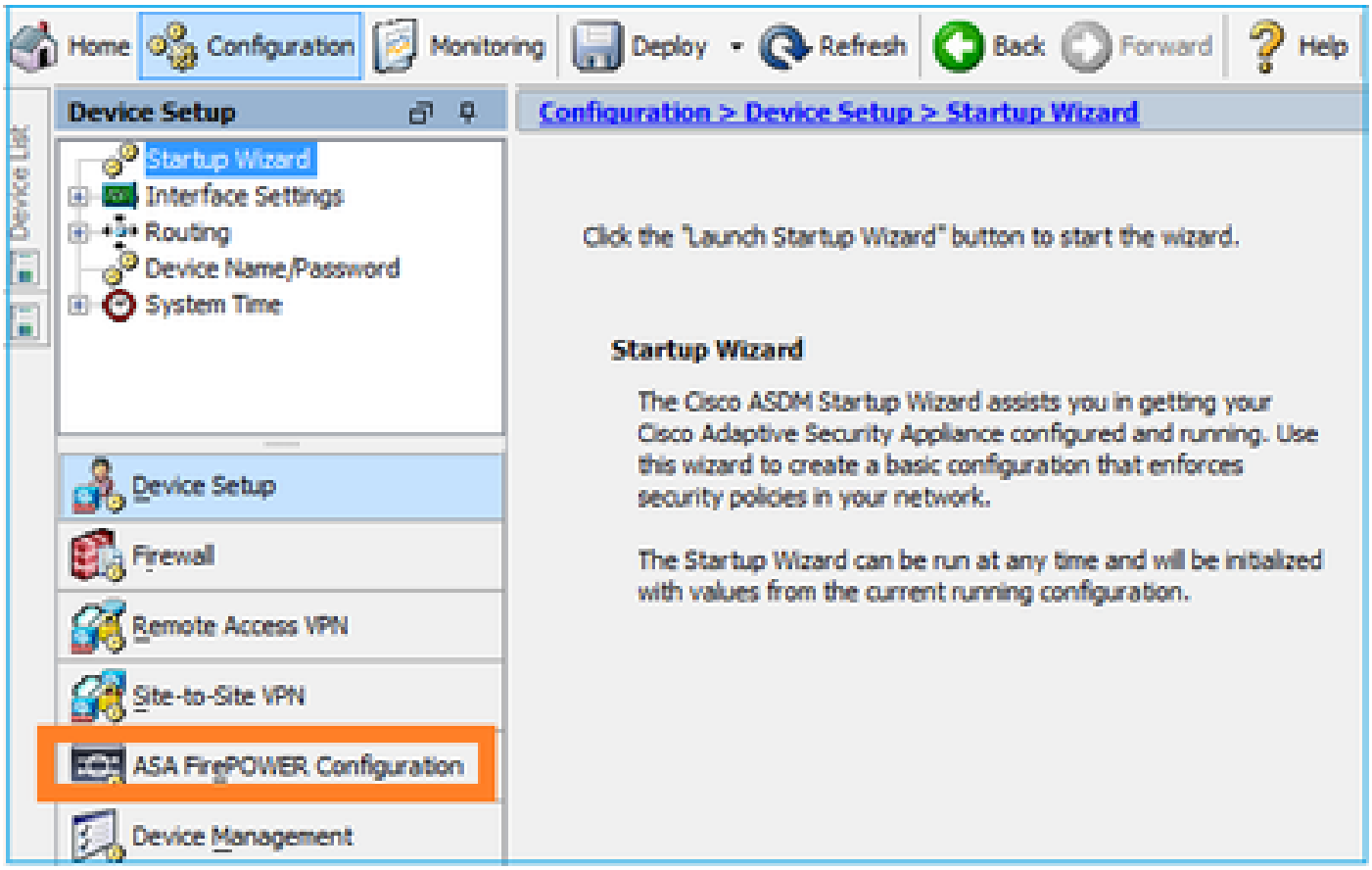
After the successful authentication, the ASDM retrieves the Menu Items from the FirePOWER device:



The retrieved tabs are shown in this example:

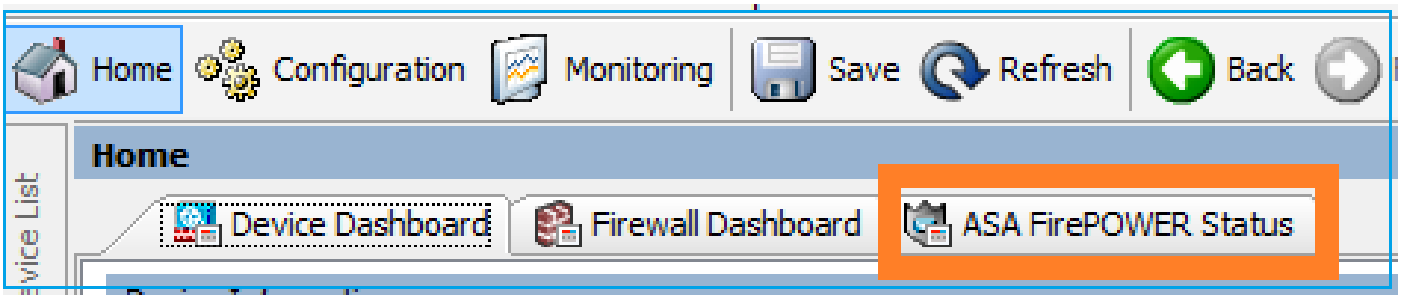


It also retrieves the ASA FirePOWER Configuration Menu Item:

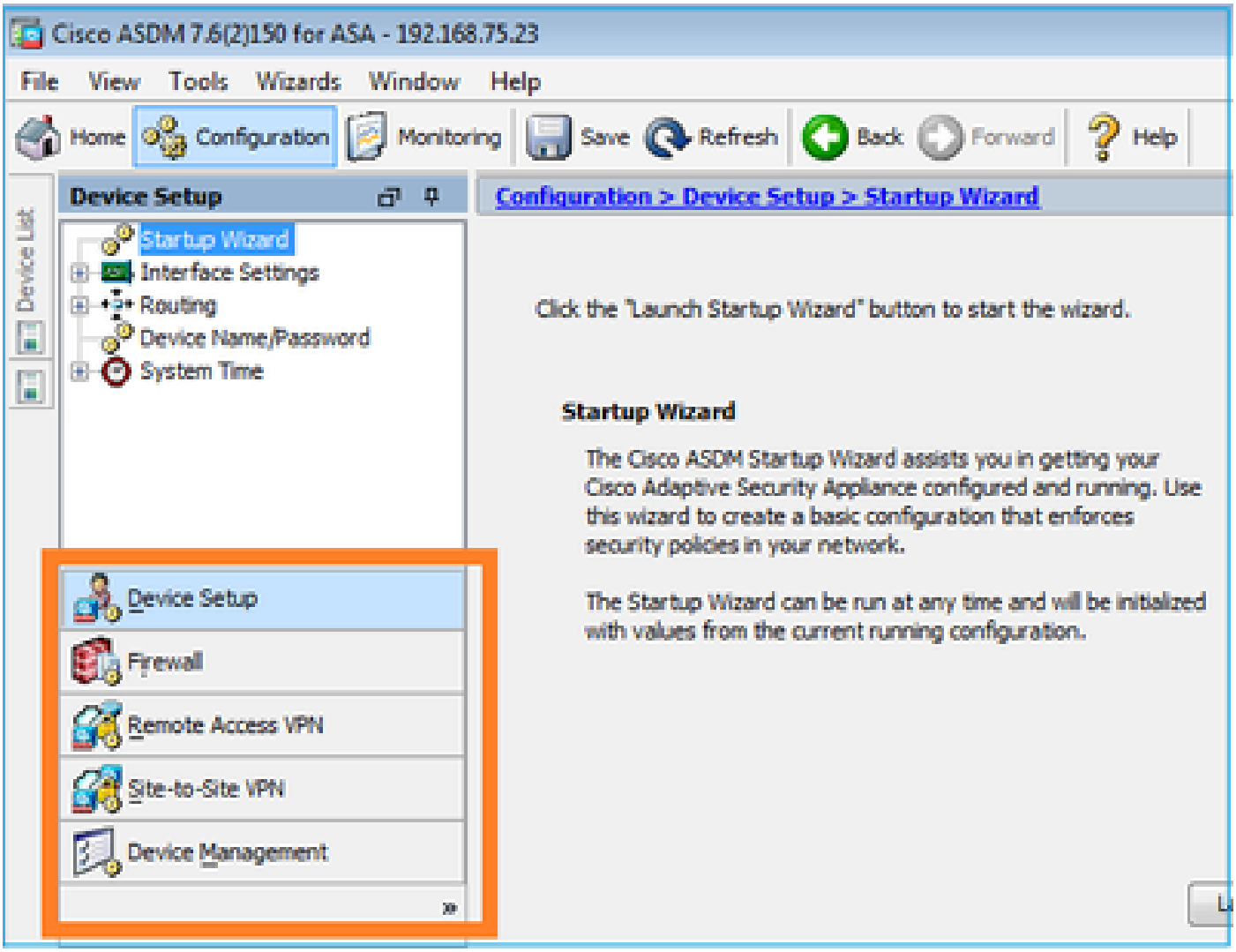


Troubleshoot

In case ASDM cannot establish an SSL tunnel with the FirePOWER Management IP address, it only loads this FirePOWER Menu Item:



The ASA FirePOWER Configuration Item is missing as well:



Verification 1

Make sure that the ASA management interface is UP and the switchport connected to it is in the proper VLAN:

```
<#root>

ASA5525#

show interface  ip brief | include Interface|Management0/0

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

up                    up
```

Recommended Troubleshooting

- Set the proper VLAN.
- Bring the port UP (check the cable, check the switchport configuration (speed/duplex/shut)).

Verification 2

Make sure that the FirePOWER module is fully initialized, UP, and running:

```
<#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
----------------------------------------------------

>
```

Recommended Troubleshooting

- Check the output of the **show module sfr log console** command for errors or failures.

Verification 3

Check basic connectivity between the ASDM host and the FirePOWER module management IP with commands such as **ping** and **tracert/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.
```

Recommended Troubleshooting

- Check routing along the path.
- Verify that there are no devices in the path that block the traffic.

Verification 4

If the ASDM host and the FirePOWER management IP address are in the same Layer 3 network, check the Address Resolution Protocol (ARP) table on the ASDM host:

```
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
```

Recommended Troubleshooting

- If there are no ARP entries, use Wireshark in order to check the ARP communication. Ensure the

MAC addresses of the packets are correct.
- If there are ARP entries, ensure they are correct.

Verification 5

Enable capture on the ASDM device while you connect via ASDM in order to see if there is proper TCP communication between the host and the FirePOWER module. At a minimum, you then see:

- TCP 3-way handshake between the ASDM host and the ASA.
- SSL tunnel established between the ASDM host and the ASA.
- TCP 3-way handshake between the ASDM host and the FirePOWER module management IP address.
- SSL tunnel established between the ASDM host and the FirePOWER module management IP address.

Recommended Troubleshooting

- If the TCP 3-way handshake fails, ensure that there is not asymmetric traffic or devices in the path that block the TCP packets.
- If SSL fails, check if there is no device in the path doing man-in-the-middle (MITM) (the Server Certificate Issuer gives a hint for this).

Verification 6

In order to check the traffic to and from the FirePOWER module, enable capture on the asa_mgmt_plane interface. In the capture, you can see the:

- ARP request from the ASDM host (packet 42).
- ARP reply from the FirePOWER module (packet 43).
- TCP 3-way handshake between the ASDM host and the FirePOWER module (packets 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

Recommended Troubleshooting

- Same as in Verification 5.

Verification 7

Verify that the ASDM user has privilege level 15. One way to confirm this is to enter the **debug http 255** command while it connects via ASDM:

<#root>

ASA5525#

debug http 255

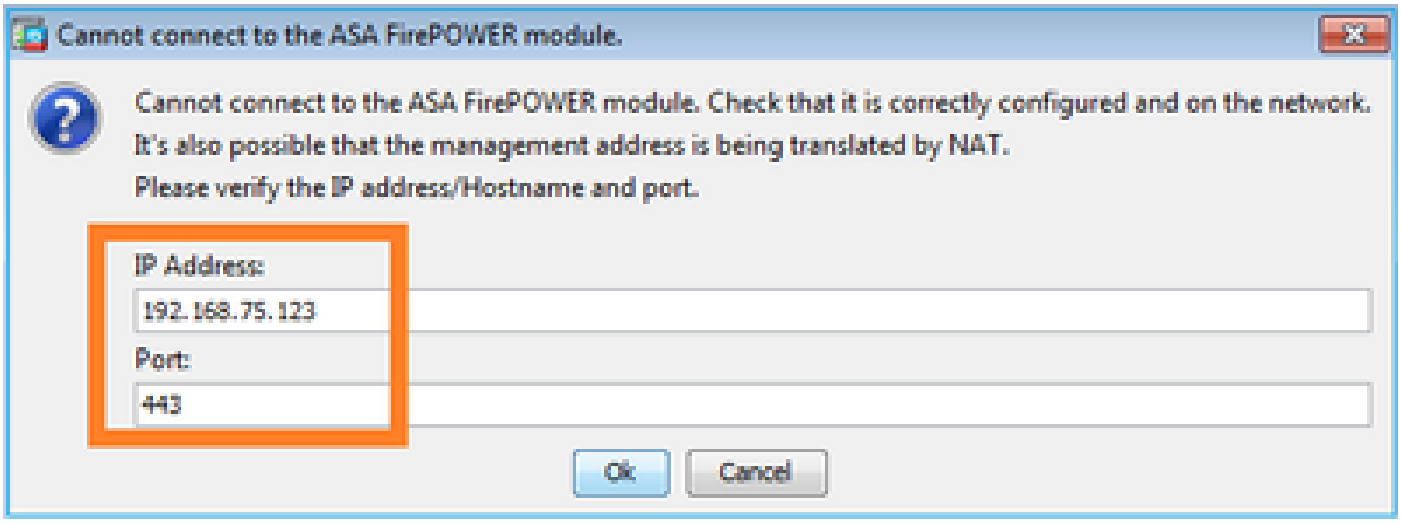
```
debug http enabled at level 255.
HTTP: processing ASDM request [/admin/asdm_banner] with cookie-based authentication (aware_webvpn_conf.
HTTP: check admin session. Cookie index [2][c8a06c50]
HTTP: Admin session cookie [A27614B@20480@78CF@58989AACB80CE5159544A1B3EE62661F99D475DC]
HTTP: Admin session idle-timeout reset
HTTP: admin session verified =  [1]
HTTP: username = [user1],
privilege = [14]
```

Recommended Troubleshooting

- If the privilege level is not 15, then try with a user that has level 15.

Verification 8

If between the ASDM host and the FirePOWER module there is network adddress translation (NAT) for the FirePOWER Management IP address, then you need to specify the NATed IP address:



Recommended Troubleshooting

- Captures at the end points (ASA/SFR and end-host) confirms this.

Verification 9

Make sure that the FirePOWER module is not already managed by FMC, because in that case the FirePOWER tabs in ASDM is missing:

```
<#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.
```

>

Another method is with the **show module sfr details** command:

<#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
```

Recommended Troubleshooting

- If the device is already managed, you need to unregister it before you manage it from ASDM. See the Firepower Management Center Configuration Guide.

Verification 10

Check the wireshark capture in order to ensure the ASDM client connects with a proper TLS version (for example, TLSv1.2).

Recommended Troubleshooting

- Tune the browser SSL settings.
- Try with another browser.
- Try from another end-host.

Verification 11

Verify in the Cisco ASA Compatibility guide that the ASA/ASDM images are compatible.

Recommended Troubleshooting

- Use a compatible ASDM image.

Verification 12

Verify in the Cisco ASA Compatibility guide that the FirePOWER device is compatible with the ASDM version.

Recommended Troubleshooting

- Use a compatible ASDM image.

Related Information

- **Cisco ASA FirePOWER Module Quick Start Guide**
- **ASA with FirePOWER Services Local Management Configuration Guide, Version 6.1.0**
- **ASA FirePOWER Module User Guide for the ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X, and ASA5516-X, Version 5.4.1**
- **Technical Support & Documentation - Cisco Systems**