Verwenden von ASDM zum Verwalten eines FirePOWER-Moduls auf einer ASA

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Architektur
Hintergrundoperation Wenn ein Benutzer über ASDM eine Verbindung mit einer ASA herstellt
Schritt 1: Der Benutzer initiiert die ASDM-Verbindung.
Schritt 2: Der ASDM ermittelt die ASA-Konfiguration und die IP-Adresse des FirePOWER-Moduls.
Schritt 3: Der ASDM initiiert die Kommunikation zum FirePOWER-Modul.
Schritt 4: ASDM ruft die FirePOWER-Menüelemente ab
Fehlerbehebung
Zugehörige Informationen

Einführung

In diesem Dokument wird beschrieben, wie die ASDM-Software (Adaptive Security Device Manager) mit der auf der Adaptive Security Appliance (ASA) installierten Adaptive Security Appliance und einem auf ihr installierten FirePOWER-Softwaremodul kommuniziert.

Ein auf einer ASA installiertes FirePOWER-Modul kann wie folgt verwaltet werden:

- FirePOWER Management Center (FMC) - Hierbei handelt es sich um die eigenständige Verwaltungslösung.
- ASDM - Hierbei handelt es sich um die interne Verwaltungslösung.

Voraussetzungen

Anforderungen

Eine ASA-Konfiguration für ASDM-Management:

```
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
```

Prüfen Sie die Kompatibilität zwischen dem ASA/SFR-Modul, da ansonsten die FirePOWER-Registerkarten nicht angezeigt werden.

Zusätzlich sollte auf der ASA die 3DES/AES-Lizenz aktiviert werden:

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

Stellen Sie sicher, dass das ASDM-Client-System eine unterstützte Version von Java JRE ausführt.

Verwendete Komponenten

- Ein Microsoft Windows 7-Host
- ASA5525-X mit ASA Version 9.6(2.3)
- ASDM-Version 7.6.2.150
- FirePOWER-Softwaremodul 6.1.0-330

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Architektur

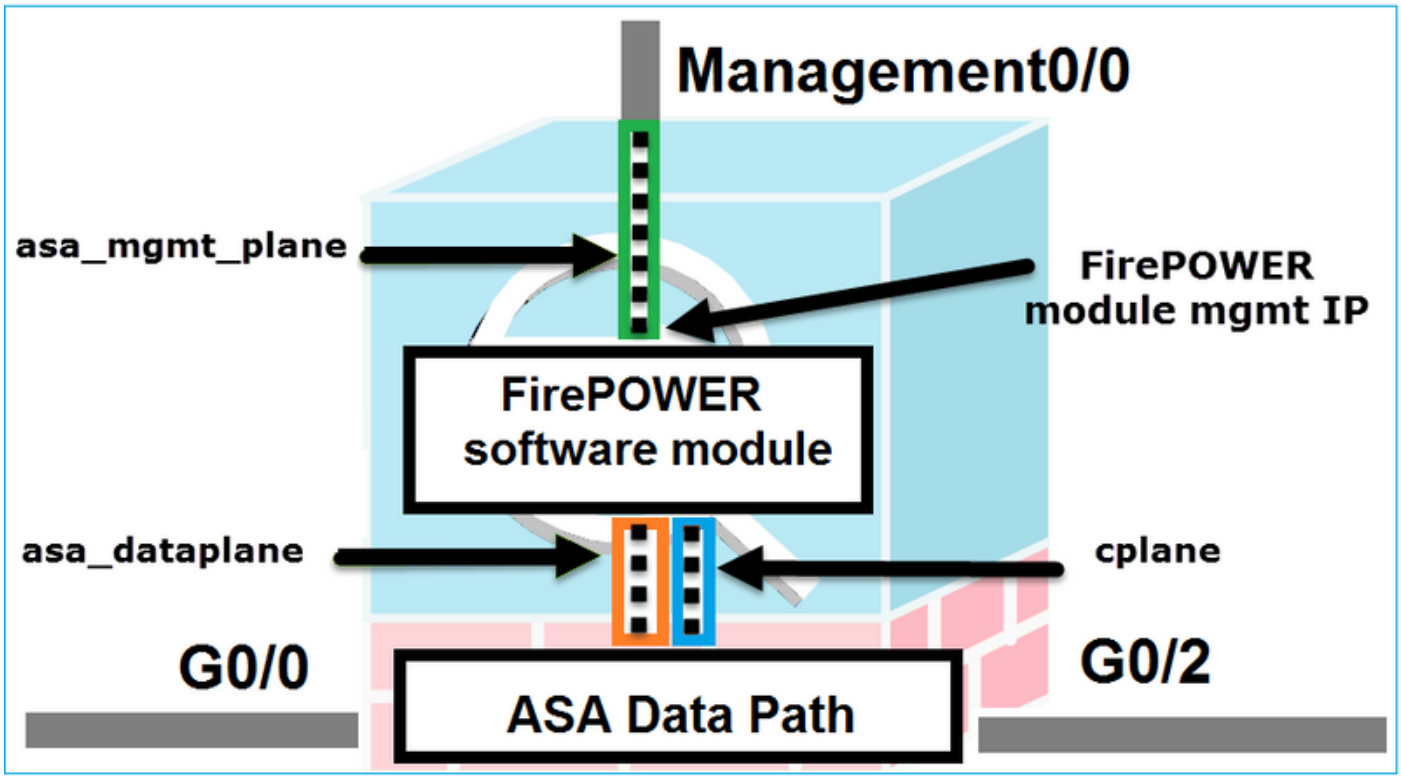
Die ASA verfügt über drei interne Schnittstellen:

- asa_dataplane - Wird zum Umleiten von Paketen vom ASA-Datenpfad zum FirePOWER-Softwaremodul verwendet.
- asa_mgmt_plane - Diese dient dazu, der FirePOWER-Verwaltungsschnittstelle die Kommunikation mit dem Netzwerk zu ermöglichen.
- Ebene - Kontrollebenen-Schnittstelle, die zum Übertragen von Keepalives zwischen ASA und dem FirePOWER-Modul verwendet wird.

Sie können den Datenverkehr an allen internen Schnittstellen erfassen:

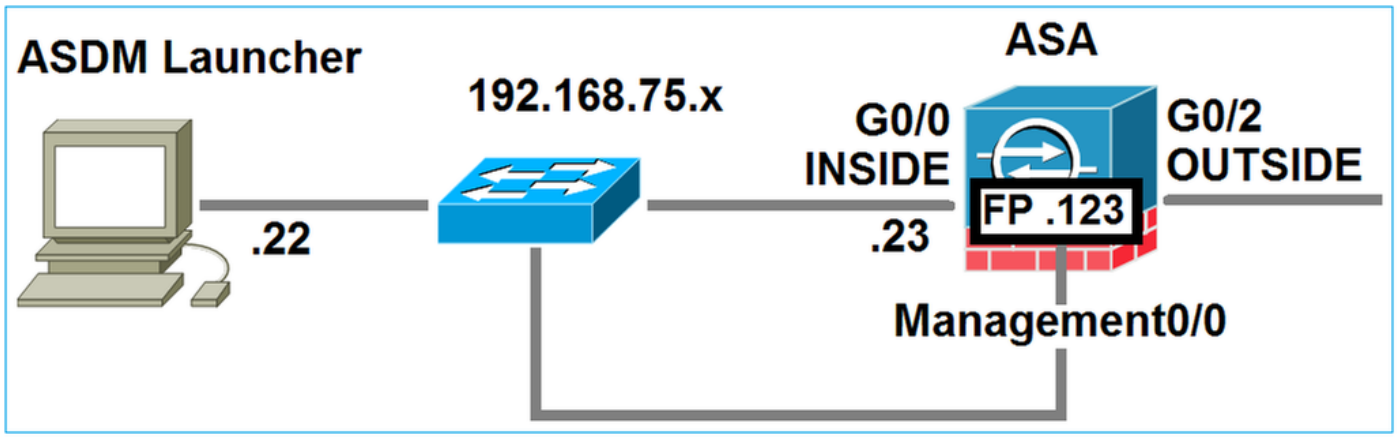
```
ASA5525# capture CAP interface ?

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

Dies kann wie folgt visualisiert werden:



Hintergrundoperation Wenn ein Benutzer über ASDM eine Verbindung mit einer ASA herstellt

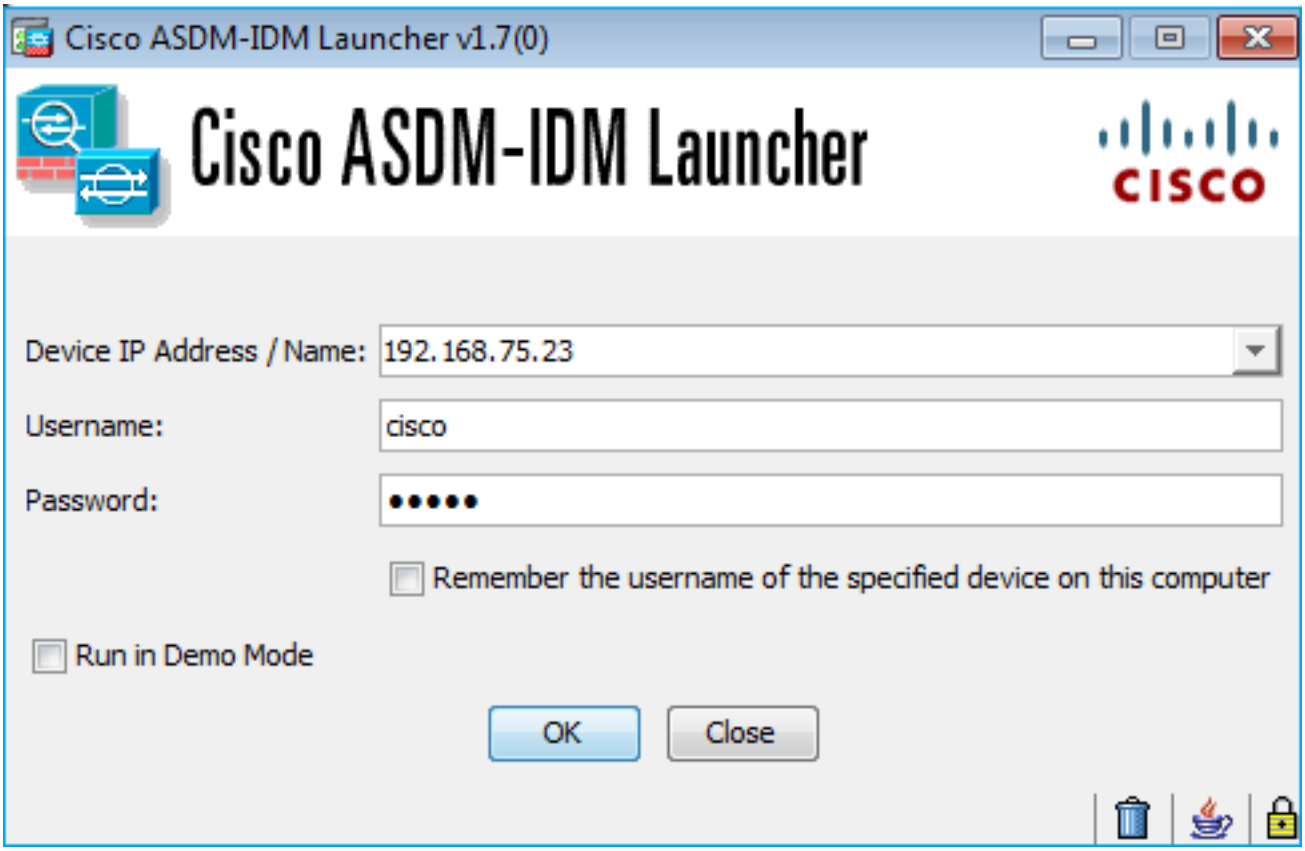
Betrachten Sie die folgende Topologie:



Wenn ein Benutzer eine ASDM-Verbindung zur ASA herstellt, treten folgende Ereignisse auf:

Schritt 1: Der Benutzer initiiert die ASDM-Verbindung.

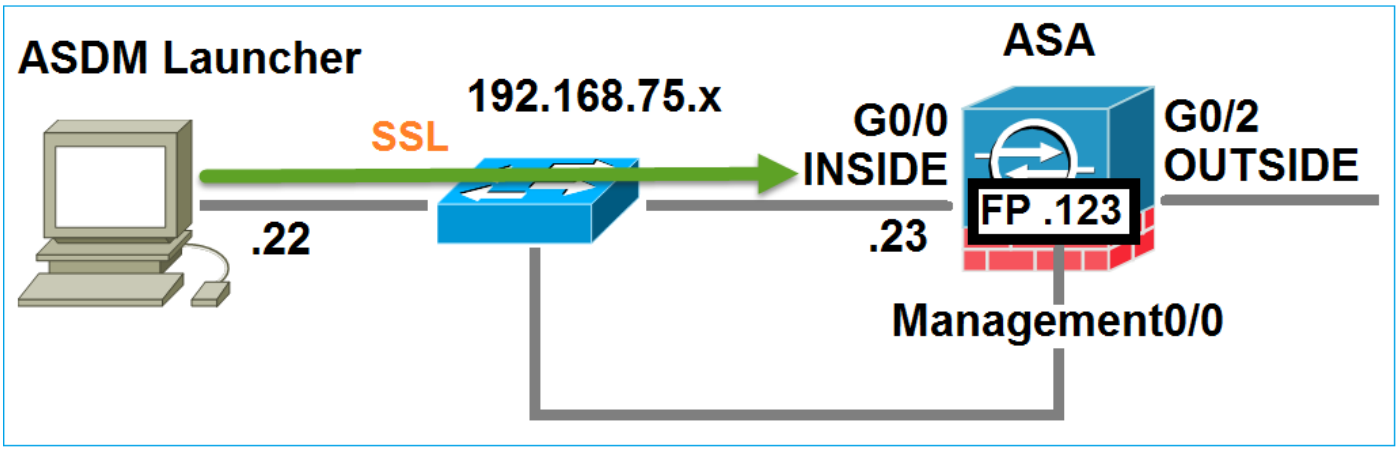
Der Benutzer gibt die für das HTTP-Management verwendete ASA-IP-Adresse an, gibt die Anmeldeinformationen ein und initiiert eine Verbindung zur ASA:



Im Hintergrund wird ein SSL-Tunnel zwischen dem ASDM und der ASA eingerichtet:

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

Dies kann wie folgt visualisiert werden:



Schritt 2: Der ASDM ermittelt die ASA-Konfiguration und die IP-Adresse des FirePOWER-Moduls.

Geben Sie den Befehl **debug http 255** auf der ASA ein, um alle im Hintergrund ausgeführten Überprüfungen anzuzeigen, wenn der ASDM eine Verbindung zur ASA herstellt:

```
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
```

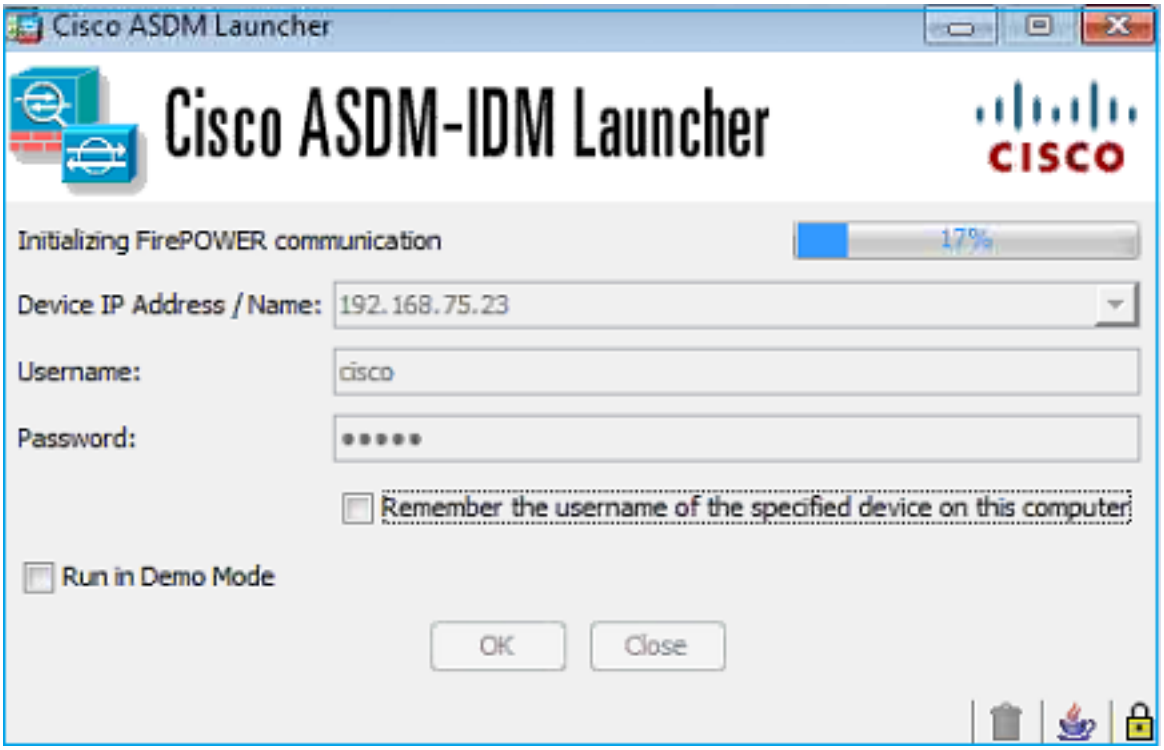
- show-Modul - Der ASDM erkennt die ASA-Module.
- show module sfr details - Der ASDM erkennt die Moduldetails, einschließlich der IP-Adresse für das FirePOWER-Management.

Diese werden im Hintergrund als eine Reihe von SSL-Verbindungen vom PC zur ASA-IP-Adresse angesehen:

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

Schritt 3: Der ASDM initiiert die Kommunikation zum FirePOWER-Modul.

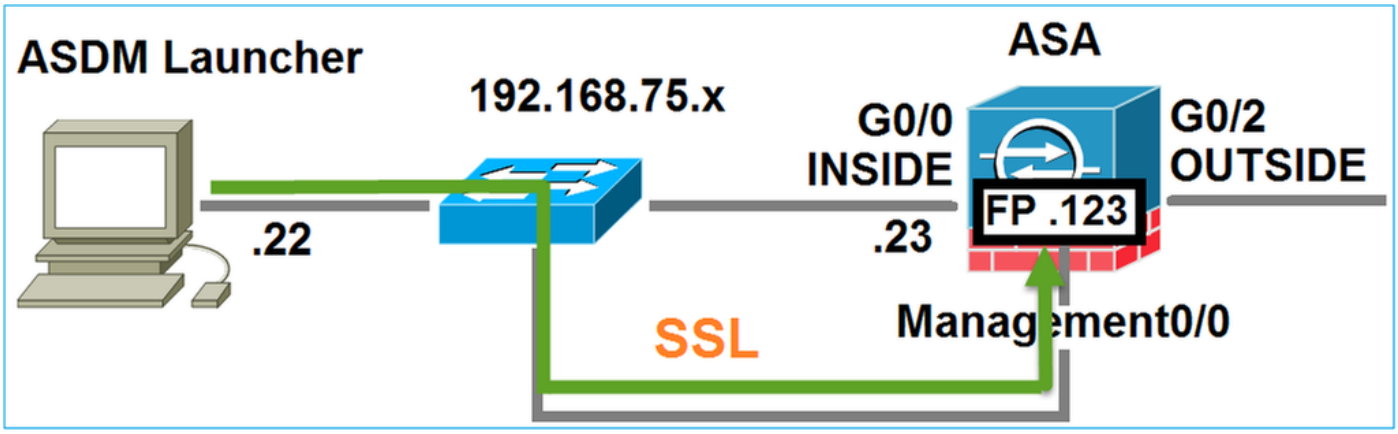
Da der ASDM die IP-Adresse für das FirePOWER-Management kennt, initiiert er SSL-Sitzungen zum Modul:



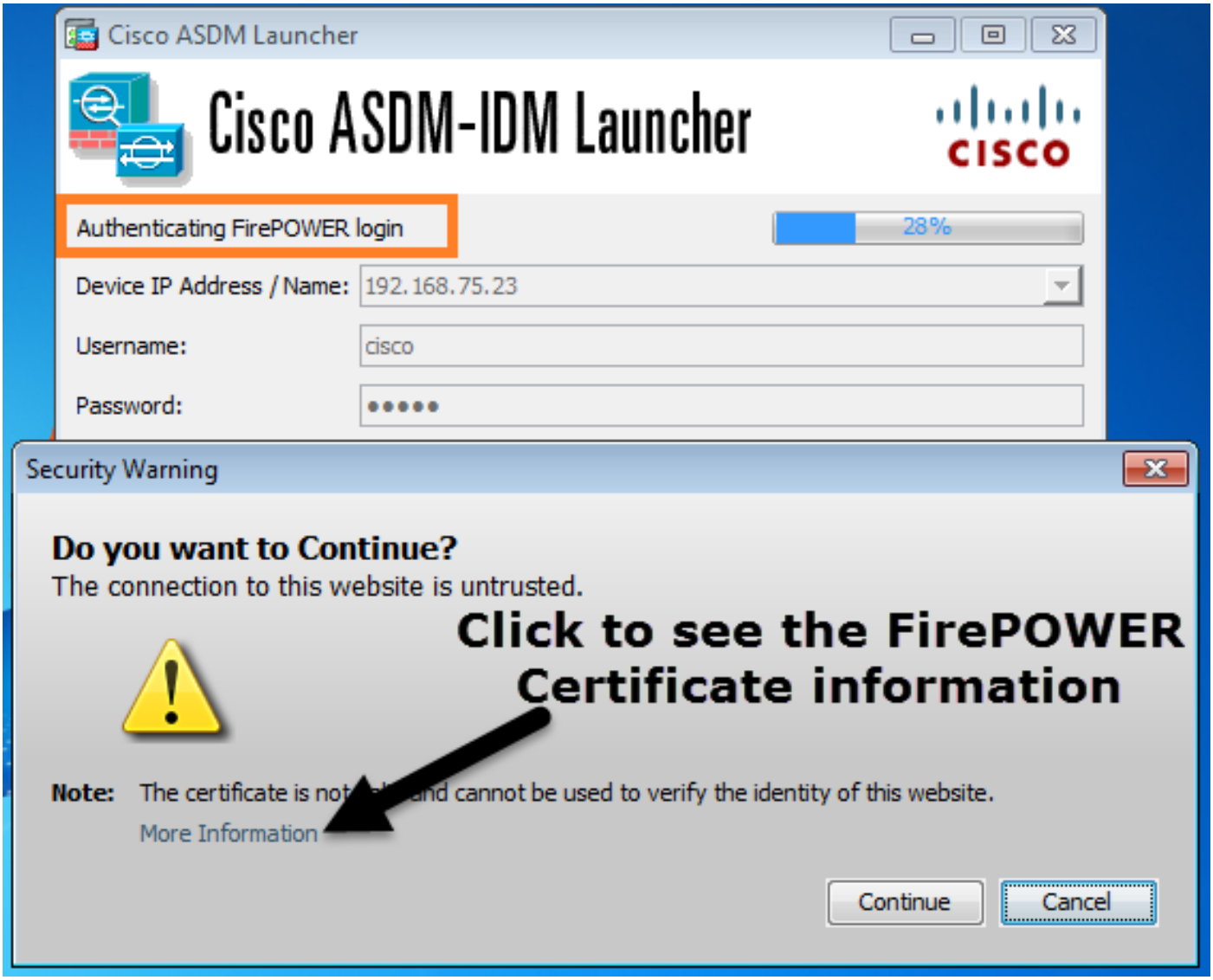
Dies wird im Hintergrund als SSL-Verbindungen vom ASDM-Host zur FirePOWER-Management-IP-Adresse betrachtet:

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

Dies kann wie folgt visualisiert werden:

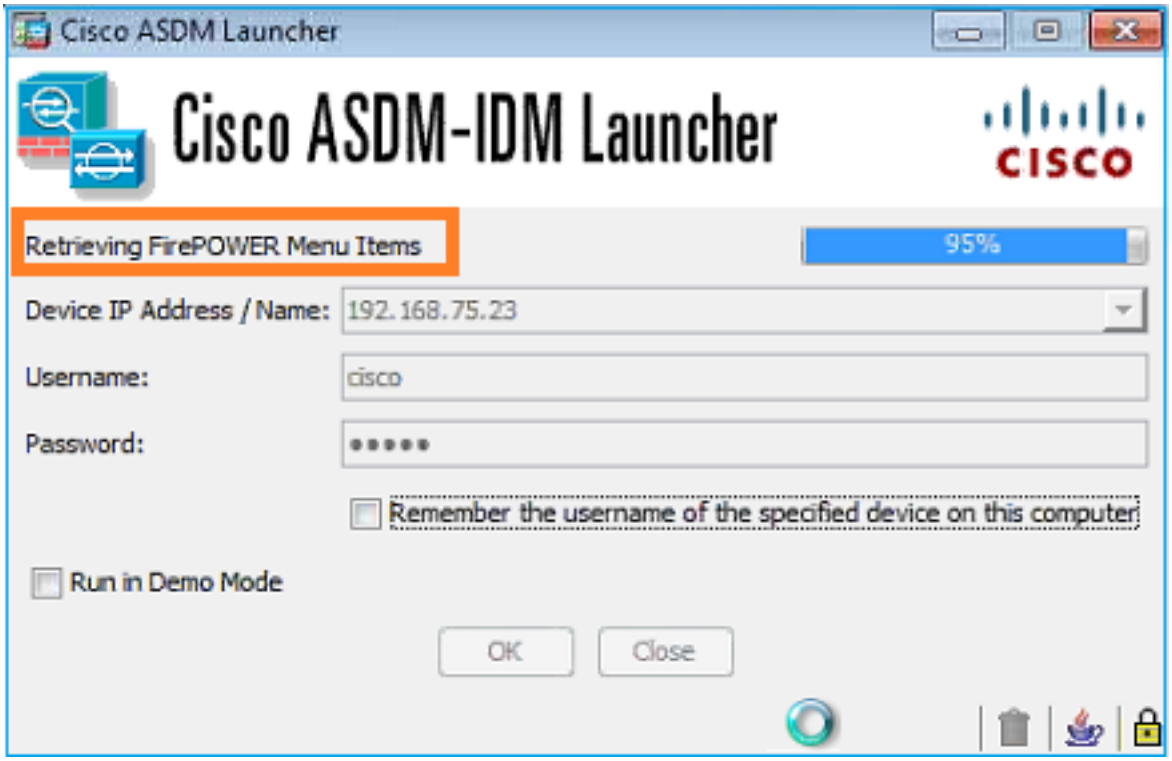


Der ASDM authentifiziert FirePOWER, und es wird eine Sicherheitswarnung angezeigt, da das FirePOWER-Zertifikat selbst signiert ist:

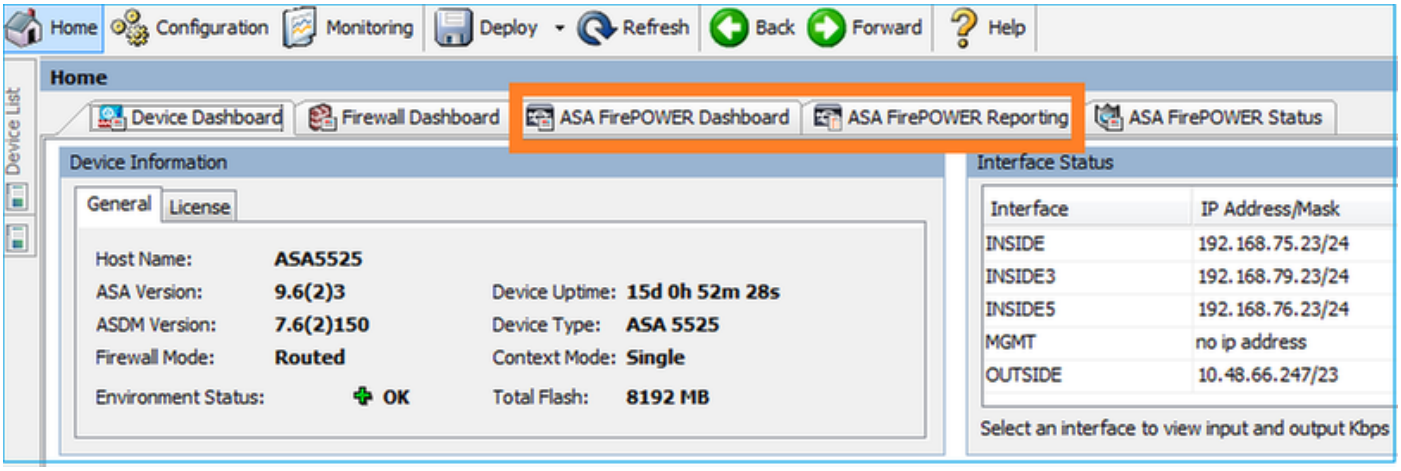


Schritt 4: ASDM ruft die FirePOWER-Menüelemente ab

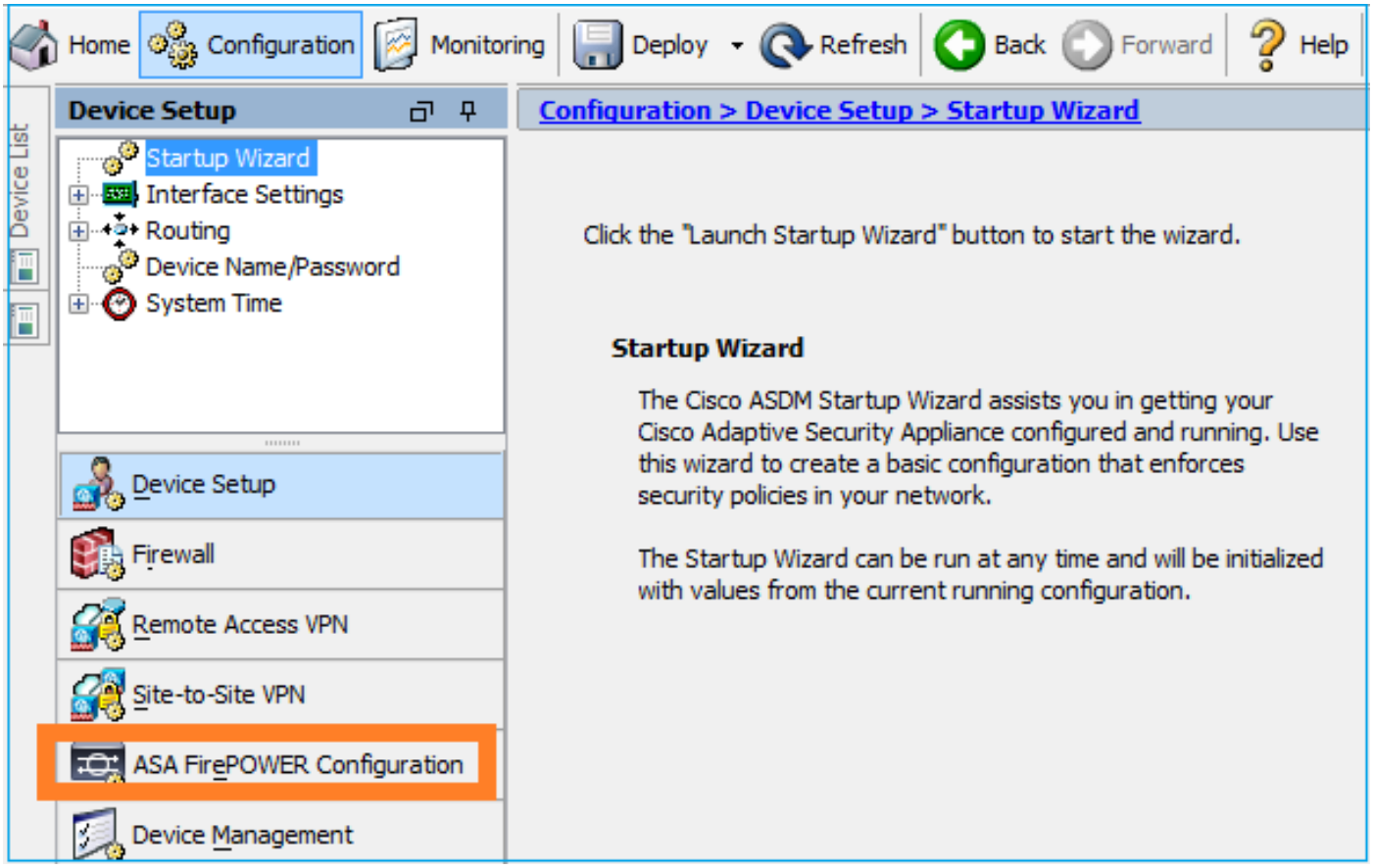
Nach erfolgreicher Authentifizierung ruft der ASDM die Menüelemente vom FirePOWER-Gerät ab:



Die abgerufenen Registerkarten sind in diesem Beispiel dargestellt:

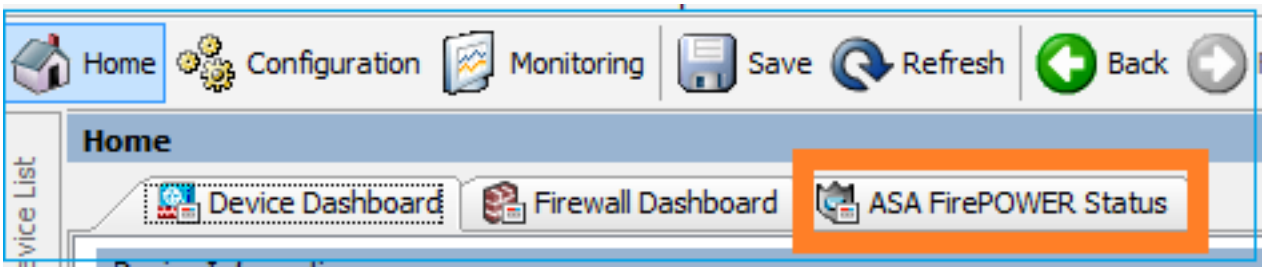


Außerdem wird das ASA FirePOWER-Konfigurationsmenüelement abgerufen:

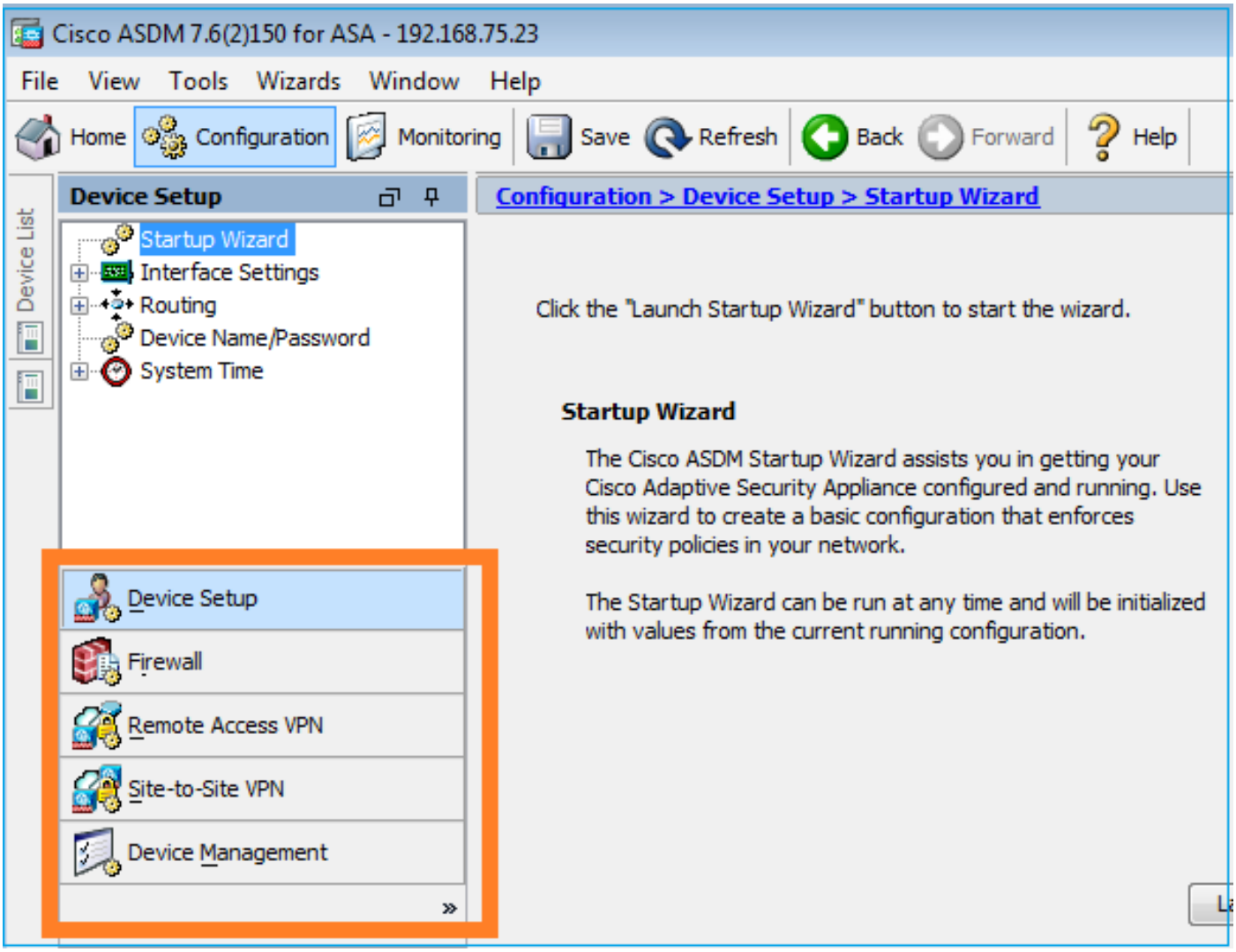


Fehlerbehebung

Falls ASDM keinen SSL-Tunnel mit der FirePOWER Management-IP-Adresse einrichten kann, wird nur dieses FirePOWER-Menüelement geladen:



Auch das ASA FirePOWER-Konfigurationselement fehlt:



Überprüfung 1

Stellen Sie sicher, dass die ASA-Verwaltungsschnittstelle UP ist und der angeschlossene Switch-Port sich im richtigen VLAN befindet:

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

Empfohlene Fehlerbehebung

- Stellen Sie das richtige VLAN ein.
- Bringen Sie den Port auf (prüfen Sie das Kabel, überprüfen Sie die Switch-Port-Konfiguration (Geschwindigkeit/Duplex/Herunterfahren)).

Überprüfung 2

Stellen Sie sicher, dass das FirePOWER-Modul vollständig initialisiert, betriebsbereit und ausgeführt ist:

```
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
------------------------------------------------------

>
```

Empfohlene Fehlerbehebung

- Prüfen Sie die Ausgabe des Befehls **show module sfr log console** auf Fehler oder Fehler.

Überprüfung 3

Überprüfen Sie die grundlegende Konnektivität zwischen dem ASDM-Host und der FirePOWER-Modul-Management-IP mithilfe von Befehlen wie **ping** und **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.
```

Empfohlene Fehlerbehebung

- Überprüfen Sie das Routing entlang des Pfads.
- Stellen Sie sicher, dass sich keine Geräte im Pfad befinden, die den Datenverkehr blockieren.

Überprüfung 4

Wenn sich der ASDM-Host und die FirePOWER-Management-IP-Adresse im selben Layer-3-Netzwerk befinden, überprüfen Sie die Tabelle Address Resolution Protocol (ARP) auf dem 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
```

Empfohlene Fehlerbehebung

- Wenn keine ARP-Einträge vorhanden sind, verwenden Sie Wireshark, um die ARP-Kommunikation zu überprüfen. Stellen Sie sicher, dass die MAC-Adressen der Pakete korrekt sind.
- Wenn ARP-Einträge vorhanden sind, stellen Sie sicher, dass sie korrekt sind.

Überprüfung 5

Aktivieren Sie die Erfassung auf dem ASDM-Gerät, während Sie eine Verbindung über ASDM herstellen, um festzustellen, ob eine ordnungsgemäße TCP-Kommunikation zwischen Host und FirePOWER-Modul besteht. Sie sollten mindestens Folgendes sehen:

- 3-Wege-TCP-Handshake zwischen dem ASDM-Host und der ASA
- Zwischen dem ASDM-Host und der ASA ist ein SSL-Tunnel eingerichtet.

- 3-Wege-TCP-Handshake zwischen dem ASDM-Host und der IP-Adresse für das FirePOWER-Modulmanagement.
- Zwischen dem ASDM-Host und der IP-Adresse für das FirePOWER-Modulmanagement wird ein SSL-Tunnel eingerichtet.

Empfohlene Fehlerbehebung

- Wenn der 3-Wege-TCP-Handshake ausfällt, stellen Sie sicher, dass der Pfad zum Blockieren der TCP-Pakete keinen asymmetrischen Datenverkehr oder Geräte aufweist.
- Wenn SSL fehlschlägt, prüfen Sie, ob sich im Pfad kein Gerät befindet, das Man-in-the-Middle (MITM) ausführt (der Server Certificate Issuer gibt einen Hinweis dafür).

Überprüfung 6

Aktivieren Sie die Erfassung, um den Datenverkehr zum und vom FirePOWER-Modul zu überprüfen, die Schnittstelle asa_mgmt_plane. In der Aufzeichnung sehen Sie:

- ARP-Anfrage vom ASDM-Host (Paket 42).
- ARP-Antwort vom FirePOWER-Modul (Paket 43).
- TCP-Handshake in drei Richtungen zwischen dem ASDM-Host und dem FirePOWER-Modul (Pakete 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
Sack
ack
```

Empfohlene Fehlerbehebung

- Wie bei Verifizierung 5.

Überprüfung 7

Überprüfen Sie, ob der ASDM-Benutzer über die Berechtigungsstufe 15 verfügt. Eine Möglichkeit, dies zu bestätigen, besteht darin, den Befehl **debug http 255** während der Verbindung über ASDM einzugeben:

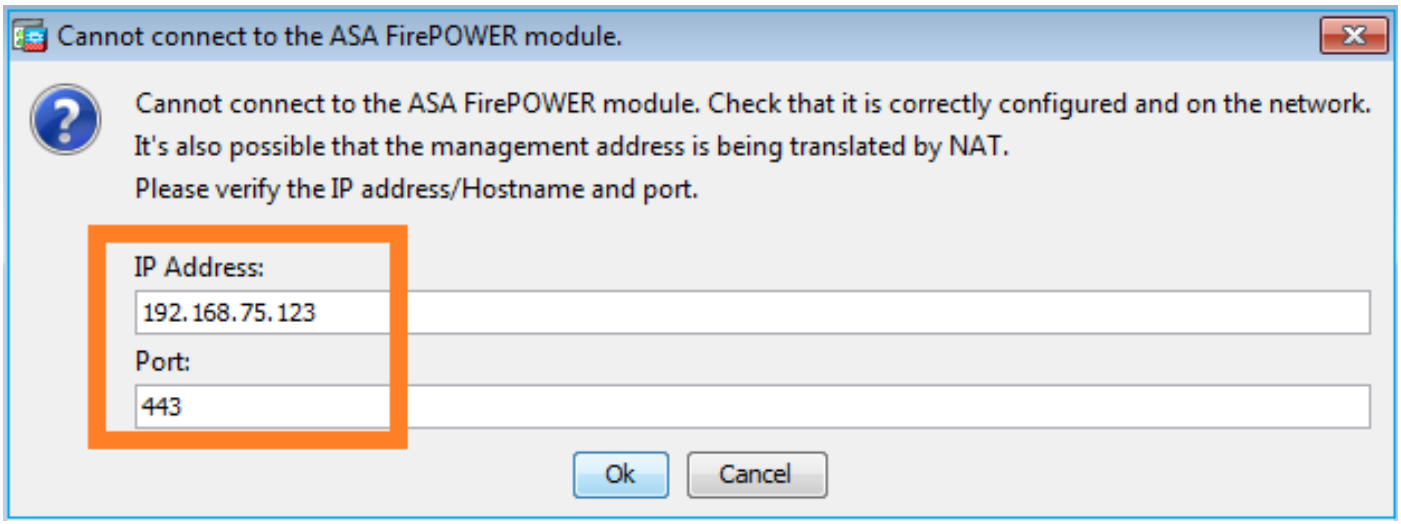
```
ASA5525# debug http 255
debug http enabled at level 255.
HTTP: processing ASDM request [/admin/asdm_banner] with cookie-based authentication
(aware_webvpn_conf.re2c:444)
HTTP: check admin session. Cookie index [2][c8a06c50]
HTTP: Admin session cookie [A27614B@20480@78CF@58989AACB80CE5159544A1B3EE62661F99D475DC]
HTTP: Admin session idle-timeout reset
HTTP: admin session verified =  [1]
HTTP: username = [user1], privilege = [14]
```

Empfohlene Fehlerbehebung

- Wenn die Berechtigungsstufe nicht 15 ist, versuchen Sie es mit einem Benutzer der Stufe 15.

Überprüfung 8

Wenn zwischen dem ASDM-Host und dem FirePOWER-Modul eine Network Address Translation (NAT) für die IP-Adresse des FirePOWER-Managements vorhanden ist, müssen Sie die NATed-IP-Adresse angeben:



Empfohlene Fehlerbehebung

- Dies wird durch Aufzeichnungen an den Endpunkten (ASA/SFR und End-Host) bestätigt.

Überprüfung 9

Stellen Sie sicher, dass das FirePOWER-Modul nicht bereits von FMC verwaltet wird, da in diesem Fall die FirePOWER-Registerkarten im ASDM fehlen:

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

>
```

Eine weitere Methode ist der Befehl **show module sfr details**:

```
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
```

Empfohlene Fehlerbehebung

- Wenn das Gerät bereits verwaltet wird, müssen Sie die Registrierung aufheben, bevor Sie es über ASDM verwalten können. Weitere Informationen finden Sie im Konfigurationsleitfaden für das FirePOWER Management Center.

Überprüfung 10

Überprüfen Sie die Wireshark-Erfassung, um sicherzustellen, dass der ASDM-Client eine Verbindung mit einer geeigneten TLS-Version herstellt (z. B. TLSv1.2).

Empfohlene Fehlerbehebung

- Ändern Sie die SSL-Einstellungen des Browsers.
- Versuchen Sie es mit einem anderen Browser.
- Versuchen Sie es von einem anderen End-Host.

Überprüfung 11

Überprüfen Sie im Cisco ASA Compatibility Guide (Cisco ASA-Kompatibilitätsleitfaden), ob die ASA/ASDM-Images kompatibel sind.

Empfohlene Fehlerbehebung

- Verwenden Sie ein kompatibles ASDM-Image.

Überprüfung 12

Überprüfen Sie im Cisco ASA Compatibility Guide (Cisco ASA-Kompatibilitätsleitfaden), ob das FirePOWER-Gerät mit der ASDM-Version kompatibel ist.

Empfohlene Fehlerbehebung

- Verwenden Sie ein kompatibles ASDM-Image.

Zugehörige Informationen

- Cisco ASA FirePOWER-Modul - Kurzreferenz
- ASA mit FirePOWER Services - Konfigurationsleitfaden für lokales Management, Version 6.1.0
- ASA FirePOWER-Modul - Benutzerhandbuch für ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X und ASA5516-X, Version 5.4.1
- Technischer Support und Dokumentation - Cisco Systems