Gebruik ASDM om een FirePOWER-module op een ASA te beheren

Inhoud

Inleiding

In dit document wordt beschreven hoe de software van Adaptieve Security Devices Manager (ASDM) communiceert met de Adaptieve security applicatie (ASA) en een FirePOWER-softwaremodule die erop is geïnstalleerd.

Een FirePOWER-module die op een ASA is geïnstalleerd kan worden beheerd door:

- Firepower Management Center (FMC) - Dit is de off-box beheeroplossing.
- ASDM - Dit is de on-box beheeroplossing.

Voorwaarden

Vereisten

Een ASA-configuratie om ASDM-beheer mogelijk te maken:

```
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
```

Controleer de compatibiliteit tussen de ASA/SFR-module, anders worden de tabbladen FirePOWER niet gezien.

Bovendien moet de 3DES/AES-licentie op de ASA-licentie worden ingeschakeld:

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

Zorg ervoor dat het ASDM-clientsysteem een ondersteunde versie van Java JRE uitvoert.

Gebruikte componenten

- Een Microsoft Windows 7-host
- ASA 5525-X met ASA versie 9.6(2.3)
- ASDM versie 7.6.2.15.0
- FirePOWER-softwaremodule 6.1.0-30

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Architectuur

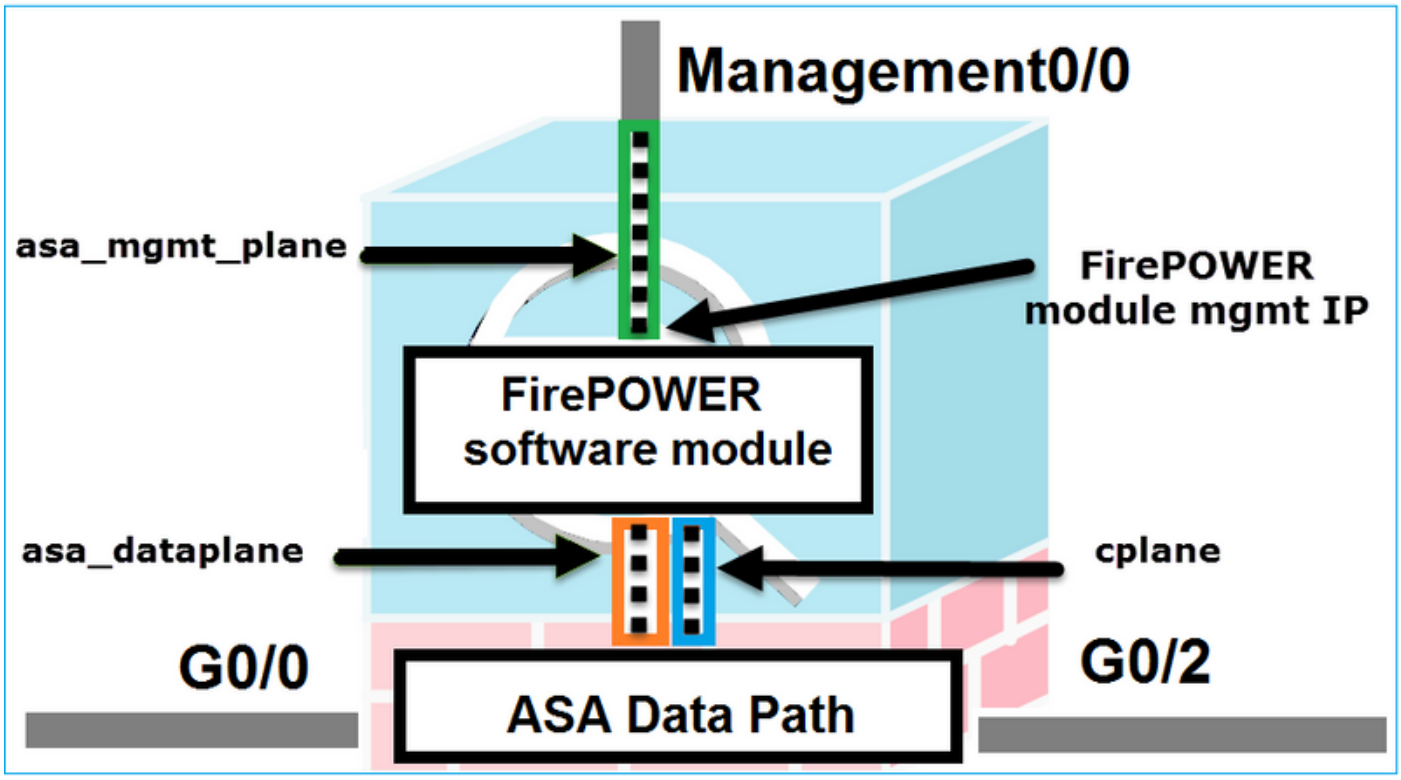
ASA heeft drie interne interfaces:

- ASA_dataplane - Het wordt gebruikt om pakketten van de ASA Data Path naar de FirePOWER-softwaremodule te richten.
- asa_mgmt_plane - Het wordt gebruikt om de FirePOWER managementinterface te laten communiceren met het netwerk.
- vlak - interface van het besturingsplane die wordt gebruikt om keepalieven over te brengen tussen de ASA en de FirePOWER module.

U kunt verkeer in alle interne interfaces opnemen:

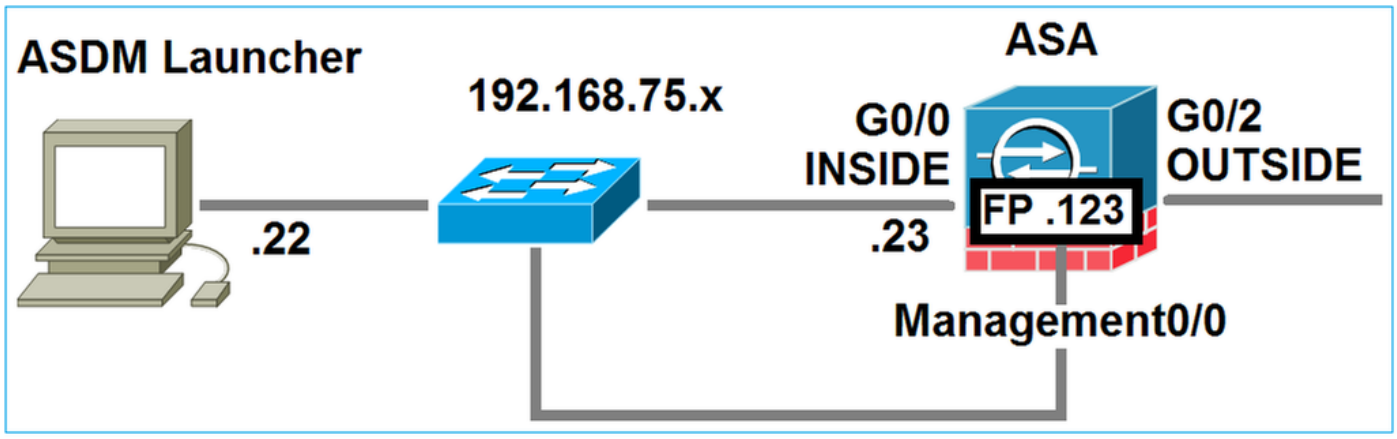
```
ASA5525# capture CAP interface ?

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

Dit kan als volgt worden geïsoleerd:



Achtergrondbediening wanneer een gebruiker via ASDM verbonden is met een ASA

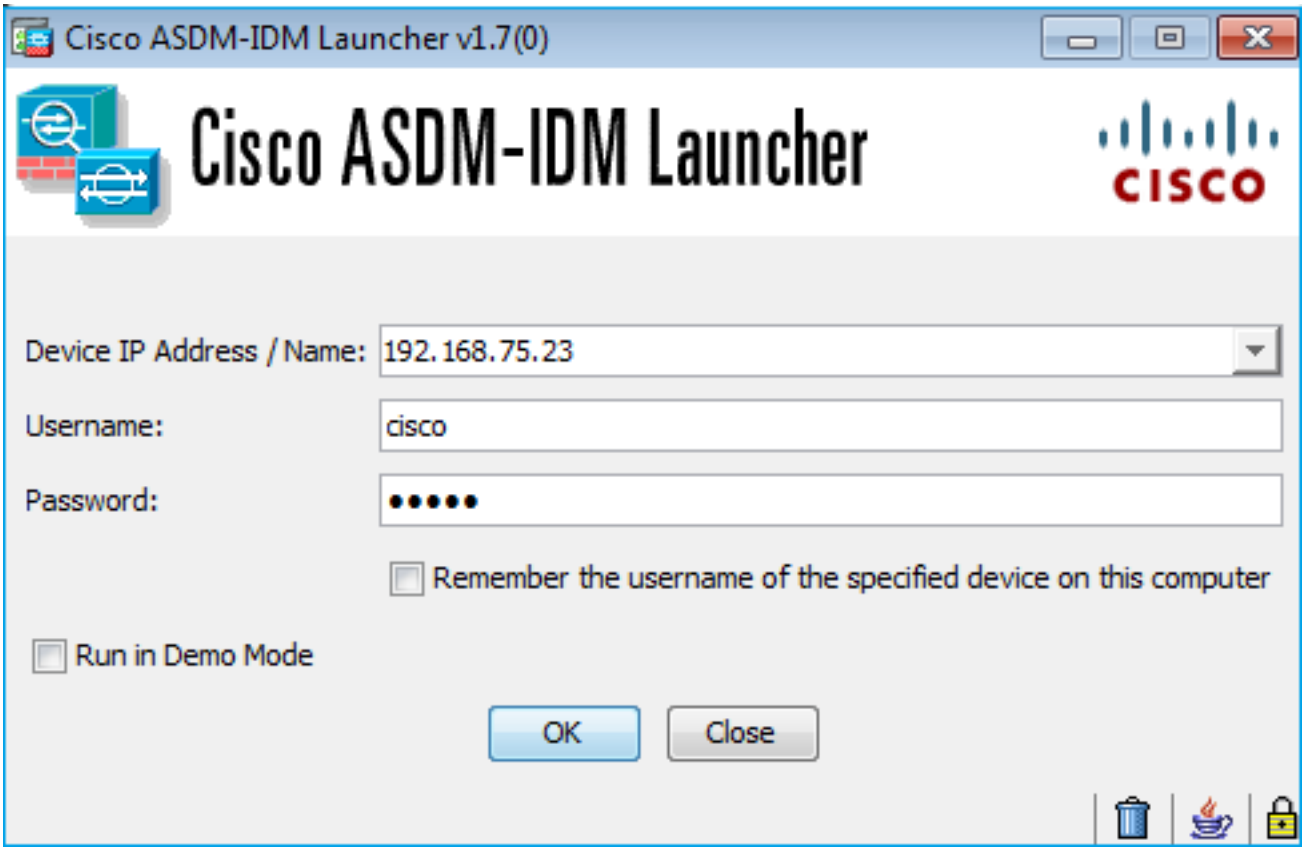
Neem deze topologie in overweging:



Wanneer een gebruiker een ASDM-verbinding met de ASA initieert, zullen deze gebeurtenissen plaatsvinden:

Stap 1 - De gebruiker start de ASDM-verbinding.

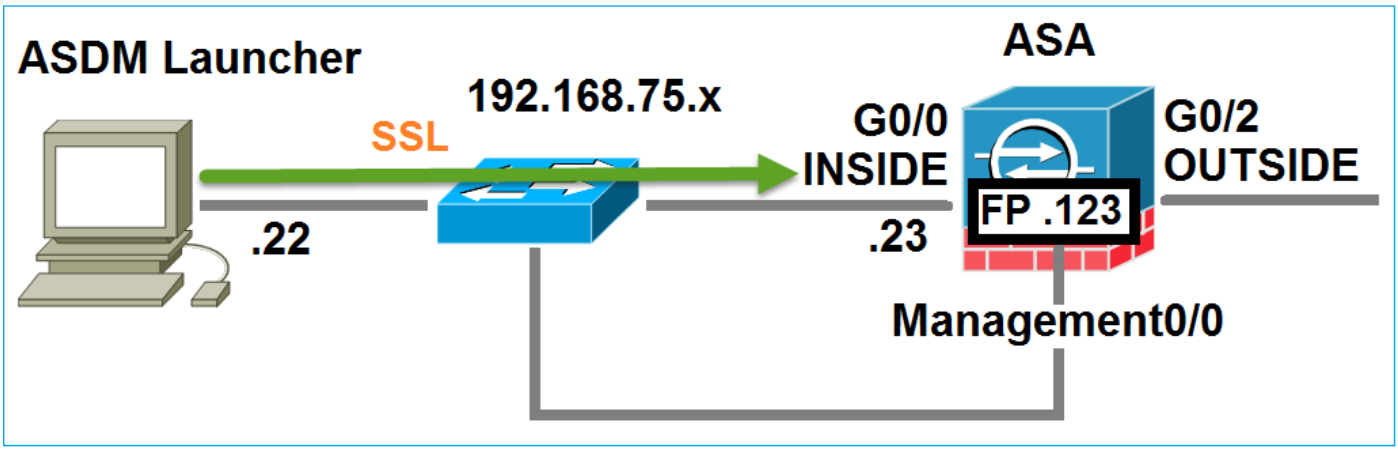
De gebruiker specificeert het ASA IP-adres dat gebruikt wordt voor HTTP-beheer, geeft de aanmeldingsgegevens in en start een verbinding met de ASA:



Op de achtergrond wordt een SSL-tunnel tussen de ASDM en de ASA tot stand gebracht:

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

Dit kan als volgt worden geïsoleerd:



Stap 2 - ASDM maakt de ASA Configuration en het FirePOWER Module-IP bekend

Voer de opdracht **debug http 255** op de ASA in om alle controles te tonen die op de achtergrond worden uitgevoerd wanneer ASDM op de ASA aansluit:

```
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
```

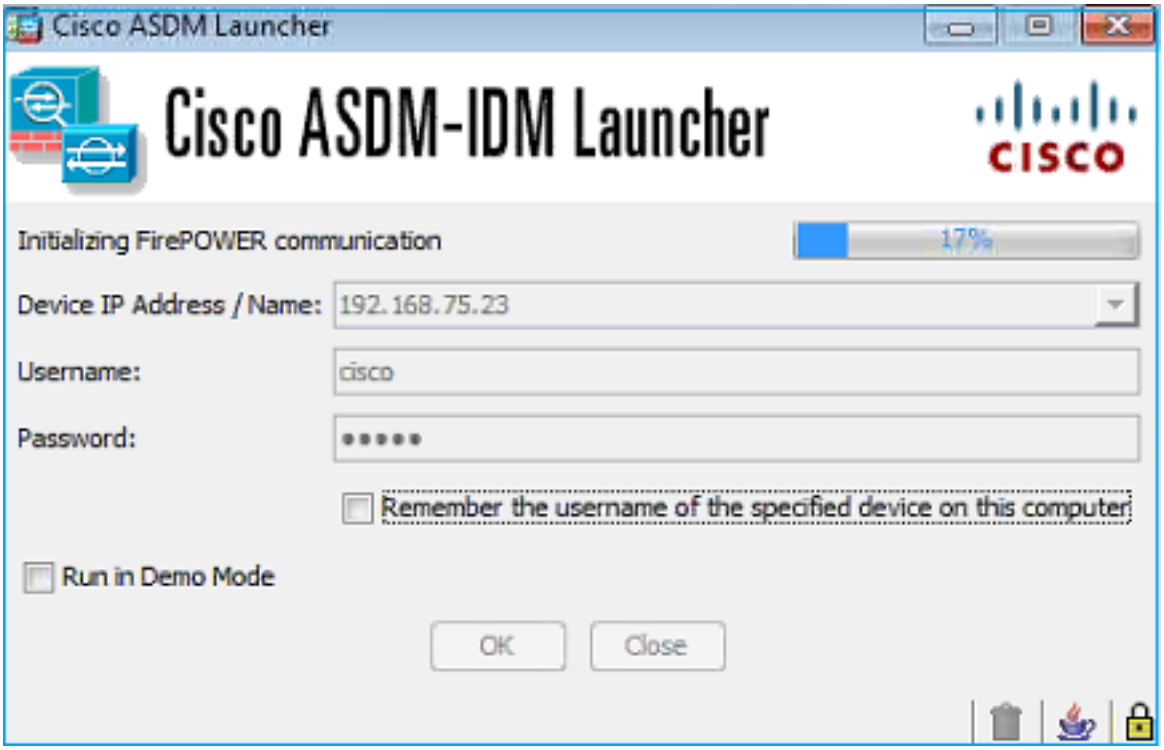
- Module tonen - De ASDM ontdekt de ASA modules.
- toont module sfr details - de ASDM ontdekt de moduledetails, die het FirePOWER beheers IP adres omvatten.

Deze zullen op de achtergrond als een reeks SSL-verbindingen van de PC naar het ASA IP-adres worden gezien:

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

Stap 3 - ASDM start communicatie naar de FirePOWER-module

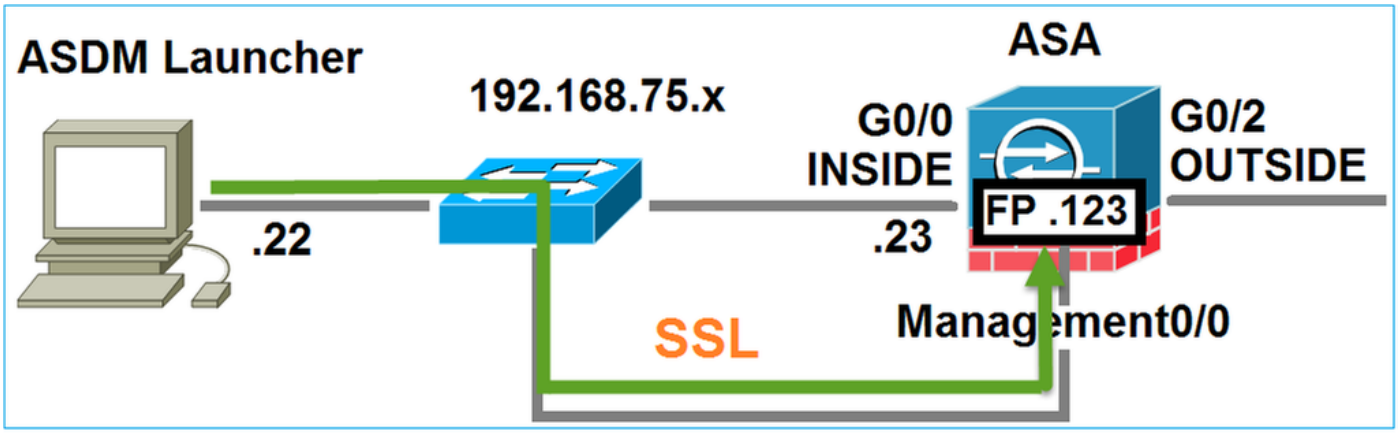
Aangezien ASDM het FirePOWER Management IP-adres weet, start het SSL-sessies naar de module:



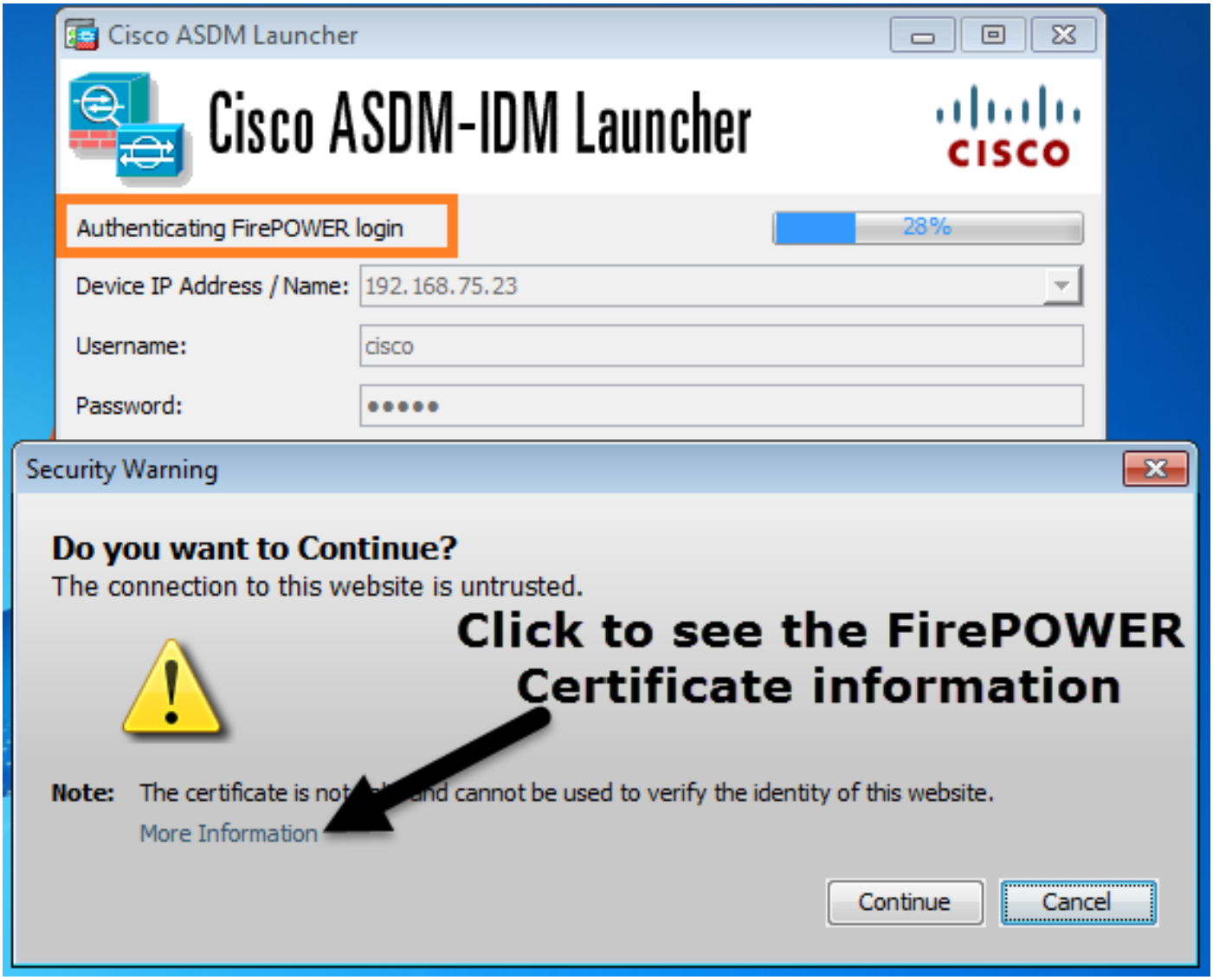
Dit wordt op de achtergrond gezien als SSL-verbindingen van de ASDM-host naar het FirePOWER Management IP-adres:

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

Dit kan als volgt worden geïsoleerd:

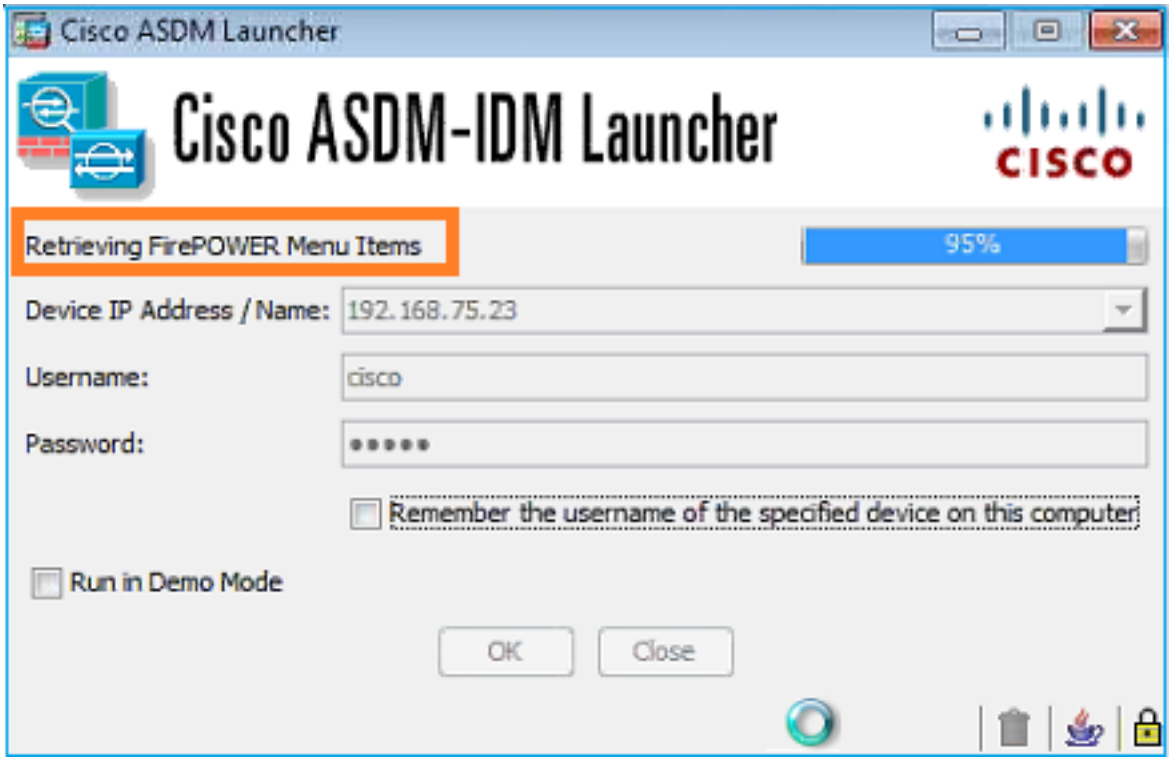


ASDM echt FirePOWER en er wordt een veiligheidswaarschuwing weergegeven omdat het FirePOWER-certificaat zelf is ondertekend:

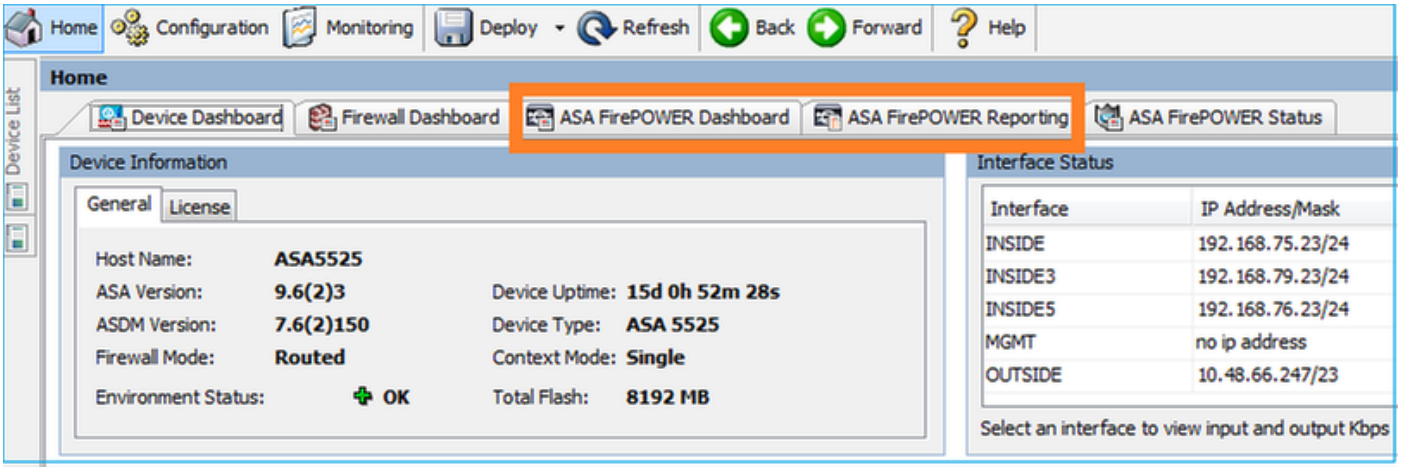


Stap 4 - ASDM haalt de items van het menu FirePOWER op

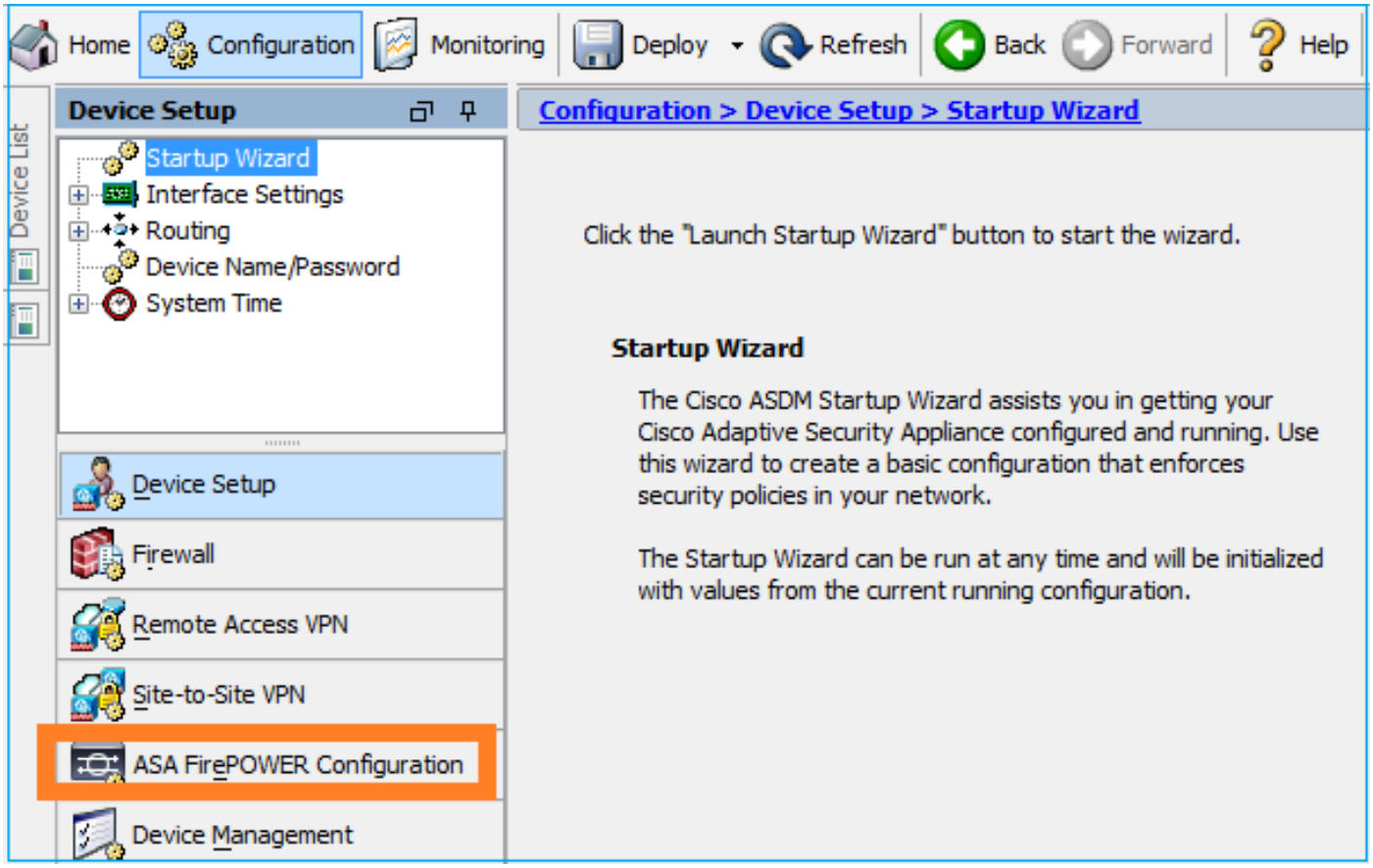
Na de succesvolle authenticatie haalt ASDM de Menu-items van het FirePOWER-apparaat terug:



De opgehaalde tabbladen worden in dit voorbeeld getoond:

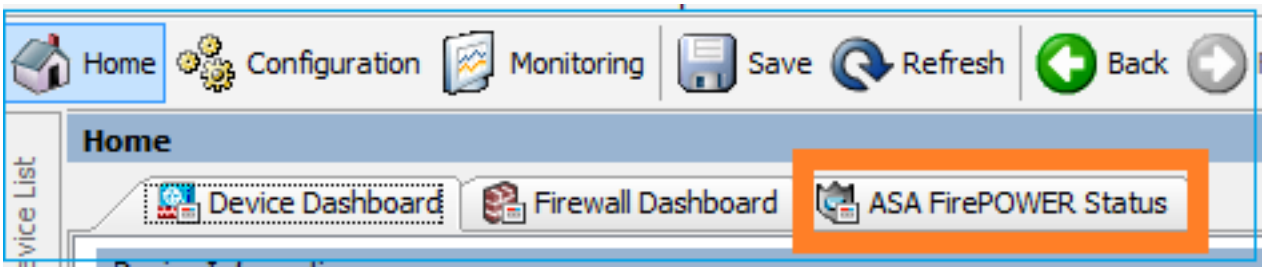


Het haalt ook het ASA FirePOWER Configuration Menu-item terug:

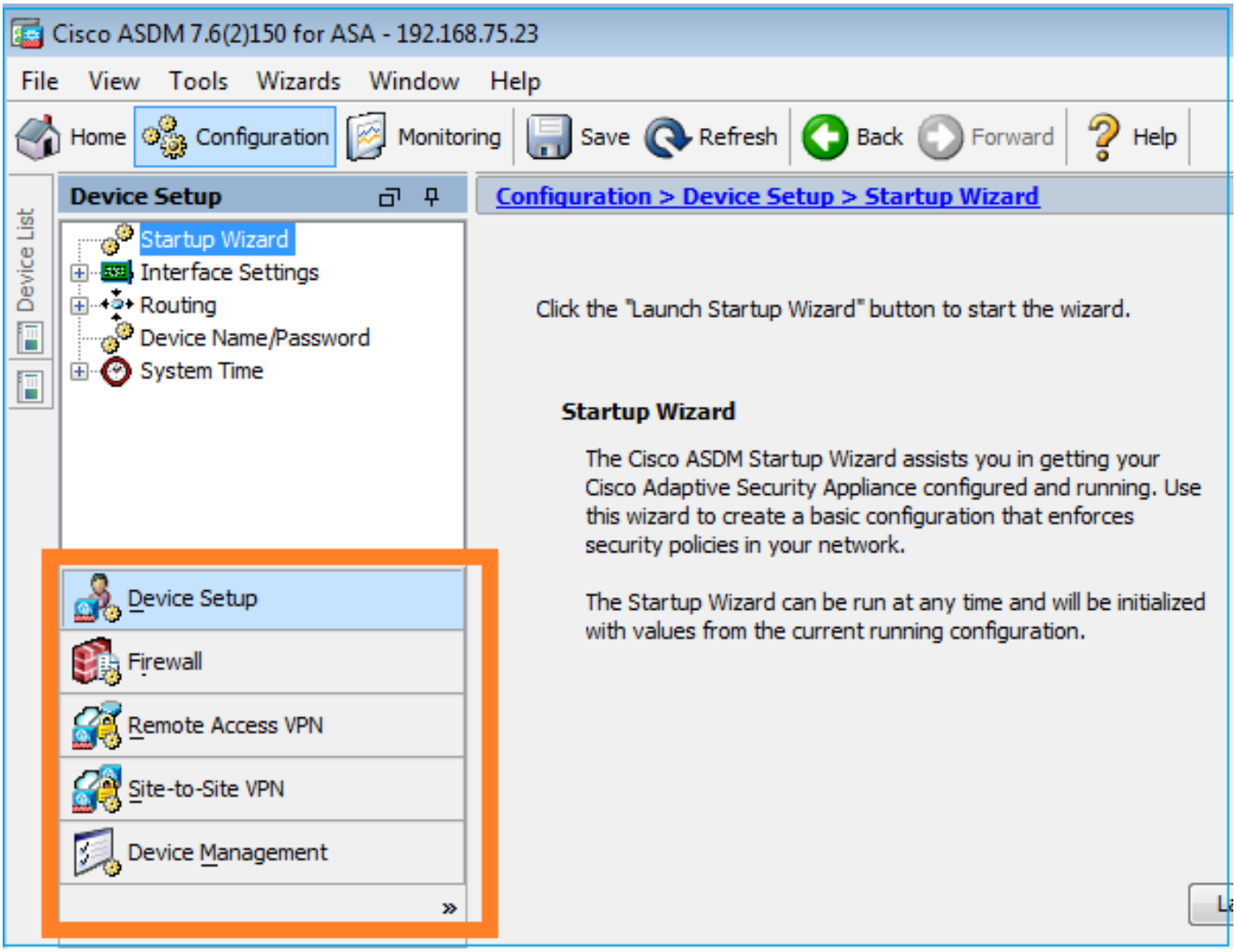


Problemen oplossen

Indien ASDM geen SSL-tunnel met het FirePOWER Management IP-adres kan maken, dan laadt het alleen dit FirePOWER Menu-item:



Ook het ASA FirePOWER Configuration-item zal ontbreken:



Verificatie 1

Zorg ervoor dat de ASA beheerinterface UP is en de daaraan gekoppelde switchpoort in het juiste VLAN is:

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

Aanbevolen probleemoplossing

- Stel het juiste VLAN in.
- Breng de poort naar UP (controleer de kabel, controleer de switchpoortconfiguratie (snelheid/duplex/uitgeschakeld).

Verificatie 2

Zorg dat de FirePOWER-module volledig wordt geformatteerd, omhoog en omloop:

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

>
```

Aanbevolen probleemoplossing

- Controleer de uitvoer van de **opdracht voor het logconsole van de showmodule** op fouten of mislukkingen.

Verificatie 3

Controleer basisconnectiviteit tussen de ASDM gastheer en de FirePOWER module beheer IP met opdrachten zoals **ping** en **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.
```

Aanbevolen probleemoplossing

- Controleer de routing langs het pad.
- Controleer dat er geen apparaten in het pad zijn die het verkeer blokkeren.

Verificatie 4

Als de ASDM-host en het FirePOWER Management IP-adres in hetzelfde Layer 3-netwerk zijn geplaatst, controleert u de tabel Adretoen Protocol (ARP) op de 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
```

Aanbevolen probleemoplossing

- Als er geen ARP-vermeldingen zijn, gebruikt u Wireshark om de ARP-communicatie te controleren. Zorg ervoor dat de MAC-adressen van de pakketten juist zijn.
- Als er ARP-vermeldingen zijn, zorg er dan voor dat deze correct zijn.

Verificatie 5

Schakel opname op het ASDM-apparaat in terwijl u via ASDM verbinding maakt om te zien of er een juiste TCP-communicatie tussen de host en de FirePOWER-module is. U dient ten minste te zien:

- TCP 3-handdruk tussen de ASDM-host en de ASA.
- SSL-tunnel ingesteld tussen de ASDM-host en de ASA.
- TCP 3-manier handshake tussen de ASDM host en het FirePOWER module Management IP-adres.

- SSL-tunnel die tussen de ASDM-host en het FirePOWER-IP-adres voor modulebeheer is ingesteld.

Aanbevolen probleemoplossing

- Als de TCP 3-handdruk mislukt, zorg er dan voor dat er geen asymmetrisch verkeer of apparaten in het pad is dat de TCP-pakketten blokkeert.
- Als SSL niet werkt, controleer of er geen apparaat in het pad is dat man-in-het-midden (MITM) doet (de uitgevende instelling van het servercertificaat geeft hier een hint voor).

Verificatie 6

Om het verkeer naar en van de module FirePOWER te controleren, schakelt u opname in de asa_mgmt_plane interface in. In de opname ziet u het volgende:

- ARP-verzoek van de ASDM-host (pakket 42).
- ARP-antwoord van de FirePOWER-module (pakket 43).
- TCP 3-manier handdruk tussen de ASDM-host en de FirePOWER-module (pakketten 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
```

Aanbevolen probleemoplossing

- Hetzelfde als in Verificatie 5.

Verificatie 7

Controleer dat de ASDM-gebruiker voorkeursniveau 15 heeft. Eén manier om dit te bevestigen is de **debug http 255** opdracht in te voeren terwijl deze via ASDM verbonden is:

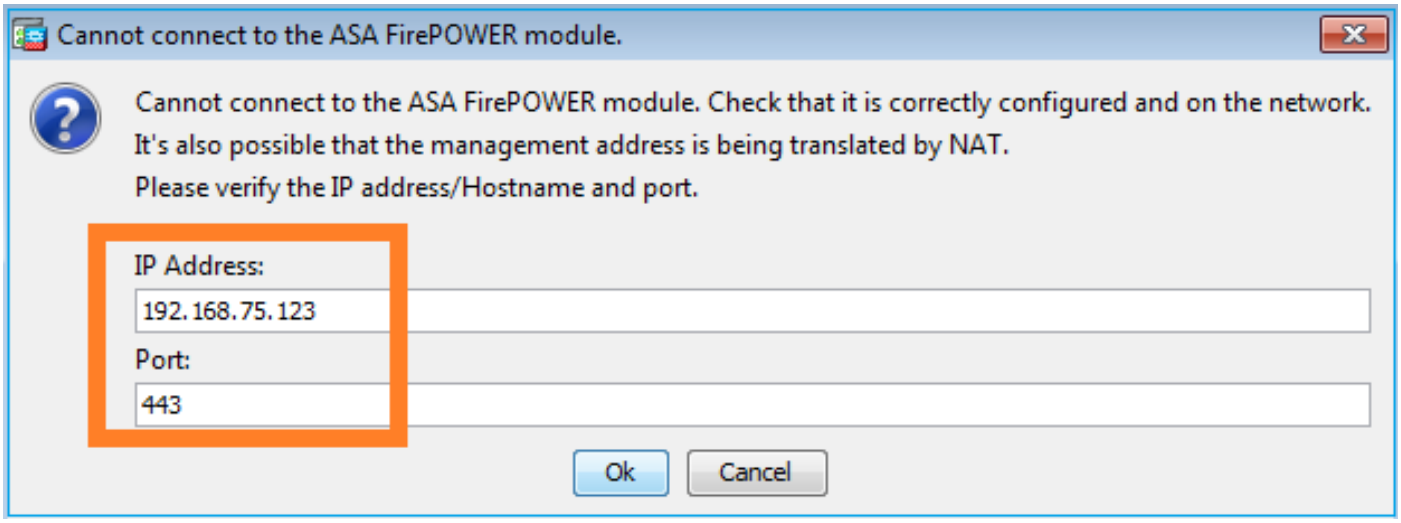
```
ASA5525# debug http 255
debug http enabled at level 255.
HTTP: processing ASDM request [/admin/asdm_banner] with cookie-based authentication
(aware_webvpn_conf.re2c:444)
HTTP: check admin session. Cookie index [2][c8a06c50]
HTTP: Admin session cookie [A27614B@20480@78CF@58989AACB80CE5159544A1B3EE62661F99D475DC]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

Aanbevolen probleemoplossing

- Als het voorkeursniveau niet 15 is, probeer dan met een gebruiker die niveau 15 heeft.

Verificatie 8

Als er tussen de ASDM-host en de FirePOWER-module een netwerkadresomzetting (NAT) is voor het FirePOWER Management IP-adres, dan moet u het NATed IP-adres specificeren:



Aanbevolen probleemoplossing

- Captures op de eindpunten (ASA/SFR en end-host) zullen dit bevestigen.

Verificatie 9

Zorg ervoor dat de FirePOWER-module niet al door FMC wordt beheerd, omdat in dat geval de FirePOWER-tabbladen in ASDM ontbreken:

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

>
```

Een andere methode is met de opdracht **voor** de sfr van de **show module**:

```
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
```

Aanbevolen probleemoplossing

- Als het apparaat al beheerd wordt, moet u het uit het register halen voordat u het vanuit ASDM beheert. Zie de Firepower Management Center Configuration Guide.

Verificatie 10

Controleer de afvang van de dradenhaai om er zeker van te zijn dat de ASDM-client wordt aangesloten op een juiste TLS-versie (bijvoorbeeld TLSv1.2).

Aanbevolen probleemoplossing

- Tune de browser SSL instellingen.
- Probeer met een andere browser.
- Probeer van een andere eindhost.

Verificatie 11

Controleer in de Cisco ASA Compatibiliteit gids dat de ASA/ASDM beelden compatibel zijn.

Aanbevolen probleemoplossing

- Gebruik een compatibel ASDM-beeld.

Verificatie 12

Controleer in de Cisco ASA Compatibiliteit geleider dat het FirePOWER-apparaat compatibel is met de ASDM versie.

Aanbevolen probleemoplossing

- Gebruik een compatibel ASDM-beeld.

Gerelateerde informatie

- Cisco ASA FirePOWER-module - Snel startgids
- ASA met FirePOWER Services Local Management Guide, versie 6.1.0
- ASA FirePOWER Module-gebruikershandleiding voor de ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X en ASA 5516-X, versie 5.4.1
- Technische ondersteuning en documentatie – Cisco Systems