Usando el ASDM para manejar un módulo de FirePOWER en el ASA

Contenido

Introducción

Un módulo de FirePOWER que está instalado en el ASA se puede manejar por cualquiera:

- Centro de administración de FirePOWER (FMC) – Ésta es la solución de administración del apagado-cuadro
- Administrador de dispositivos de seguridad adaptante (ADSM) – Ésta es la solución de administración del en-cuadro

La meta de este documento es explicar cómo el software ASDM comunica con el ASA y un módulo de software de FirePOWER instalados en él.

Componentes usados

- Un host de Windows 7
- ASA5525-X que funciona con el código ASA 9.6.2-3
- Software ASDM 7.6.2.150
- Módulo de software 6.1.0-330 de FirePOWER

Prerequisites

Configuración ASA para habilitar la Administración del ASDM:

```
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
```

Además, en el ASA la licencia 3DES/AES debe ser habilitada:

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

Arquitectura

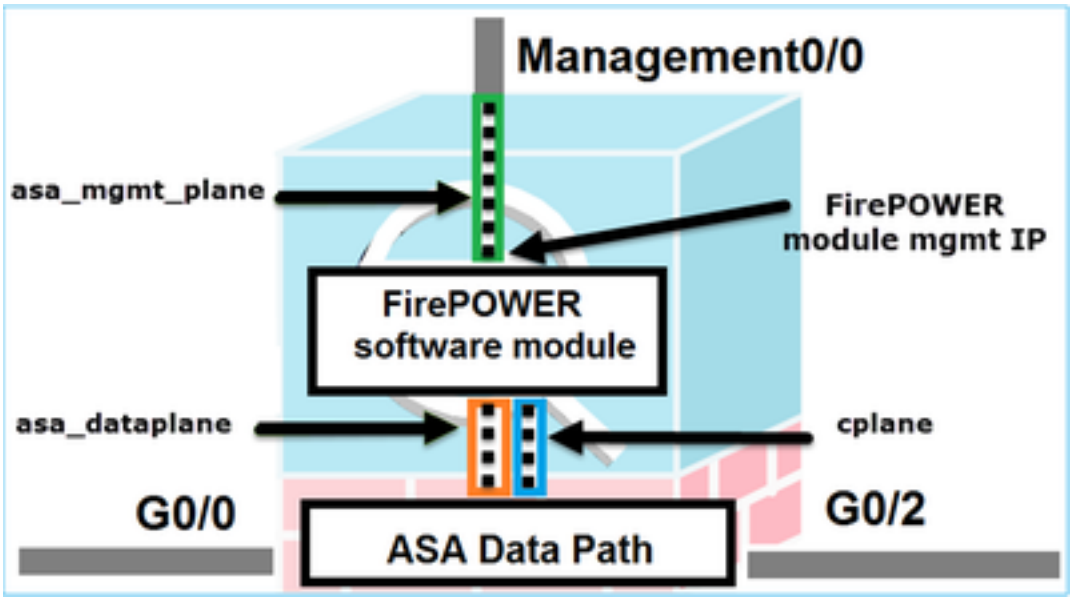
El ASA tiene 3 interfaces internas:

- **asa_dataplane** = se utiliza para reorientar los paquetes del trayecto de datos ASA al módulo de software de FirePOWER
- **asa_mgmt_plane** = se utiliza para permitir que la interfaz de administración de FirePOWER comunique con la red
- interfaz del avión del **cplane** = del control que se utiliza para transferir el Keepalives entre el ASA y el módulo de FirePOWER

Usted puede capturar el tráfico en todas las interfaces internas:

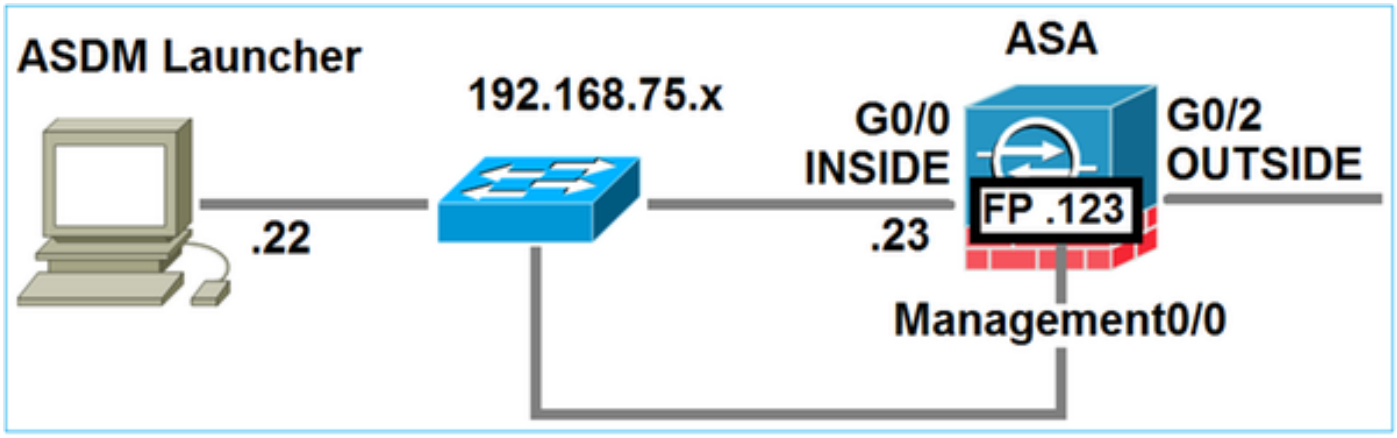
```
ASA5525# capture CAP interface ?

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

El antedicho puede ser visualizado como sigue:



Operación de fondo cuando un usuario conecta con el ASA vía el ASDM

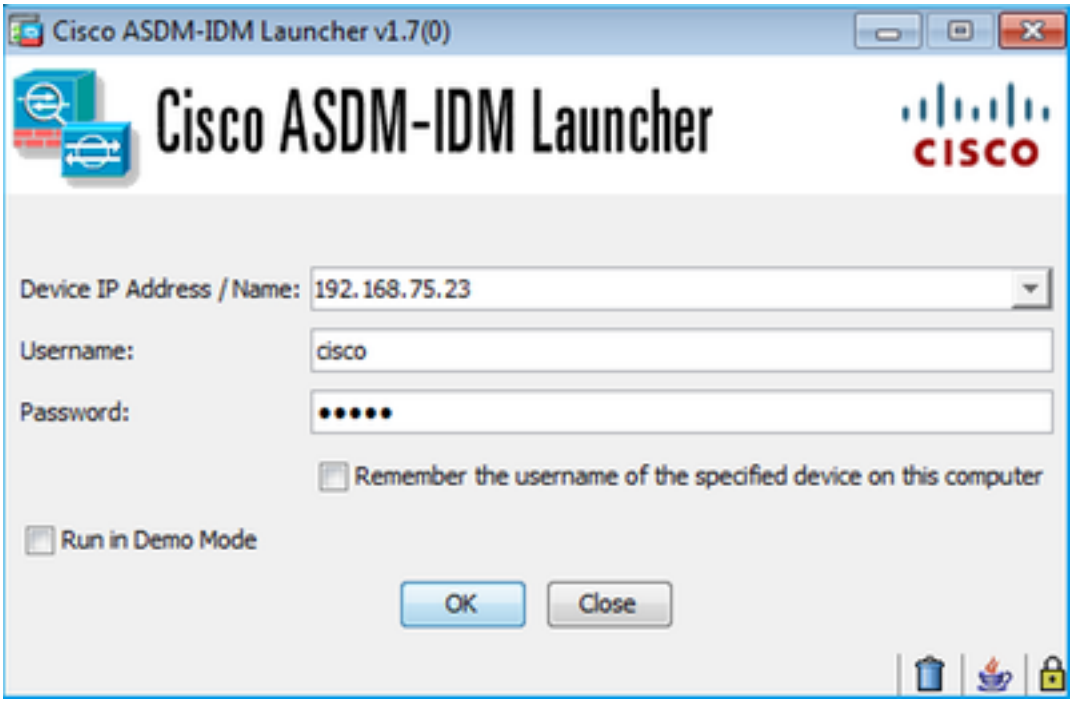
Considere la topología siguiente



Cuando un usuario inicia una conexión del ASDM al ASA los eventos siguientes ocurrirán:

Paso 1 – El usuario inicia la conexión del ASDM

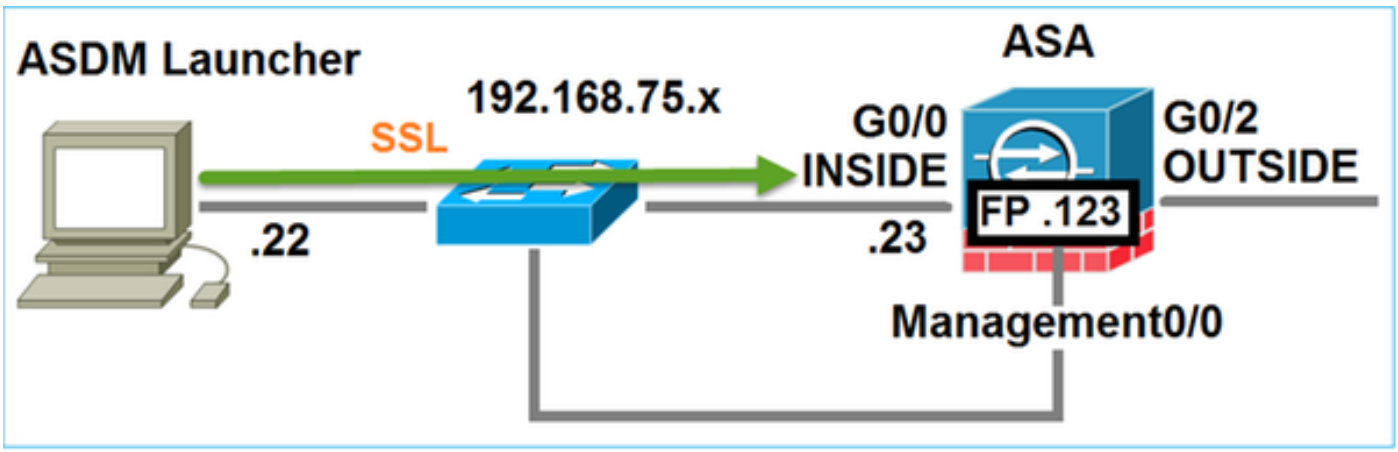
El usuario especifica el IP ASA usado para la Administración HTTP, ingresa las credenciales e inicia una conexión hacia el ASA:



En el fondo un túnel SSL entre el ASDM y el ASA se establece:

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

Esto puede ser visualizada como sigue:



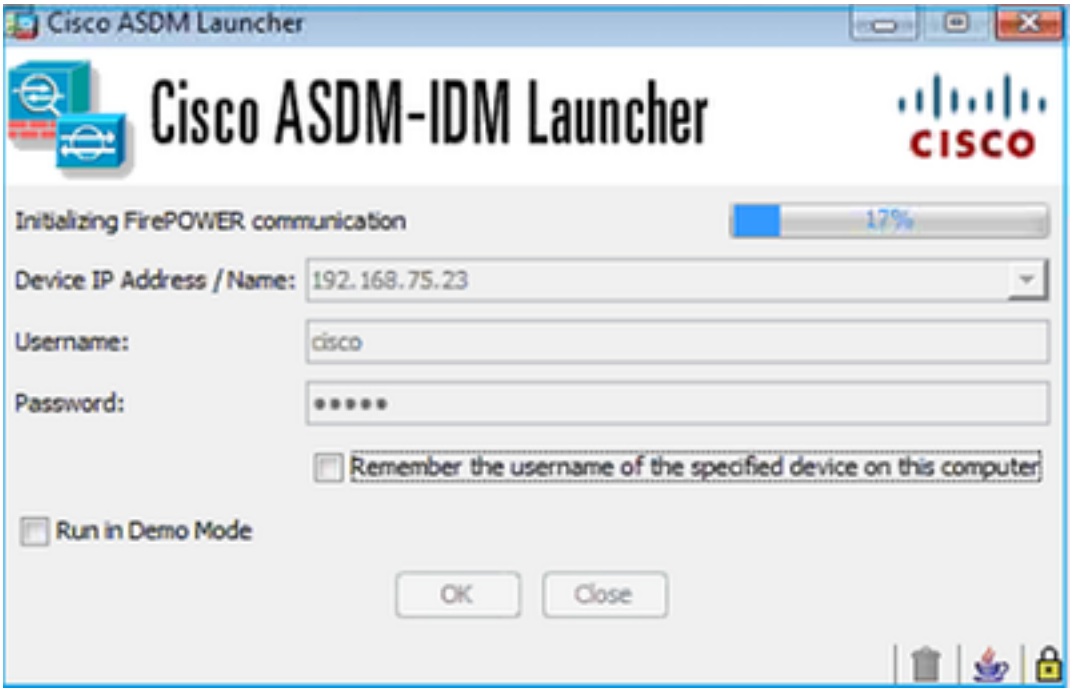
Paso 2 – El ASDM descubre la configuración ASA y el IP del módulo de FirePOWER

Habilitar **HTTP 255 del debug** en el ASA mostrará todos los controles que se hacen en el fondo cuando el ASDM conecta con el 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
```

- el módulo show = El ASDM descubre los módulos ASA
- los detalles del sfr del módulo show = El ASDM descubren los detalles del módulo incluyendo el IP de administración de FirePOWER

El antedicho será visto en el fondo como serie de conexiones SSL del PC hacia el IP ASA:



```
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
```

Paso 3 – La comunicación de los iniciados del ASDM hacia el módulo de FirePOWER

Puesto que el ASDM conoce el IP de administración de FirePOWER inicia a las sesiones SSL hacia el módulo:

Initializing FirePOWER communication 17%

Device IP Address / Name: 192.168.75.23

Username: cisco

Password: *****

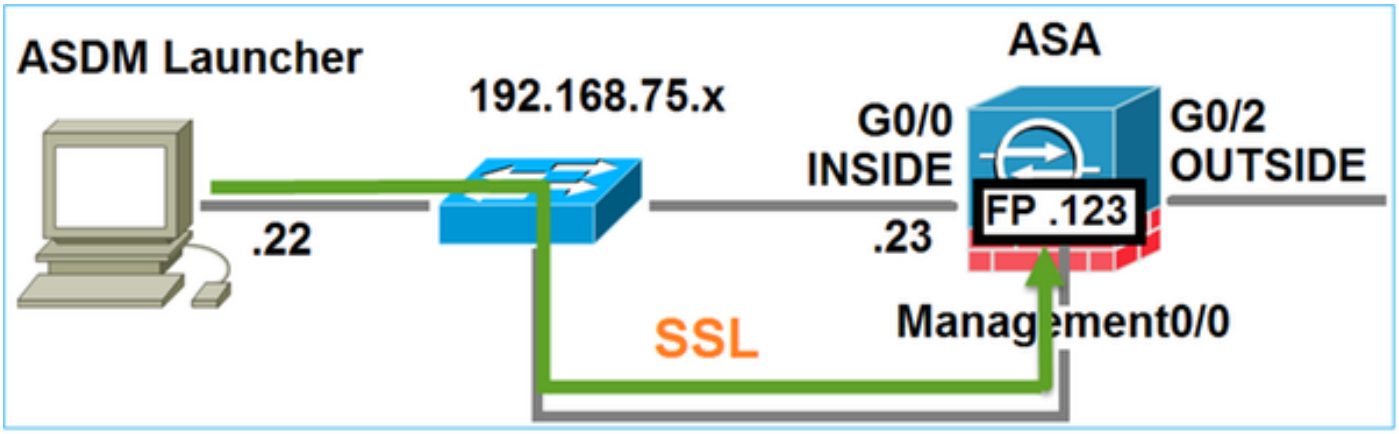
☐ Remember the username of the specified device on this computer

☐ Run in Demo Mode

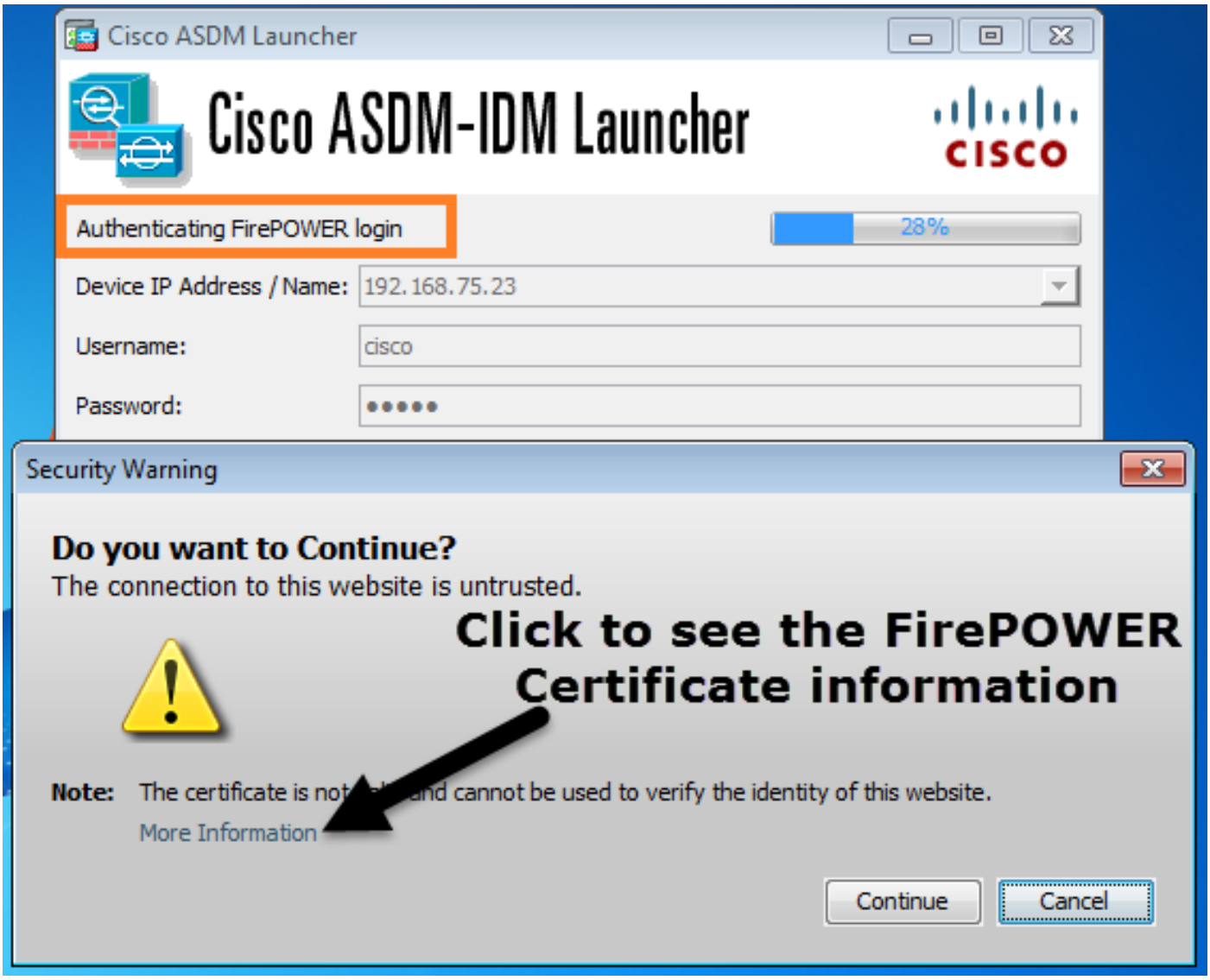
El antedicho será visto en el fondo como las conexiones SSL del host del ASDM hacia el IP de administración de FirePOWER:

```
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
```

Esto puede ser visualizada como sigue:

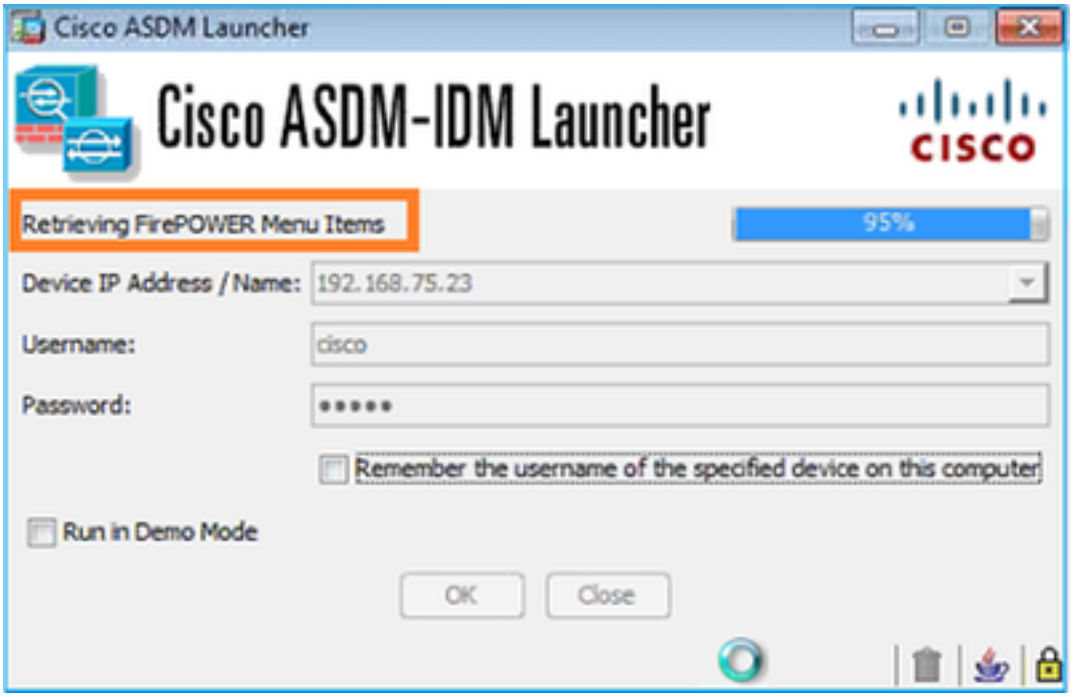


El ASDM autentica FirePOWER y se muestra una advertencia de seguridad puesto que uno mismo-se firma el certificado de FirePOWER:

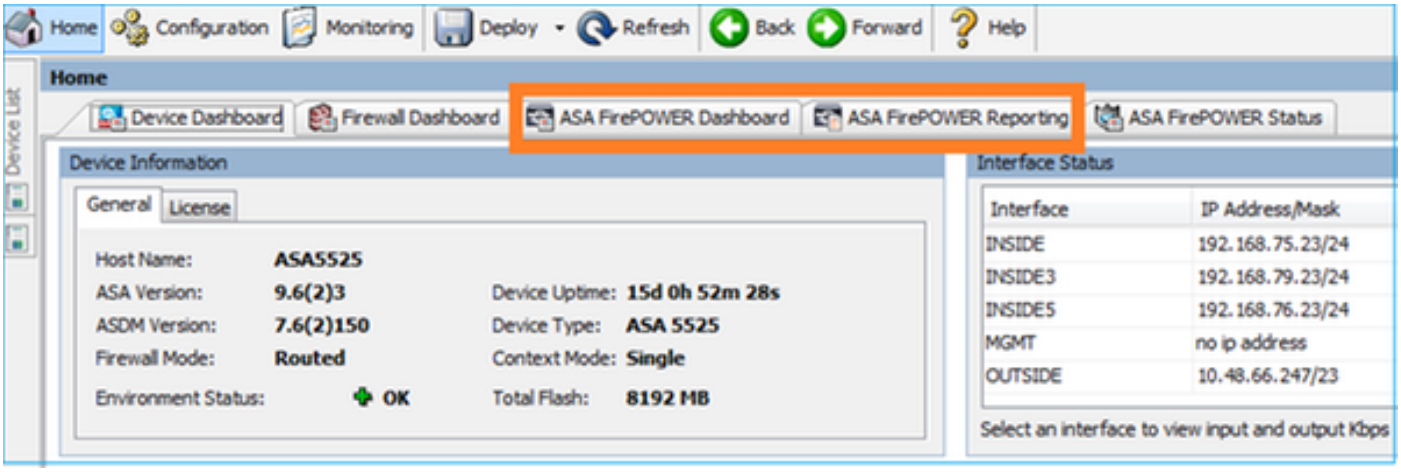


Paso 4 – El ASDM extrae los elementos de menú de FirePOWER

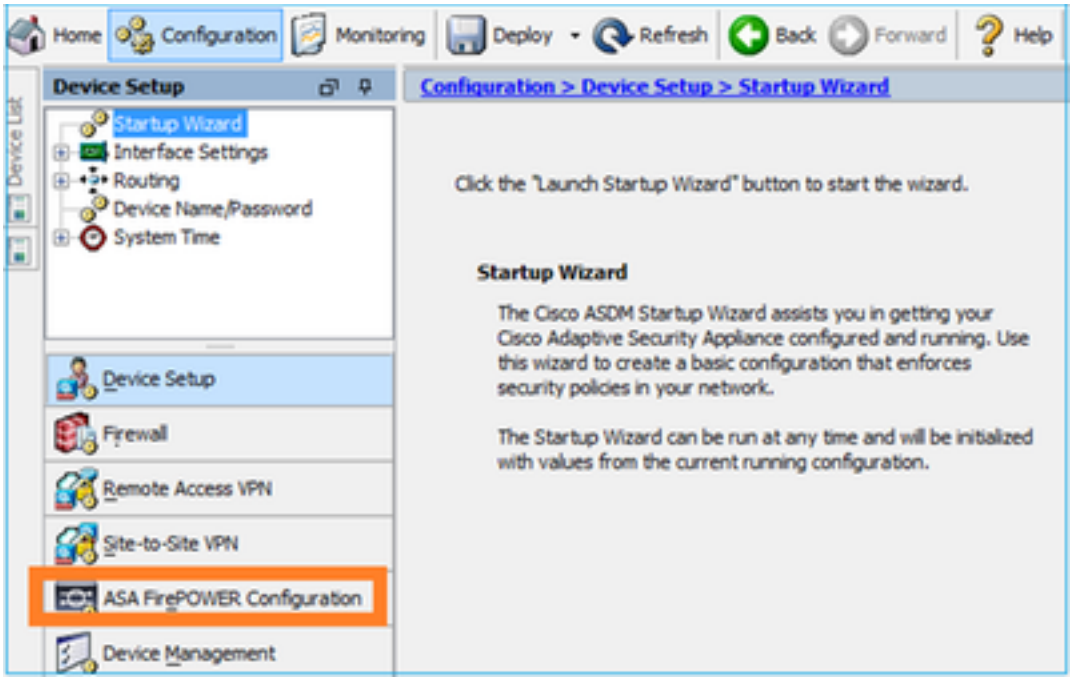
Después de la autenticación satisfactoria el ASDM extrae de FirePOWER los elementos de menú:



Las lenguetas extraídas:

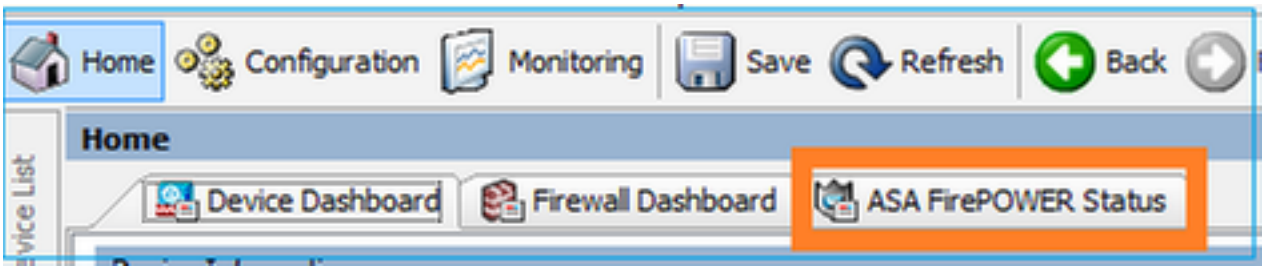


También extrae el elemento de menú de la configuración ASA FirePOWER:

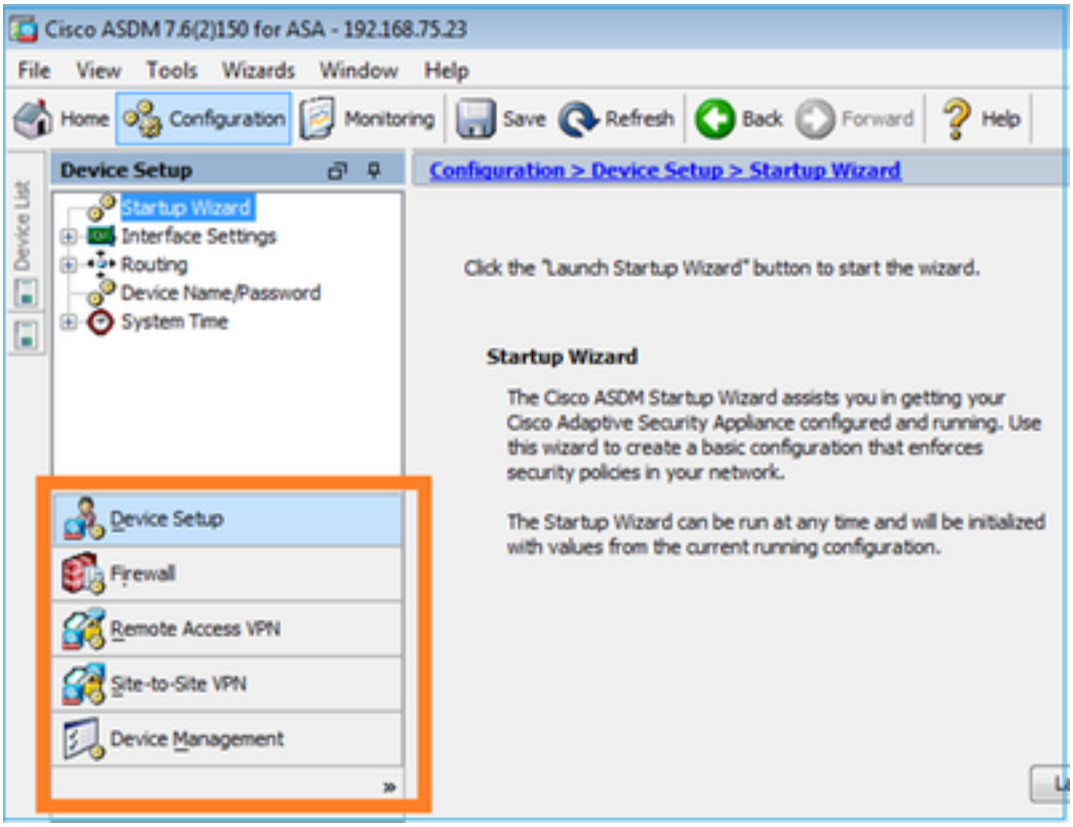


Resolución de problemas

En caso de que el ASDM no pueda establecer un túnel SSL con el IP de administración FP entonces cargará solamente el elemento de menú siguiente de FirePOWER:



El elemento de configuración ASA FirePOWER faltará también:



Acciones recomendadas

Verificación 1

Aseegurese que la interfaz de administración ASA es ASCENDENTE y el switchport conectado con él está en el VLA N apropiado:

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

Verificación 2

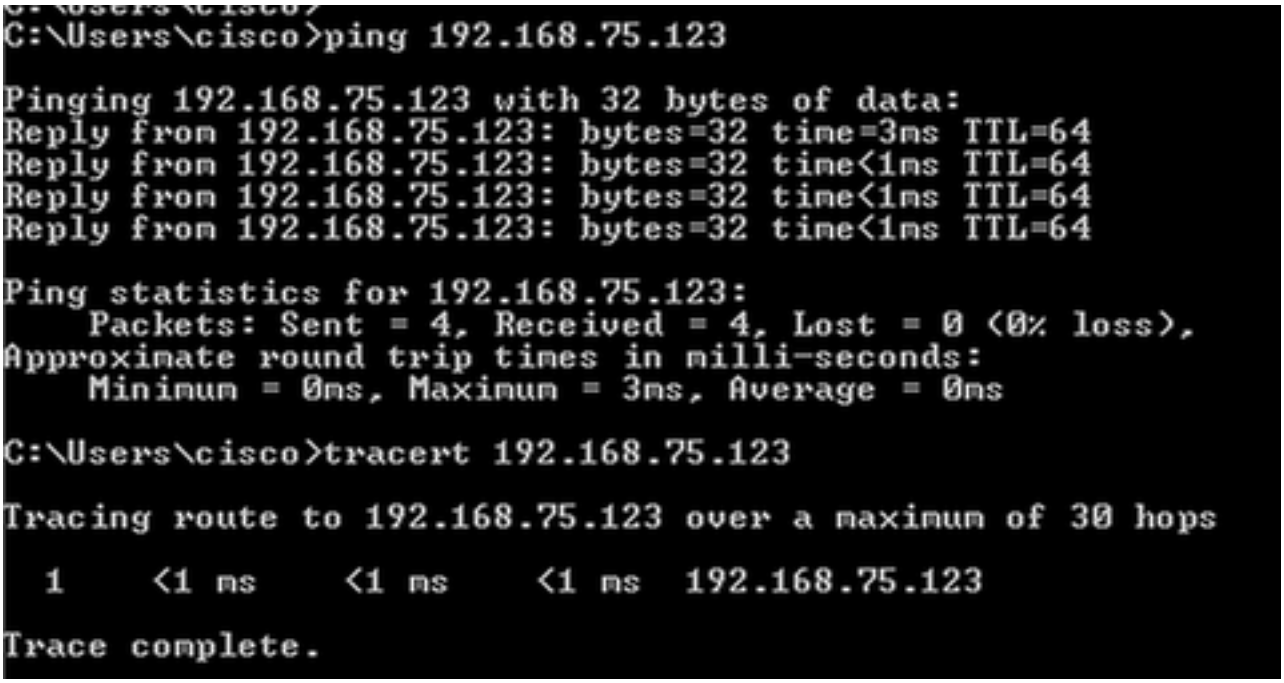
Aseegurese que el módulo de FirePOWER está inicializado completamente, en servicio:

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

>
```

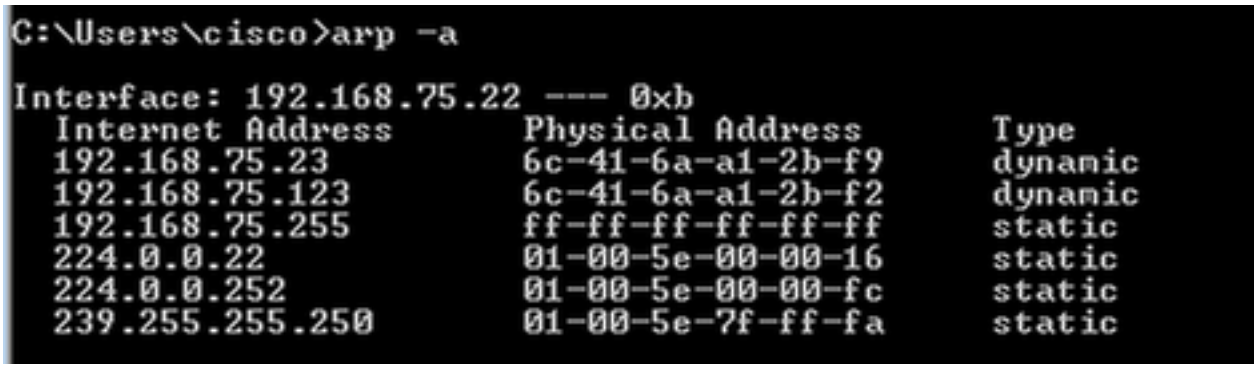
Verificación 3

Conectividad básica del control entre el host del ASDM y el IP de administración del módulo de FirePOWER usando las herramientas como el **ping** y el **tracert/el traceroute:**



Verificación 4

Si el host del ASDM y el IP de administración de FirePOWER son en el mismo control de la red L3 la tabla ARP en el host del ASDM:



Verificación 5

Captura del permiso en el dispositivo del ASDM mientras que usted está conectando vía el ASDM para ver si hay comunicación TCP apropiada entre el host y el módulo de FirePOWER. En el mínimo usted debe ver:

- Apretón de manos de tres vías TCP entre el host del ASDM y el ASA
- Túnel SSL establecido entre el host del ASDM y el ASA
- Apretón de manos de tres vías TCP entre el host del ASDM y el IP de administración del módulo de FirePOWER
- Túnel SSL establecido entre el host del ASDM y el IP de administración del módulo de FirePOWER

Verificación 6

Para marcar el tráfico a y desde el módulo de FirePOWER usted puede habilitar la captura en la interfaz del asa_mgmt_plane. En la captura debajo de ella puede ser visto:

- Pedido ARP del host del ASDM (paquete 42)
- Respuesta ARP del módulo de FirePOWER (paquete 43)
- Apretón de manos de tres vías TCP entre el host y el módulo de FirePOWER (paquetes del ASDM 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
```

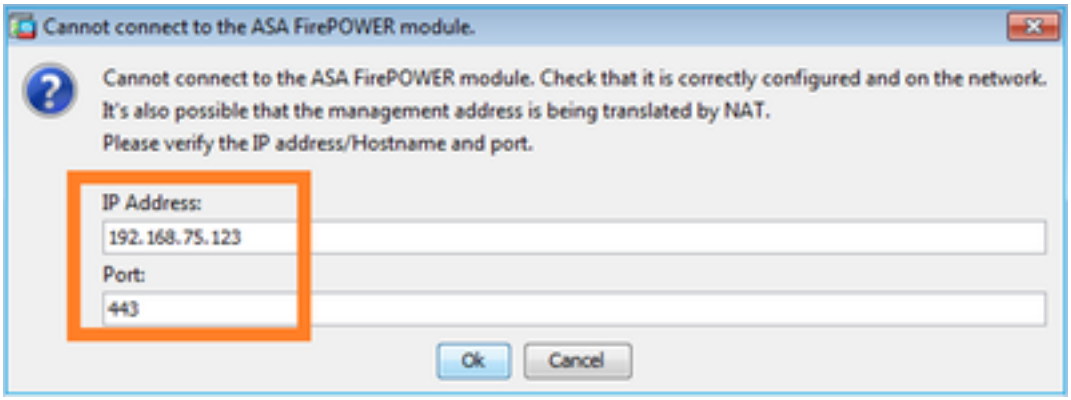
Verificación 7

Verifique que el usuario del ASDM tenga nivel de privilegio 15. Una manera de confirmar esto está ejecutando **HTTP 255 del debug** mientras que conecta vía el ASDM:

```
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]
```

Verificación 8

Si entre el host del ASDM y el módulo de FirePOWER hay NAT para el IP de administración de FirePOWER entonces usted necesidad de especificar el IP del NATed:



Verificación 9

Aseegurese que el módulo de FirePOWER no es manejado ya por el centro de administración de FirePOWER (FMC) porque en ese caso las lenguetas de FirePOWER en el ASDM faltarán:

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

>
```

Otra manera:

```
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
```

Verificación 10

Verifique en la guía de la compatibilidad ASA que las imágenes ASA/ASDM sean compatibles:

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

Verificación 11

Verifique en la guía de la compatibilidad de FirePOWER que el dispositivo de FirePOWER sea compatible con la versión del ASDM:

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

Documentos Relacionados

Guía de inicio rápido del módulo de Cisco ASA FirePOWER

ASA con la guía de configuración de la administración local de los servicios de FirePOWER, versión 6.1.0

Guía del usuario del módulo ASA FirePOWER para el ASA5506-X, el ASA5506H-X, el ASA5506W-X, el ASA5508-X, y el ASA5516-X, versión 5.4.1