

Usando el ASDM para manejar un módulo de la potencia de fuego en el ASA

Contenido

[Introducción](#)

[Componentes usados](#)

[prerrequisitos](#)

[Arquitectura](#)

[Operación de fondo cuando un usuario conecta con el ASA vía el ASDM](#)

[¿Paso 1? El usuario inicia la conexión del ASDM](#)

[¿Paso 2? El ASDM descubre la configuración ASA y el IP del módulo de la potencia de fuego](#)

[¿Paso 3? El ASDM inicia la comunicación hacia el módulo de la potencia de fuego](#)

[¿Paso 4? El ASDM extrae los elementos de menú de la potencia de fuego](#)

[Resolución de problemas](#)

[Acciones recomendadas](#)

[Documentos Relacionados](#)

Introducción

Un módulo de la potencia de fuego que está instalado en el ASA se puede manejar por cualquiera:

- ¿Centro de administración de la potencia de fuego (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 la potencia de fuego 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 la potencia de fuego

Prerrequisitos

Configuración ASA para habilitar la Administración del ASDM:

```
ASA5525(config)# interface GigabitEthernet0/0ASA5525(config-if)# nameif INSIDEASA5525(config-if)# security-level 100ASA5525(config-if)# ip address 192.168.75.23 255.255.255.0ASA5525(config-if)# no shutdownASA5525(config)#ASA5525(config)# http server enableASA5525(config)# http 192.168.75.0 255.255.255.0 INSIDEASA5525(config)# asdm image disk0:/asdm-762150.binASA5525(config)#ASA5525(config)# aaa authentication http console LOCALASA5525(config)#
```

```
username cisco password cisco
```

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

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

Arquitectura

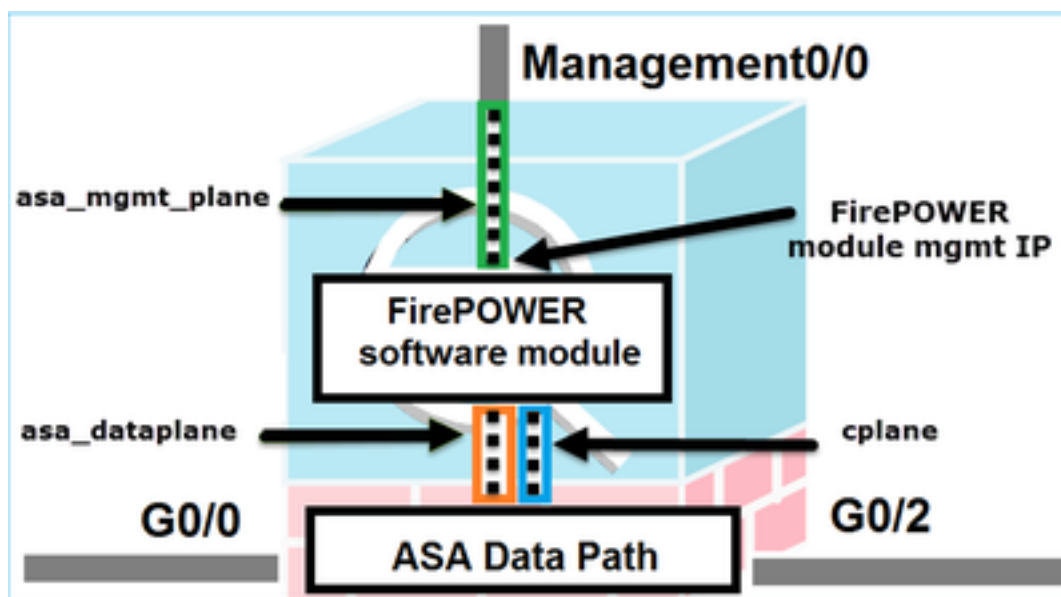
El ASA tiene 3 interfaces internas:

- **asa_dataplane** = se utiliza para reorientar los paquetes del trayecto de datos ASA al módulo de software de la potencia de fuego
- **asa_mgmt_plane** = se utiliza para permitir que la interfaz de administración de la potencia de fuego 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 la potencia de fuego

Usted puede capturar el tráfico en todas las interfaces internas:

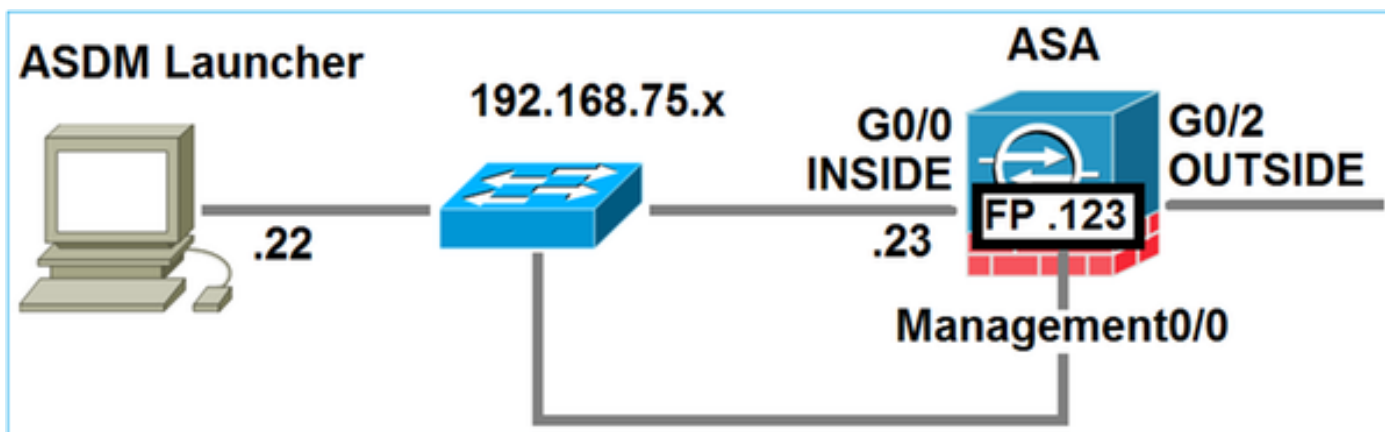
```
ASA5525# capture CAP interface ? asa_dataplane Capture packets on dataplane interface  
asa_mgmt_plane Capture packets on managementplane interface cplane Capture packets on  
controlplane interface
```

El antedicho puede ser visualizado como sigue:



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

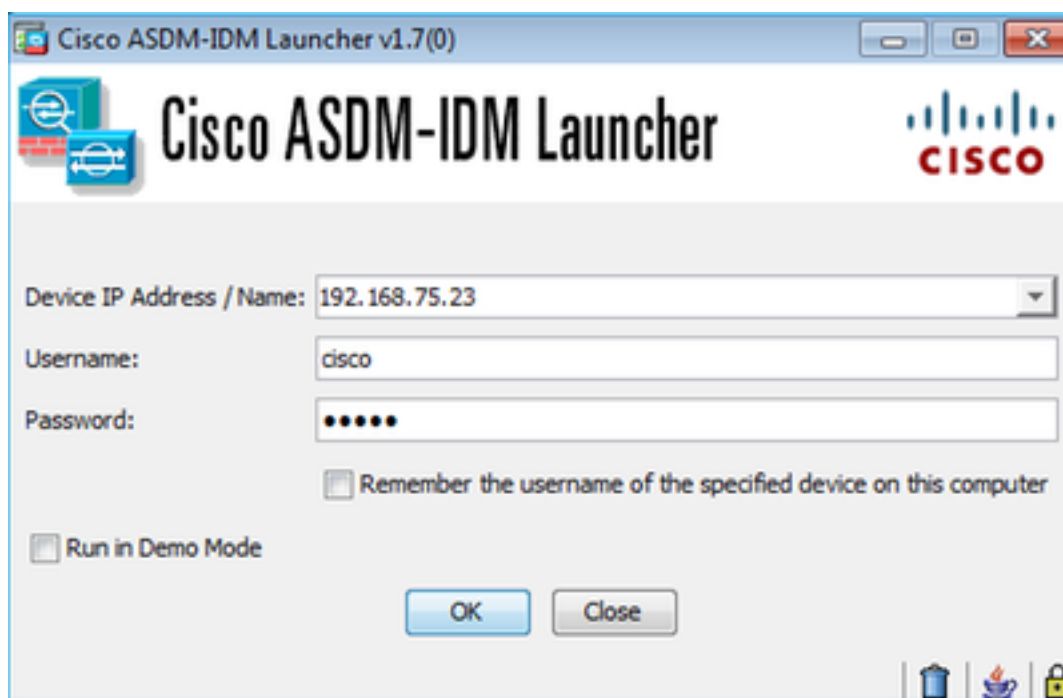
Considere la topología siguiente



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

¿Paso 1? El usuario inicia la conexión del ASDM

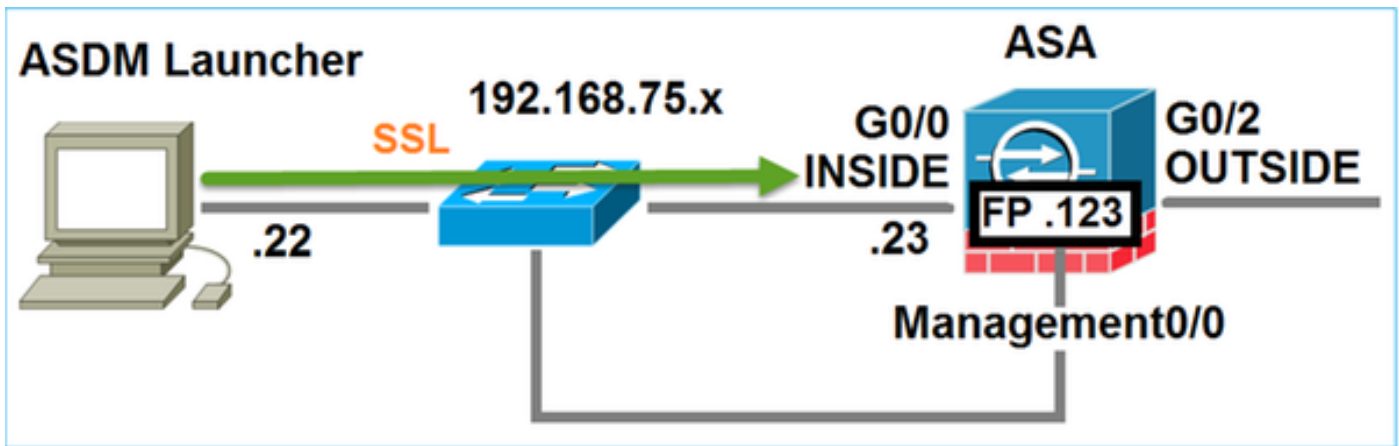
El usuario especifica el IP ASA usado para la Administración HTTP, ingresa las credenciales e inicia una conexión hacia el ASA:



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 la potencia de fuego

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 la potencia de fuego

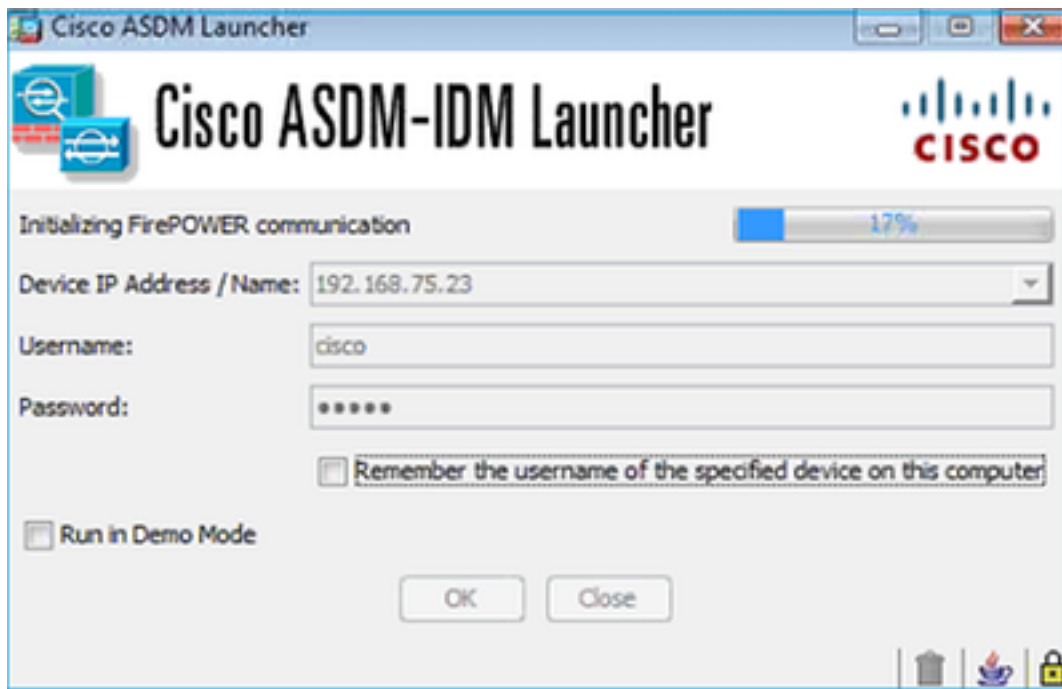
El antedicho será visto en el fondo como serie de conexiones SSL del PC hacia el IP ASA:

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 la potencia de fuego

Puesto que el ASDM conoce el IP de administración de la potencia de fuego inicia a las sesiones

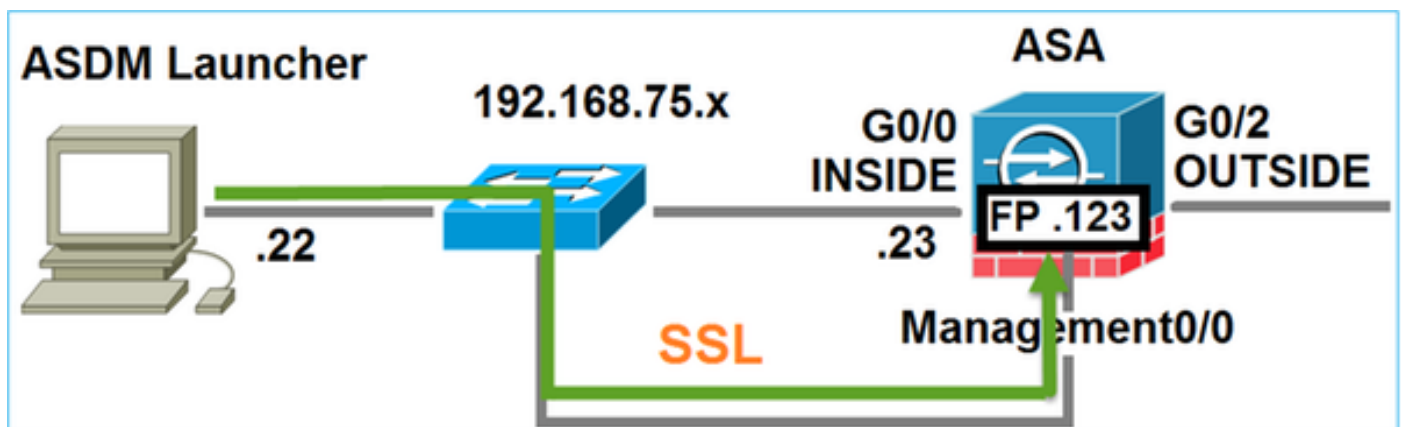
SSL hacia el módulo:



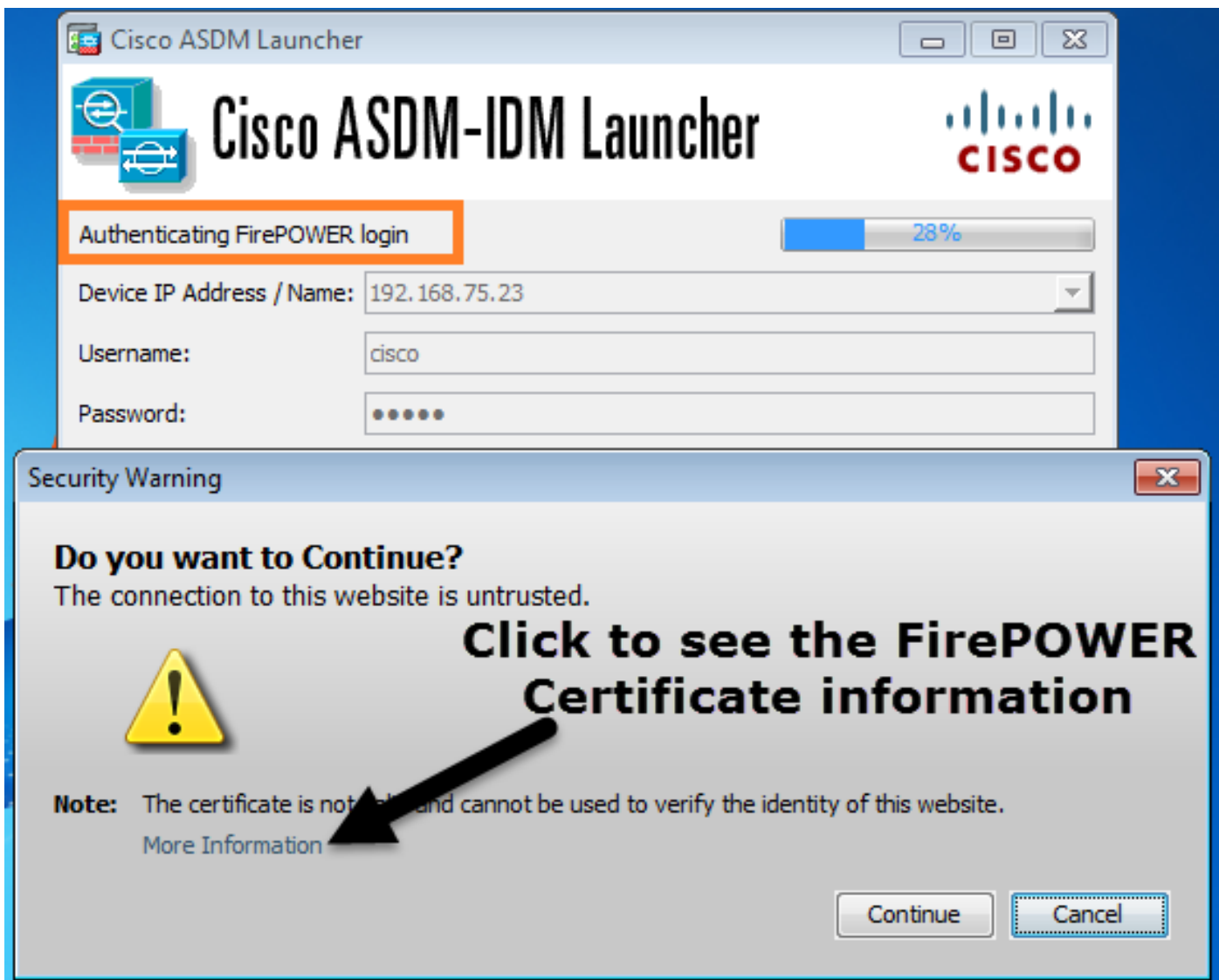
El antedicho será visto en el fondo como las conexiones SSL del host del ASDM hacia el IP de administración de la potencia de fuego:

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:

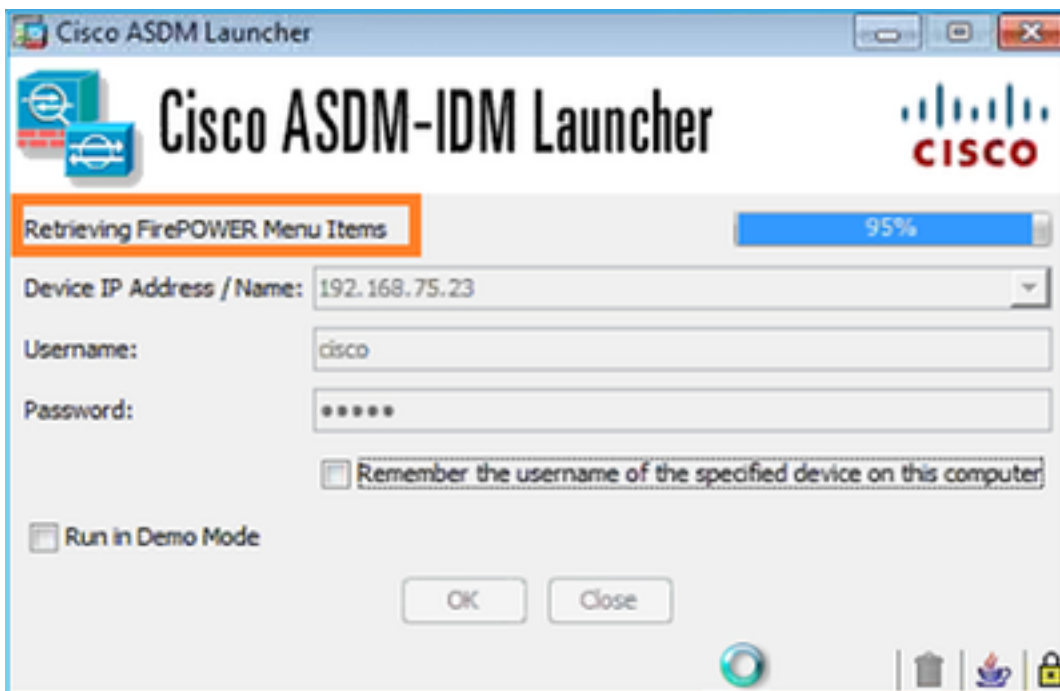


El ASDM autentica la potencia de fuego y se muestra una advertencia de seguridad puesto que uno mismo se firma el certificado de la potencia de fuego:

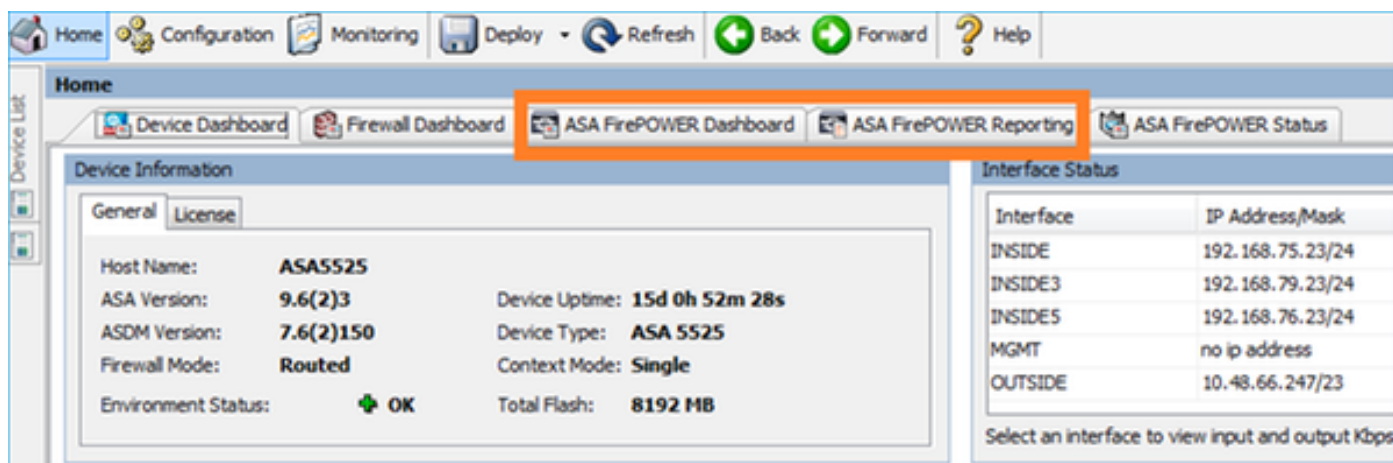


¿Paso 4? El ASDM extrae los elementos de menú de la potencia de fuego

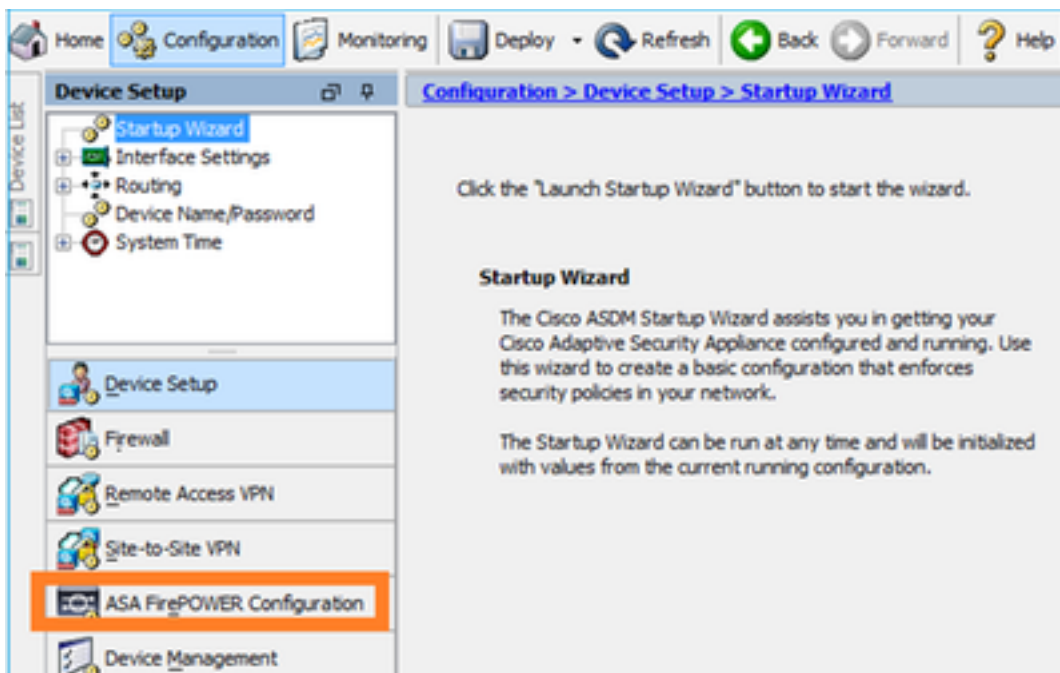
Después de la autenticación satisfactoria el ASDM extrae de la potencia de fuego los elementos de menú:



Las lenguetas extraídas:

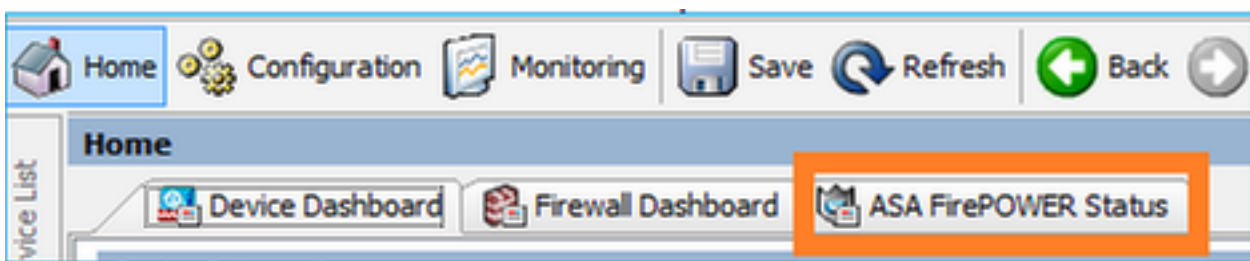


También extrae el elemento de menú de la configuración de la potencia de fuego ASA:

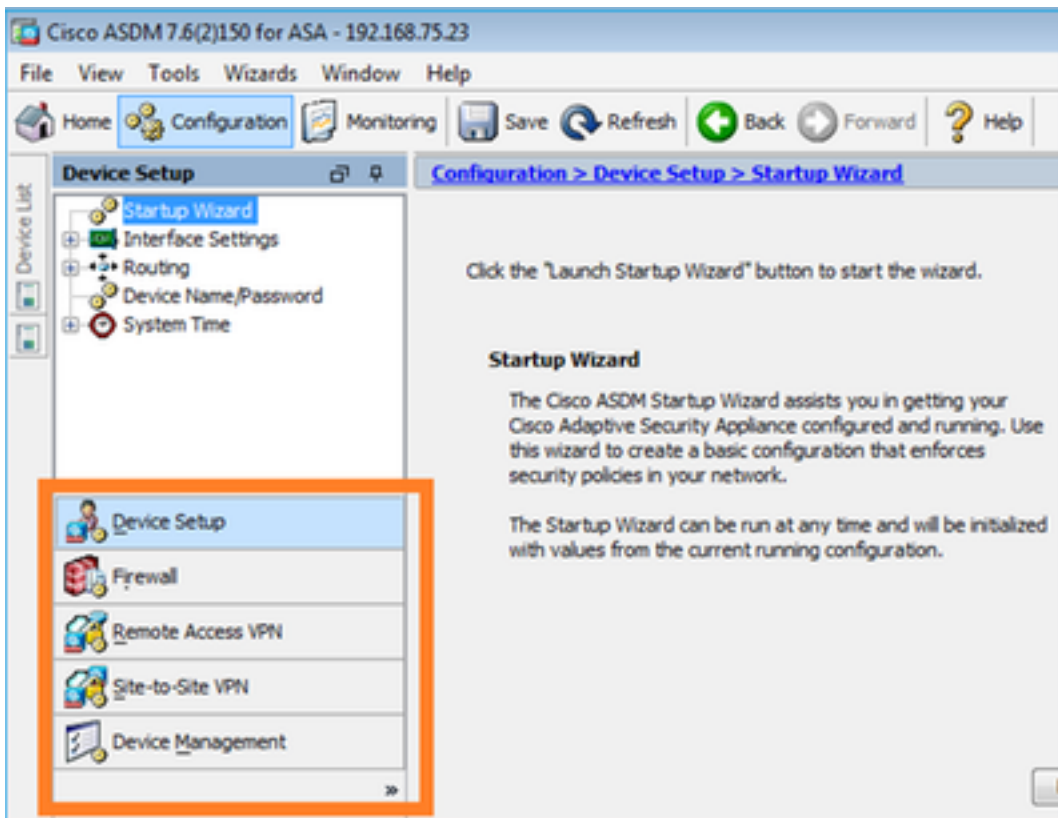


Resolución de problemas

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 la potencia de fuego:



El elemento de configuración de la potencia de fuego ASA faltará también:



Acciones recomendadas

Verificación 1

Asegurese 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

Asegurese que el módulo de la potencia de fuego 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-vrtVDB version : 270----->
```

Verificación 3

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

```
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
  0   <1 ms    <1 ms    <1 ms   192.168.75.123
Trace complete.
```

Verificación 4

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

```
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
```

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 la potencia de fuego. 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 la potencia de fuego
- Túnel SSL establecido entre el host del ASDM y el IP de administración del módulo de la potencia de fuego

Verificación 6

Para marcar el tráfico a y desde el módulo de la potencia de fuego 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 la potencia de fuego (paquete 43)
- Apretón de manos de tres vías TCP entre el host y el módulo de la potencia de fuego (paquetes del ASDM 44-46)

```
ASA5525# capture FP_MGMT interface asa_mgmt_planeASA5525# 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
```

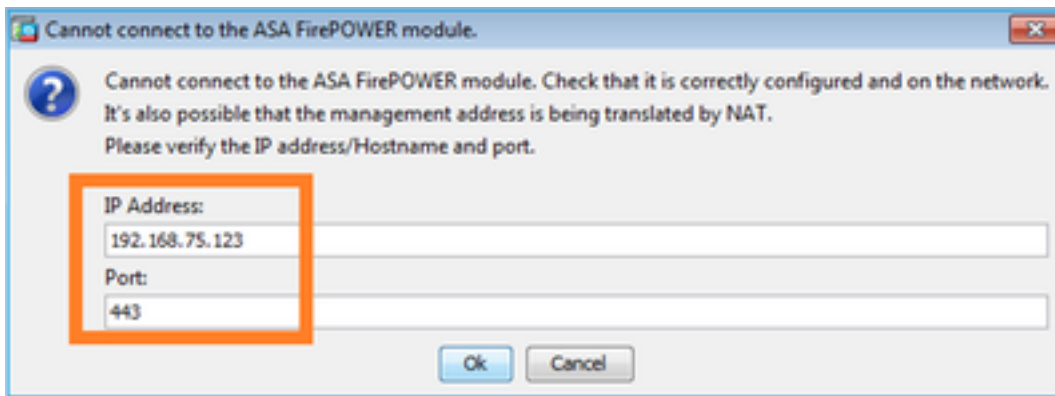
Verificación 7

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 255debug 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
resetHTTP: admin session verified = [1]HTTP: username = [user1], privilege = [14]
```

Verificación 8

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



Verificación 9

Asegúrese que el módulo de la potencia de fuego no es manejado ya por el centro de administración de la potencia de fuego (FMC) porque en ese caso las lengüetas de la potencia de fuego en el ASDM faltarán:

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

Otra manera:

```
ASA5525# show module sfr detailsGetting details from the Service Module, please wait...Card  
Type: FirePOWER Services Software ModuleModel: ASA5525Hardware version: N/ASerial Number:  
FCH1719J54RFirmware version: N/ASoftware version: 6.1.0-330MAC Address Range: 6c41.6aa1.2bf2 to  
6c41.6aa1.2bf2App. name: ASA FirePOWERApp. Status: UpApp. Status Desc: Normal OperationApp.  
version: 6.1.0-330Data Plane Status: UpConsole session: ReadyStatus: UpDC addr: No DC  
ConfiguredMgmt IP addr: 192.168.75.123Mgmt Network mask: 255.255.255.0Mgmt Gateway:  
192.168.75.23Mgmt web ports: 443Mgmt 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 la potencia de fuego que el dispositivo de la potencia de fuego 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 la potencia de fuego de Cisco ASA](#)

[El ASA con la potencia de fuego mantiene la guía de configuración de la administración local, versión 6.1.0](#)

[Guía del usuario del módulo de la potencia de fuego ASA para el ASA5506-X, el ASA5506H-X, el ASA5506W-X, el ASA5508-X, y el ASA5516-X, versión 5.4.1](#)