

Uso de ASDM para administrar un módulo FirePOWER en un ASA

Contenido

[Introducción](#)

[Antecedentes](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Arquitectura](#)

[Funcionamiento en segundo plano cuando un usuario se conecta a un ASA mediante ASDM](#)

[Paso 1 - El usuario inicia la conexión ASDM](#)

[Paso 2: el ASDM detecta la configuración del ASA y la dirección IP del módulo FirePOWER](#)

[Paso 3: El ASDM inicia la comunicación con el módulo FirePOWER](#)

[Paso 4: El ASDM recupera los elementos del menú de FirePOWER](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo el software ASDM se comunica con el Adaptive Security Appliance (ASA) y un módulo de software FirePOWER instalado en él.

Antecedentes

Un módulo FirePOWER instalado en un ASA se puede administrar mediante:

- FirePOWER Management Center (FMC): es la solución de gestión externa.
- Adaptive Security Device Manager (ASDM): se trata de la solución de gestión integrada.

Prerequisites

Requirements

Una configuración de ASA para habilitar la administración de ASDM:

```
<#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
```

Compruebe la [compatibilidad](#) entre el módulo ASA/SFR; de lo contrario, no se verán las fichas de FirePOWER.

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

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

Asegúrese de que el sistema cliente ASDM ejecuta una versión compatible de Java JRE.

Componentes Utilizados

- Un host de Microsoft Windows 7
- ASA5525-X que ejecuta ASA versión 9.6(2.3)
- ASDM versión 7.6.2.150
- Módulo de software FirePOWER 6.1.0-330

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Arquitectura

El ASA tiene tres interfaces internas:

- `asa_dataplane`: se utiliza para redirigir paquetes de la ruta de datos de ASA al módulo de software FirePOWER.
- `asa_mgmt_plane`: se utiliza para permitir que la interfaz de gestión de FirePOWER se comunique con la red.
- `cplane`: interfaz del plano de control que se utiliza para transferir señales de mantenimiento entre el ASA y el módulo FirePOWER.

Puede capturar el tráfico en todas las interfaces internas:

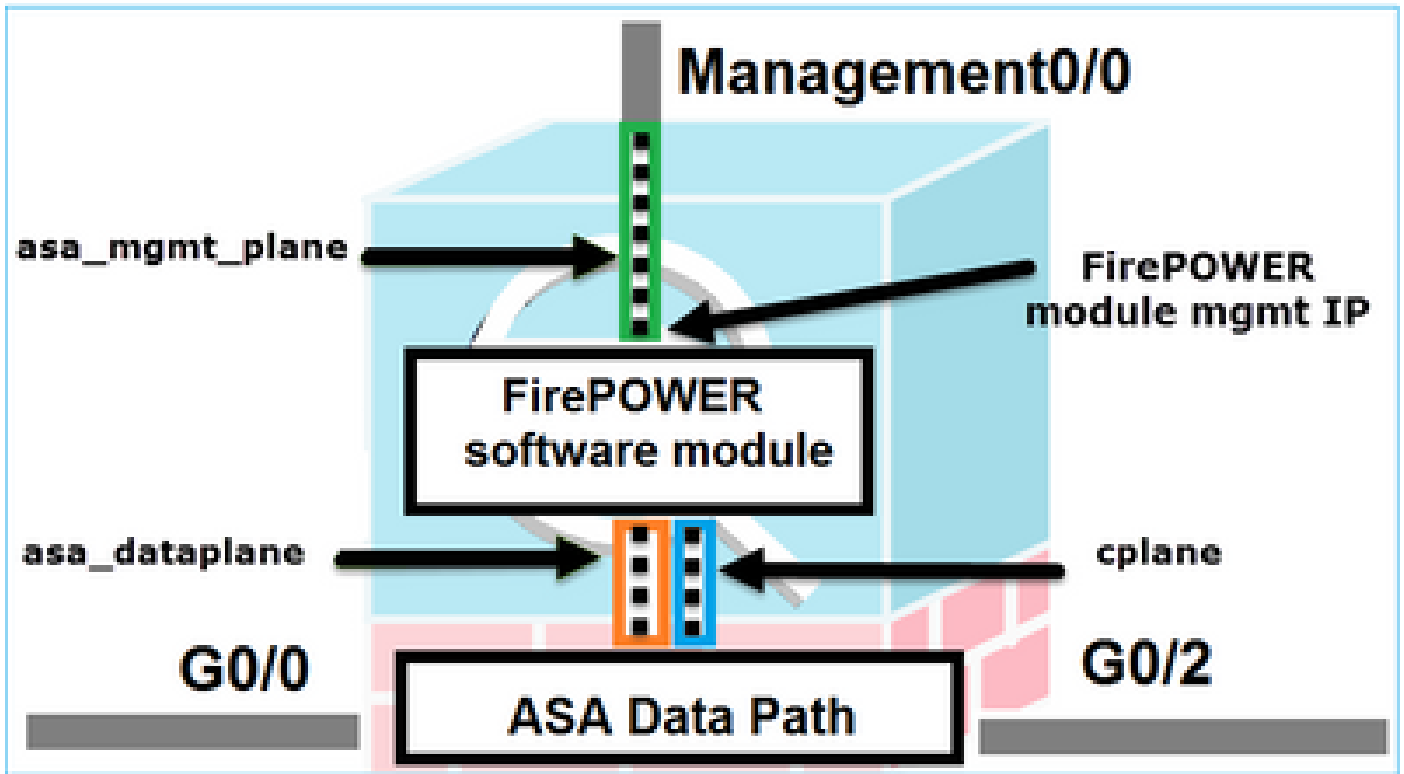
```
<#root>
```

```
ASA5525#
```

```
capture CAP interface ?
```

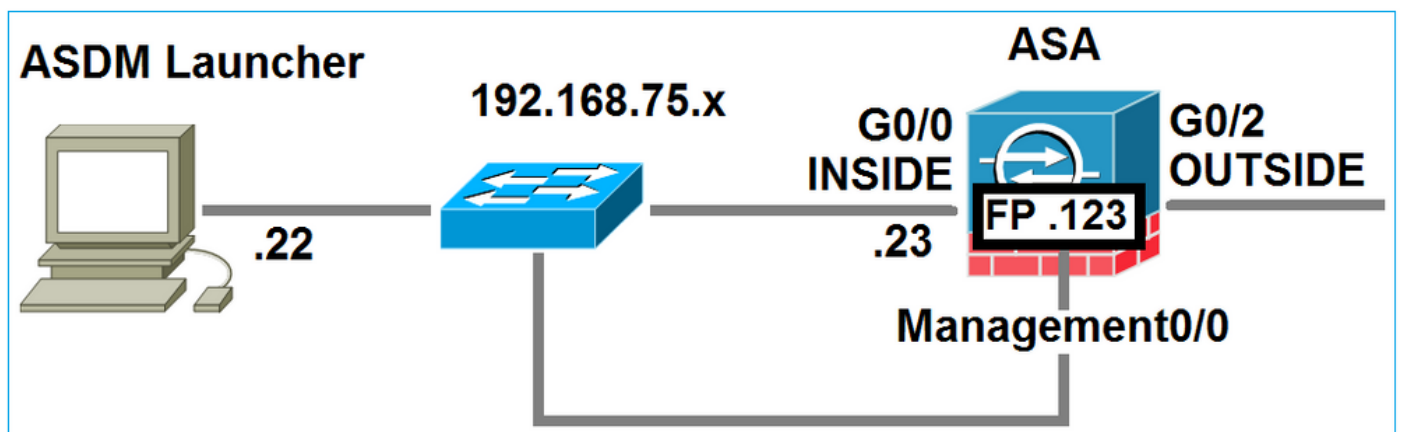
```
asa_dataplane  Capture packets on dataplane interface
asa_mgmt_plane Capture packets on managementplane interface
cplane         Capture packets on controlplane interface
```

Esto se puede visualizar de la siguiente manera:



Funcionamiento en segundo plano cuando un usuario se conecta a un ASA mediante ASDM

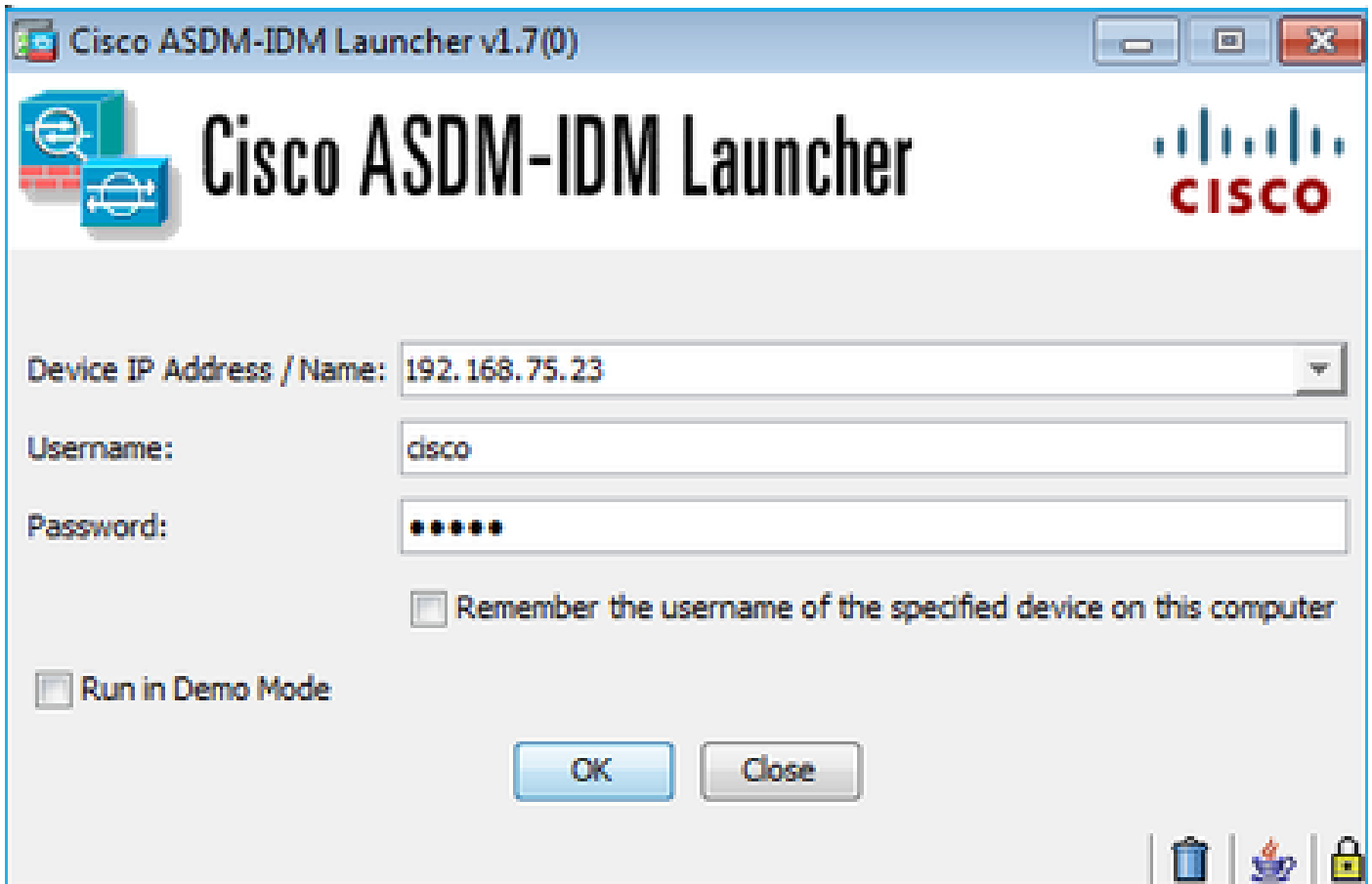
Tenga en cuenta esta topología:



Cuando un usuario inicia una conexión ASDM al ASA, ocurren estos eventos:

Paso 1 - El usuario inicia la conexión ASDM

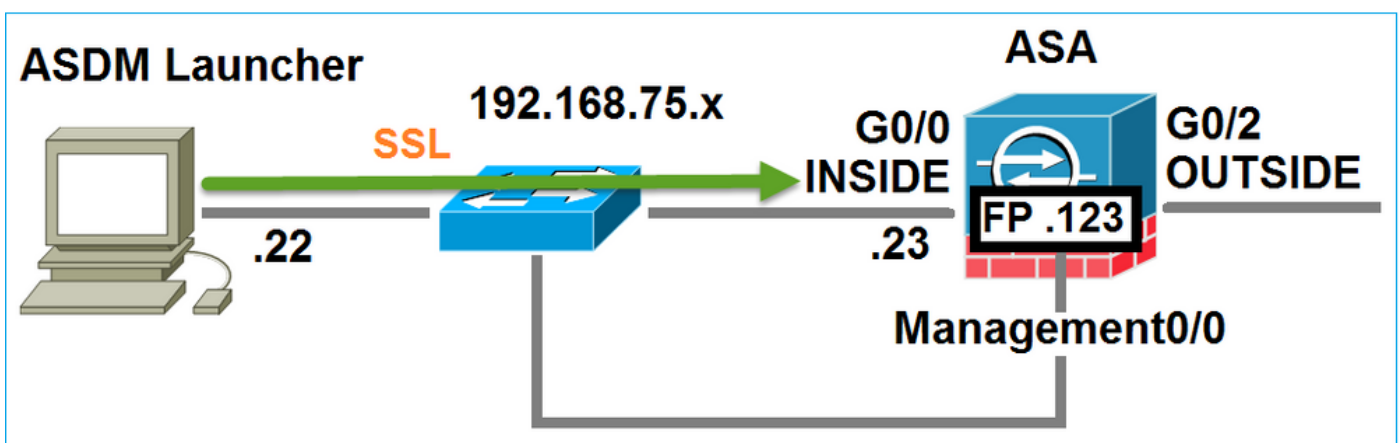
El usuario especifica la dirección IP de ASA utilizada para la administración HTTP, ingresa las credenciales e inicia una conexión hacia el ASA:



En segundo plano, se establece un túnel SSL entre el ASDM y el ASA:

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

Esto se puede visualizar de la siguiente manera:



Paso 2: el ASDM detecta la configuración del ASA y la dirección IP del módulo FirePOWER

Ingrese el comando debug http 255 en ASA para mostrar todas las comprobaciones que se hacen

en segundo plano cuando el ASDM se conecta al 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 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/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
```

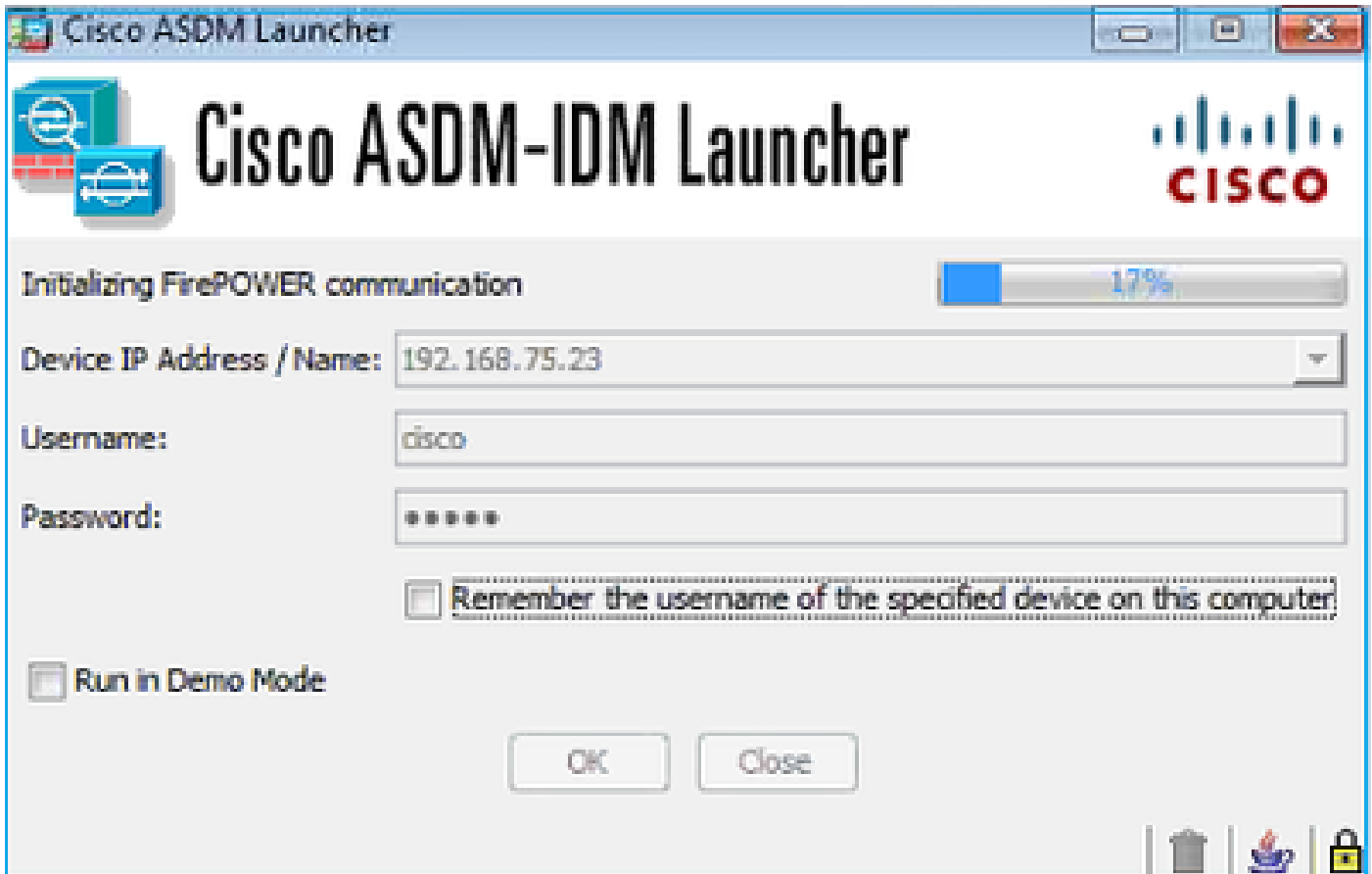
- show module - El ASDM detecta los módulos ASA.
- show module sfr details - El ASDM detecta los detalles del módulo, que incluyen la dirección IP de administración de FirePOWER.

Estos se ven en segundo plano como una serie de conexiones SSL desde la PC hacia la dirección IP de 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: El ASDM inicia la comunicación con el módulo FirePOWER

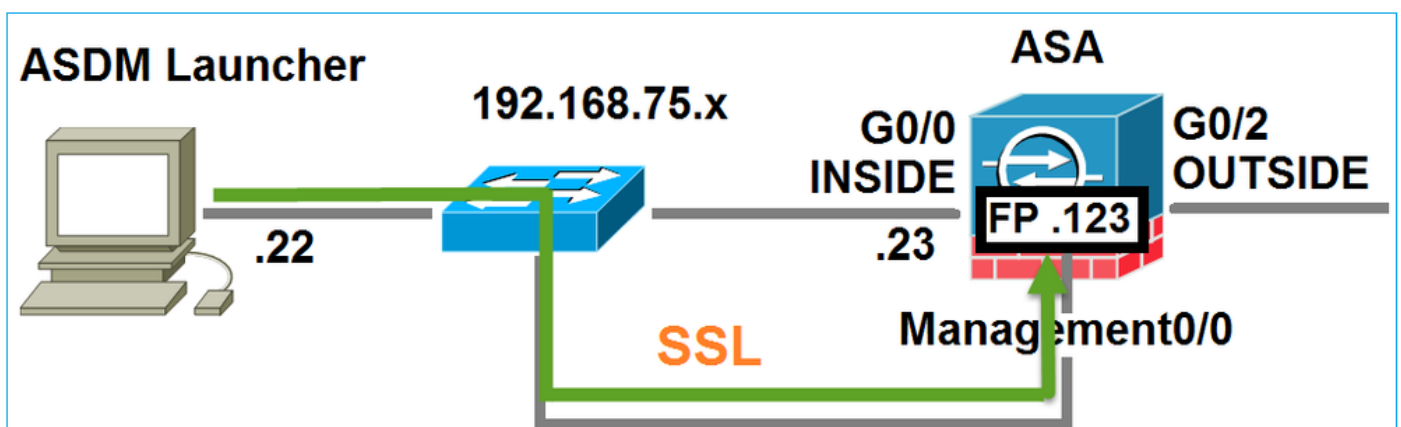
Dado que el ASDM conoce la dirección IP de administración de FirePOWER, inicia sesiones SSL hacia el módulo:



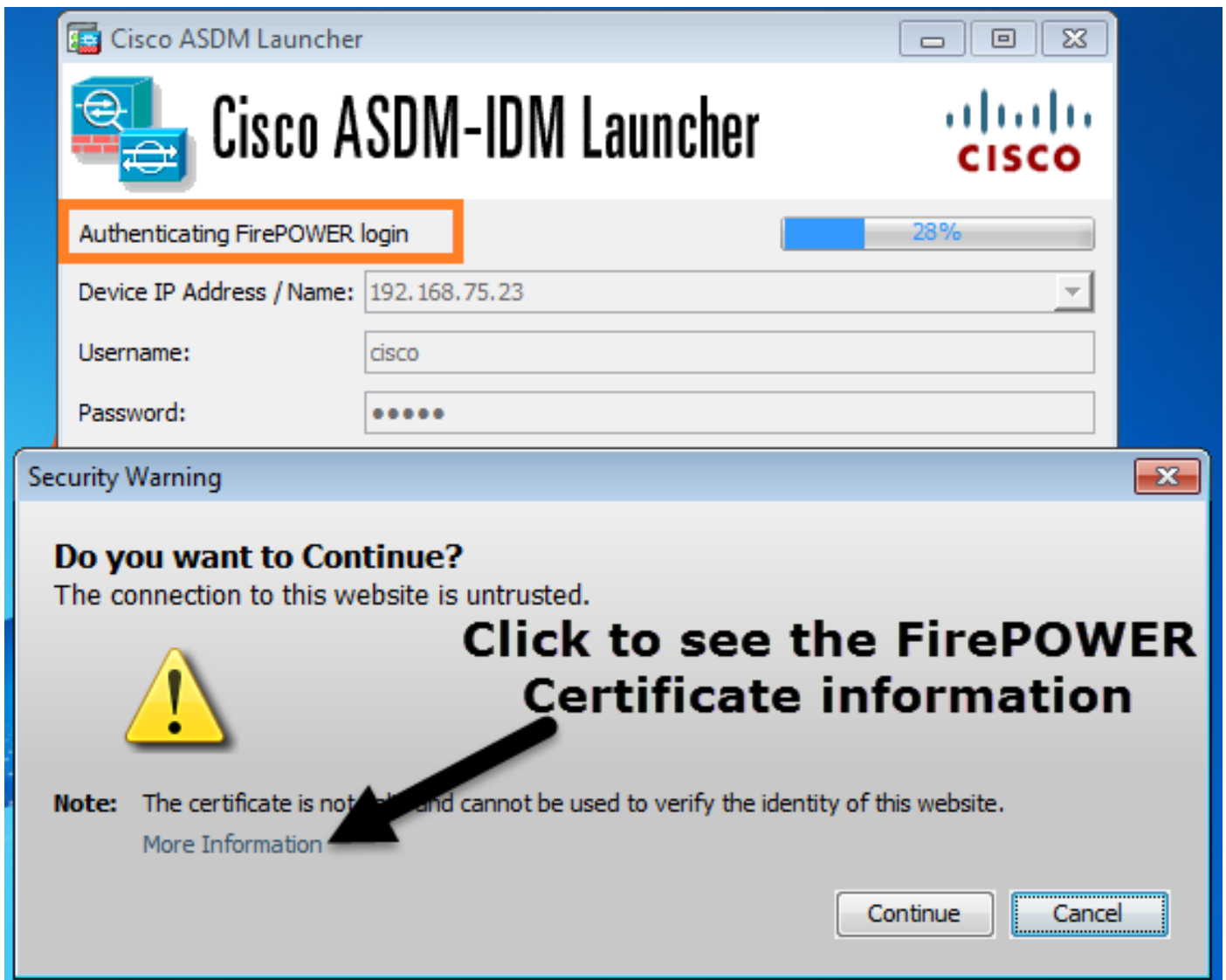
Esto se ve en segundo plano como conexiones SSL desde el host ASDM hacia la dirección IP de administración de FirePOWER:

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 se puede visualizar de la siguiente manera:

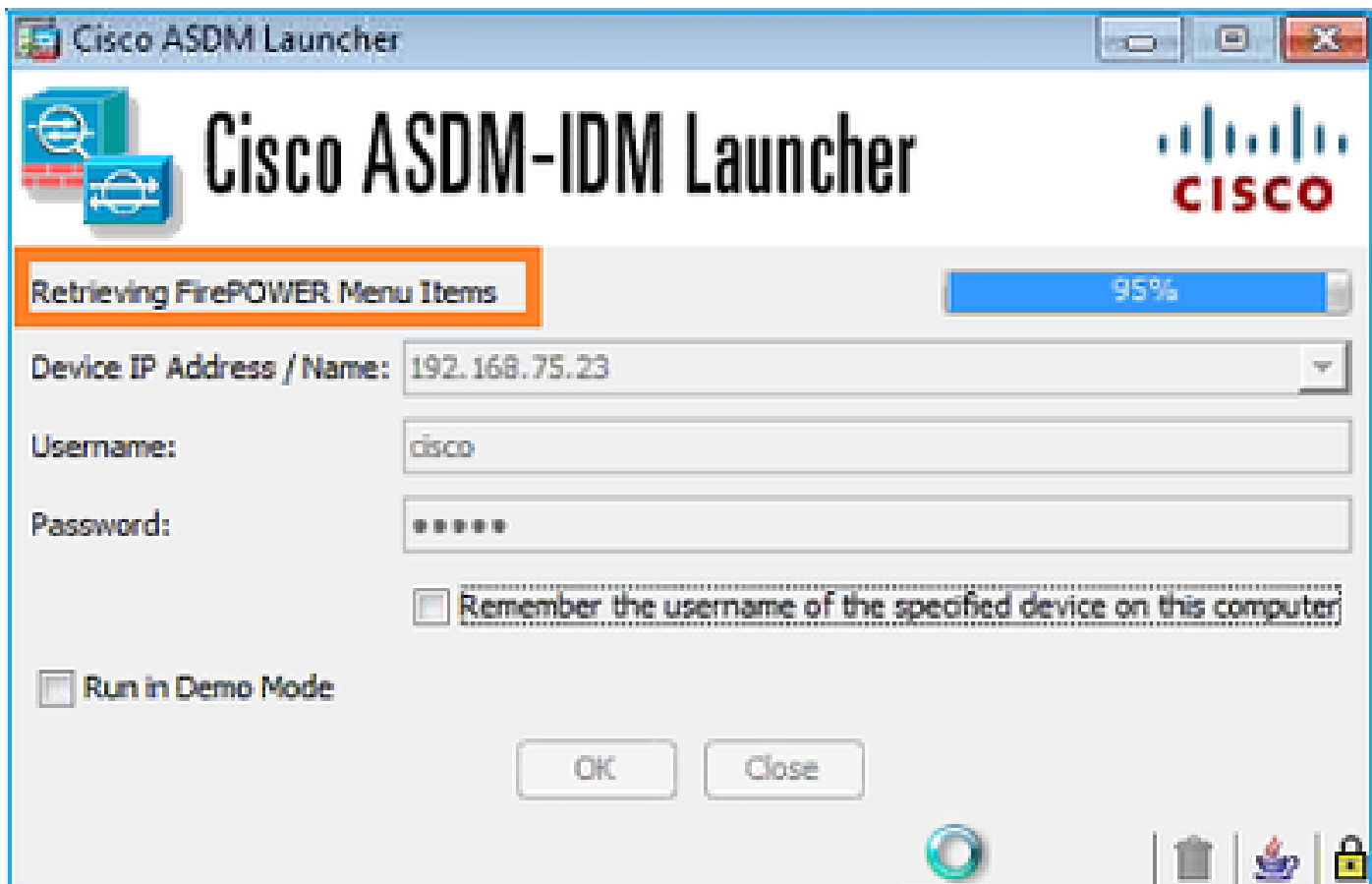


El ASDM autentica el FirePOWER y se muestra una advertencia de seguridad, ya que el certificado de FirePOWER está autofirmado:

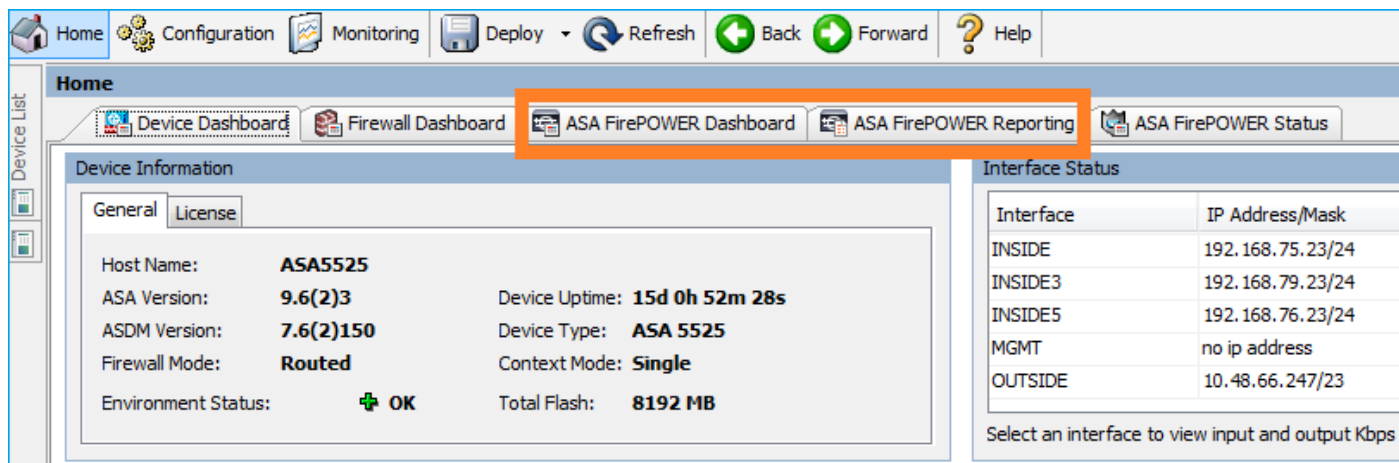


Paso 4: El ASDM recupera los elementos del menú de FirePOWER

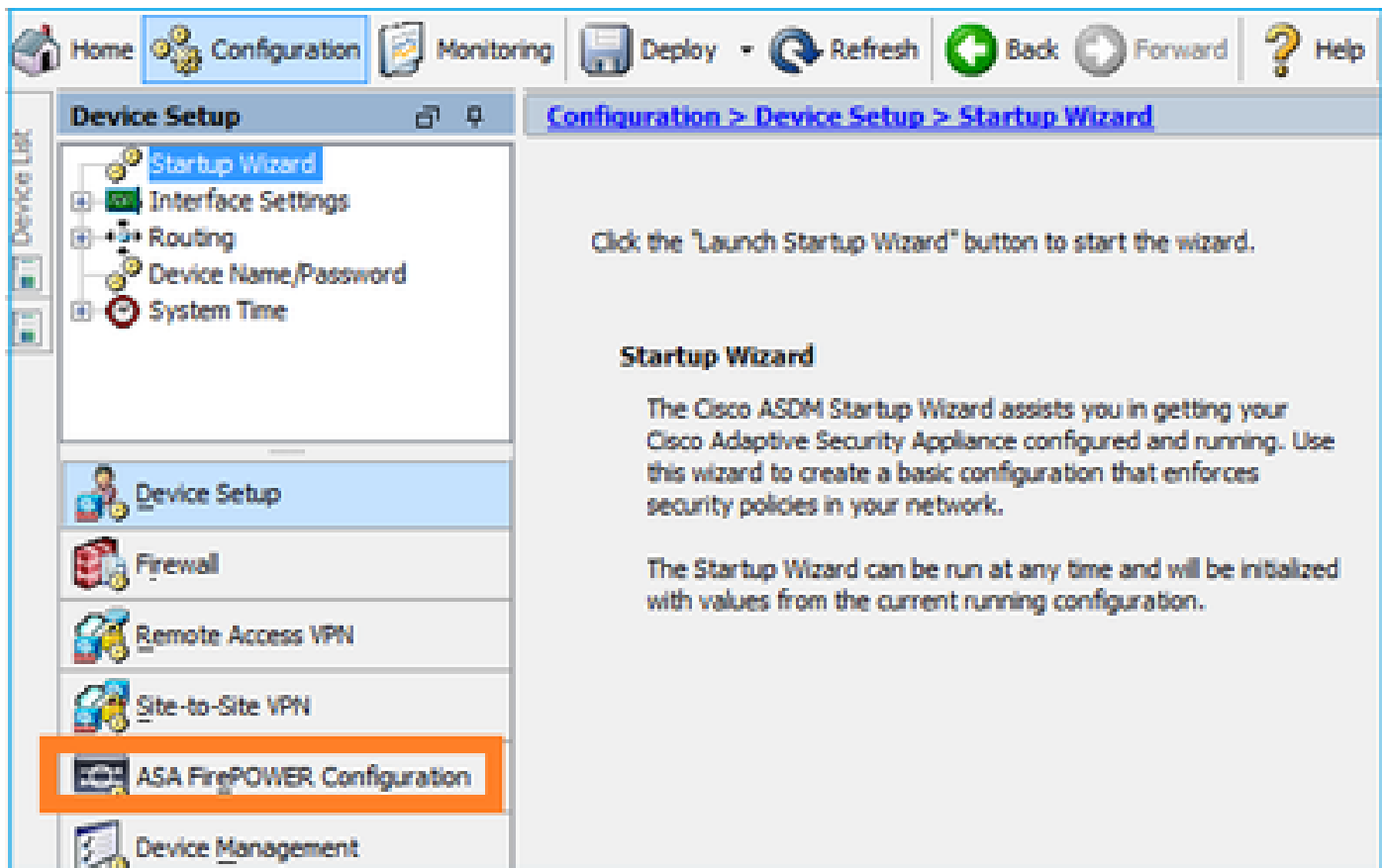
Después de la autenticación correcta, el ASDM recupera los elementos de menú del dispositivo FirePOWER:



Las fichas recuperadas se muestran en este ejemplo:

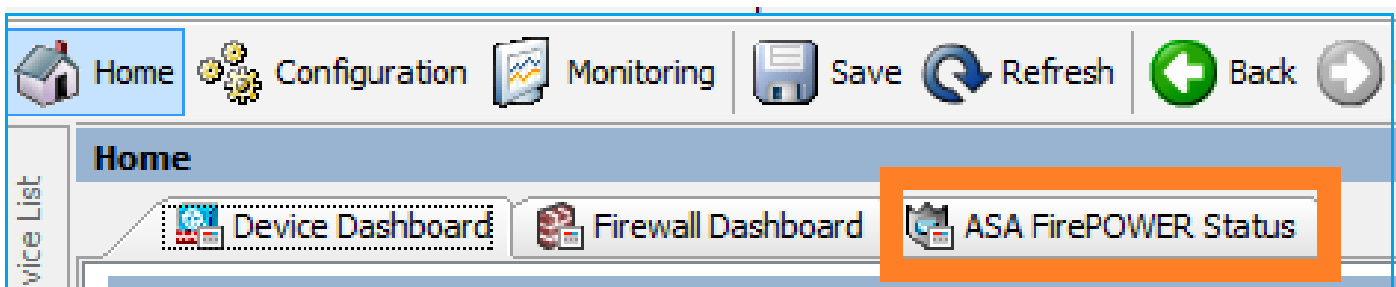


También recupera el elemento de menú Configuración de ASA FirePOWER:

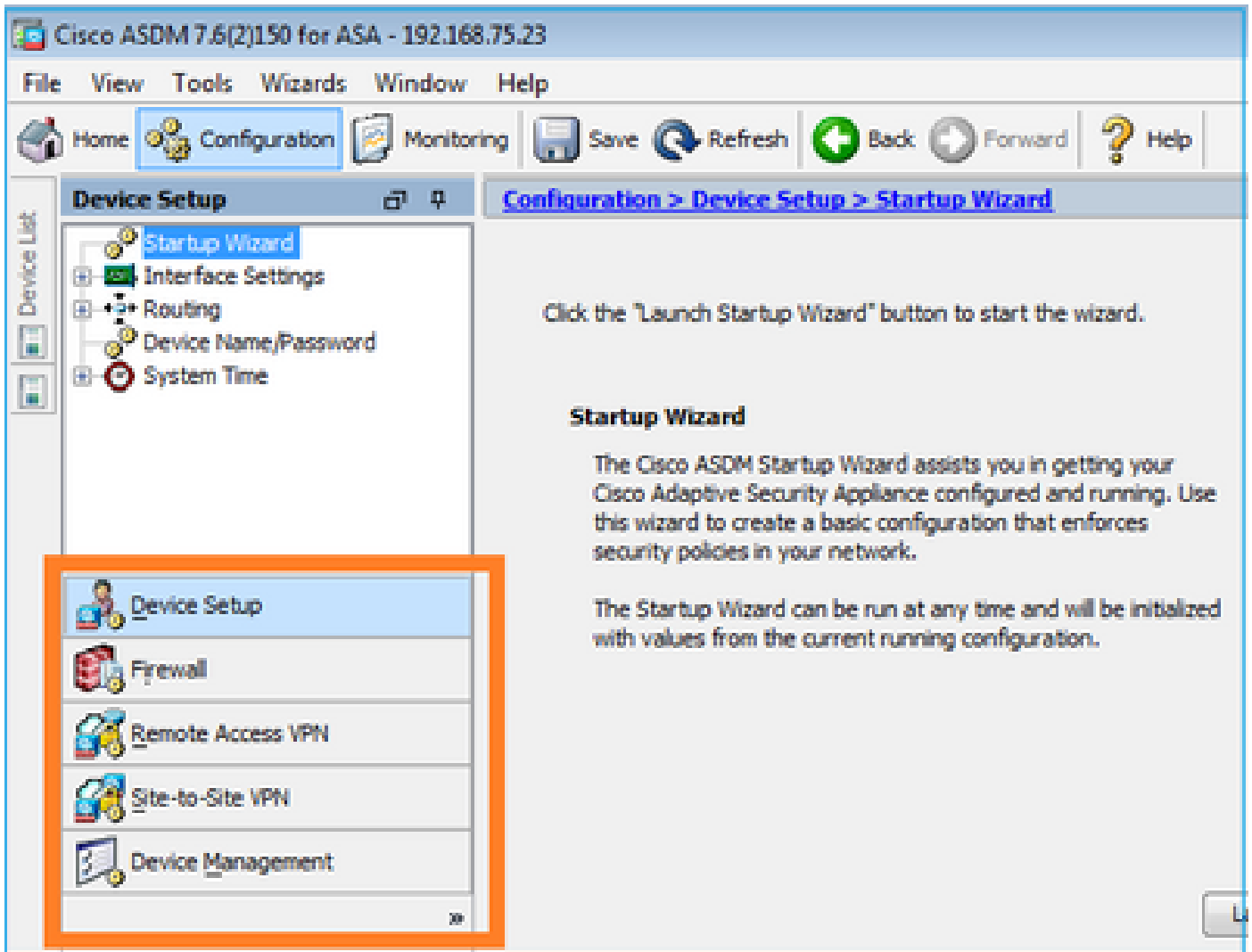


Troubleshoot

En caso de que ASDM no pueda establecer un túnel SSL con la dirección IP de administración de FirePOWER, solo cargará este elemento de menú de FirePOWER:



También falta el elemento de configuración de ASA FirePOWER:



Verificación 1

Asegúrese de que la interfaz de administración de ASA esté ACTIVA y que el puerto de switch conectado a ella esté en la VLAN adecuada:

<#root>

ASA5525#

```
show interface ip brief | include Interface|Management0/0
```

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

Solución de problemas recomendada

- Establezca la VLAN adecuada.
- Ponga el puerto en posición de ELEVACIÓN (compruebe el cable y la configuración del puerto del switch (velocidad/dúplex/apagado)).

Verificación 2

Asegúrese de que el módulo FirePOWER está completamente inicializado, en funcionamiento y:

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

```
>
```

Solución de problemas recomendada

- Verifique el resultado del comando show module sfr log console para ver si hay errores o fallas.

Verificación 3

Verifique la conectividad básica entre el host ASDM y la IP de administración del módulo FirePOWER con comandos como ping y 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.
```

Solución de problemas recomendada

- Verifique el ruteo a lo largo del trayecto.
- Verifique que no haya dispositivos en el trayecto que bloqueen el tráfico.

Verificación 4

Si el host ASDM y la dirección IP de administración de FirePOWER se encuentran en la misma red de capa 3, compruebe la tabla del protocolo de resolución de direcciones (ARP) en el host 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
```

Solución de problemas recomendada

- Si no hay entradas ARP, utilice Wireshark para verificar la comunicación ARP. Asegúrese de que las direcciones MAC de los paquetes sean correctas.
- Si hay entradas ARP, asegúrese de que sean correctas.

Verificación 5

Habilite la captura en el dispositivo ASDM mientras se conecta a través de ASDM para ver si hay una comunicación TCP adecuada entre el host y el módulo FirePOWER. Como mínimo, verá lo siguiente:

- Protocolo de enlace TCP de 3 vías entre el host ASDM y ASA.
- Túnel SSL establecido entre el host ASDM y ASA.
- Protocolo de enlace TCP de 3 vías entre el host ASDM y la dirección IP de administración del módulo FirePOWER.
- Túnel SSL establecido entre el host ASDM y la dirección IP de administración del módulo FirePOWER.

Solución de problemas recomendada

- Si el protocolo de enlace de 3 vías TCP falla, asegúrese de que no haya tráfico asimétrico ni dispositivos en la trayectoria que bloqueen los paquetes TCP.
- Si SSL falla, verifique si no hay ningún dispositivo en la trayectoria que realiza el comando man-in-the-middle (MITM) (el emisor del certificado del servidor da una pista para esto).

Verificación 6

Para verificar el tráfico hacia y desde el módulo FirePOWER, habilite la captura en la interfaz asa_mgmt_plane. En la captura, puede ver lo siguiente:

- Solicitud ARP del host ASDM (paquete 42).
- Respuesta ARP del módulo FirePOWER (paquete 43).
- Protocolo de enlace TCP de 3 vías entre el host ASDM y el módulo FirePOWER (paquetes 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
```

Solución de problemas recomendada

- Igual que en la verificación 5.

Verificación 7

Verifique que el usuario de ASDM tenga el nivel de privilegio 15. Una manera de confirmar esto es ingresar el comando **debug http 255** mientras se conecta a través de 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],
```

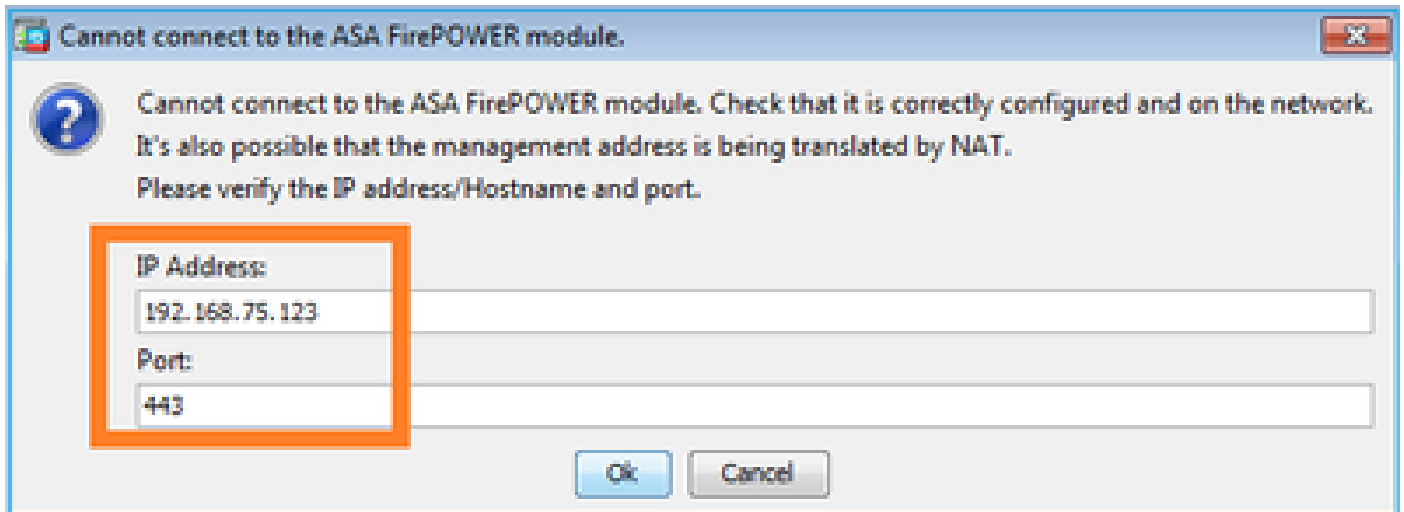
```
privilege = [14]
```

Solución de problemas recomendada

- Si el nivel de privilegio no es 15, intente con un usuario que tenga el nivel 15.

Verificación 8

Si entre el host ASDM y el módulo FirePOWER hay traducción de direcciones de red (NAT) para la dirección IP de administración de FirePOWER, debe especificar la dirección IP con NAT:



Solución de problemas recomendada

- Las capturas en los terminales (ASA/SFR y host final) lo confirman.

Verificación 9

Asegúrese de que el módulo FirePOWER no esté gestionado ya por FMC, ya que en ese caso faltan las fichas de FirePOWER en ASDM:

```
<#root>
```

```
ASA5525#
```

```
session sfr console
```

```
Opening console session with module sfr.  
Connected to module sfr. Escape character sequence is 'CTRL-AX'.  
>
```

```
show managers
```

```
Managed locally.
```

```
>
```

Otro método es con el comando **show module sfr details**:

```
<#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

Solución de problemas recomendada

- Si el dispositivo ya está administrado, debe anular su registro antes de administrarlo desde ASDM. Consulte la [Guía de configuración de Firepower Management Center](#).

Verificación 10

Verifique la captura de Wireshark para asegurarse de que el cliente ASDM se conecte con una versión de TLS adecuada (por ejemplo, TLSv1.2).

Solución de problemas recomendada

- Ajuste la configuración SSL del explorador.
- Pruebe con otro navegador.
- Pruebe desde otro host final.

Verificación 11

Verifique en la guía de [Compatibilidad de Cisco ASA](#) que las imágenes de ASA/ASDM sean compatibles.

Solución de problemas recomendada

- Utilice una imagen ASDM compatible.

Verificación 12

Verifique en la guía de compatibilidad de [Cisco ASA](#) que el dispositivo FirePOWER sea compatible con la versión de ASDM.

Solución de problemas recomendada

- Utilice una imagen ASDM compatible.

Información Relacionada

- [Guía de inicio rápido del módulo Cisco ASA FirePOWER](#)
- [Guía de configuración de la administración local de ASA con FirePOWER Services, versión 6.1.0](#)
- [Guía del usuario del módulo ASA FirePOWER para ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X y ASA5516-X, versión 5.4.1](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).