Uso di ASDM per gestire un modulo FirePOWER su un'ASA

Sommario

Introduzione

In questo documento viene descritta la modalità di comunicazione del software ASDM con l'appliance ASA (Adaptive Security Appliance) e con il modulo software FirePOWER installato.

Premesse

Un modulo FirePOWER installato su un'ASA può essere gestito da:

- Firepower Management Center (FMC): è la soluzione di gestione off-box.
- Adaptive Security Device Manager (ASDM) - Soluzione di gestione integrata.

Prerequisiti

Requisiti

Una configurazione ASA per abilitare la gestione 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
```

Verificare la compatibilità tra il modulo ASA/SFR, altrimenti le schede FirePOWER non vengono visualizzate.

Inoltre, sull'appliance ASA la licenza 3DES/AES deve essere abilitata:

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

Assicurarsi che il sistema client ASDM esegua una versione supportata di Java JRE.

Componenti usati

- Un host Microsoft Windows 7
- ASA 5525-X con ASA versione 9.6(2.3)
- ASDM versione 7.6.2.150
- Modulo software FirePOWER 6.1.0-330

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Architettura

L'ASA ha tre interfacce interne:

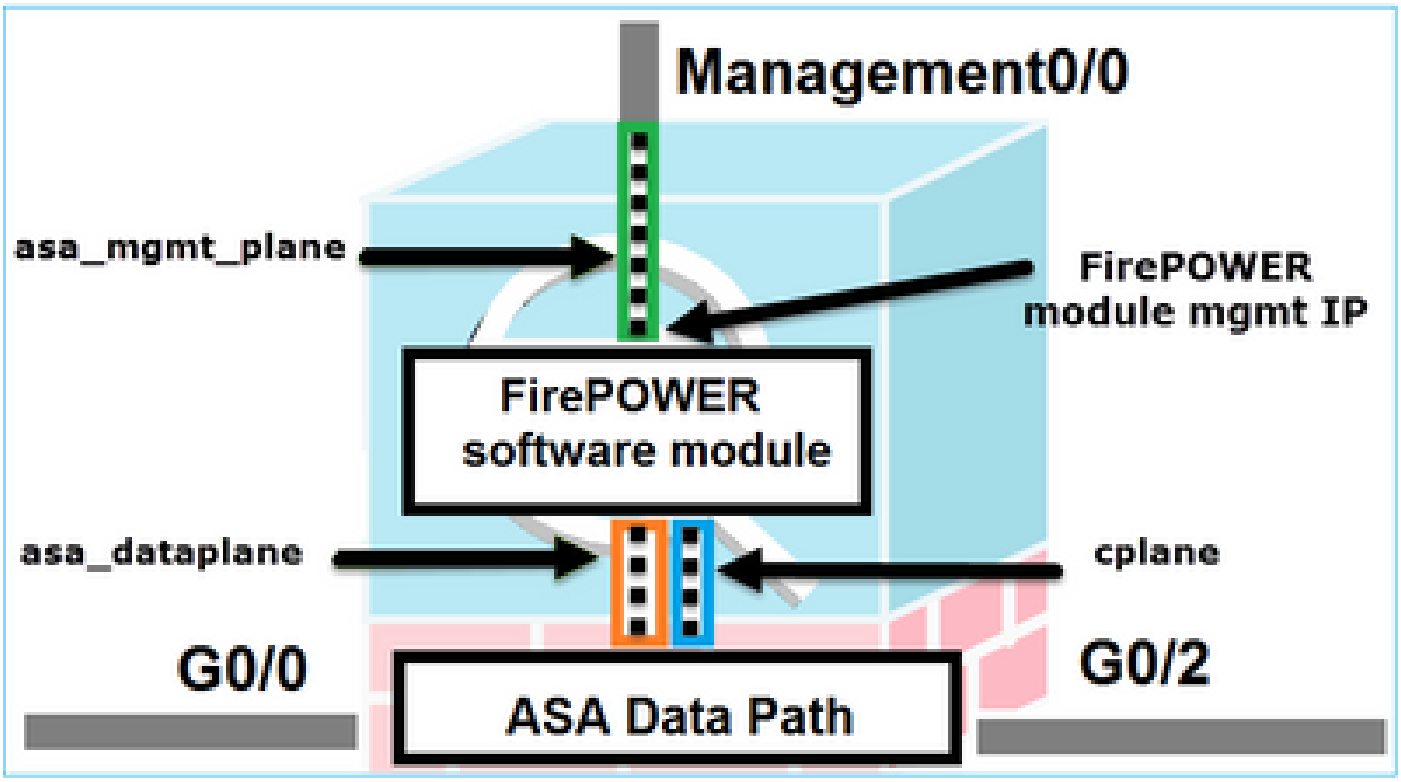
- asa_dataplane - Viene usato per reindirizzare i pacchetti dal percorso dati dell'ASA al modulo software FirePOWER.
- asa_mgmt_plane - Viene utilizzato per consentire all'interfaccia di gestione FirePOWER di comunicare con la rete.
- cplane - Interfaccia del Control Plane utilizzata per trasferire pacchetti keepalive tra l'ASA e il modulo FirePOWER.

È possibile acquisire il traffico in tutte le interfacce interne:

<#root>

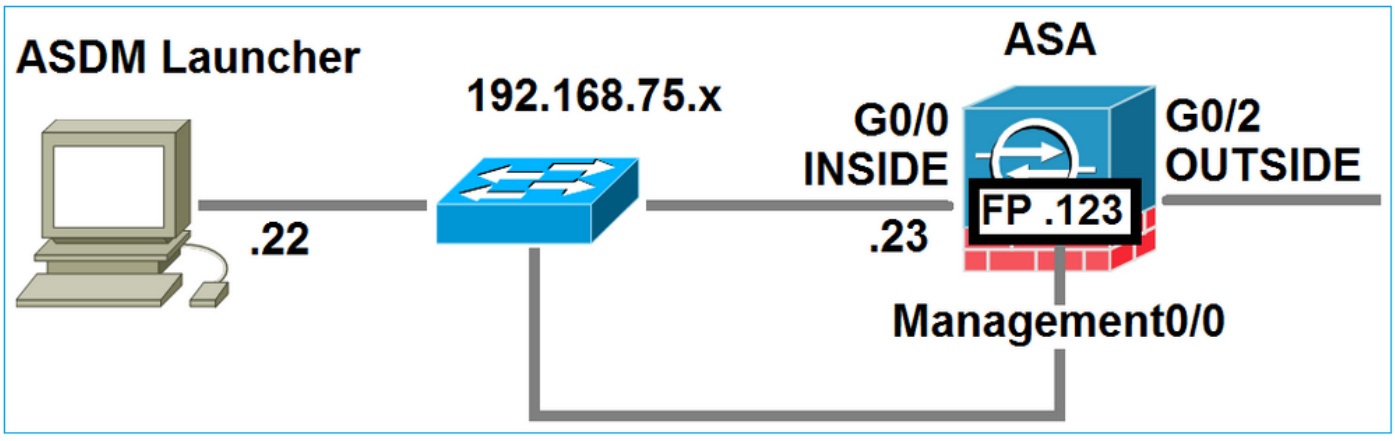
```
ASA5525#

capture CAP interface ?


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

È possibile visualizzare quanto segue:



Operazione in background quando un utente si connette a un'ASA tramite ASDM

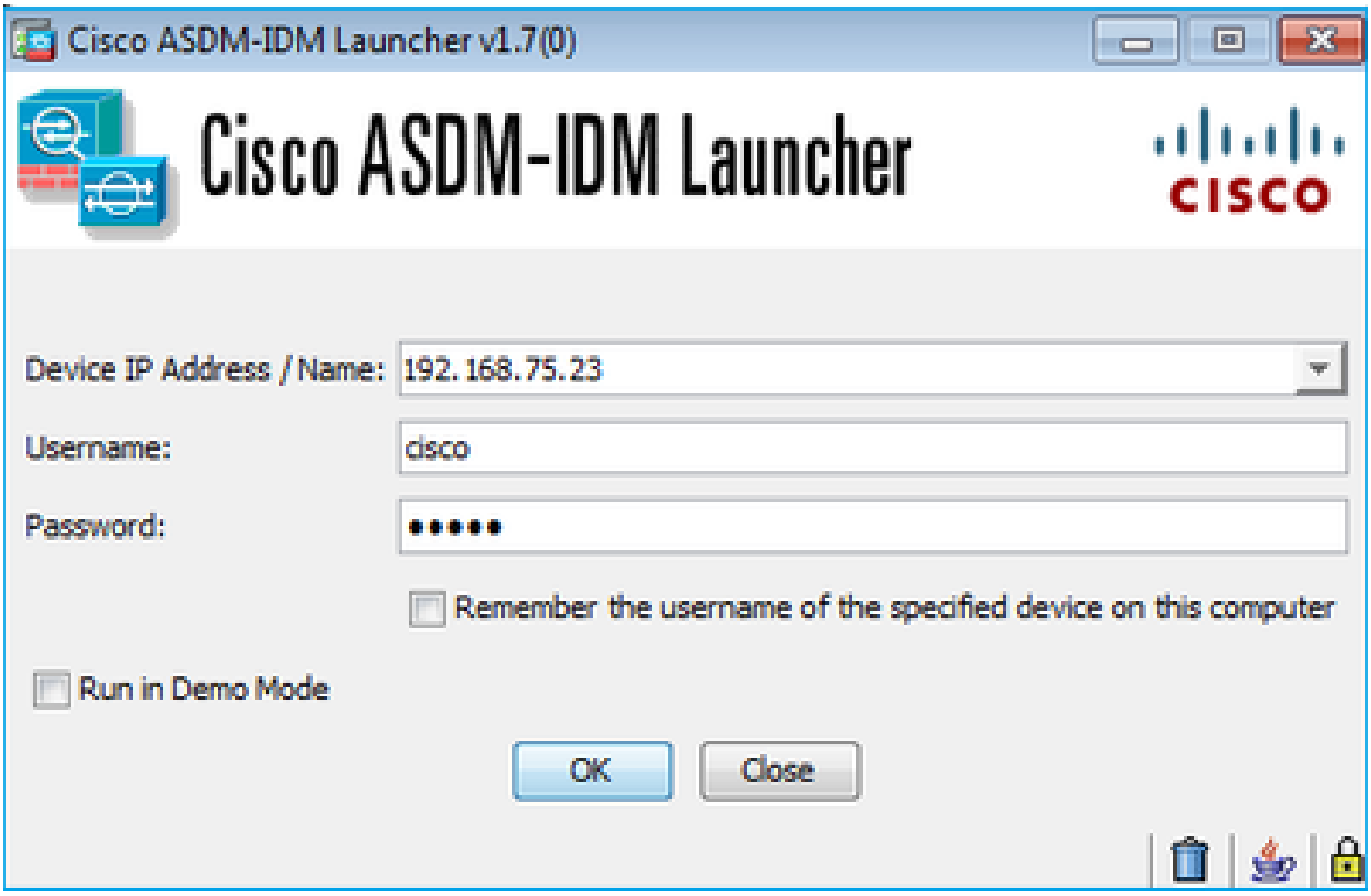
Supponiamo di avere questa topologia:



Quando un utente avvia una connessione ASDM all'appliance ASA, si verificano i seguenti eventi:

Fase 1 - L'utente avvia la connessione ASDM

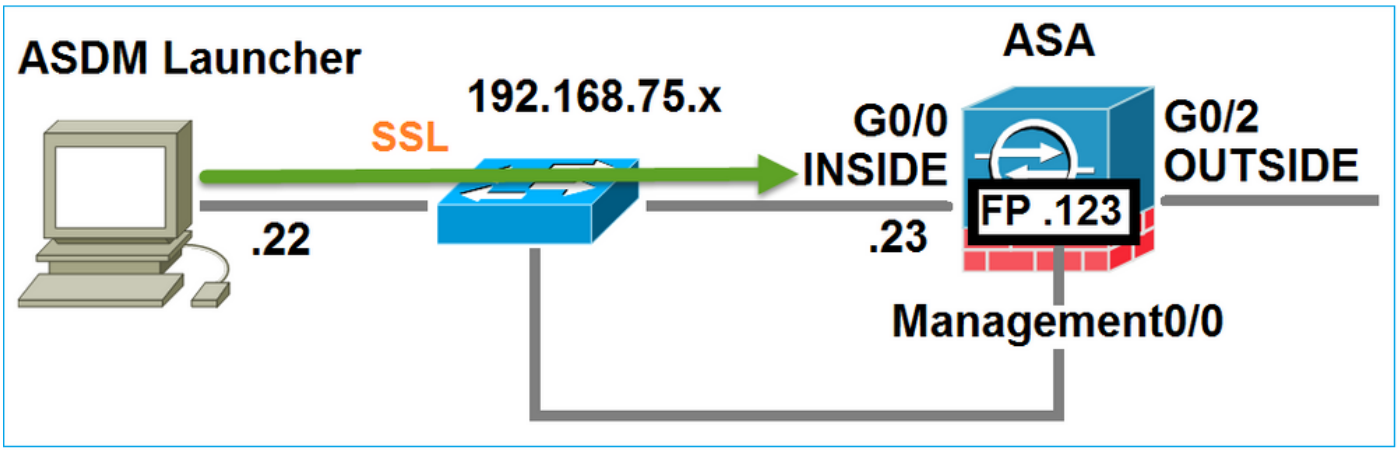
L'utente specifica l'indirizzo IP ASA utilizzato per la gestione HTTP, immette le credenziali e avvia una connessione all'appliance ASA:



In background, viene stabilito un tunnel SSL tra l'ASDM e l'ASA:

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

È possibile visualizzare quanto segue:



Fase 2 - L'ASDM rileva la configurazione ASA e l'indirizzo IP del modulo FirePOWER

Immettere il comando debug http 255 sull'appliance ASA per visualizzare tutti i controlli eseguiti in

background quando l'appliance ASDM si connette all'appliance 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 authenticatio
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
```

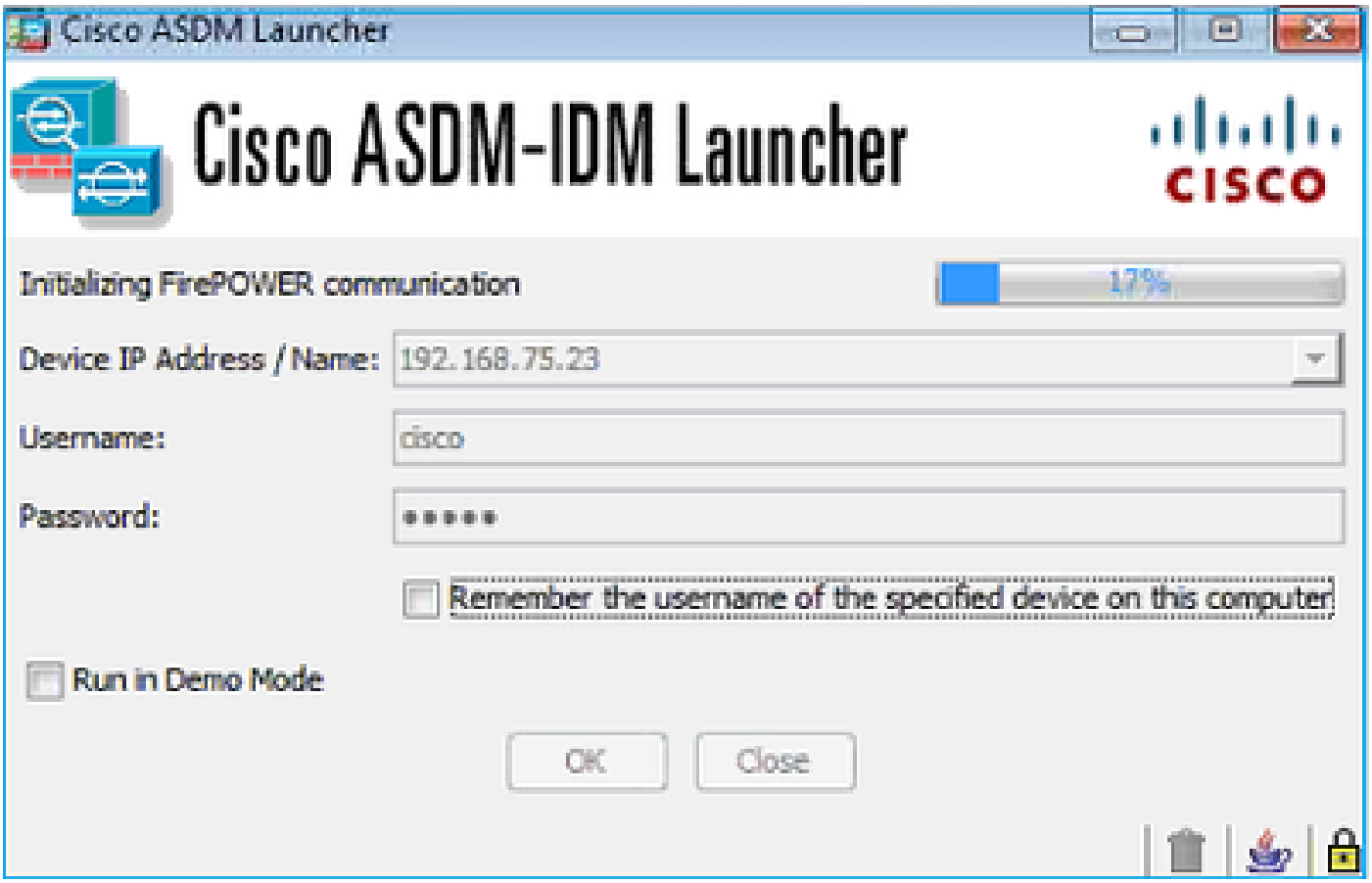
- show module: l'ASDM rileva i moduli ASA.
- show module sfr details: l'ASDM rileva i dettagli del modulo, tra cui l'indirizzo IP di gestione FirePOWER.

Sullo sfondo, vengono visualizzate come una serie di connessioni SSL dal PC all'indirizzo IP dell'appliance 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

Fase 3 - L'ASDM avvia la comunicazione verso il modulo FirePOWER

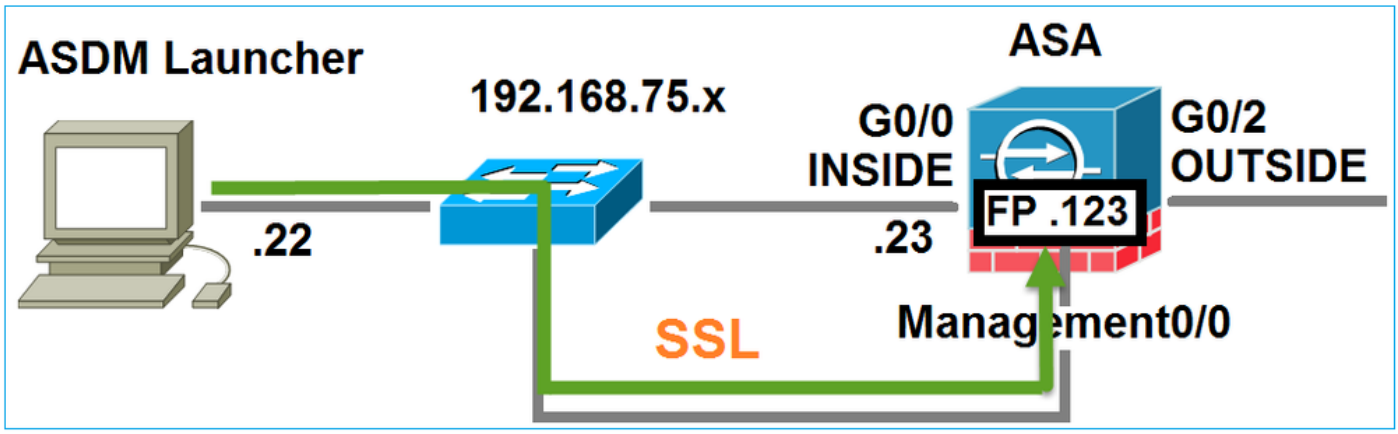
Poiché ASDM conosce l'indirizzo IP di gestione FirePOWER, avvia le sessioni SSL verso il modulo:



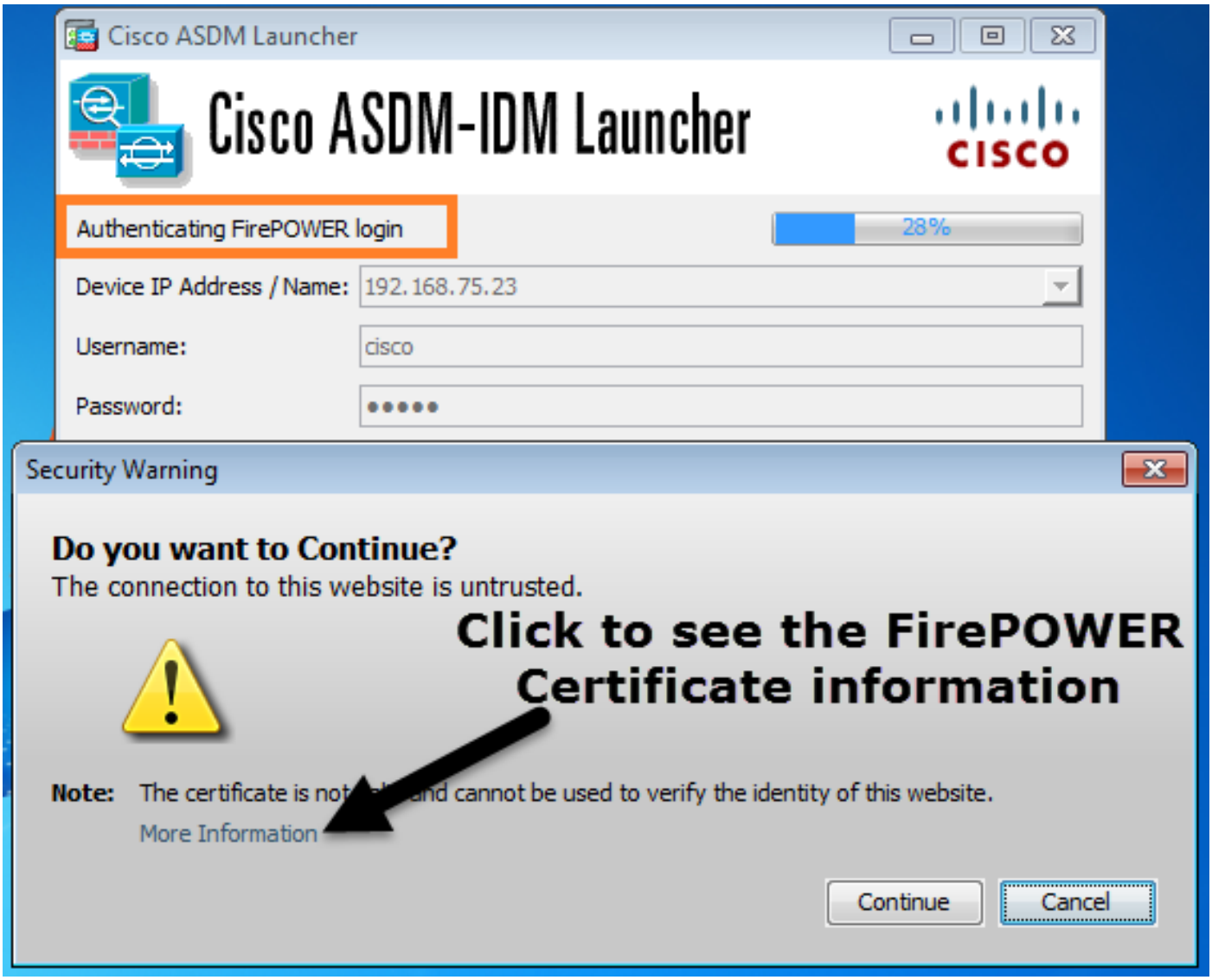
Questa condizione viene vista in background come connessioni SSL dall'host ASDM all'indirizzo IP di gestione FirePOWER:

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

È possibile visualizzare quanto segue:

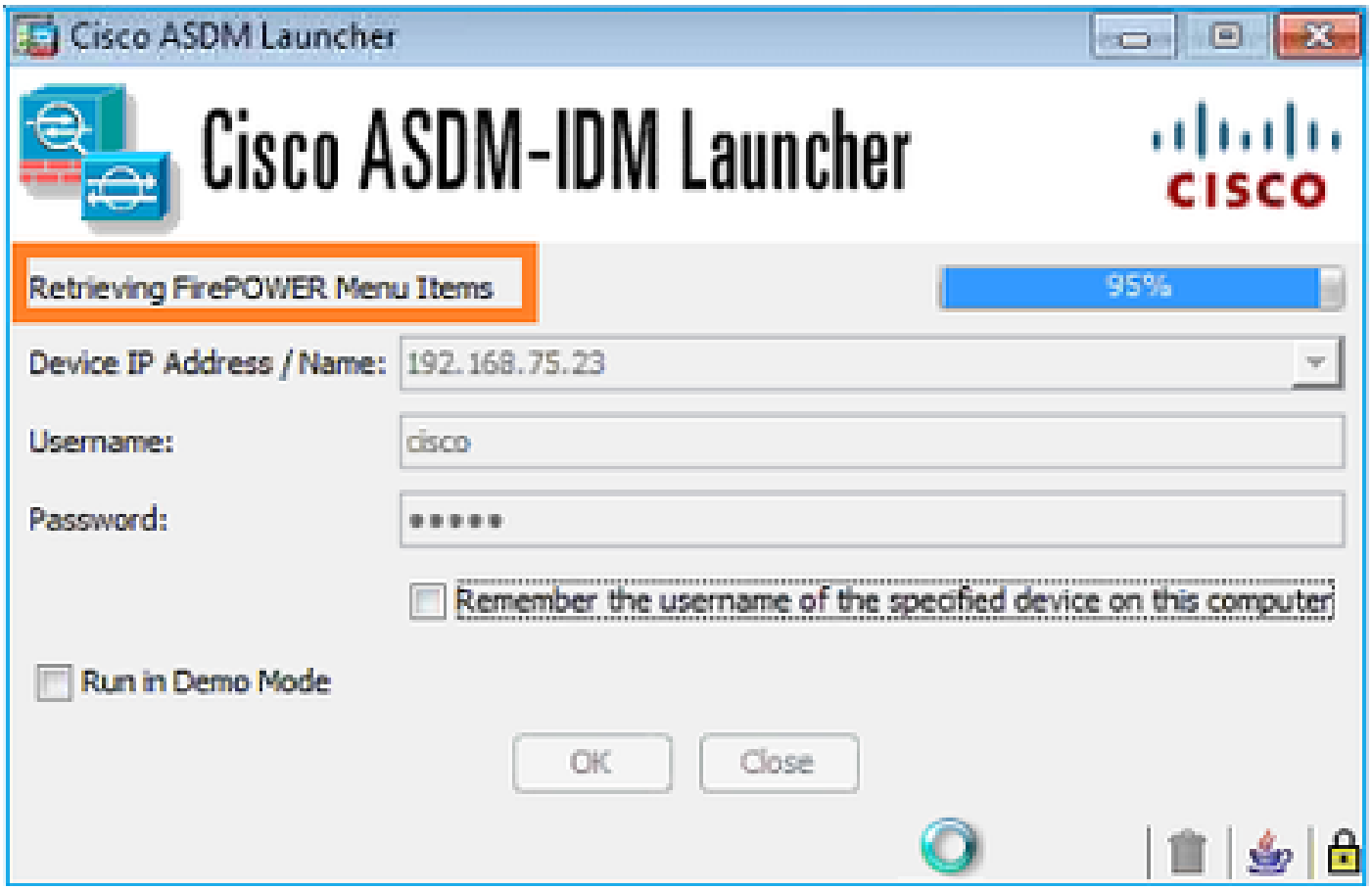


L'ASDM autentica FirePOWER e viene visualizzato un avviso di sicurezza poiché il certificato FirePOWER è autofirmato:

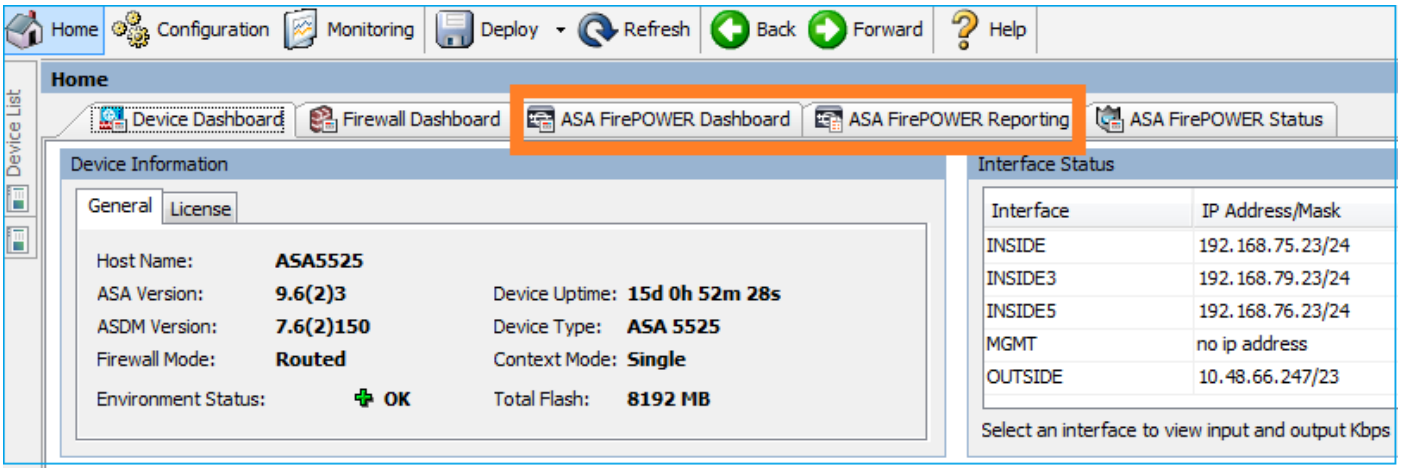


Fase 4 - L'ASDM recupera le voci del menu FirePOWER

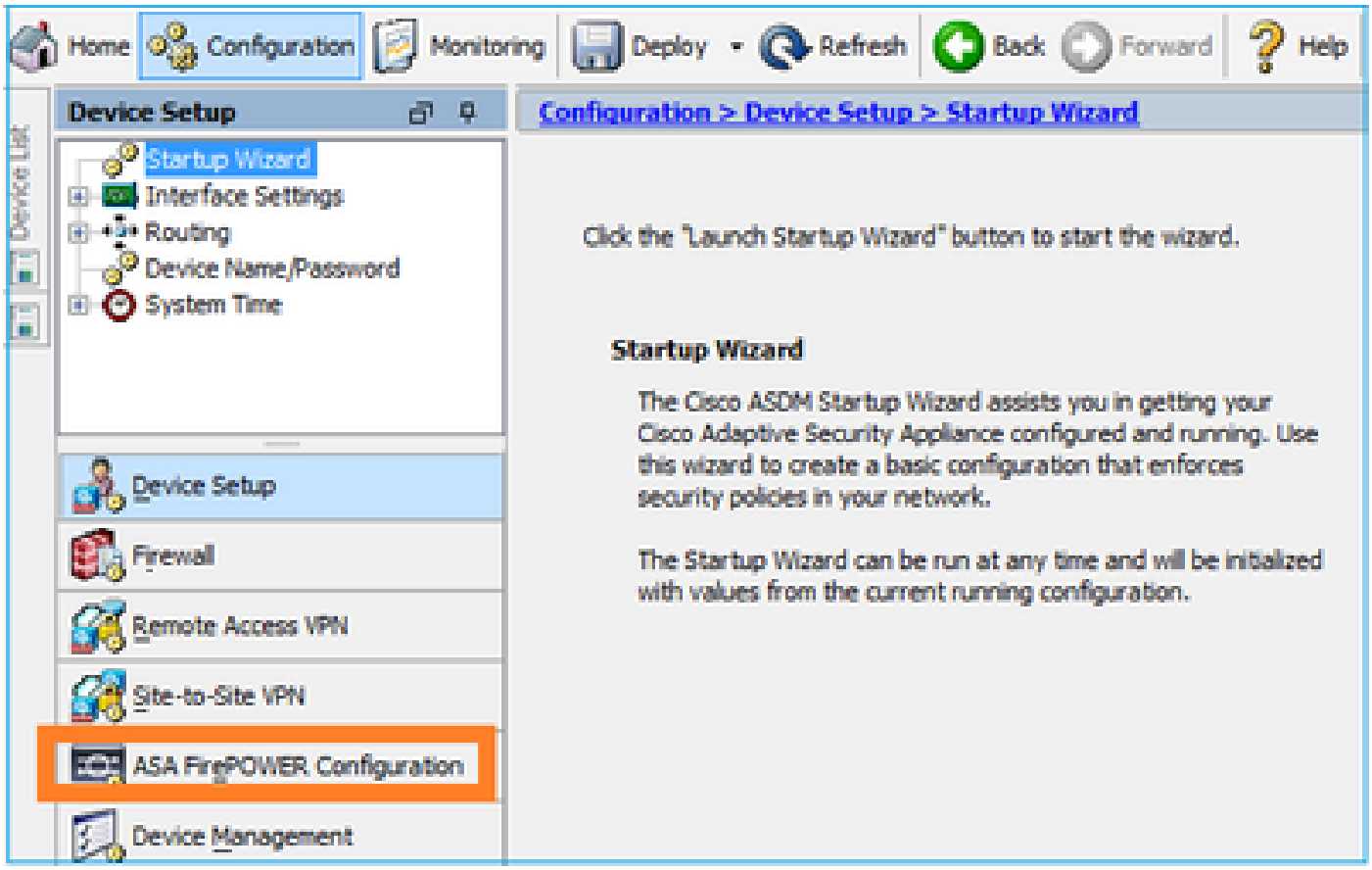
Una volta completata l'autenticazione, ASDM recupera le voci di menu dal dispositivo FirePOWER:



Le schede recuperate sono mostrate in questo esempio:

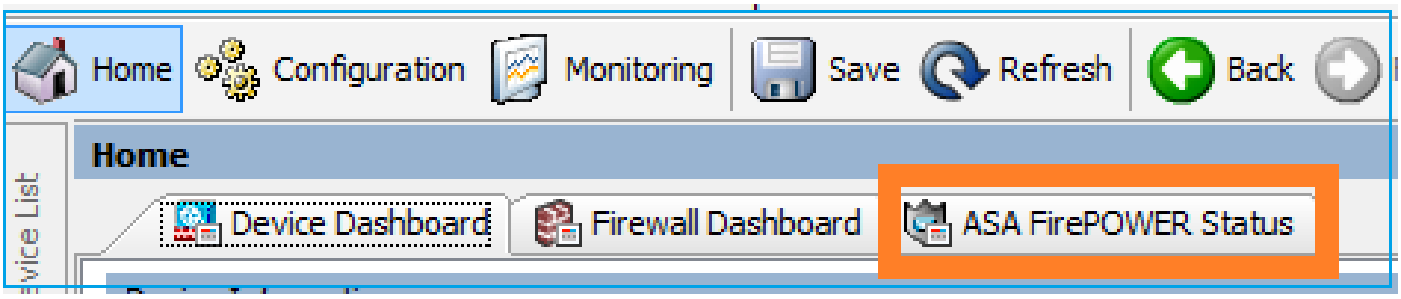


Recupera anche la voce di menu ASA FirePOWER Configuration:

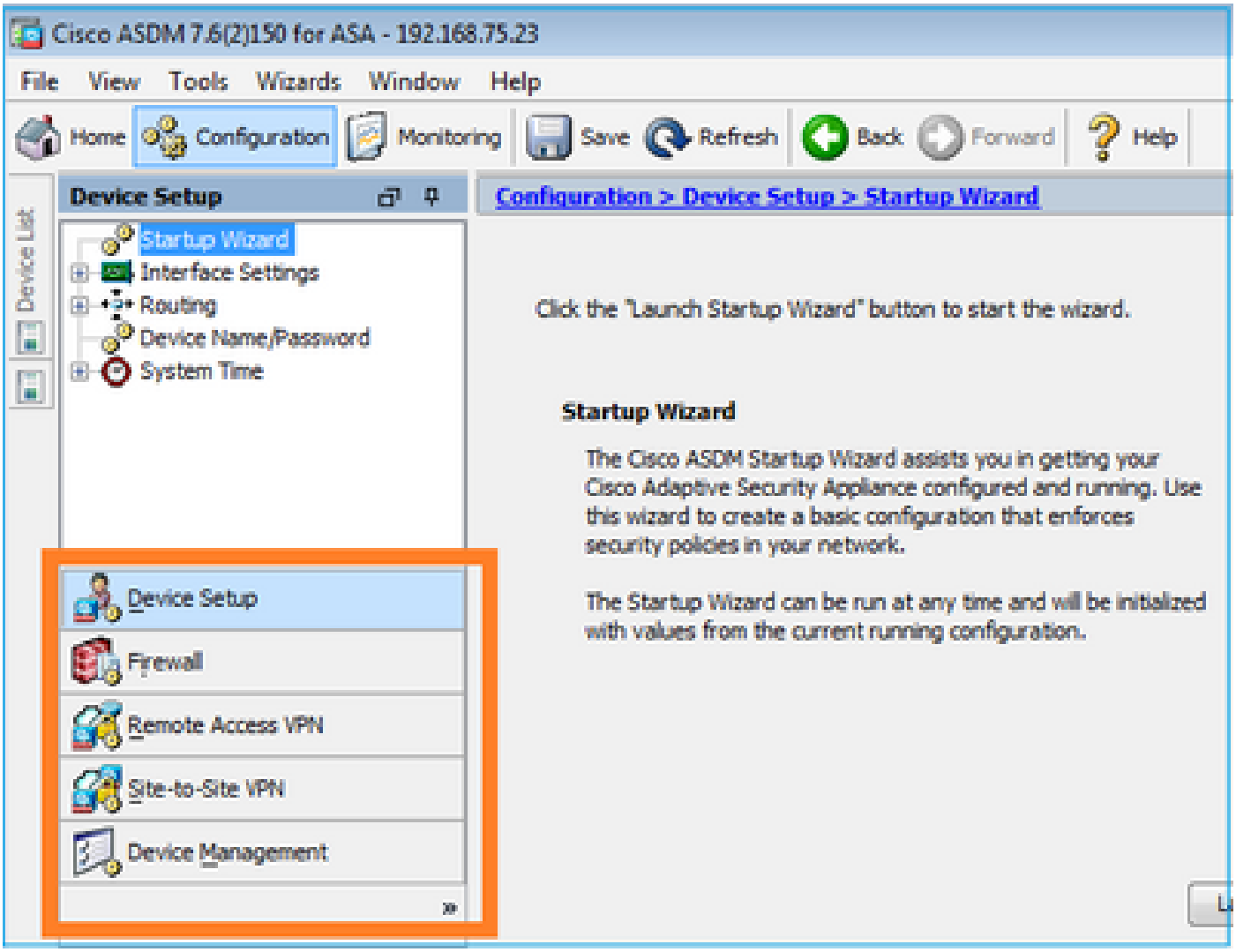


Risoluzione dei problemi

Nel caso in cui ASDM non sia in grado di stabilire un tunnel SSL con l'indirizzo IP di FirePOWER Management, viene caricata solo la seguente voce di menu FirePOWER:



Manca anche l'elemento di configurazione ASA FirePOWER:



Verifica 1

Verificare che l'interfaccia di gestione ASA sia attiva e che la porta dello switch connessa si trovi nella VLAN corretta:

<#root>

```
ASA5525#

show interface  ip brief | include Interface|Management0/0

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

up                    up
```

Procedura di risoluzione consigliata

- Impostare la VLAN corretta.
- Portare la porta su (controllare il cavo, controllare la configurazione della porta dello switch (velocità/duplex/chiusura)).

Verifica 2

Verificare che il modulo FirePOWER sia completamente inizializzato, attivo e in esecuzione:

<#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
----------------------------------------------------

>
```

Procedura di risoluzione consigliata

- Controllare l'output del comando show module sfr log console per verificare la presenza di errori o errori.

Verifica 3

Verificare la connettività di base tra l'host ASDM e l'IP di gestione del modulo FirePOWER con comandi quali ping e traceroute/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.
```

Procedura di risoluzione consigliata

- Controllare la stesura lungo il percorso.
- Verificare che il percorso non contenga dispositivi che bloccano il traffico.

Verifica 4

Se l'host ASDM e l'indirizzo IP di gestione FirePOWER si trovano nella stessa rete di layer 3, controllare la tabella Address Resolution Protocol (ARP) sull'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
```

Procedura di risoluzione consigliata

- Se non sono presenti voci ARP, utilizzare Wireshark per controllare la comunicazione ARP. Verificare che gli indirizzi MAC dei pacchetti siano corretti.
- Se sono presenti voci ARP, verificare che siano corrette.

Verifica 5

Abilitare la cattura sul dispositivo ASDM durante la connessione tramite ASDM per verificare che la comunicazione TCP tra l'host e il modulo FirePOWER sia corretta. Verrà visualizzato quanto meno quanto segue:

- Handshake TCP a 3 vie tra l'host ASDM e l'ASA.
- Tunnel SSL stabilito tra l'host ASDM e l'appliance ASA.
- Handshake TCP a 3 vie tra l'host ASDM e l'indirizzo IP di gestione del modulo FirePOWER.
- Tunnel SSL stabilito tra l'host ASDM e l'indirizzo IP di gestione del modulo FirePOWER.

Procedura di risoluzione consigliata

- Se l'handshake a 3 vie TCP ha esito negativo, verificare che il percorso non includa traffico asimmetrico o dispositivi che bloccano i pacchetti TCP.
- Se SSL non riesce, verificare se nel percorso non è presente alcun dispositivo che esegua il comando man-in-the-middle (MITM). A tale scopo, l'autorità di certificazione del server fornisce un suggerimento.

Verifica 6

Per controllare il traffico da e verso il modulo FirePOWER, abilitare l'acquisizione sull'interfaccia asa_mgmt_plane. Nell'acquisizione è possibile visualizzare:

- Richiesta ARP dall'host ASDM (pacchetto 42).
- Risposta ARP dal modulo FirePOWER (pacchetto 43).
- Handshake TCP a 3 vie tra l'host ASDM e il modulo FirePOWER (pacchetti 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

45: 20:27:28.532549 192.168.75.123.443 > 192.168.75.22.48391:
S 1324352332:1324352332(0)
ack 2861923943 win 14600

46: 20:27:28.532839 192.168.75.22.48391 > 192.168.75.123.443: .
ack 1324352333 win 16695

Procedura di risoluzione consigliata

- Come nella verifica 5.

Verifica 7

Verificare che l'utente ASDM disponga del livello di privilegio 15. Per verificare questa condizione, immettere il comando debug http 255 durante la connessione tramite ASDM:

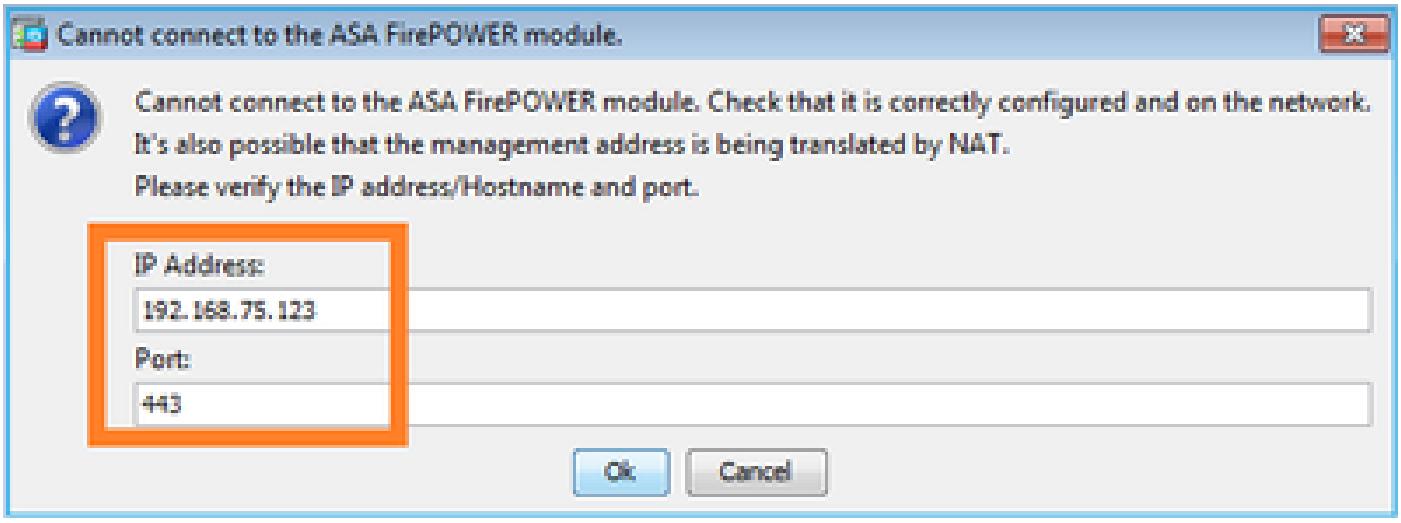
```
<#root>

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]
```

Procedura di risoluzione consigliata

- Se il livello di privilegio non è 15, provare con un utente con il livello 15.

Verifica 8

Se tra l'host ASDM e il modulo FirePOWER è presente un NAT (Network Address Translation) per l'indirizzo IP di FirePOWER Management, è necessario specificare l'indirizzo IP NAT:



Procedura di risoluzione consigliata

- Le acquisizioni agli endpoint (ASA/SFR e host finale) confermano questa condizione.

Verifica 9

Verificare che il modulo FirePOWER non sia già gestito da FMC, in quanto in tal caso le schede FirePOWER in ASDM risultano mancanti:

<#root>

```
ASA5525#

session sfr console

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

show managers

Managed locally.


>
```

Un altro metodo consiste nell'utilizzare il 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
```

Procedura di risoluzione consigliata

- Se il dispositivo è già gestito, è necessario annullare la registrazione prima di gestirlo da ASDM. Vedere la Guida alla configurazione di Firepower Management Center.

Verifica 10

Controllare l'acquisizione di wireshark per verificare che il client ASDM si connetta con una versione TLS corretta (ad esempio, TLSv1.2).

Procedura di risoluzione consigliata

- Ottimizzare le impostazioni SSL del browser.
- Prova con un altro browser.
- Provare da un altro host finale.

Verifica 11

Verificare nella guida alla compatibilità Cisco ASA che le immagini ASA/ASDM siano compatibili.

Procedura di risoluzione consigliata

- Usare un'immagine ASDM compatibile.

Verifica 12

Verificare nella guida alla compatibilità Cisco ASA che il dispositivo FirePOWER sia compatibile con la versione ASDM.

Procedura di risoluzione consigliata

- Usare un'immagine ASDM compatibile.

Informazioni correlate

- Guida introduttiva al modulo Cisco ASA FirePOWER
- ASA con guida alla configurazione della gestione locale dei servizi FirePOWER, versione 6.1.0
- ASA FirePOWER Module - Guida dell'utente per ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X e ASA5516-X, versione 5.4.1
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).