

# Utilisant l'ASDM pour gérer un module de FirePOWER sur l'ASA

## Contenu

[Introduction](#)

[Composants utilisés](#)

[Conditions préalables](#)

[Architecture](#)

[Traitement de fond quand un utilisateur se connecte à l'ASA par l'intermédiaire de l'ASDM](#)

[Étape 1 – L'utilisateur initie la connexion ASDM](#)

[Étape 2 – L'ASDM découvre la configuration ASA et l'IP de module de FirePOWER](#)

[Étape 3 – L'ASDM initie la transmission vers le module de FirePOWER](#)

[Étape 4 – L'ASDM récupère les commandes de menu de FirePOWER](#)

[Dépannage](#)

[Actions recommandées](#)

[Documents connexes](#)

## Introduction

Un module de FirePOWER qui est installé sur l'ASA peut être géré par l'un ou l'autre :

- Centre de Gestion de FirePOWER (FMC) – C'est la solution de Gestion de hors fonction-case
- Adaptive Security Device Manager (ADSM) – C'est la solution de Gestion de sur-case

Le but de ce document est d'expliquer comment le logiciel ASDM communique avec l'ASA et un module logiciel de FirePOWER installés là-dessus.

## Composants utilisés

- Un hôte de Windows 7
- ASA5525-X exécutant le code ASA 9.6.2-3
- Logiciel 7.6.2.150 ASDM
- Module logiciel 6.1.0-330 de FirePOWER

## Conditions préalables

Configuration ASA pour activer la Gestion 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
```

Supplémentaire, sur l'ASA le permis 3DES/AES devrait être activé :

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

## Architecture

L'ASA a 3 interfaces internes :

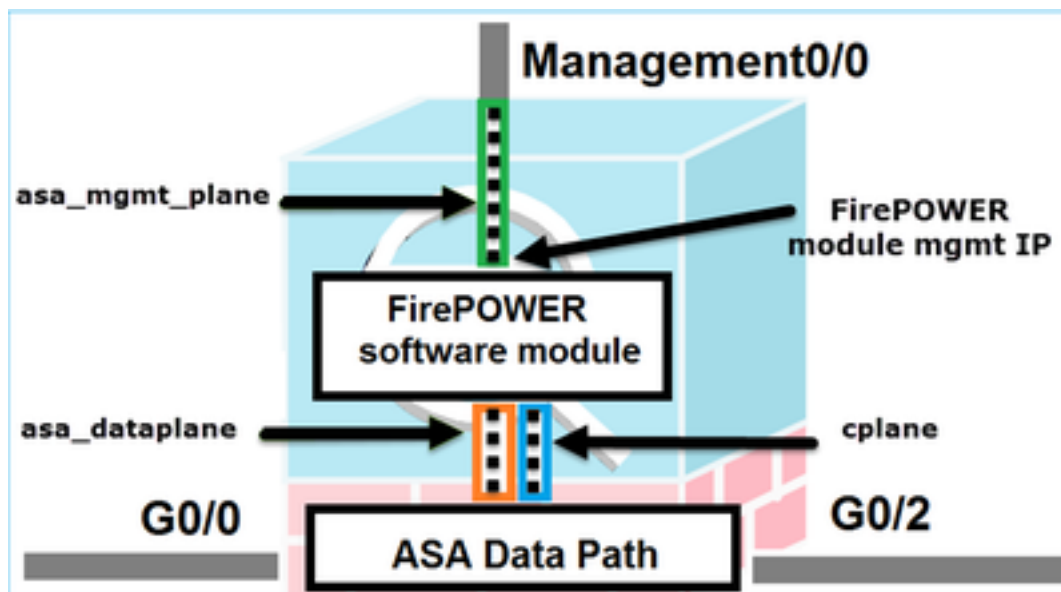
- **asa\_dataplane** = il est utilisé pour réorienter des paquets du chemin de données ASA au module logiciel de FirePOWER
- **asa\_mgmt\_plane** = il est utilisé pour permettre à l'interface de gestion de FirePOWER pour communiquer avec le réseau
- **cplane** = interface plate de contrôle qui est utilisée pour transférer le Keepalives entre l'ASA et le module de FirePOWER

Vous pouvez capturer le trafic dans toutes les interfaces internes :

```
ASA5525# capture CAP interface ?
```

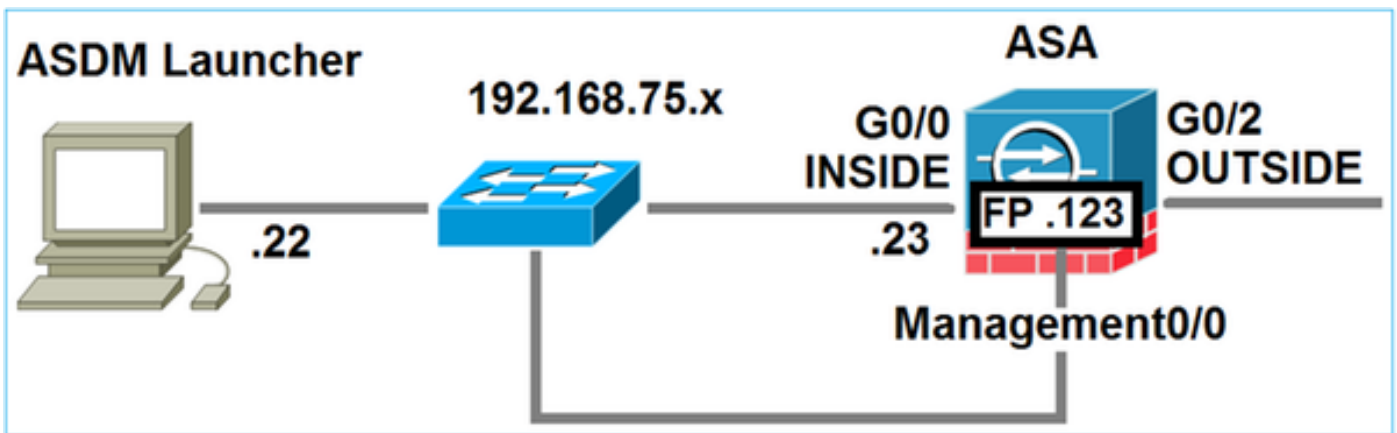
```
asa_dataplane  Capture packets on dataplane interface
asa_mgmt_plane Capture packets on managementplane interface
cplane         Capture packets on controlplane interface
```

Ce qui précède peut être visualisé comme suit :



# Traitement de fond quand un utilisateur se connecte à l'ASA par l'intermédiaire de l'ASDM

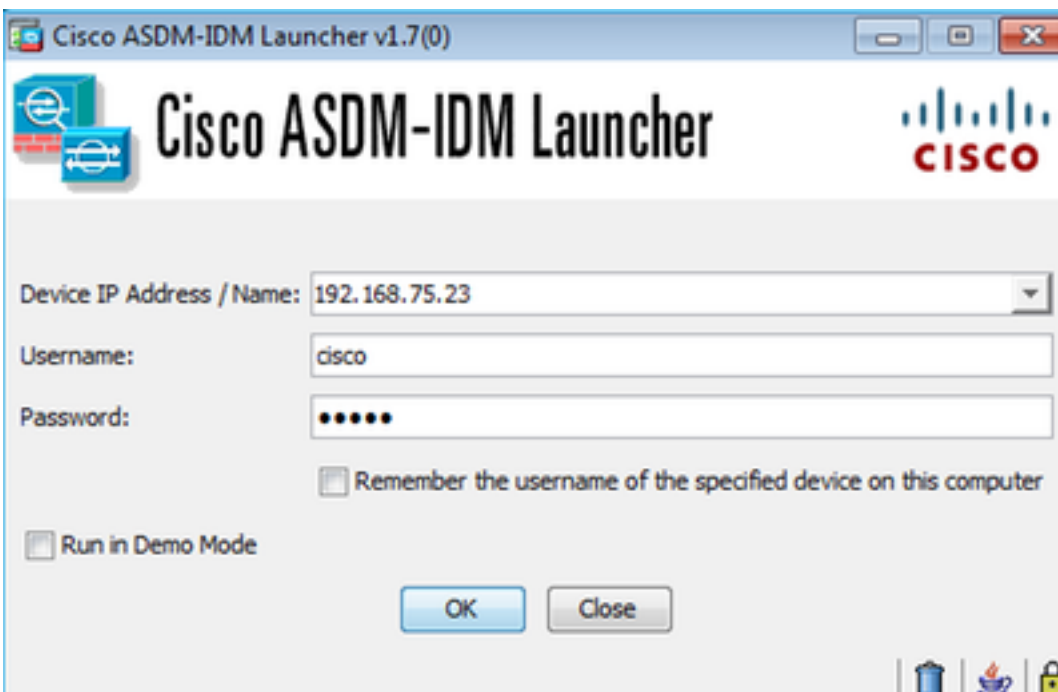
Considérez la topologie suivante



Quand un utilisateur initie une connexion ASDM à l'ASA les événements suivants se produiront :

## Étape 1 – L'utilisateur initie la connexion ASDM

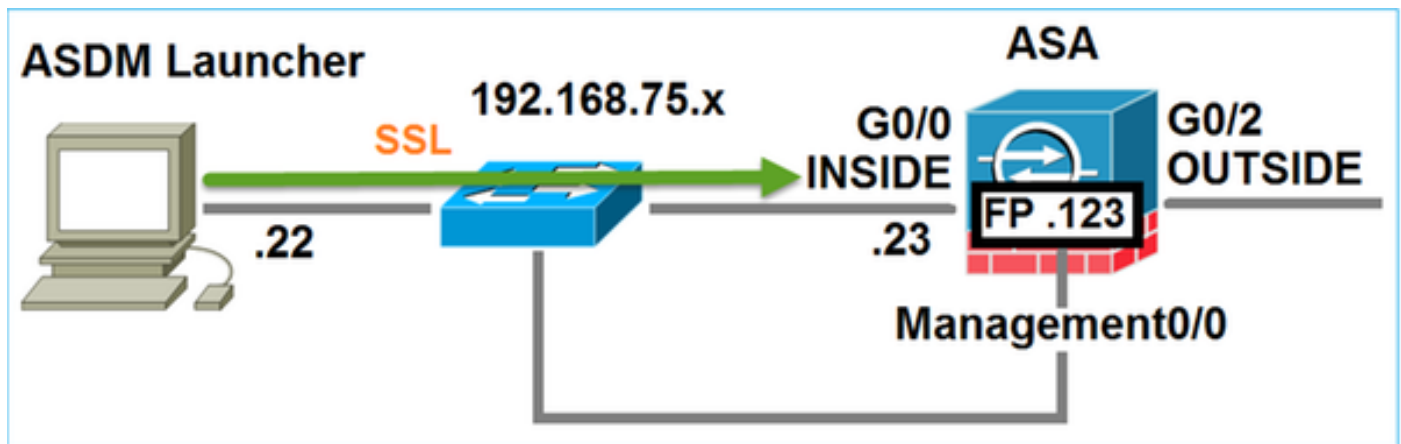
L'utilisateur spécifie l'IP ASA utilisé pour la Gestion de HTTP, entre dans les qualifications et initie une connexion vers l'ASA :



À l'arrière-plan un tunnel SSL entre l'ASDM et l'ASA est établi :

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

Ceci peut être visualisé comme suit :



## Étape 2 – L'ASDM découvre la configuration ASA et l'IP de module de FirePOWER

L'activation **mettent au point le HTTP 255** sur l'ASA affichera tous les contrôles qui sont faits à l'arrière-plan quand l'ASDM se connecte à l'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
```

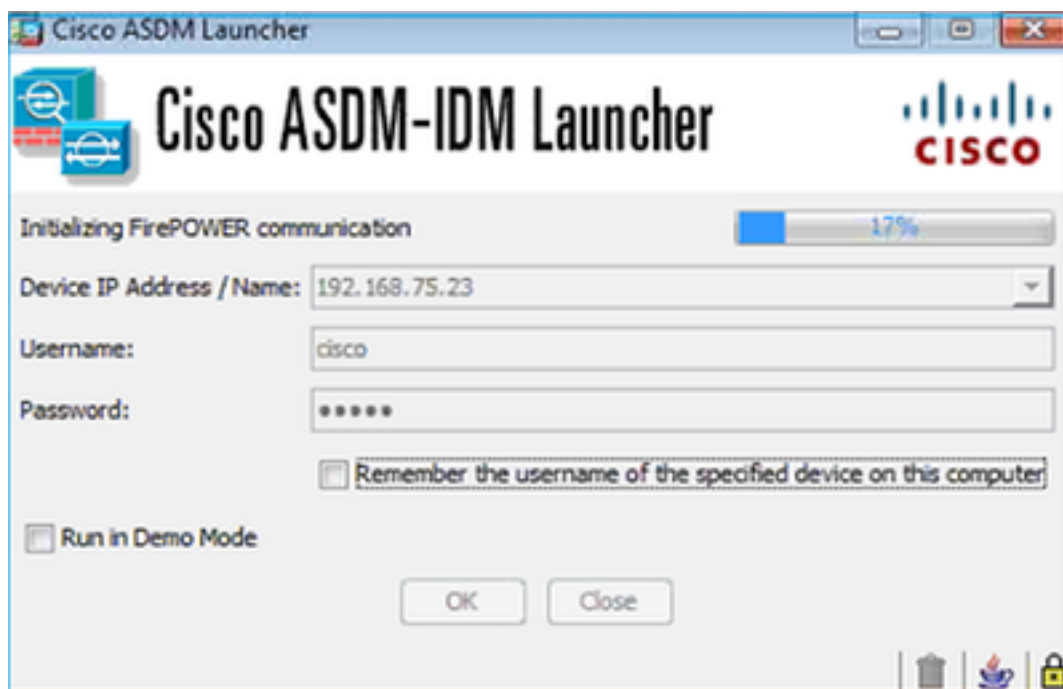
- le show module = L'ASDM découvre les modules ASA
- les détails de sfr de show module = L'ASDM découvre les détails de module comprenant l'IP de Gestion de FirePOWER

Ce qui précède sera vu à l'arrière-plan comme gamme de connexions SSL du PC vers l'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

### Étape 3 – L'ASDM initie la transmission vers le module de FirePOWER

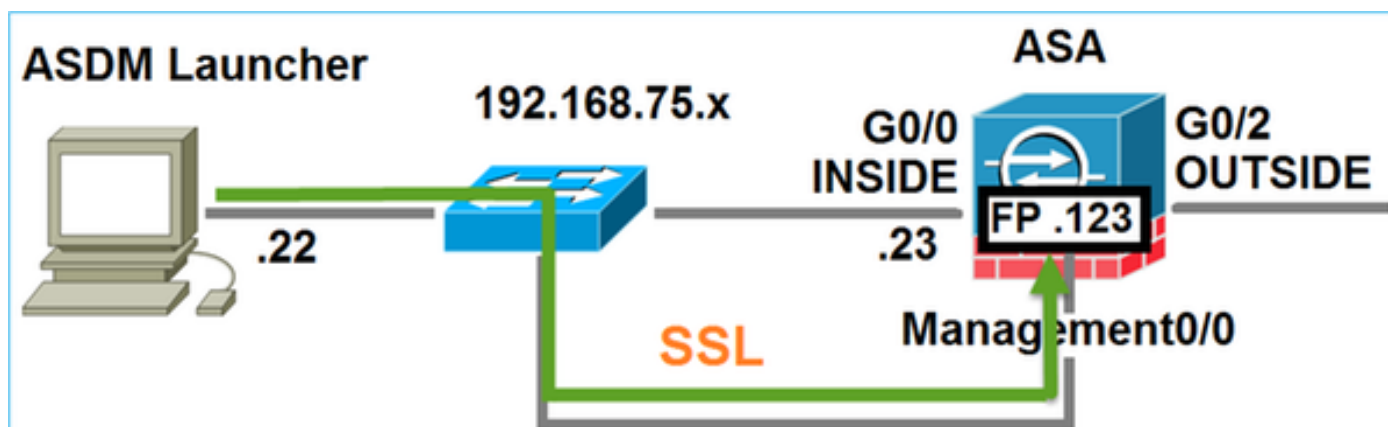
Puisque l'ASDM connaît l'IP de Gestion de FirePOWER il initie des sessions SSL vers le module :



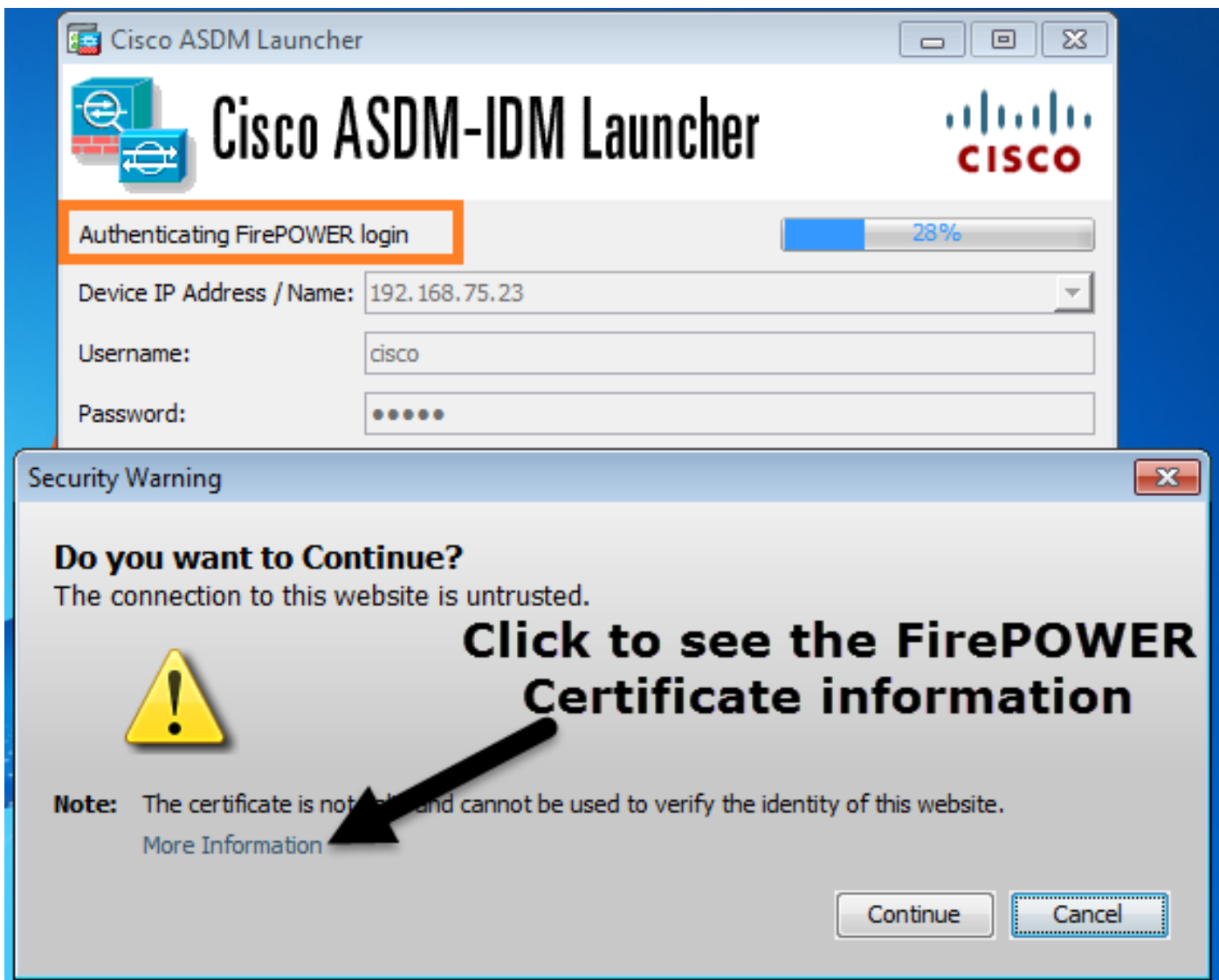
Ce qui précède sera vu à l'arrière-plan comme des connexions SSL de l'hôte ASDM vers l'IP de Gestion de FirePOWER :

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	

Ceci peut être visualisé comme suit :

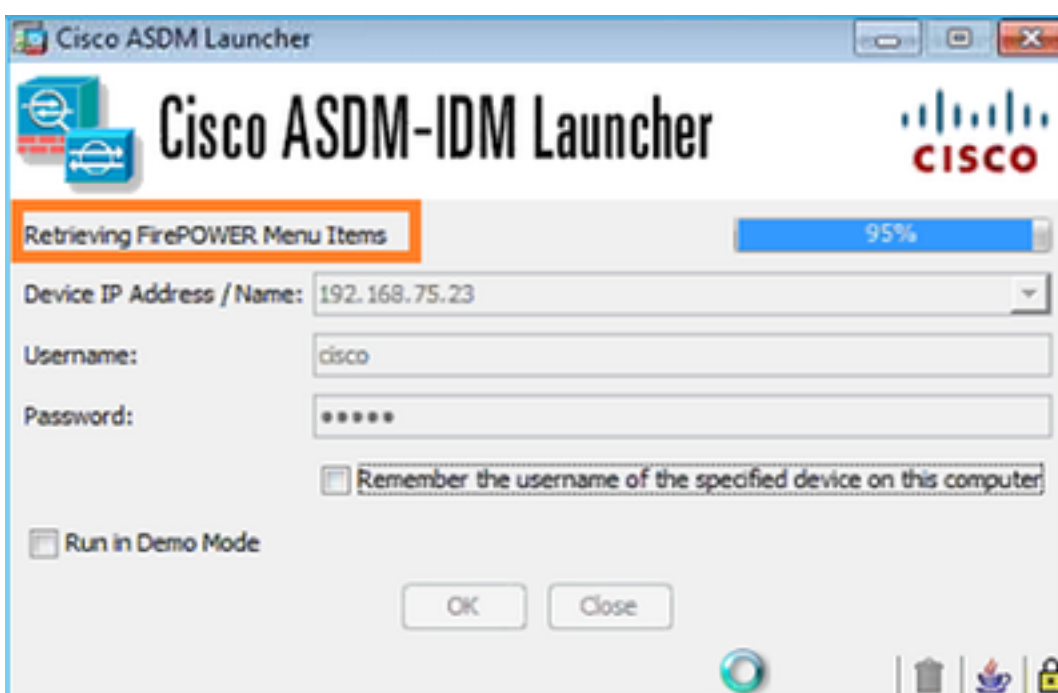


L'ASDM authentifie FirePOWER et une alerte de sécurité est affichée puisque le certificat de FirePOWER auto-est signé :

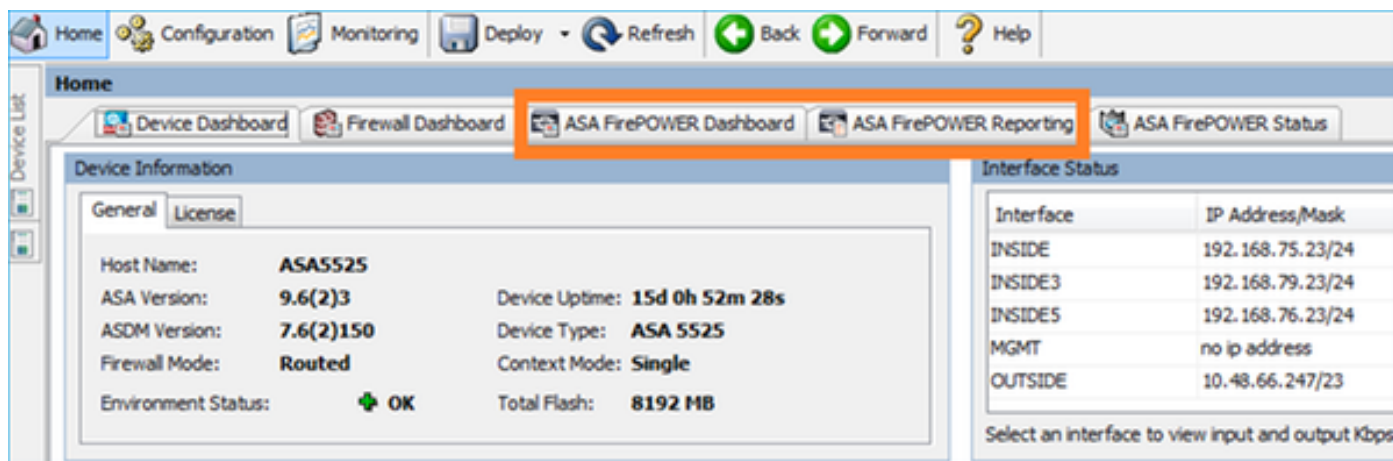


#### Étape 4 – L'ASDM récupère les commandes de menu de FirePOWER

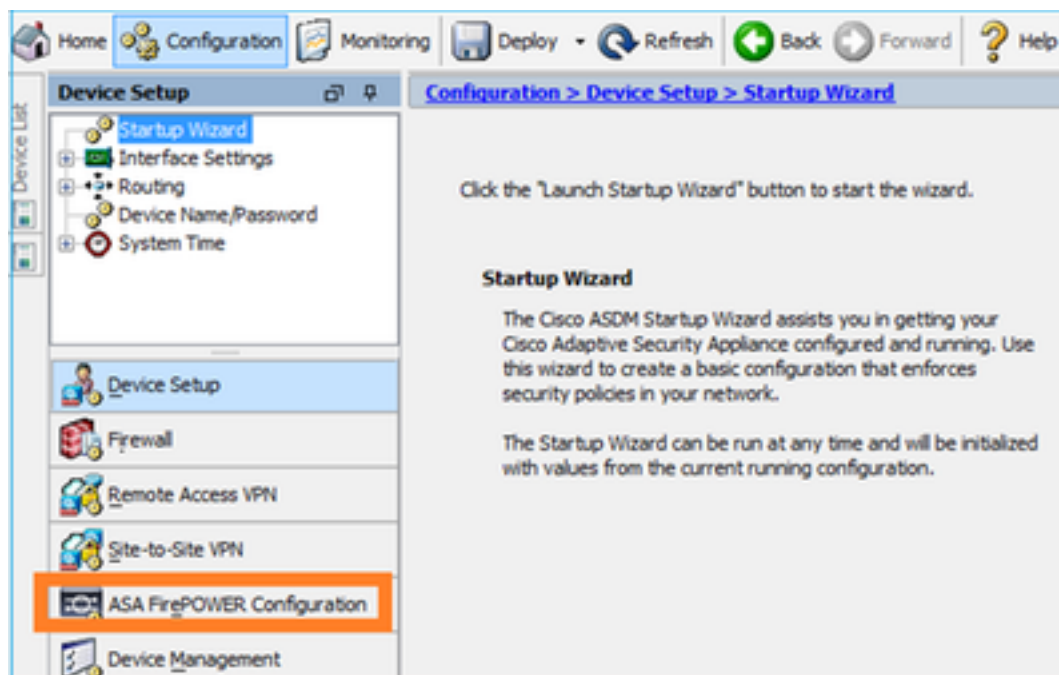
Après l'authentification réussie l'ASDM récupère de FirePOWER les commandes de menu :



Les onglets récupérés :

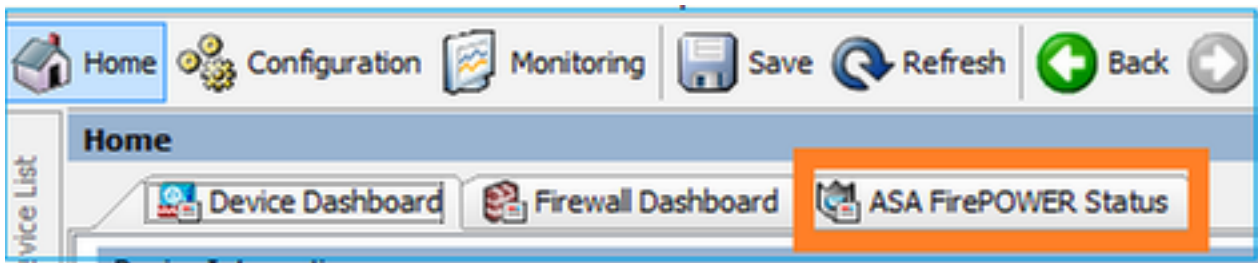


Il récupère également l'élément de menu de configuration ASA FirePOWER :

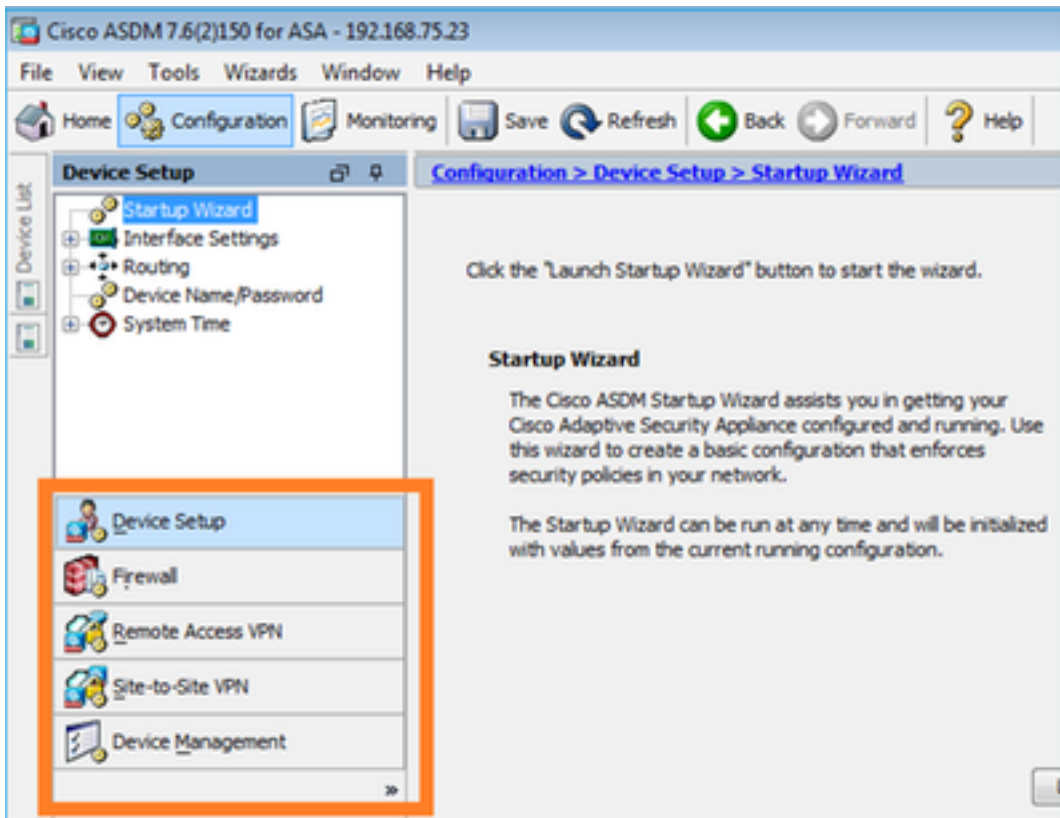


## Dépannage

Au cas où l'ASDM ne pourrait pas établir un tunnel SSL avec l'IP de Gestion point de gel puis il chargera seulement la commande de menu suivante de FirePOWER :



L'élément de configuration ASA FirePOWER manquera aussi bien :



## Actions recommandées

### Vérification 1

Assurez-vous que l'interface de gestion ASA est EN HAUSSE et le switchport connecté à lui est dans le VLAN approprié :

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

### Vérification 2



Assurez-vous que le module de FirePOWER est entièrement initialisé, en service :

```
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
-----
>
```

### Vérification 3

Vérifiez la Connectivité de base entre l'hôte ASDM et l'IP de Gestion de module de FirePOWER à l'aide des outils comme le **ping** et le **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
  0  <1 ms    <1 ms    <1 ms    192.168.75.123
Trace complete.
```

#### Vérification 4

Si l'hôte ASDM et l'IP de Gestion de FirePOWER sont dans le même contrôle du réseau L3 la table ARP sur l'hôte 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
```

#### Vérification 5

Activez la capture sur le périphérique ASDM tandis que vous vous connectez par l'intermédiaire de l'ASDM pour voir s'il y a transmission appropriée de TCP entre l'hôte et le module de FirePOWER. Au minimum vous devriez voir :

- Prise de contact à trois voies de TCP entre l'hôte ASDM et l'ASA
- Tunnel SSL établi entre l'hôte ASDM et l'ASA
- Prise de contact à trois voies de TCP entre l'hôte ASDM et l'IP de Gestion de module de FirePOWER
- Tunnel SSL établi entre l'hôte ASDM et l'IP de Gestion de module de FirePOWER

## Vérification 6

Pour vérifier le trafic à et du module de FirePOWER vous pouvez activer la capture sur l'interface d'asa\_mgmt\_plane. Dans la capture au-dessous de lui peut être vu :

- Demande d'ARP de l'hôte ASDM (paquet 42)
- Réponse d'ARP du module de FirePOWER (paquet 43)
- Prise de contact à trois voies de TCP entre l'hôte ASDM et le module de FirePOWER (paquets 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
```

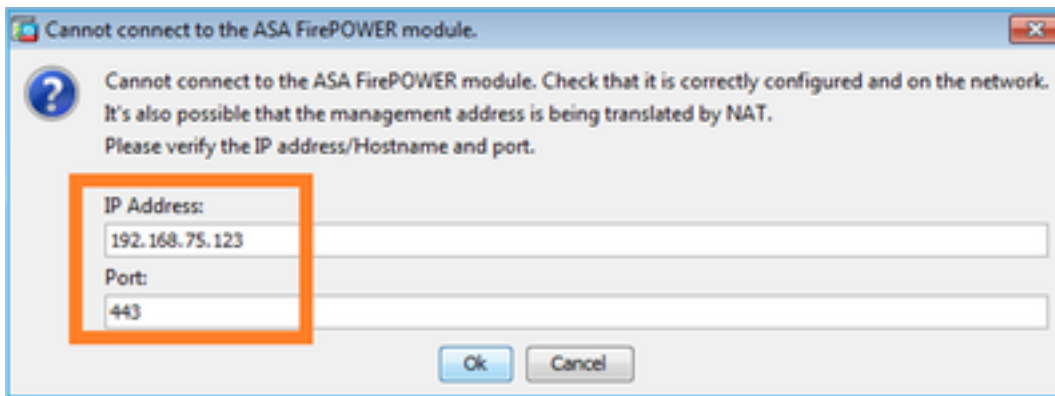
## Vérification 7

Vérifiez que l'utilisateur ASDM a le niveau de privilège 15. Une manière de confirmer ceci est en s'exécutant **mettent au point le HTTP 255** tout en se connectant par l'intermédiaire de l'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]
```

## Vérification 8

Si entre l'hôte ASDM et le module de FirePOWER il y a NAT pour l'IP de Gestion de FirePOWER puis vous le besoin de spécifier l'IP de NATed :



## Vérification 9

Assurez-vous que le module de FirePOWER n'est pas déjà géré par le centre de Gestion de FirePOWER (FMC) parce que dans cela le cas que FirePOWER tabule dans l'ASDM manquera :

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

>
```

Une autre manière :

```
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
```

## Vérification 10

Vérifiez du guide de compatibilité ASA que les images ASA/ASDM sont compatibles :

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

## Vérification 11

Vérifiez du guide de compatibilité de FirePOWER que le périphérique de FirePOWER est compatible avec la version ASDM :

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

## Documents connexes

[Guide de démarrage rapide de module de Cisco ASA FirePOWER](#)

[ASA avec le guide de configuration de gestion local de services de FirePOWER, version 6.1.0](#)

[Guide de l'utilisateur de module ASA FirePOWER pour l'ASA5506-X, l'ASA5506H-X, l'ASA5506W-X, l'ASA5508-X, et l'ASA5516-X, version 5.4.1](#)