Utilisation d'ASDM pour gérer un module FirePOWER sur un ASA

Table des matières

Introduction

Ce document décrit comment le logiciel ASDM communique avec le dispositif de sécurité adaptatif (ASA) et un module logiciel FirePOWER installé sur celui-ci.

Informations générales

Un module FirePOWER installé sur un ASA peut être géré par l'une des méthodes suivantes :

- Firepower Management Center (FMC) : il s'agit de la solution de gestion prête à l'emploi.
- Adaptive Security Device Manager (ASDM) : il s'agit de la solution de gestion intégrée.

Conditions préalables

Exigences

Une configuration ASA pour activer la gestion 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
```

Vérifiez la compatibilité entre le module ASA/SFR, sinon les onglets FirePOWER ne sont pas visibles.

En outre, sur l'ASA, la licence 3DES/AES doit être activée :

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

Assurez-vous que le système client ASDM exécute une version prise en charge de Java JRE.

Composants utilisés

- Un hôte Microsoft Windows 7
- ASA5525-X qui exécute ASA Version 9.6(2.3)
- ASDM version 7.6.2.150
- Module logiciel FirePOWER 6.1.0-330

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Architecture

L'ASA dispose de trois interfaces internes :

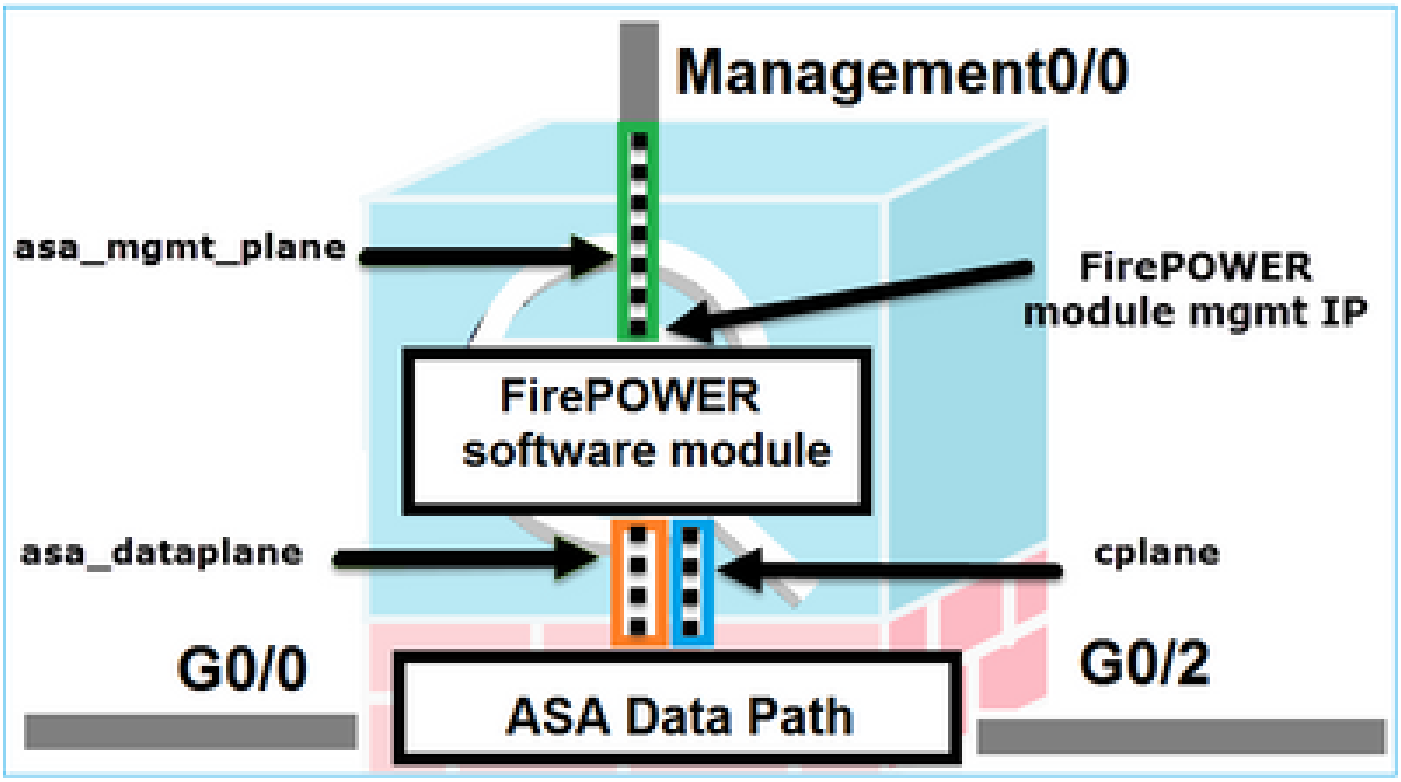
- asa_dataplane : permet de rediriger les paquets du chemin de données ASA vers le module logiciel FirePOWER.
- asa_mgmt_plane : permet à l'interface de gestion FirePOWER de communiquer avec le réseau.
- cplane : interface du plan de contrôle utilisée pour transférer les messages de veille entre l'ASA et le module FirePOWER.

Vous pouvez capturer le trafic dans toutes les interfaces internes :

<#root>

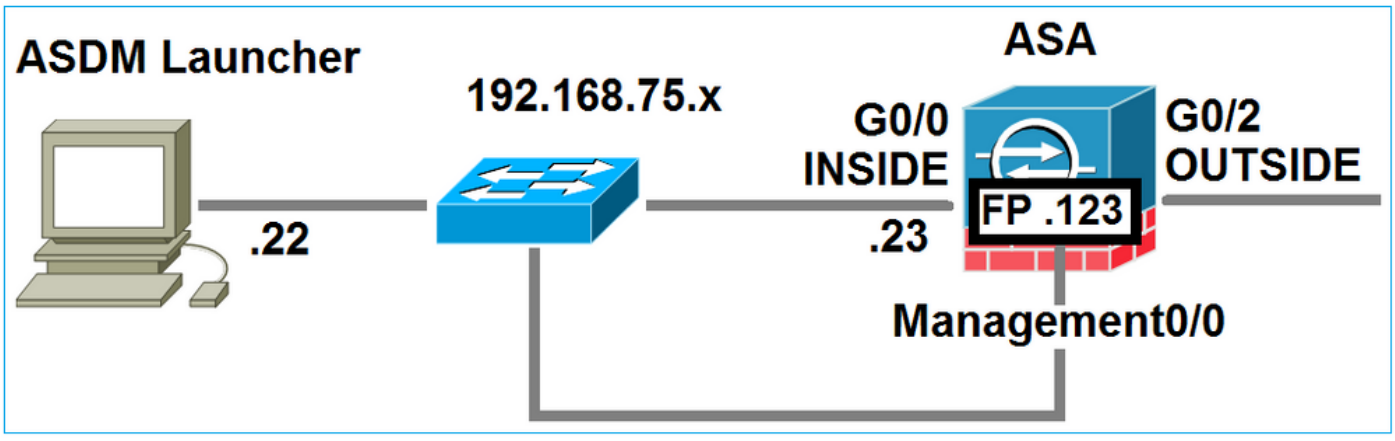
```
ASA5525#

capture CAP interface ?


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

Ceci peut être visualisé comme suit :



Fonctionnement en arrière-plan Lorsqu'un utilisateur se connecte à un ASA via ASDM

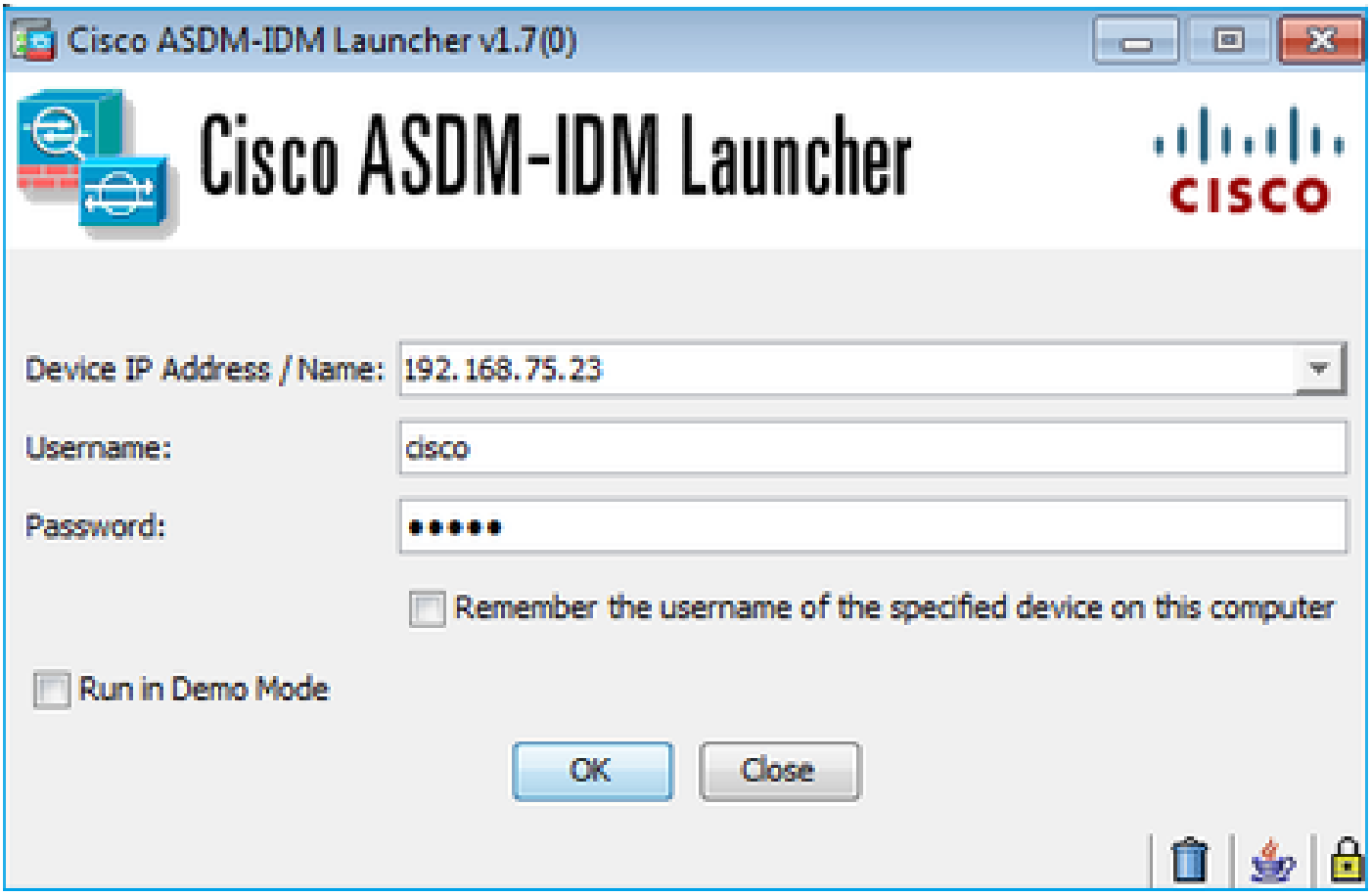
Considérez cette topologie :



Lorsqu'un utilisateur initie une connexion ASDM à l'ASA, ces événements se produisent :

Étape 1 - L'utilisateur lance la connexion ASDM

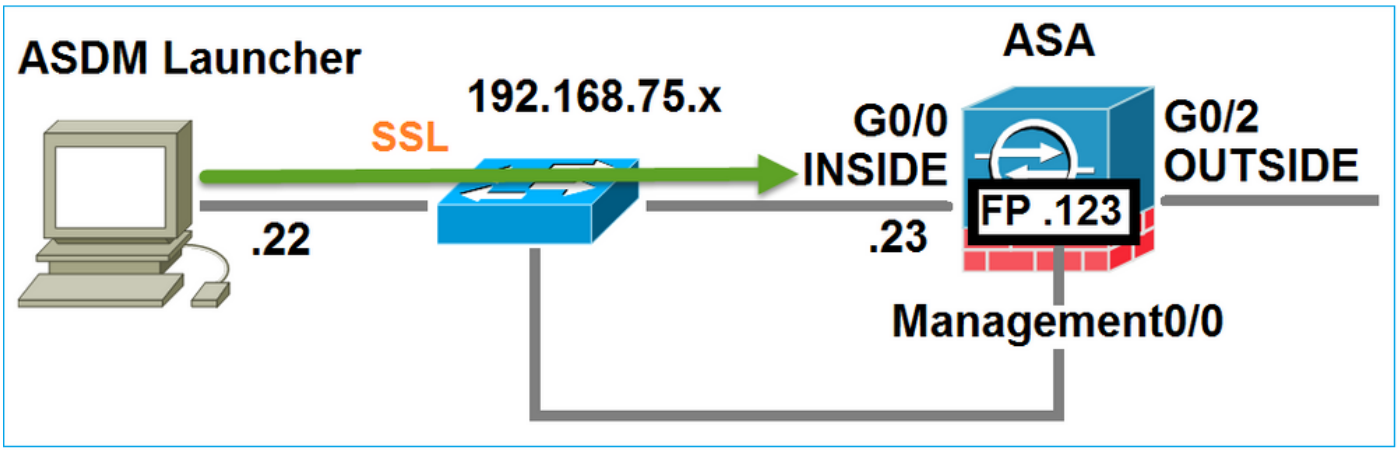
L'utilisateur spécifie l'adresse IP ASA utilisée pour la gestion HTTP, entre les informations d'identification et initie une connexion vers l'ASA :



En 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 détecte la configuration ASA et l'adresse IP du module FirePOWER

Entrez la commande debug http 255 sur l'ASA afin d'afficher toutes les vérifications qui sont faites

en arrière-plan quand l'ASDM se connecte à l'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
```

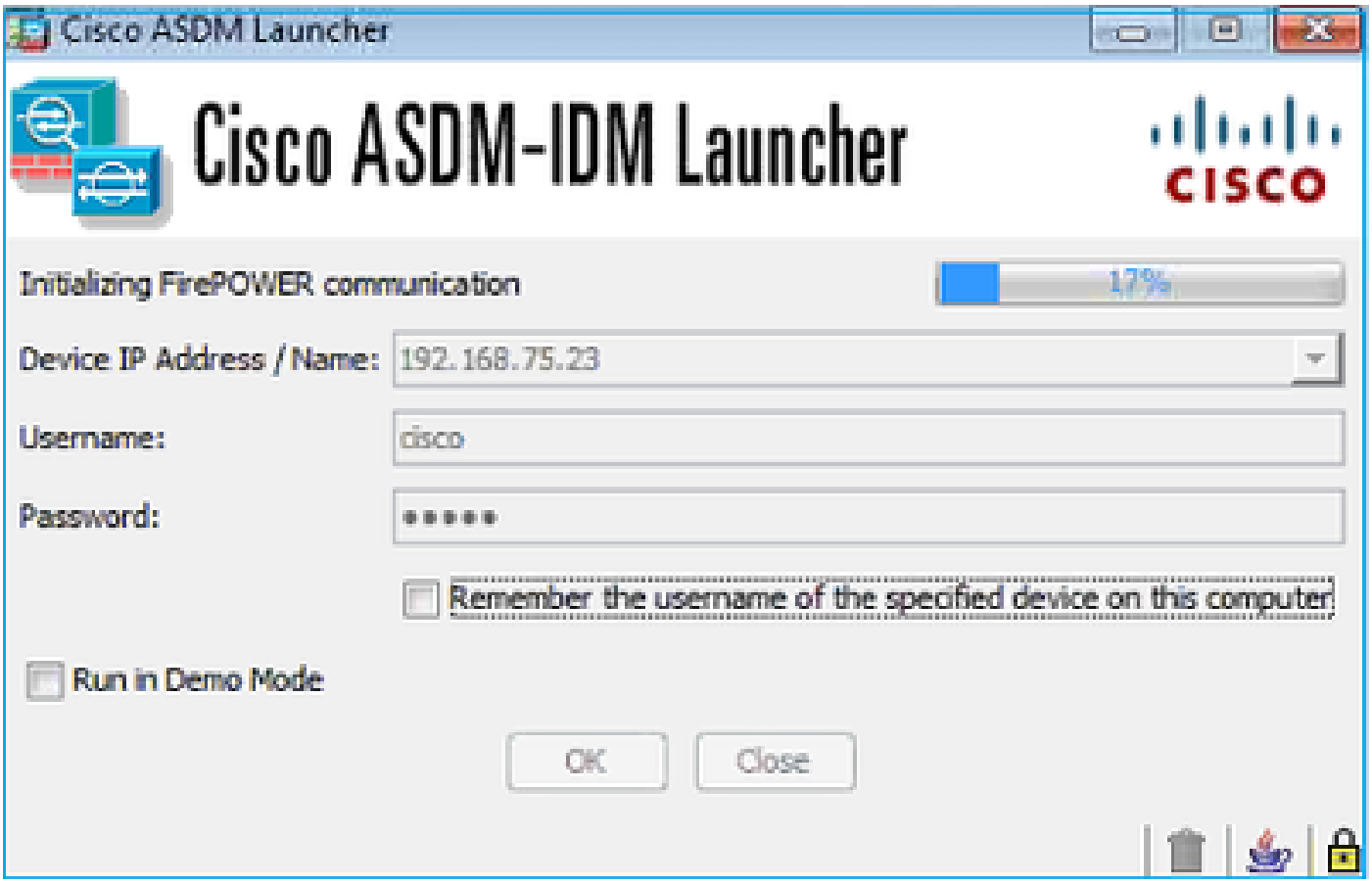
- show module - L'ASDM détecte les modules ASA.
- show module sfr details - L'ASDM détecte les détails du module, notamment l'adresse IP de gestion FirePOWER.

Ceux-ci sont vus en arrière-plan comme une série de connexions SSL du PC vers l'adresse 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 établit une communication avec le module FirePOWER

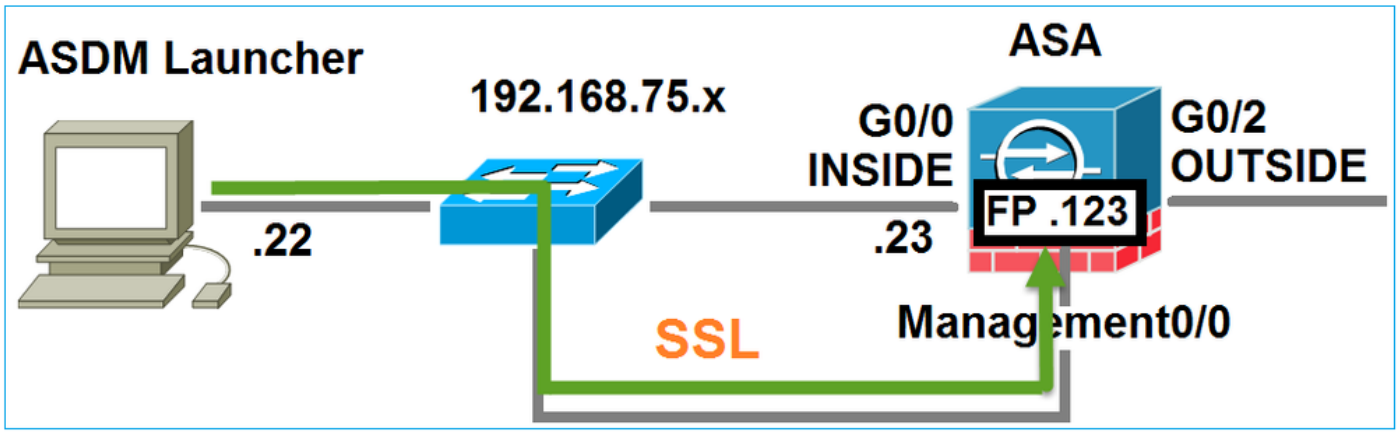
Puisque l'ASDM connaît l'adresse IP de gestion FirePOWER, il initie des sessions SSL vers le module :



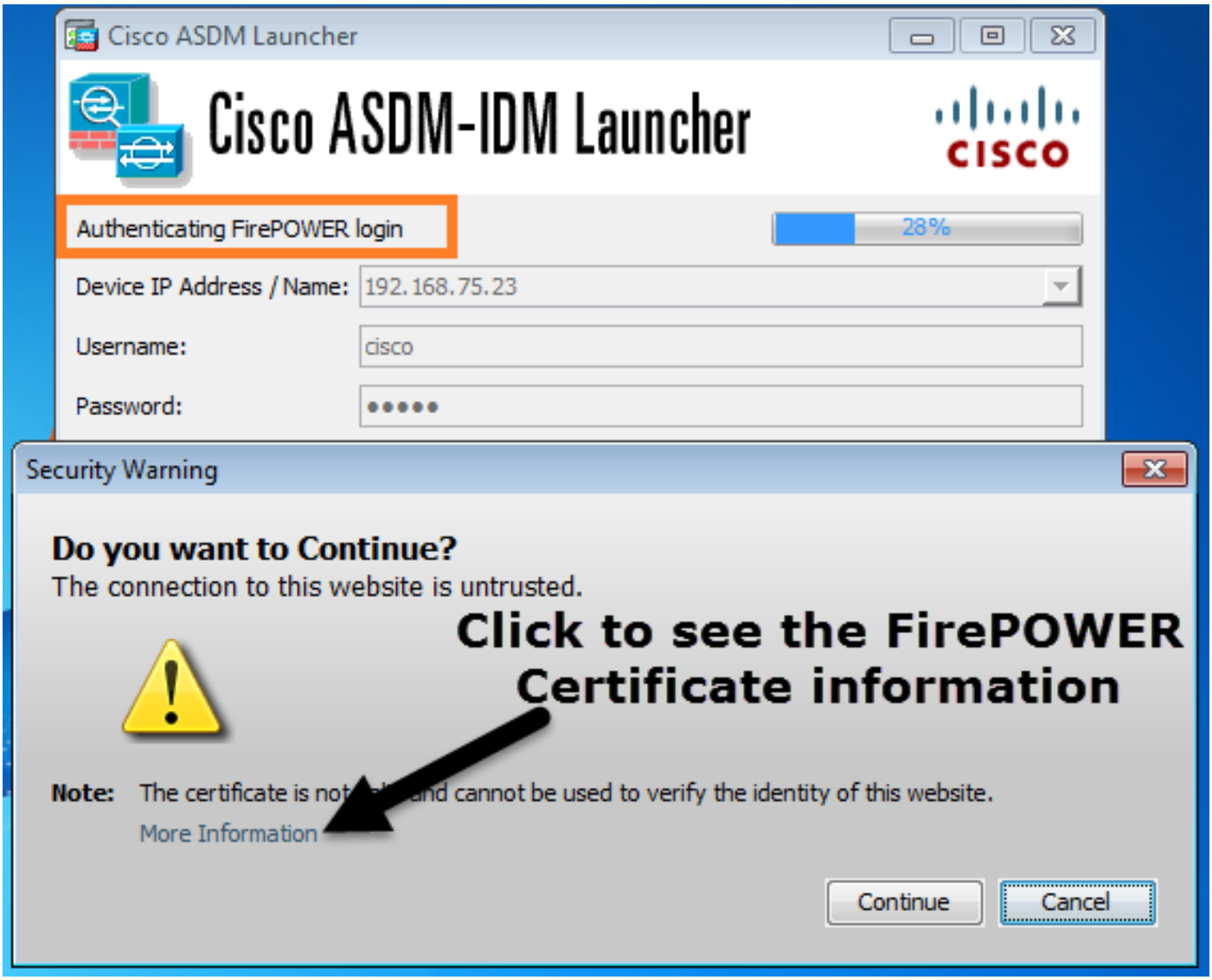
Ceci se voit en arrière-plan comme des connexions SSL de l'hôte ASDM vers l'adresse IP de gestion FirePOWER :

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 :

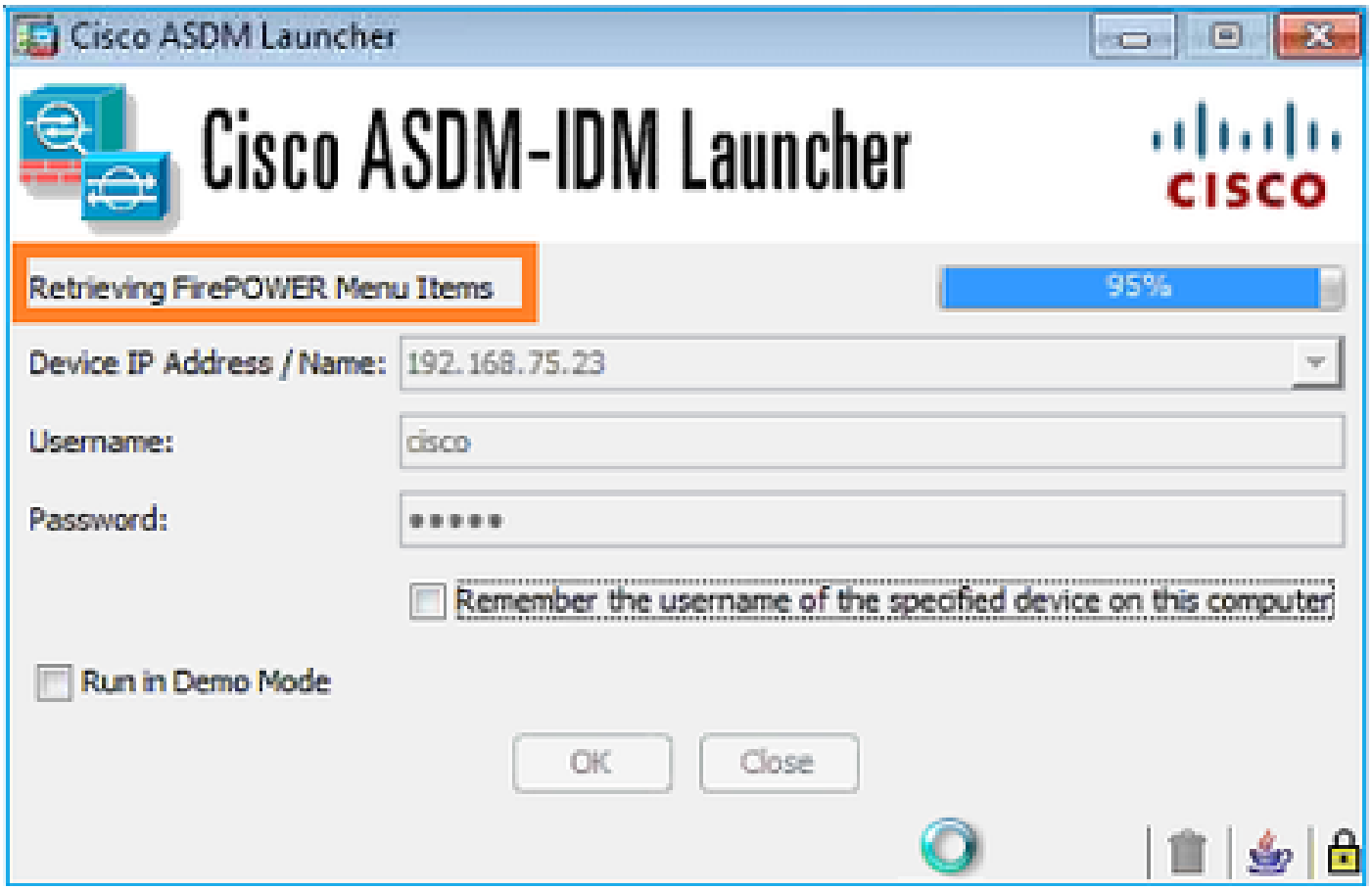


L'ASDM authentifie FirePOWER et un avertissement de sécurité s'affiche car le certificat FirePOWER est auto-signé :

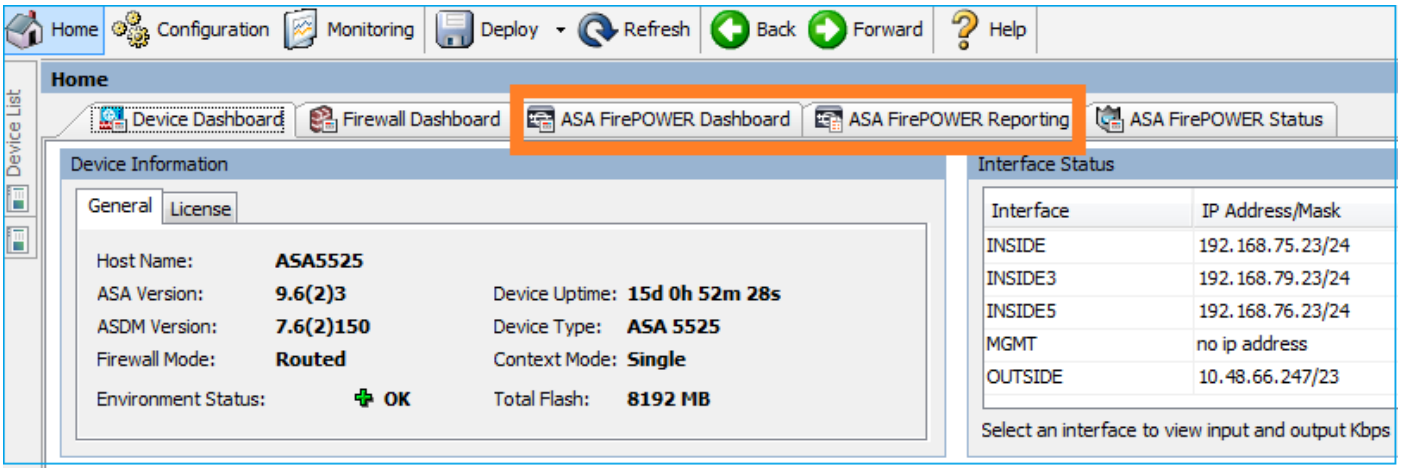


Étape 4 - L'ASDM récupère les éléments du menu FirePOWER

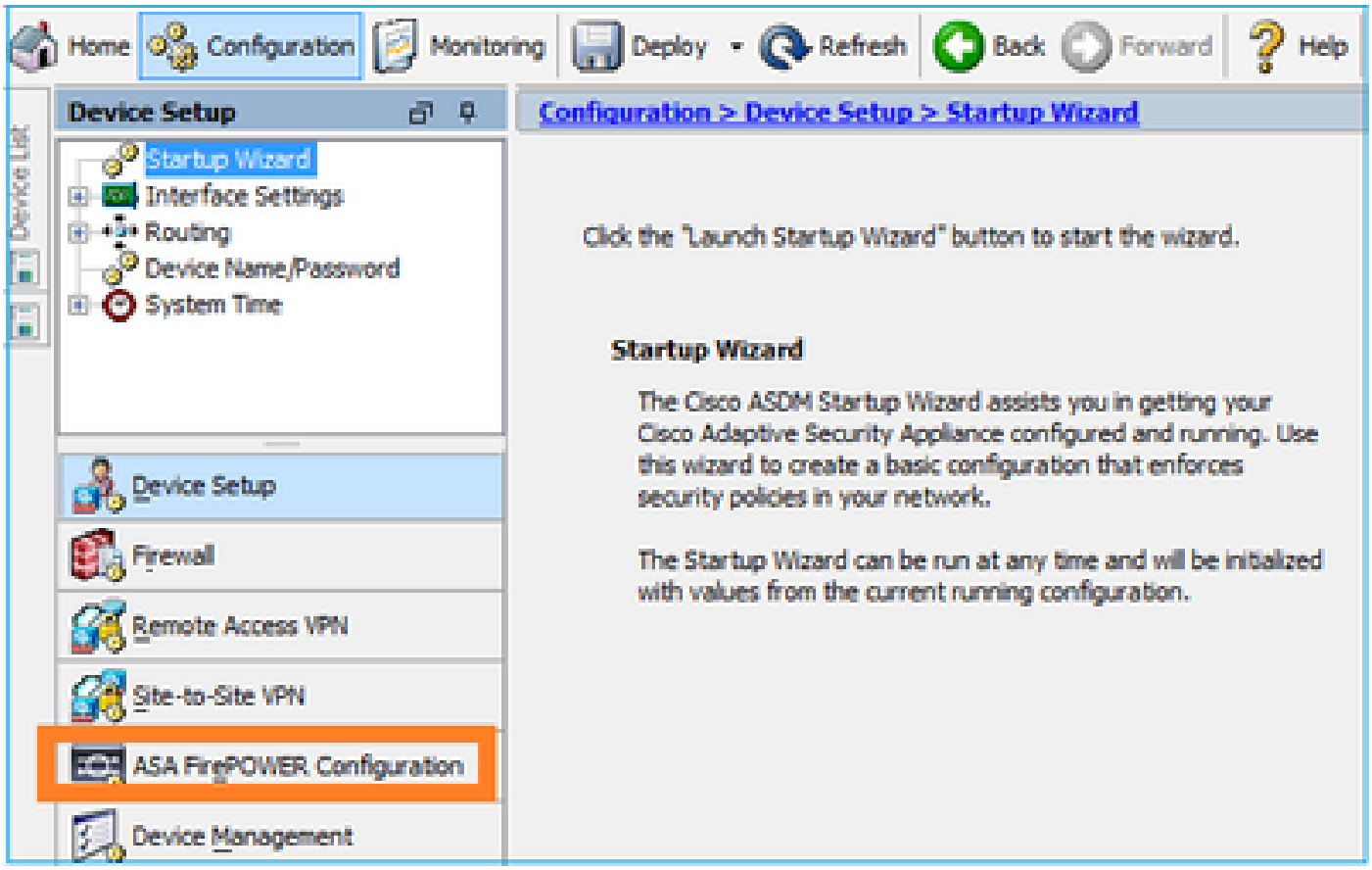
Une fois l'authentification réussie, l'ASDM récupère les éléments de menu à partir du périphérique FirePOWER :



Les onglets récupérés sont présentés dans cet exemple :

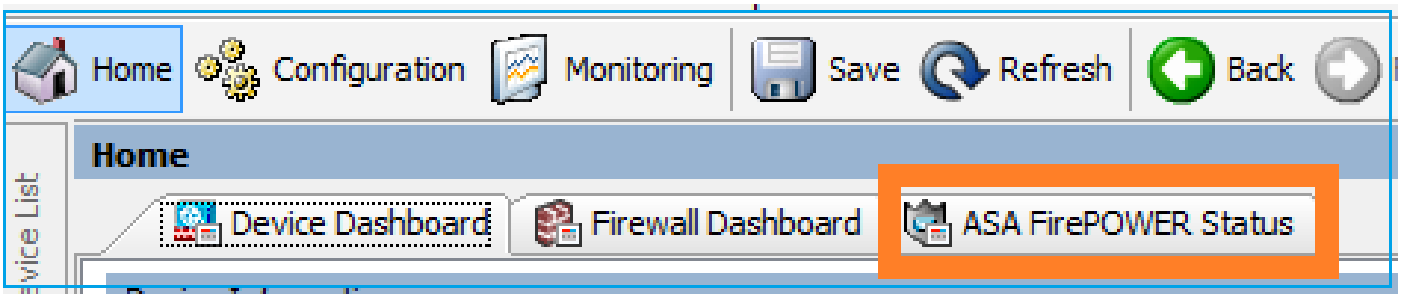


Il récupère également l'élément de menu de configuration ASA FirePOWER :

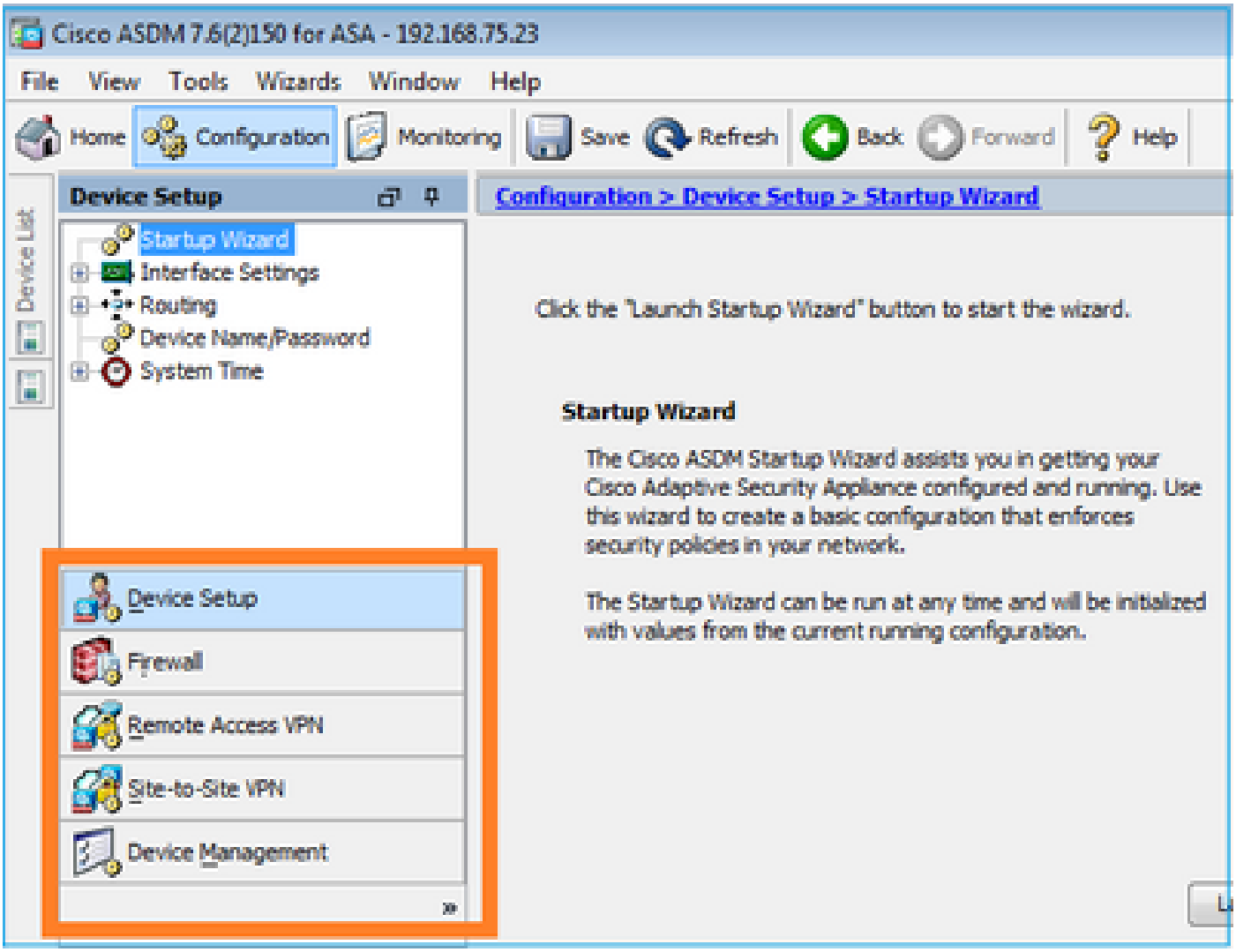


Dépannage

Si ASDM ne peut pas établir de tunnel SSL avec l'adresse IP de gestion FirePOWER, il charge uniquement cet élément de menu FirePOWER :



L'élément de configuration ASA FirePOWER est également manquant :



Vérification 1

Assurez-vous que l'interface de gestion ASA est UP et que le port de commutation qui lui est connecté se trouve dans le VLAN approprié :

<#root>

```
ASA5525#

show interface  ip brief | include Interface|Management0/0

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

up                    up
```

Dépannage recommandé

- Définissez le VLAN approprié.
- Remettez le port en marche (vérifiez le câble, la configuration du port de commutation (débit/duplex/arrêt)).

Vérification 2

Assurez-vous que le module FirePOWER est entièrement initialisé, opérationnel et en cours d'exécution :

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

>

Dépannage recommandé

- Recherchez les erreurs ou les échecs dans le résultat de la commande show module sfr log console.

Vérification 3

Vérifiez la connectivité de base entre l'hôte ASDM et l'adresse IP de gestion du module FirePOWER avec des commandes telles que ping et 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.
```

Dépannage recommandé

- Vérifiez le routage le long du chemin.
- Vérifiez qu'aucun périphérique dans le chemin ne bloque le trafic.

Vérification 4

Si l'hôte ASDM et l'adresse IP de gestion FirePOWER se trouvent sur le même réseau de couche 3, vérifiez la table ARP (Address Resolution Protocol) 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
```

Dépannage recommandé

- S'il n'y a pas d'entrées ARP, utilisez Wireshark afin de vérifier la communication ARP. Assurez-vous que les adresses MAC des paquets sont correctes.
- Si des entrées ARP existent, assurez-vous qu'elles sont correctes.

Vérification 5

Activez la capture sur le périphérique ASDM pendant que vous vous connectez via ASDM afin de voir s'il existe une communication TCP appropriée entre l'hôte et le module FirePOWER. Au minimum, vous voyez alors :

- Connexion TCP en trois étapes entre l'hôte ASDM et l'ASA.
- Tunnel SSL établi entre l'hôte ASDM et l'ASA.
- Connexion TCP en trois étapes entre l'hôte ASDM et l'adresse IP de gestion du module FirePOWER.
- Tunnel SSL établi entre l'hôte ASDM et l'adresse IP de gestion du module FirePOWER.

Dépannage recommandé

- Si la connexion TCP en trois étapes échoue, assurez-vous qu'il n'y a pas de trafic asymétrique ou de périphériques sur le chemin qui bloquent les paquets TCP.
- Si SSL échoue, vérifiez s'il n'y a aucun périphérique dans le chemin d'accès qui effectue un MITM (man-in-the-middle) (l'émetteur du certificat de serveur donne un indice à ce sujet).

Vérification 6

Afin de vérifier le trafic en provenance et à destination du module FirePOWER, activez la capture sur l'interface asa_mgmt_plane. Dans la capture, vous pouvez voir les éléments suivants :

- Requête ARP de l’hôte ASDM (paquet 42).
- Réponse ARP du module FirePOWER (paquet 43).
- Connexion TCP en trois étapes entre l'hôte ASDM et le module FirePOWER (paquets 44 à 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

Dépannage recommandé

- Identique à la vérification 5.

Vérification 7

Vérifiez que l'utilisateur ASDM dispose du niveau de privilège 15. Une façon de confirmer ceci est d'entrer la commande **debug http 255** pendant qu'il se connecte via 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],
```

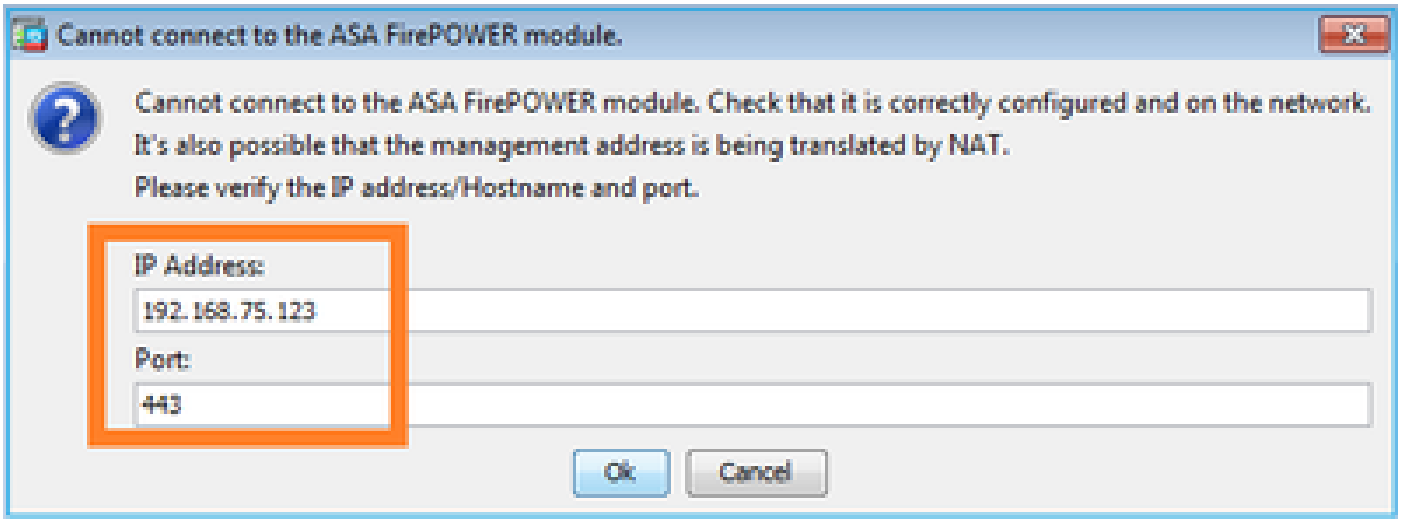
privilege = [14]

Dépannage recommandé

- Si le niveau de privilège n'est pas 15, essayez avec un utilisateur de niveau 15.

Vérification 8

Si, entre l'hôte ASDM et le module FirePOWER, il existe une traduction d'adresse réseau (NAT) pour l'adresse IP de gestion FirePOWER, vous devez spécifier l'adresse IP NATed :



Dépannage recommandé

- Les captures au niveau des points d'extrémité (ASA/SFR et hôte final) le confirment.

Vérification 9

Assurez-vous que le module FirePOWER n'est pas déjà géré par FMC, car dans ce cas, les onglets FirePOWER de l'ASDM sont manquants :

```
<#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.


>
```

Une autre méthode est avec la commande **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
```

Dépannage recommandé

- Si le périphérique est déjà géré, vous devez annuler son enregistrement avant de le gérer à partir d'ASDM. Reportez-vous au Guide de configuration de Firepower Management Center.

Vérification 10

Vérifiez la capture Wireshark afin de vous assurer que le client ASDM se connecte avec une version TLS appropriée (par exemple, TLSv1.2).

Dépannage recommandé

- Réglez les paramètres SSL du navigateur.
- Essayez avec un autre navigateur.
- Essayez à partir d'un autre hôte final.

Vérification 11

Vérifiez dans le guide Cisco ASA Compatibility que les images ASA/ASDM sont compatibles.

Dépannage recommandé

- Utiliser une image ASDM compatible.

Vérification 12

Vérifiez dans le guide de compatibilité Cisco ASA que le périphérique FirePOWER est compatible avec la version ASDM.

Dépannage recommandé

- Utiliser une image ASDM compatible.

Informations connexes

- **Guide de démarrage rapide du module Cisco ASA FirePOWER**
- **Guide de configuration de la gestion locale d'ASA avec les fonctionnalités FirePOWER, version 6.1.0**
- **Guide de l'utilisateur du module ASA FirePOWER pour ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X et ASA5516-X, version 5.4.1**
- **Assistance et documentation techniques - Cisco Systems**

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.