Использование ASDM для управления модулем FirePOWER на ASA

Содержание

Введение

Модулем FirePOWER, который установлен на ASA, можно управлять также:

- Центр управления огневой мощи (FMC)? Это - отдельное решение по управлению
- Менеджер устройств адаптивной безопасности (ASDM) (ADSM)? Это - решение по управлению на коробке

Цель этого документа состоит в том, чтобы объяснить, как программное обеспечение ASDM связывается с ASA и модулем ПО FirePOWER, установленным на нем.

Используемые компоненты

- Хост Windows 7
- ASA5525-X рабочий ASA 9.6.2-3 кодов
- Программное обеспечение ASDM 7.6.2.150
- Модуль ПО FirePOWER 6.1.0-330

Предварительные условия

Конфигурация ASA для включения управления 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
```

Кроме того, на ASA лицензия 3DES/AES должна быть включена:

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

Архитектура

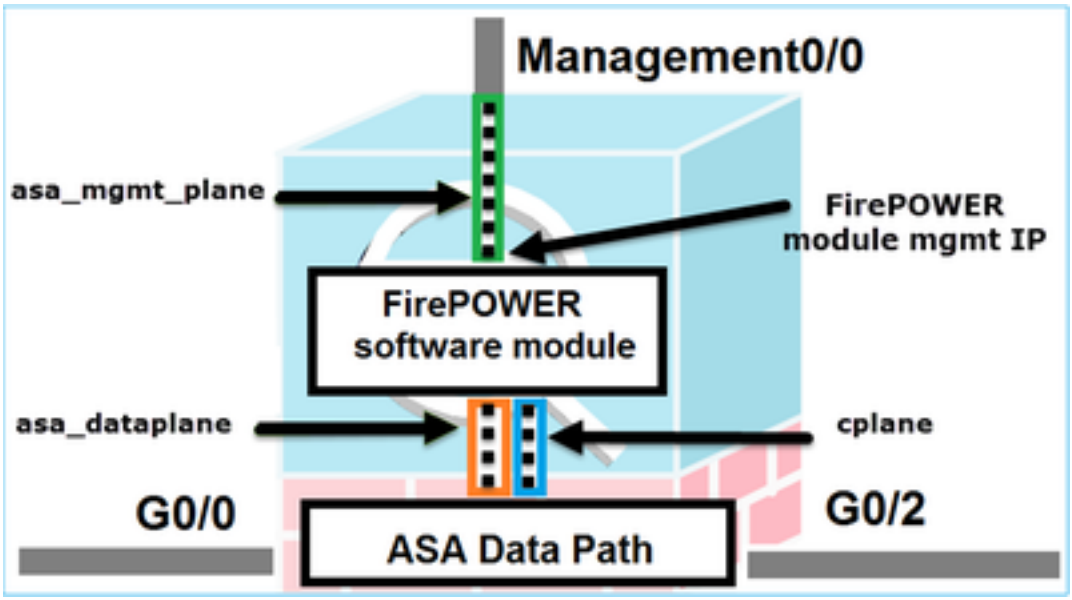
ASA имеет 3 внутренних интерфейса:

- **asa_dataplane** = Это используется для перенаправления пакетов от Пути данных ASA до модуля ПО FirePOWER
- **asa_mgmt_plane** = Это используется, чтобы позволить интерфейсу управления FirePOWER связываться с сетью
- **cplane** = интерфейс Уровня управления, который используется для передачи пакетов Keepalive между ASA и модулем FirePOWER

Можно перехватить трафик во всех внутренних интерфейсах:

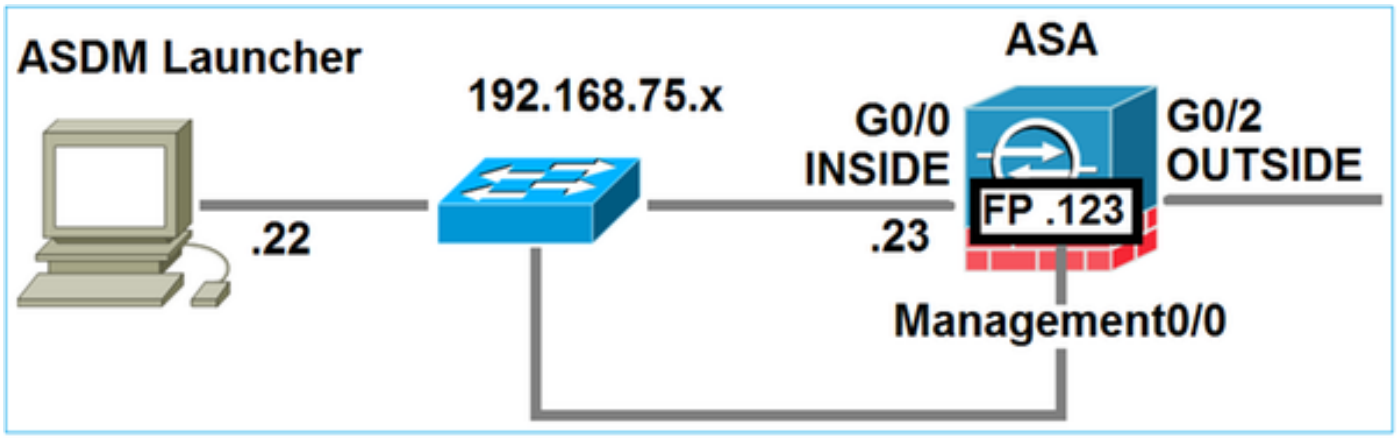
```
ASA5525# capture CAP interface ? asa_dataplane Capture packets on dataplane interface
asa_mgmt_plane Capture packets on managementplane interface cplane Capture packets on
controlplane interface
```

Вышеупомянутое может визуализироваться следующим образом:



Фоновая работа, когда пользователь соединяется с ASA через ASDM

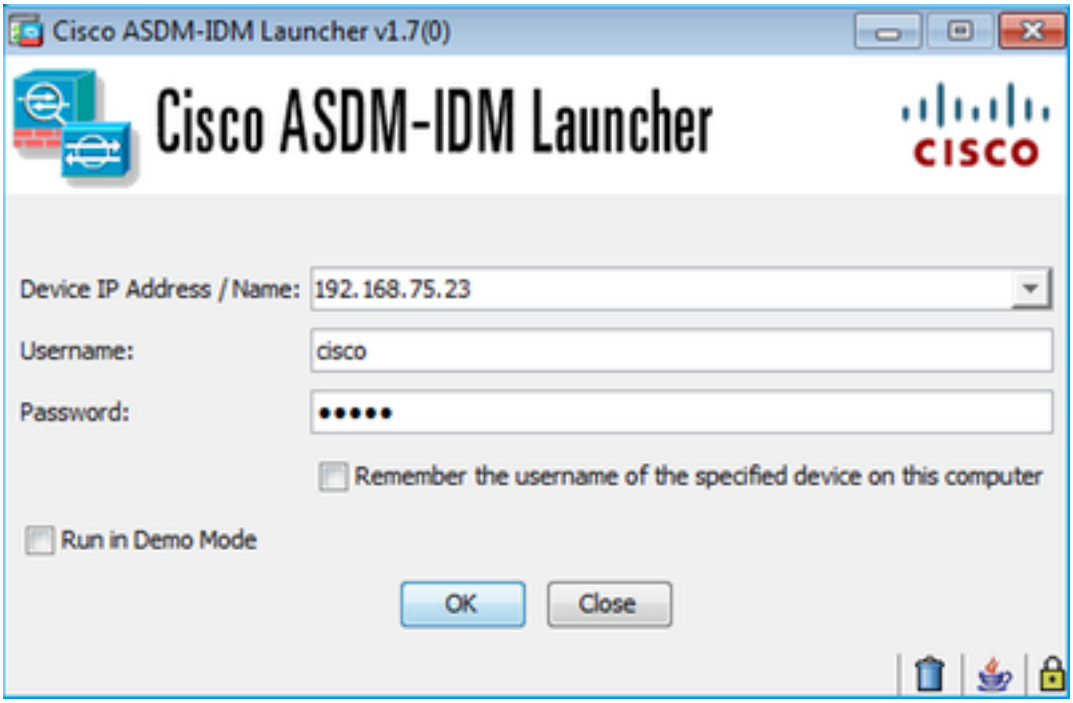
Рассмотрите следующую топологию



Когда пользователь будет инициировать соединение ASDM с ASA, следующие события будут иметь место:

Шаг 1? Пользователь инициирует соединение ASDM

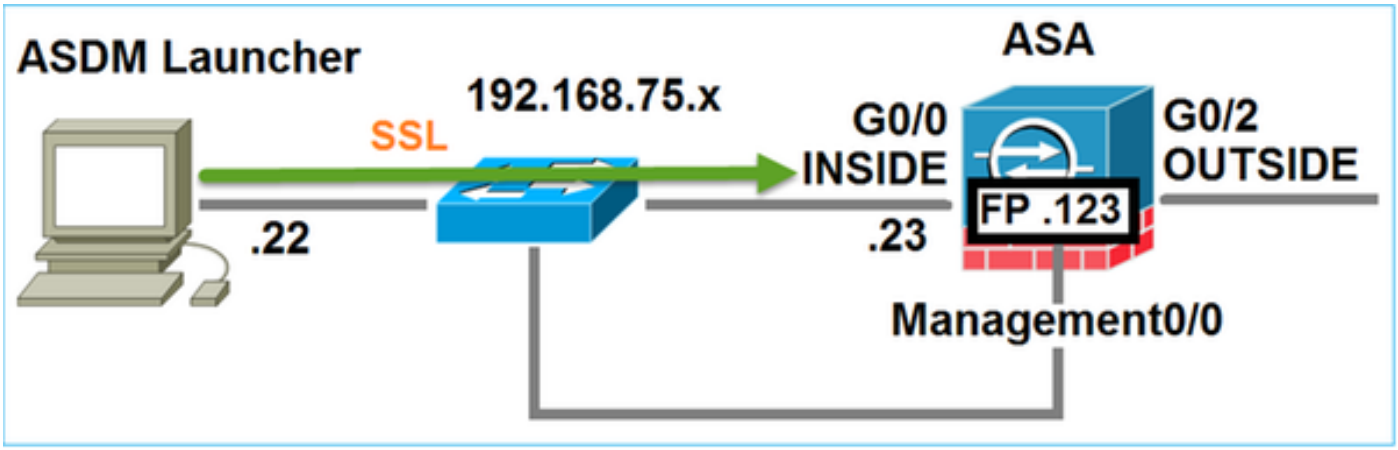
Пользователь задает IP ASA, используемого для управления HTTP, вводит учетные данные и инициирует соединение к ASA:



В фоновом режиме туннель SSL между ASDM и ASA установлен:

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

Это может визуализироваться следующим образом:



Шаг 2? ASDM обнаруживает конфигурацию ASA и IP модуля FirePOWER

Включение **http 255 отладки** на ASA покажет все проверки, которые сделаны в фоновом режиме, когда ASDM соединяется с 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
192.168.75.22HTTP: 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 192.168.75.22HTTP: processing ASDM request [/admin/exec/show+cluster+info] with
cookie-based authentication HTTP: processing GET URL '/admin/exec/show+cluster+info' from host
192.168.75.22HTTP: 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
```

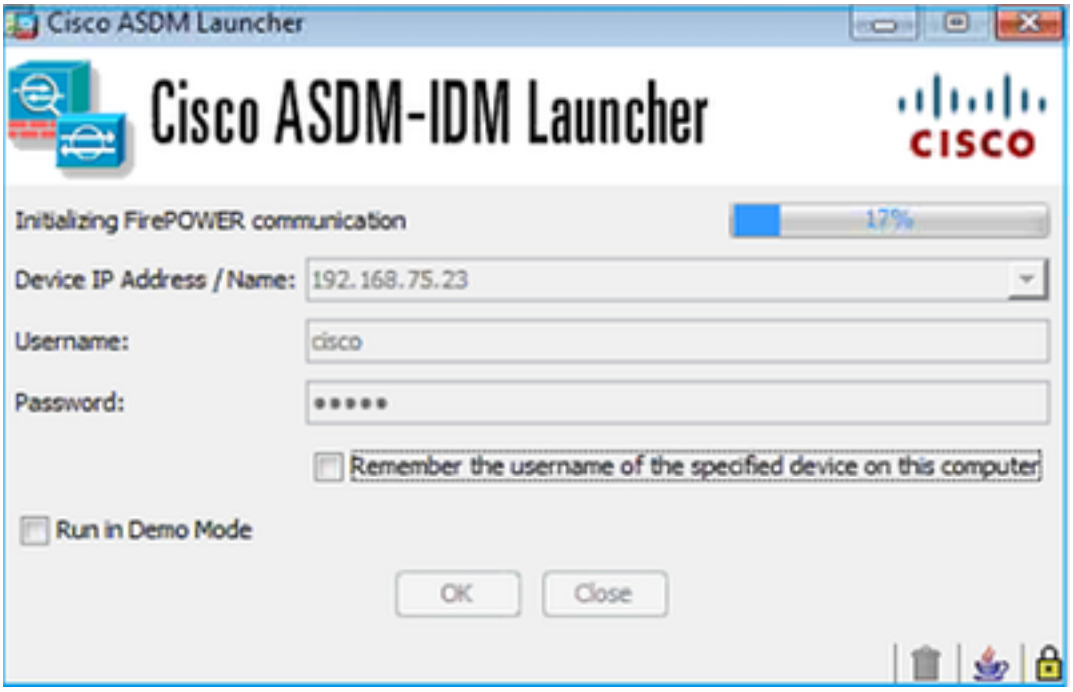
- команда "show module" = ASDM обнаруживает модули ASA
- команда "show module" sfr подробные данные = ASDM обнаруживает подробные данные модуля включая IP - управление FirePOWER

Вышеупомянутое будет замечено в фоновом режиме как серия подключений SSL от ПК к 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

Шаг 3? ASDM инициирует связь к модулю FirePOWER

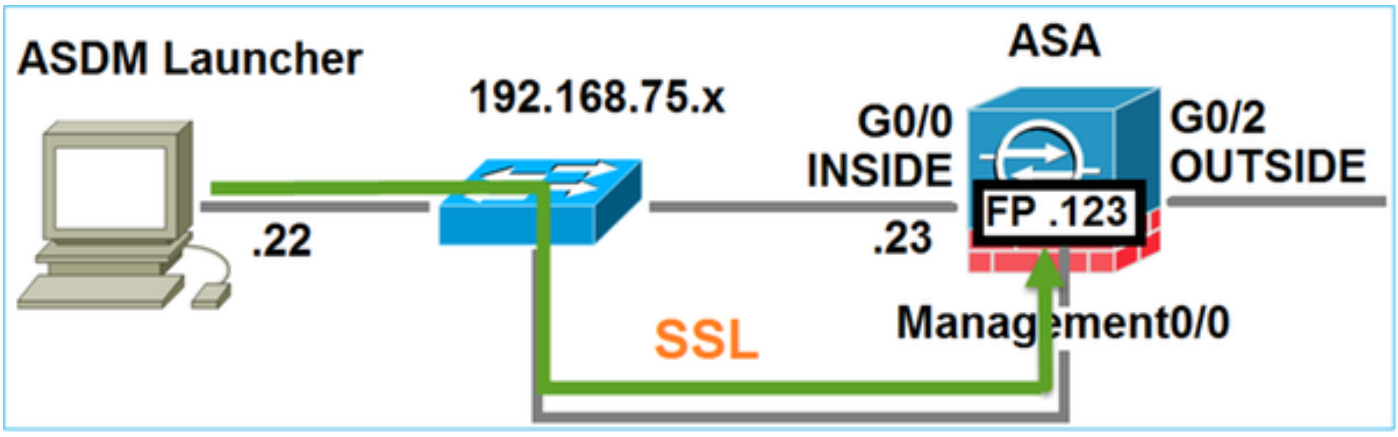
Так как ASDM знает IP - управление FirePOWER, это инициирует сеансы SSL к модулю:



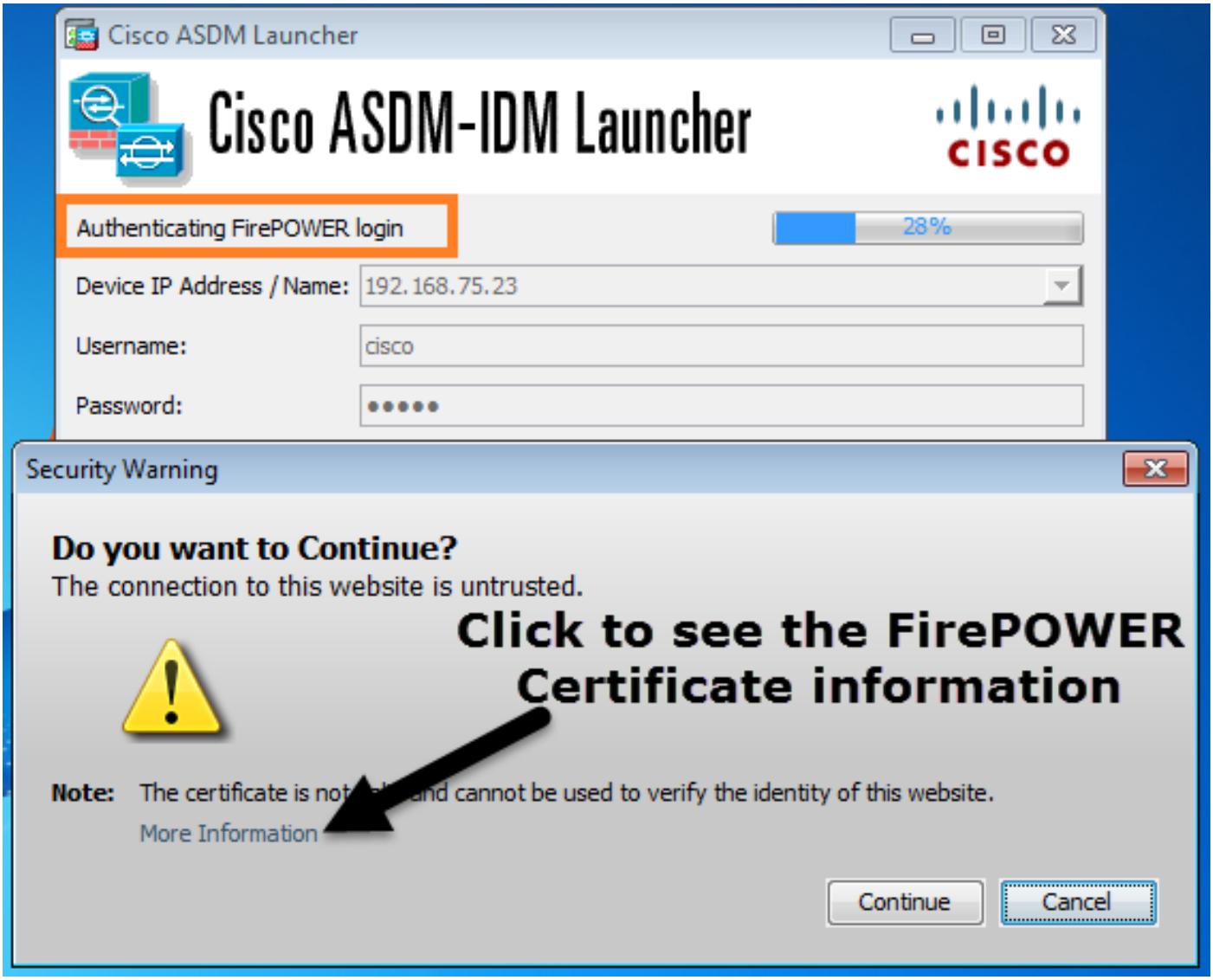
Вышеупомянутое будет замечено в фоновом режиме как подключения SSL от хоста ASDM к IP - управлению FirePOWER:

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

Это может визуализироваться следующим образом:

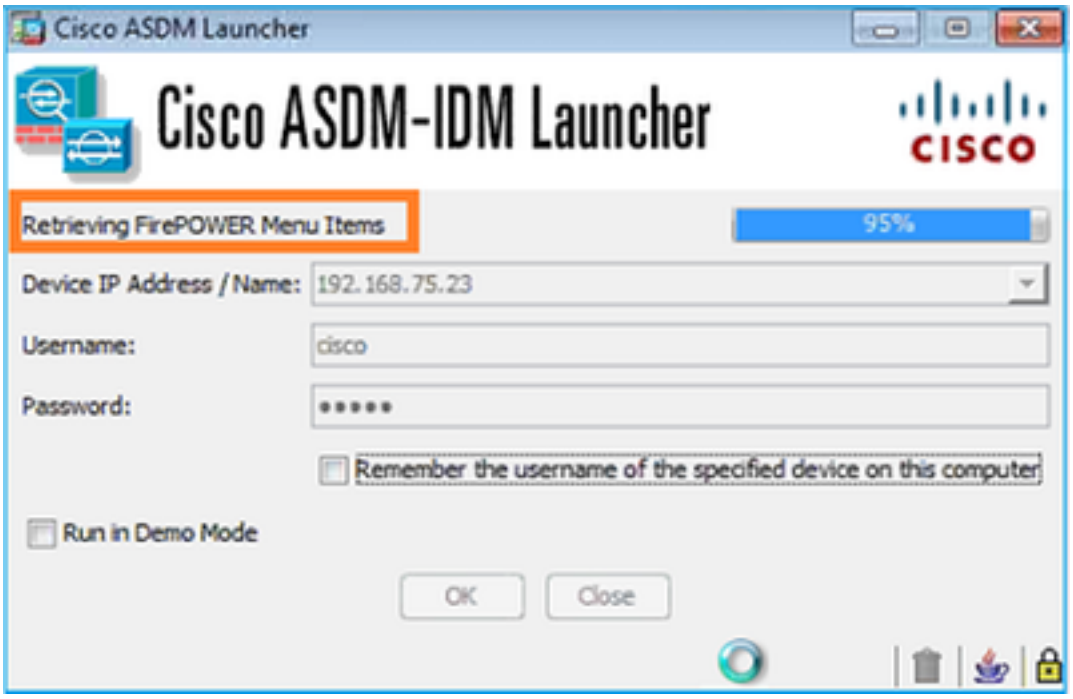


ASDM аутентифицирует FirePOWER, и Предупреждение системы безопасности показывают, так как Сертификат FirePOWER самоподписан:

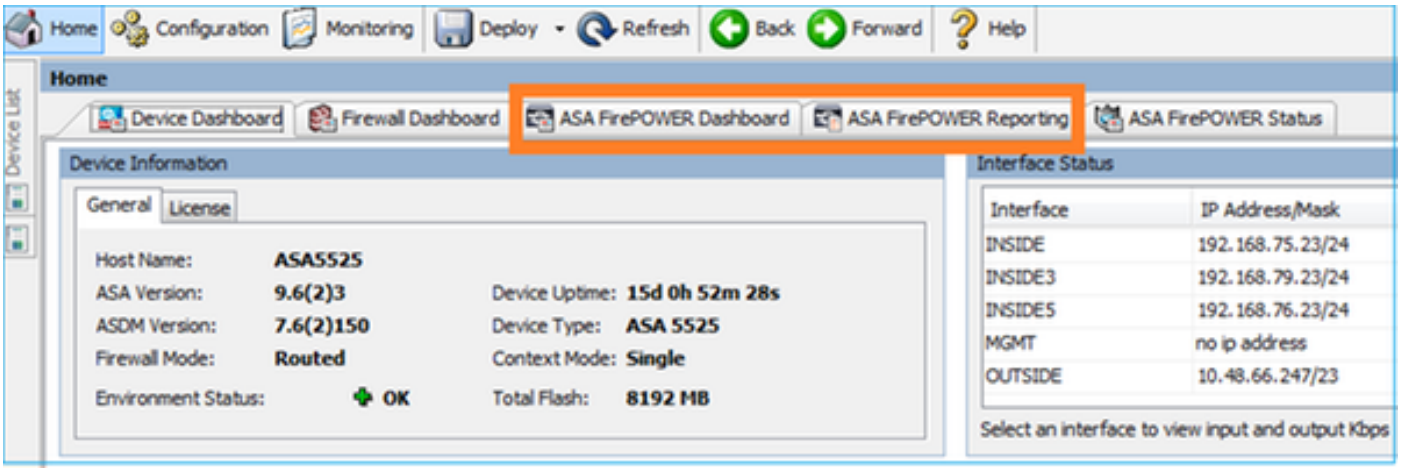


Шаг 4? ASDM получает Элементы меню FirePOWER

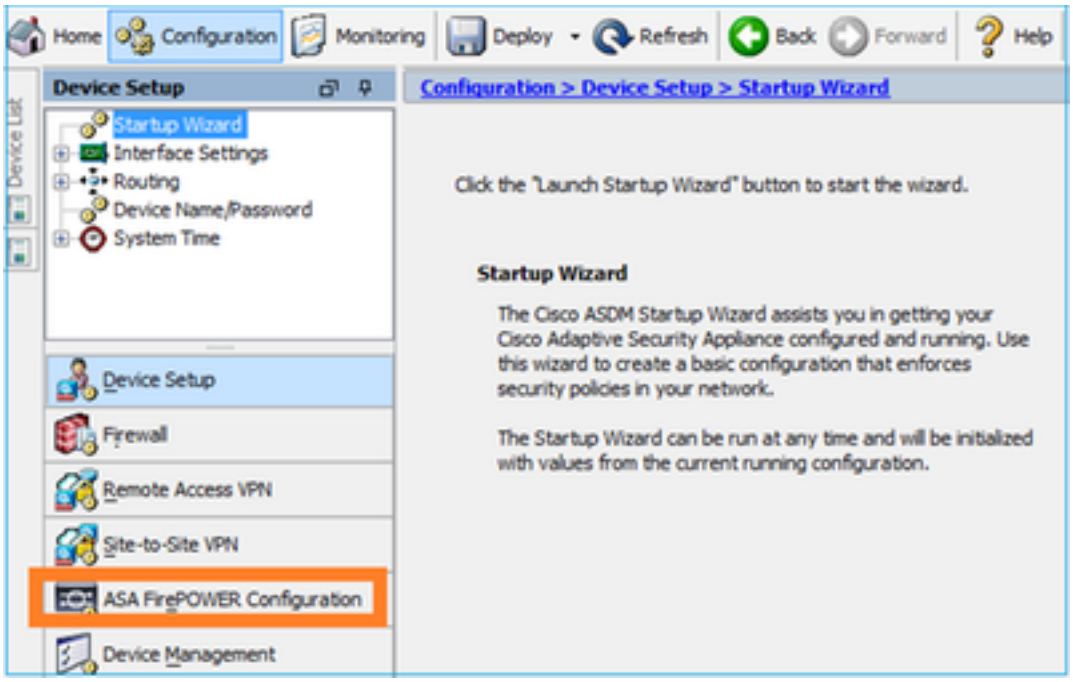
После успешной аутентификации ASDM получает из FirePOWER Элементы меню:



Полученные вкладки:

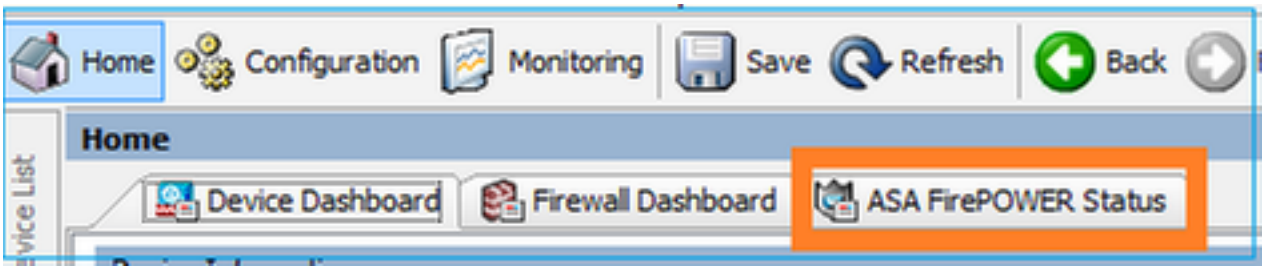


Это также получает элемент ASA FirePOWER Меню конфигурации:

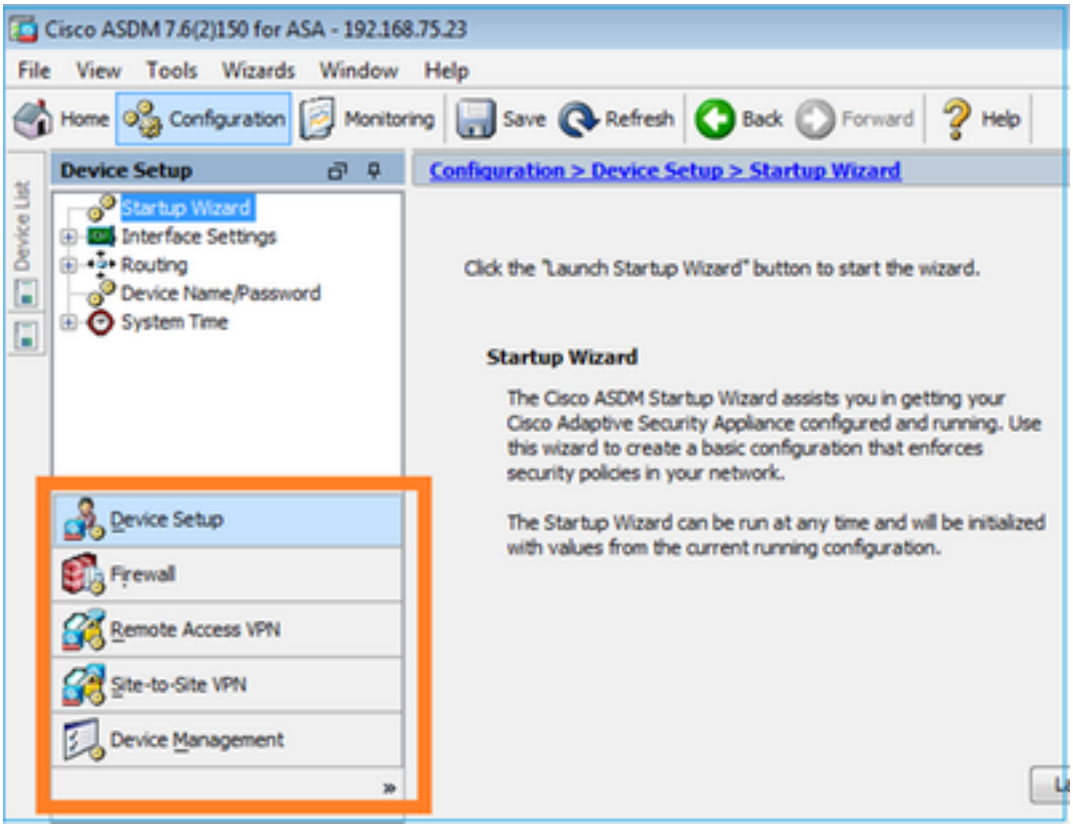


Устранение неисправностей

В случае, если ASDM не может установить туннель SSL с IP - управлением FP тогда, это только загрузит следующий Элемент меню FirePOWER:



Элемент конфигурации ASA FirePOWER будет отсутствовать также:



Рекомендуемые действия

Проверка 1

Удостоверьтесь, что интерфейс управления ASA подключен, UP и порт коммутатора, связанный с ним, находятся в надлежащей VLAN:

```
ASA5525# show interface ip brief | include Interface|Management0/0Interface IP-Address OK?
Method Status ProtocolManagement0/0 unassigned YES unset up up
```

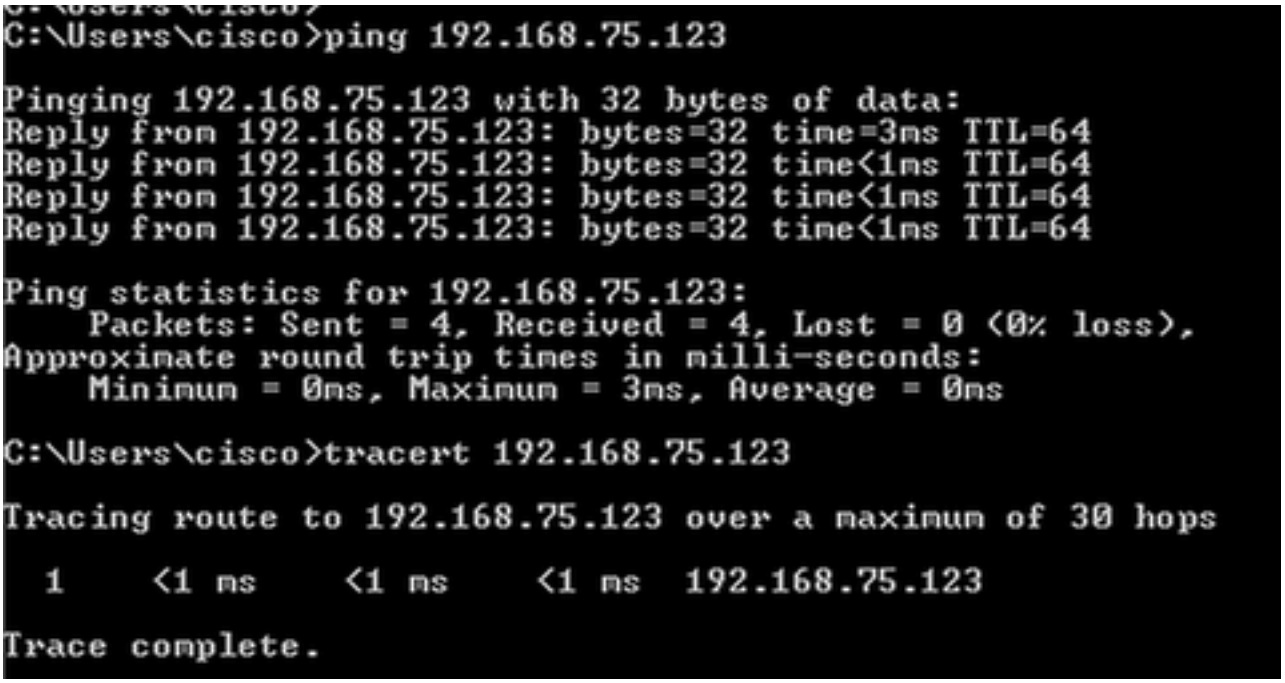
Проверка 2

Удостоверьтесь, что модуль FirePOWER полностью инициализируется, UP и выполнение:

```
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 A5525# session sfr consoleOpening 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-d6ca846264e3Rules update version : 2016-03-28-001-
vrtVDB version : 270---------------------------------------------------->
```

Проверка 3

Проверьте основное подключение между хостом ASDM и IP - управлением модуля FirePOWER при помощи программных средств как **эхо-запрос** и **tracert/traceroute:**



Проверка 4

Если хост ASDM и IP - управление FirePOWER находятся в той же проверке сети L3 таблица ARP на хосте 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
```

Проверка 5

Включите перехват на устройстве ASDM, в то время как вы соединяетесь через ASDM, чтобы видеть, существует ли надлежащий TCP - взаимодействие между хостом и модулем FirePOWER. В минимуме необходимо видеть:

- Трехстороннее квитирование TCP между хостом ASDM и ASA
- Туннель SSL, установленный между хостом ASDM и ASA
- Трехстороннее квитирование TCP между хостом ASDM и IP - управлением модуля FirePOWER
- Туннель SSL, установленный между хостом ASDM и IP - управлением модуля FirePOWER

Проверка 6

Для проверки трафика к и от модуля FirePOWER, можно включить перехват на интерфейсе asa_mgmt_plane. В перехвате ниже его может быть замечен:

- Запрос ARP от хоста ASDM (пакет 42)
- Ответ ARP от модуля FirePOWER (пакет 43)
- Трехстороннее квитирование TCP между хостом ASDM и модулем FirePOWER (пакеты 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
```

Проверка 7

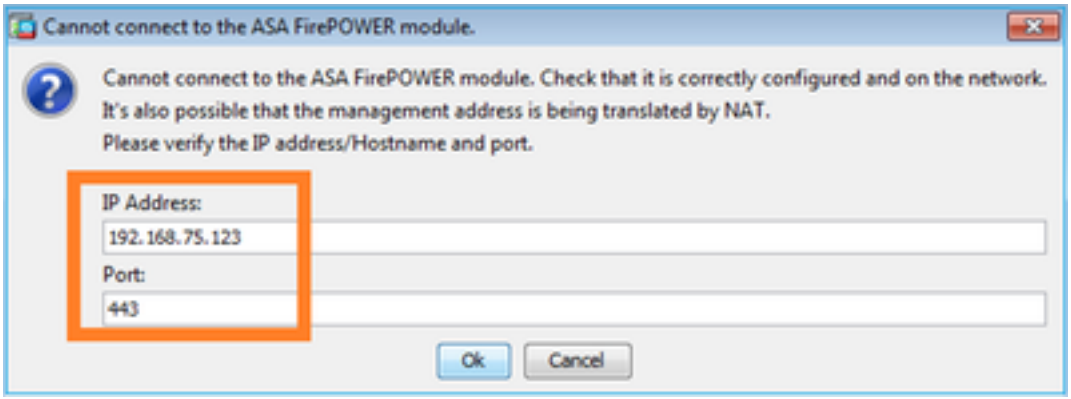
Проверьте, что у пользователя ASDM есть уровень привилегий 15. Один способ

подтвердить это путем выполнения **http 255 отладки** при соединении через 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]
```

Проверка 8

Если между хостом ASDM и модулем FirePOWER там NAT для IP - управления Огневой мощи тогда, необходимо задать преобразованного посредством NAT IP:



Проверка 9

Удостоверьтесь, что модулем FirePOWER уже не управляет Центр управления огневой мощи (FMC), потому что в этом случае будут отсутствовать вкладки FirePOWER в ASDM:

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

Иначе:

```
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
```

Проверка 10

Проверьте в Руководстве по совместимости ASA, что ASA/ОБРАЗЫ ASDM совместим:

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

Проверка 11

Проверьте в Руководстве по совместимости Огневой мощи, что устройство FirePOWER совместимо с версией ASDM:

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

Дополнительная документация

Cisco ASA Краткое руководство по началу работы модуля FirePOWER

ASA с руководством по конфигурации локального управления FirePOWER Services, версией 6.1.0

Руководство пользователя ASA FirePOWER модуля для ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X, и ASA5516-X, версии 5.4.1