ASA の FirePOWER モジュールを管理する ASDM の使用

目次

概要

ASA でインストールされている FirePOWER モジュールは次のいずれか管理することができます :

- Firepower Management Center （ FMC ） –これはオフ・ ボックス マネジメントソリューションです
- Adaptive Security Device Manager （ ADSM ） –これはオン・ ボックス マネジメントソリューションです

この資料の目標は ASDM ソフトウェアがそれでインストールされる ASA および FirePOWER ソフトウエアモジュールとどのように通信するか説明することです。

使用するコンポーネント

- Windows 7 ホスト
- ASA 9.6.2-3 コードを実行する ASA5525-X
- ASDM ソフトウェア 7.6.2.150
- FirePOWER ソフトウエアモジュール 6.1.0-330

前提条件

ASDM 管理を有効に する ASA 設定:

```
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
```

さらに、ASA で 3DES/AES ライセンスはイネーブルになるはずです:

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

アーキテクチャ

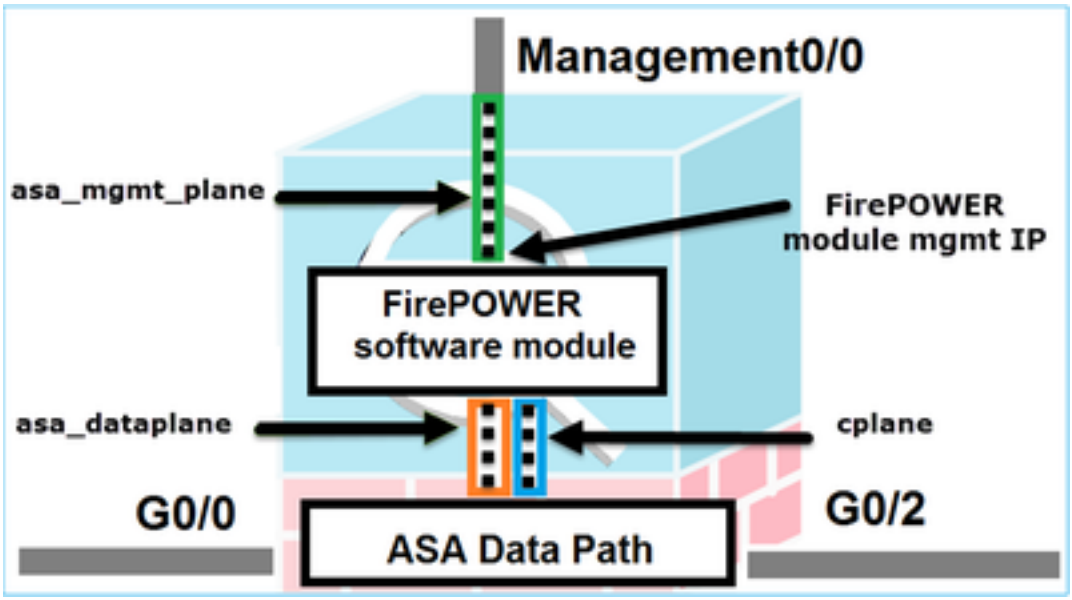
ASA に 3 つの内部 インターフェースがあります:

- asa_dataplane = ASA データパスから FirePOWER ソフトウエアモジュールにパケットをリダイレクトすることを使用します
- asa_mgmt_plane = それは FirePOWER マネージメントインターフェイスがネットワークと通信するように使用されます
- cplane = ASA と FirePOWER モジュールの間でキープアライブを転送するのに使用するコントロール プレーン インターフェイス

すべての内部 インターフェースのトラフィックをキャプチャ することができます:

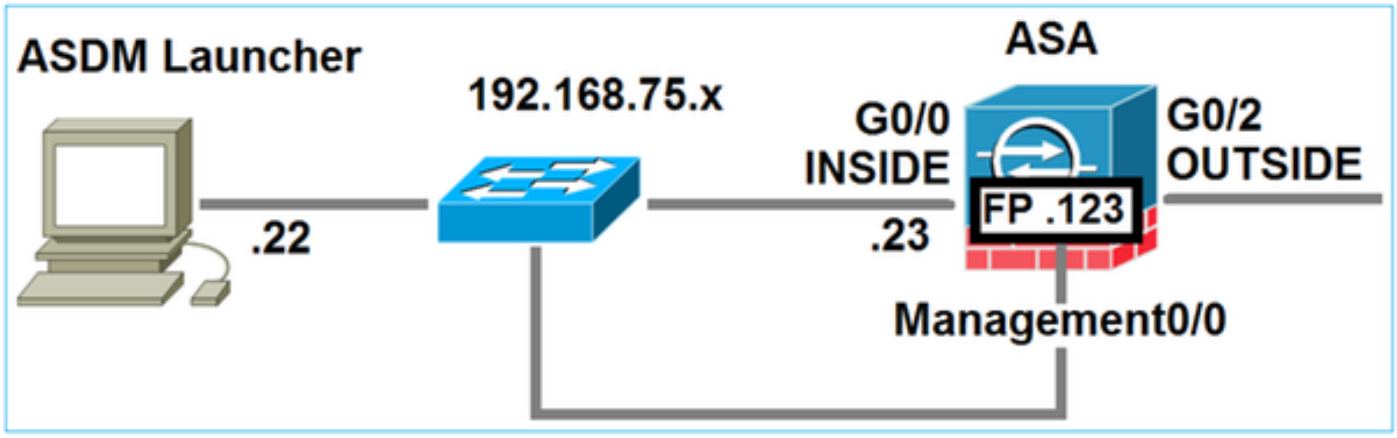
```
ASA5525# capture CAP interface ?

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

上は次の通り視覚化することができます:



ユーザが ASDM によって ASA に接続する場合のバックグラウンド操作

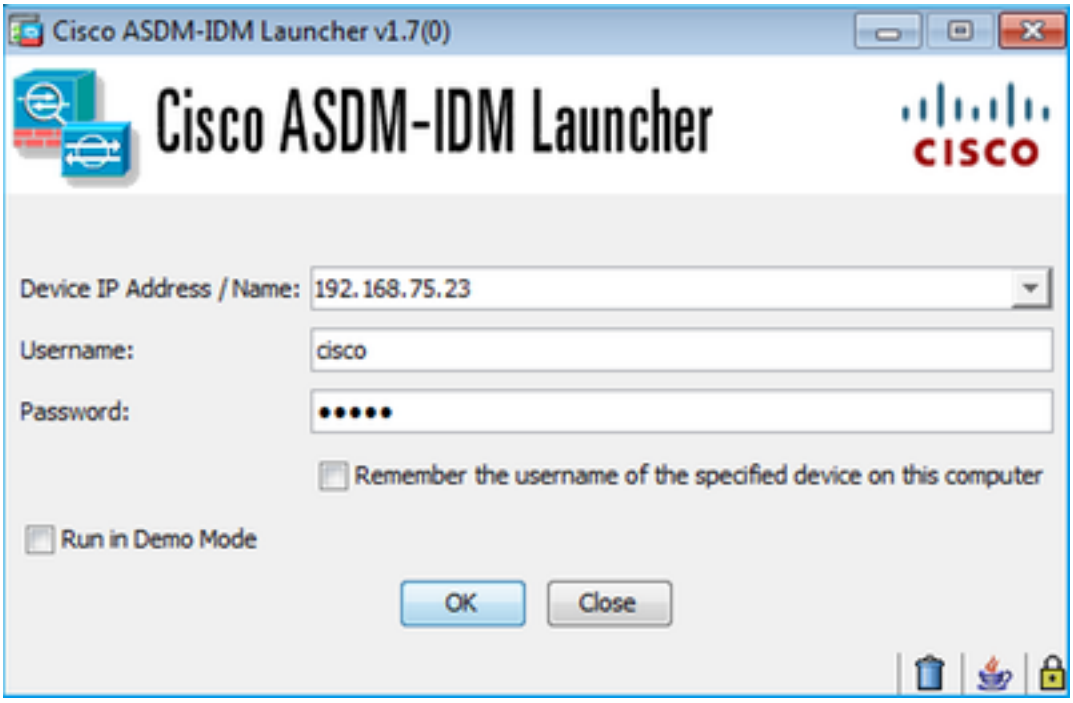
次のトポロジーを考慮して下さい



ユーザが ASA への ASDM 接続を開始する場合次のイベントは発生します:

ステップ 1 –ユーザは ASDM 接続を開始します

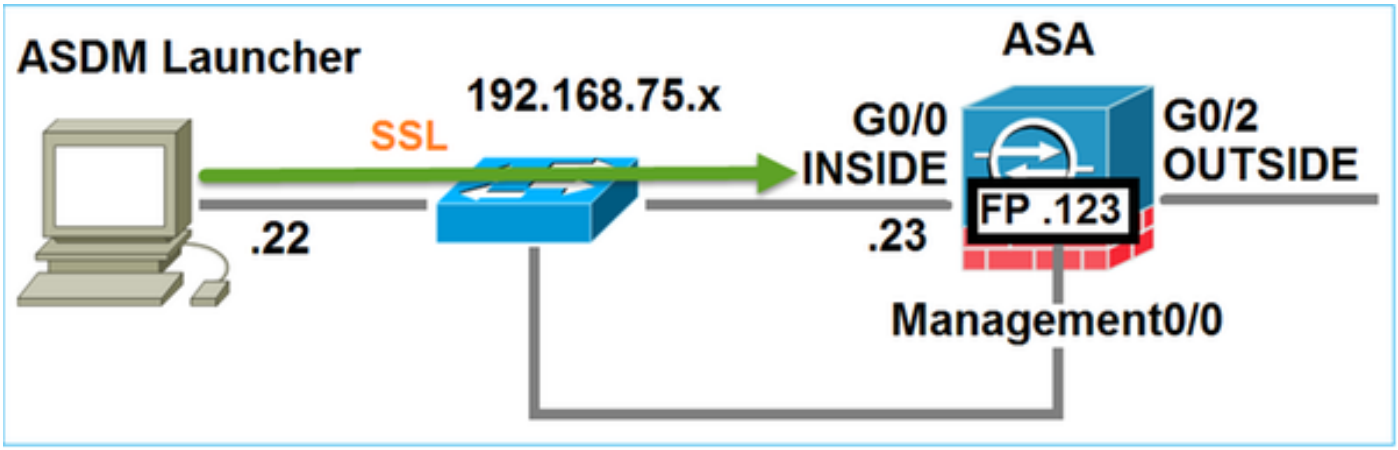
ユーザは HTTP 管理に使用する ASA IP を規定 し、信任状を入力し、ASA の方の接続を開始します:



バックグラウンドで ASDM と ASA 間の SSL トンネルは確立されます:

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

これは次の通り視覚化することができます:



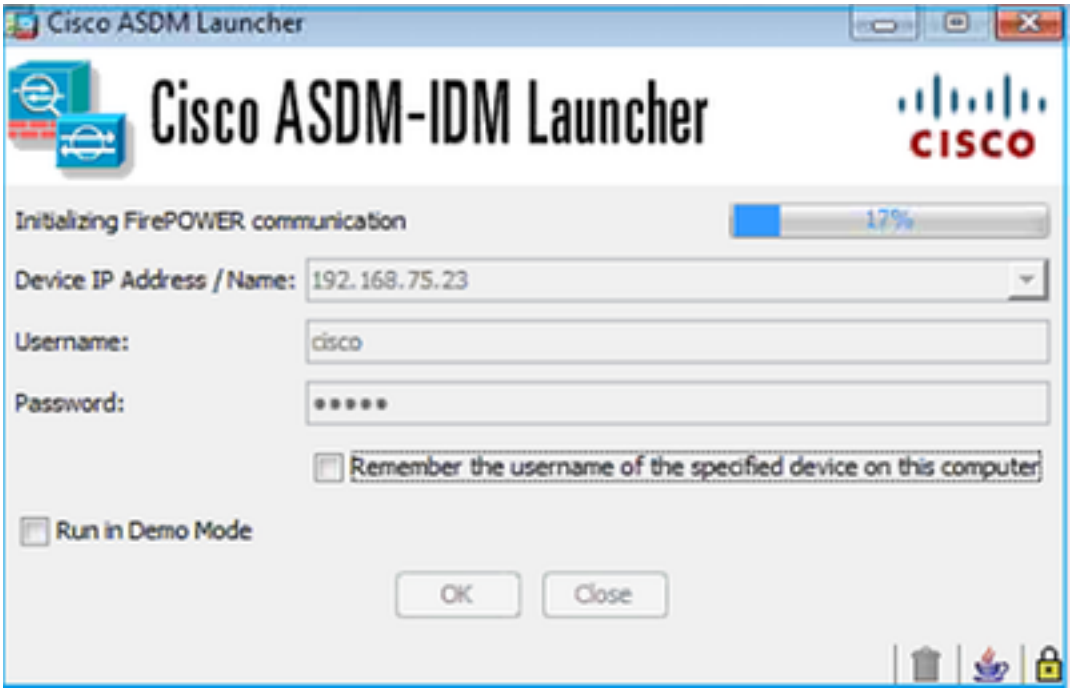
ステップ 2 – ASDM は ASA 設定および FirePOWER モジュール IP を検出します

ASA の**デバッグ http 255 を**イネーブルにすることは ASDM が ASA に接続する場合バックグラウンドで行われるすべてのチェックを示します:

```
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
```

- show module は = ASDM ASA モジュールを検出します
- show module sfr は = ASDM 検出します FirePOWER 管理 IP を含むモジュール詳細を詳述します

上は ASA IP の方の PC からの一連の SSL 接続としてバックグラウンドで見られます:



```
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
```

ステップ 3 – ASDM は FirePOWER モジュールの方の通信を始めます

ASDM は FirePOWER 管理 IP を知っているのでモジュールの方の SSL セッションを始めます:

Initializing FirePOWER communication 17%

Device IP Address / Name: 192.168.75.23

Username: cisco

Password: *****

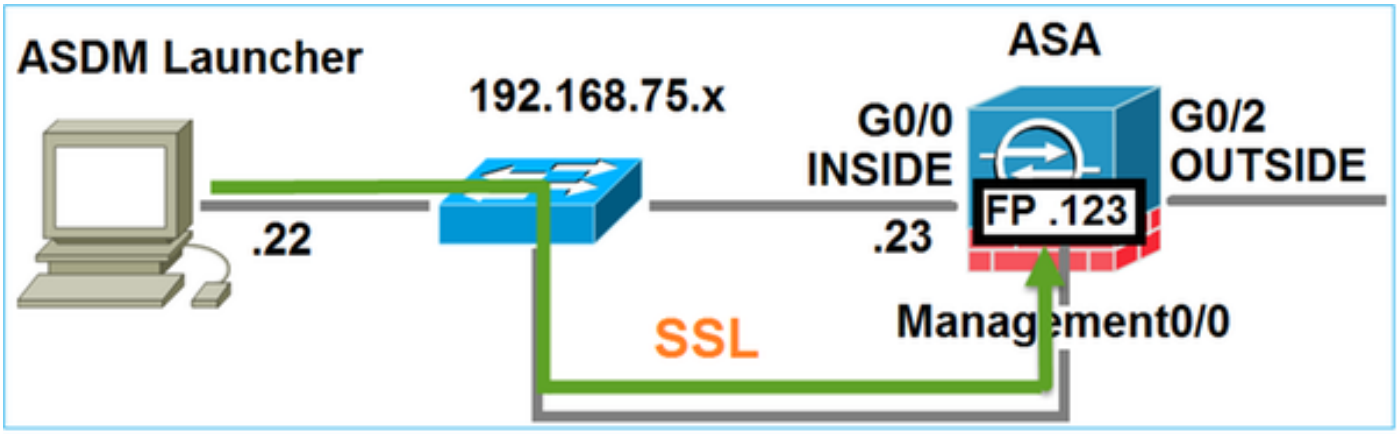
☐ Remember the username of the specified device on this computer

☐ Run in Demo Mode

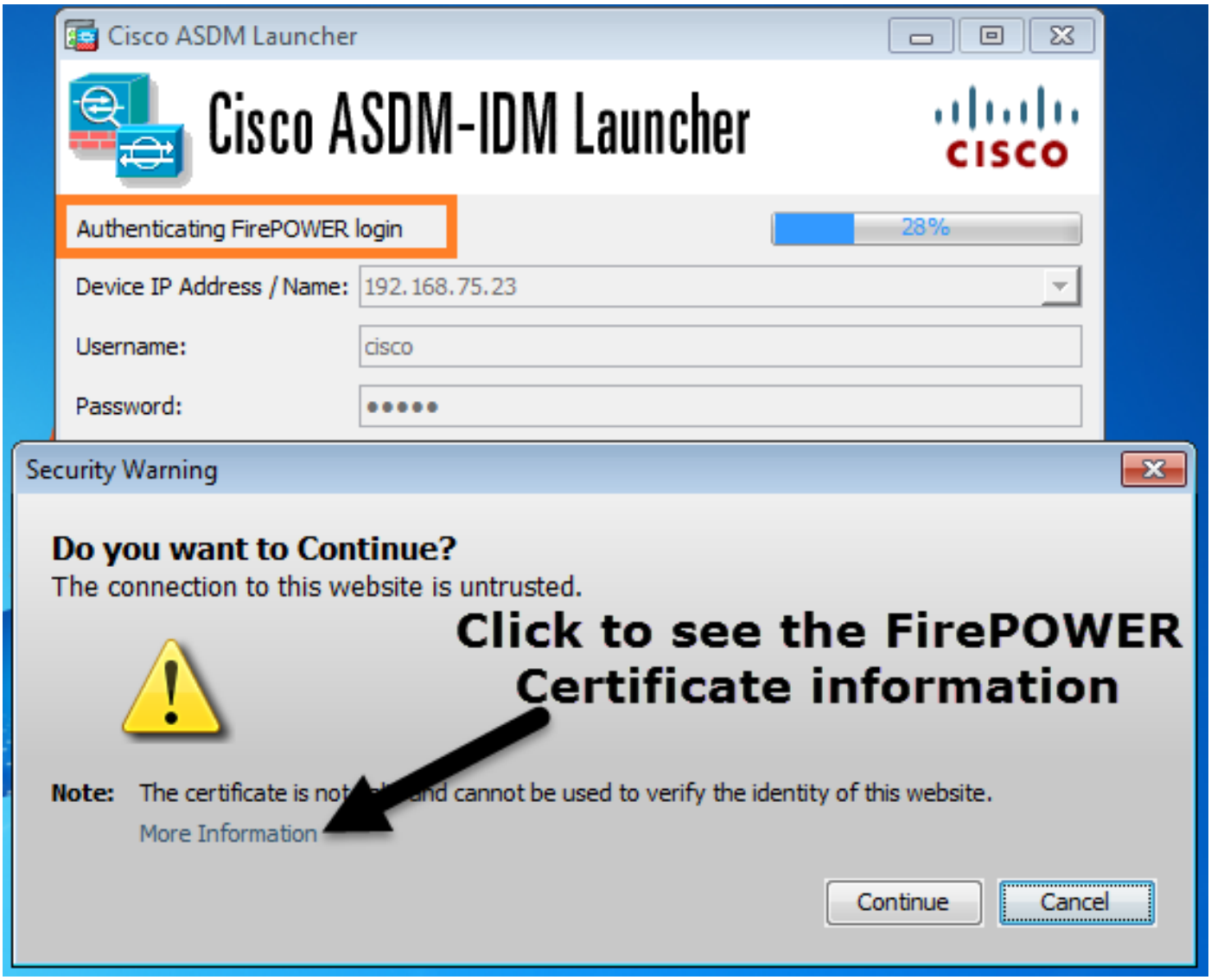
上はバックグラウンドで FirePOWER 管理 IP の方の ASDM ホストからの SSL 接続ように見られます:

```
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
```

これは次の通り視覚化することができます:

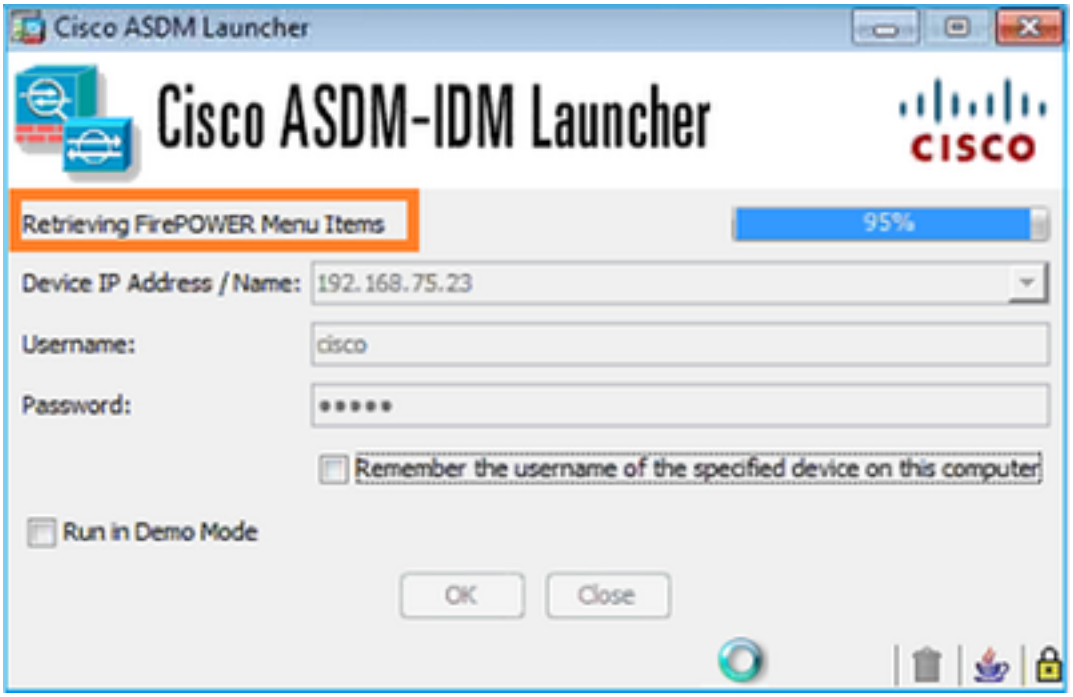


ASDM は FirePOWER を認証し、FirePOWER 証明書が自己署名であるのでセキュリティ警告は示されています:

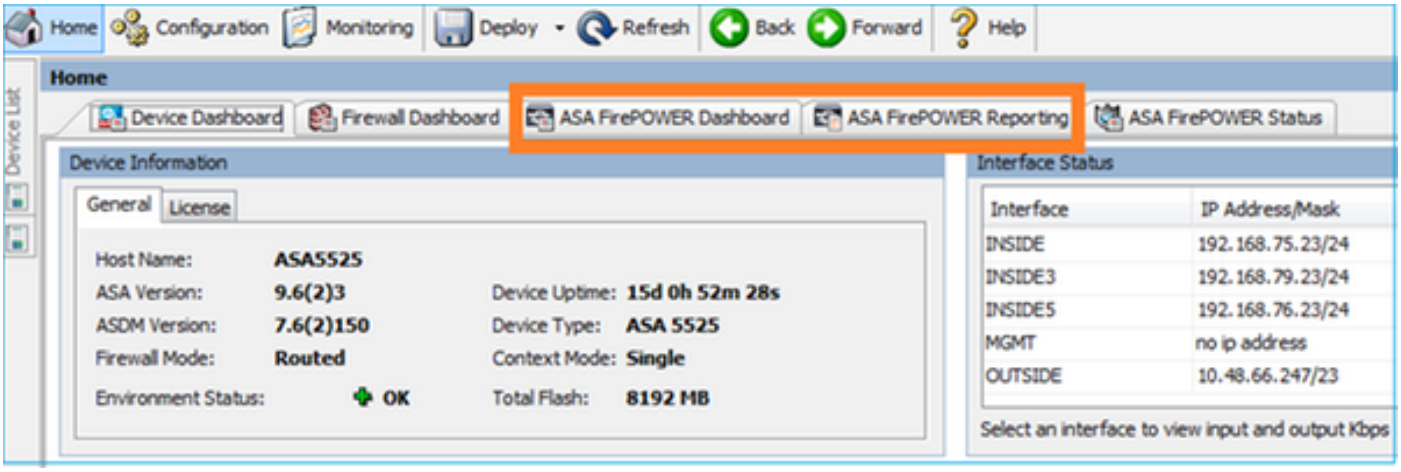


ステップ 4 – ASDM は FirePOWER メニュー項目を取得します

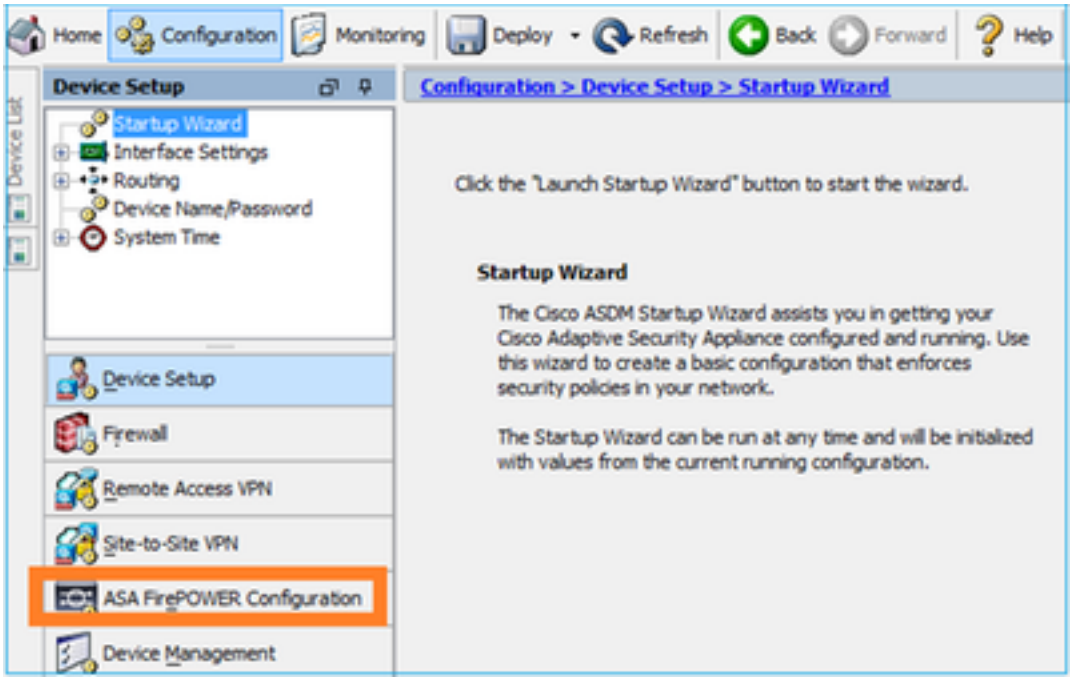
認証の成功の後で ASDM は FirePOWER からメニュー項目を取得します:



取得されたタブ:

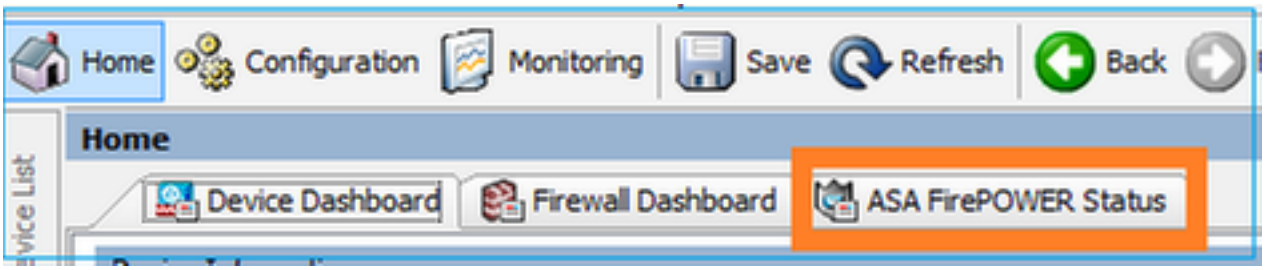


それはまた ASA FirePOWER Configuration メニュー項目を取得します:

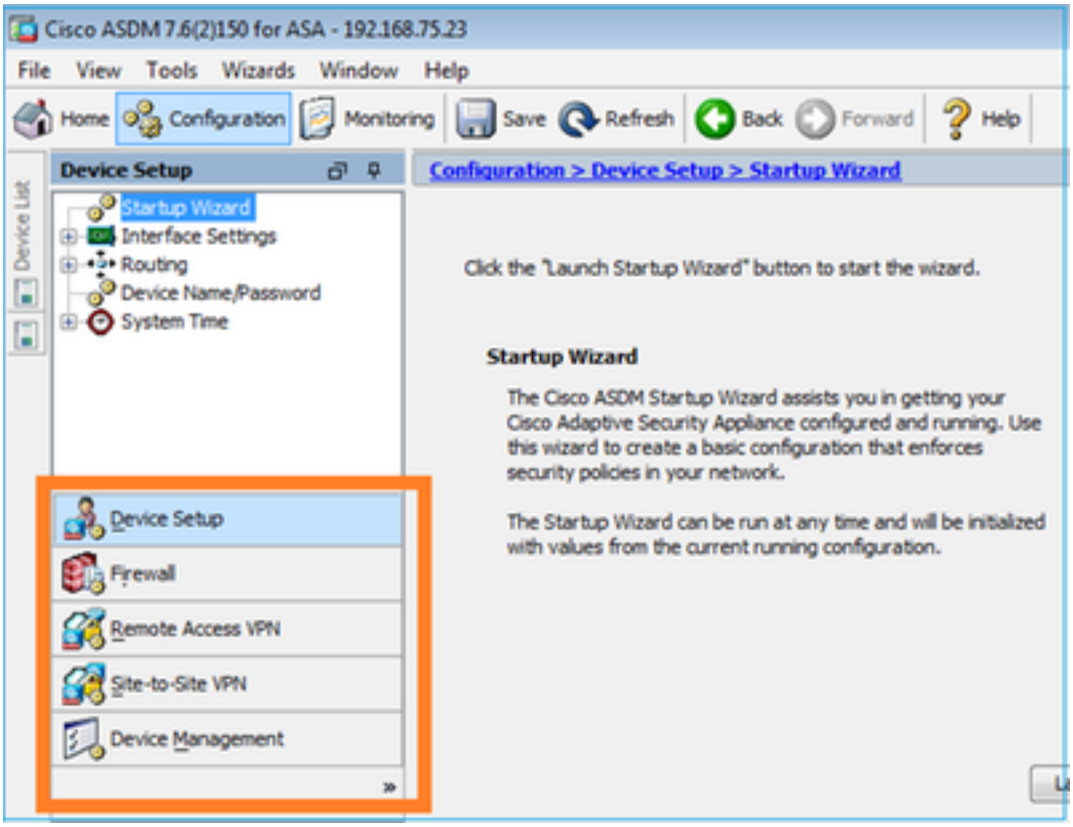


トラブルシューティング

ASDM がそして FP 管理 IP の SSL トンネルを確立できなければ FirePOWER 次のメニュー項目だけをロードします:



ASA FirePOWER コンフィギュレーションアイテムは同様に抜けています:



推奨 処置

確認 1

ASA マネージメントインターフェイスがアップであるそれに接続されるスイッチポートあります 適切な VLAN にことを確かめれば:

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

確認 2

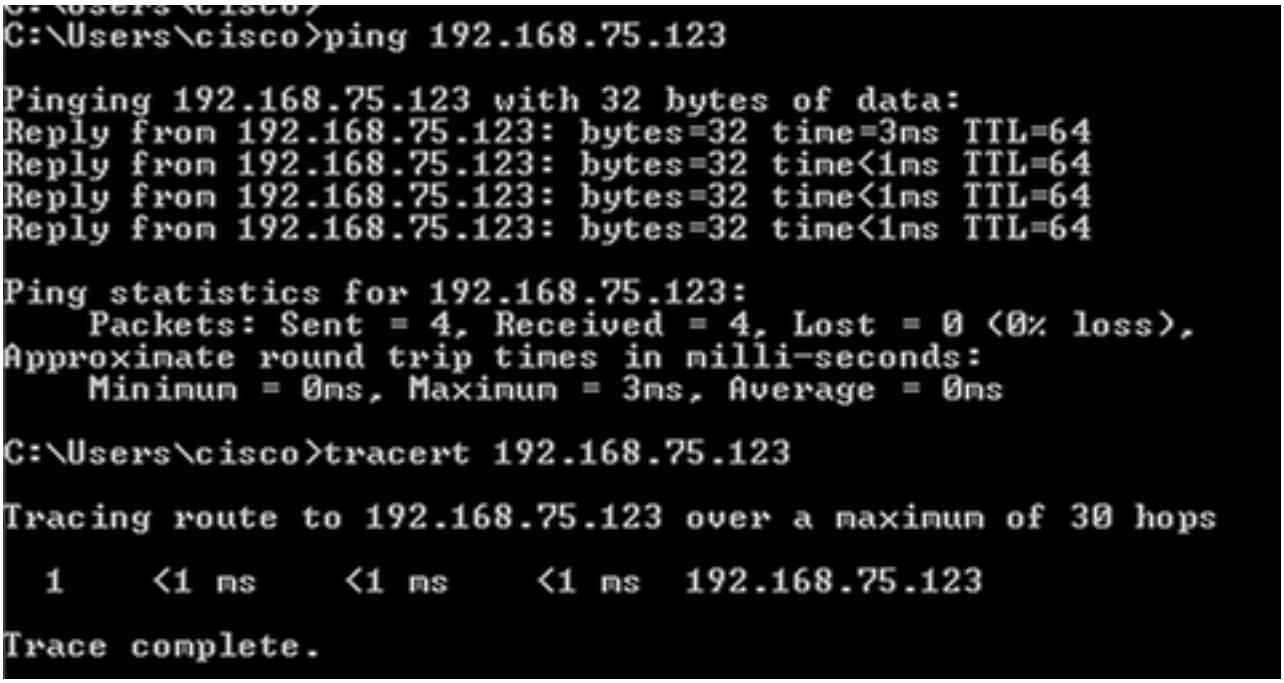
作動中ことをことを FirePOWER モジュール十分に初期化される確かめて下さい:

```
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
----------------------------------------------------

>
```

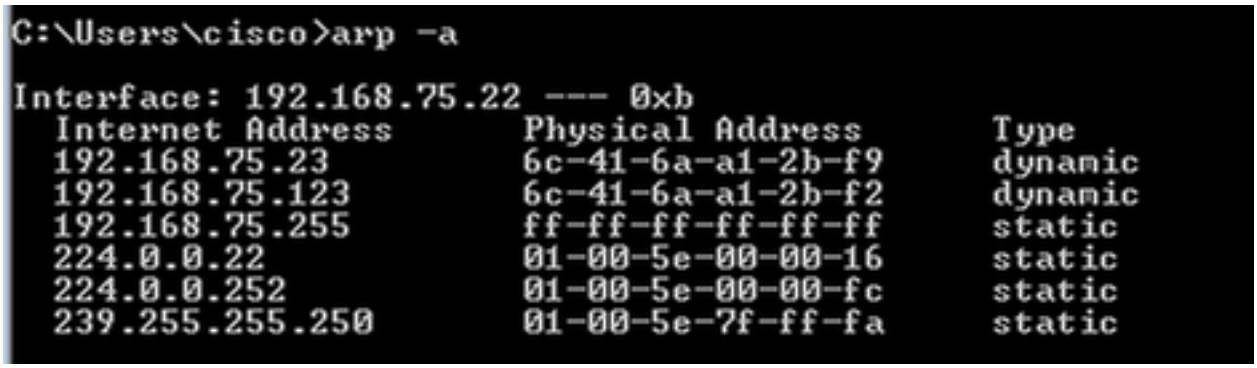
確認 3

ping および tracert/traceroute のようなツールの使用によって ASDM ホストと FirePOWER モジュール管理 IP 間の基本的な接続をチェックして下さい:



確認 4

ASDM ホストおよび FirePOWER 管理 IP が同じ L3 ネットワーク チェックに ASDM ホストの ARPテーブルなら:



確認 5

ホストと FirePOWER モジュール間に適切な TCP 通信があるかどうか見るために ASDM によって接続している間 ASDM デバイスのイネーブル キャプチャ。 少くとも見るはずです:

- ASDM ホストと ASA 間の TCP 三方ハンドシェイク
- ASDM ホストと ASA の間で確立される SSL トンネル
- ASDM ホストと FirePOWER モジュール管理 IP 間の TCP 三方ハンドシェイク
- ASDM ホストと FirePOWER モジュール管理 IP の間で確立される SSL トンネル

確認 6

トラフィックを FirePOWER モジュールに出入してチェックするために asa_mgmt_plane インターフェイスのキャプチャを有効に することができます。 それの下のキャプチャで見られる場合があります:

- ASDM ホスト (42) パケットからの ARP要求
- FirePOWER モジュール (43) パケットからの ARP応答
- ASDM ホストと FirePOWER モジュール (パケット 44-46) 間の TCP 三方ハンドシェイク

```
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
```

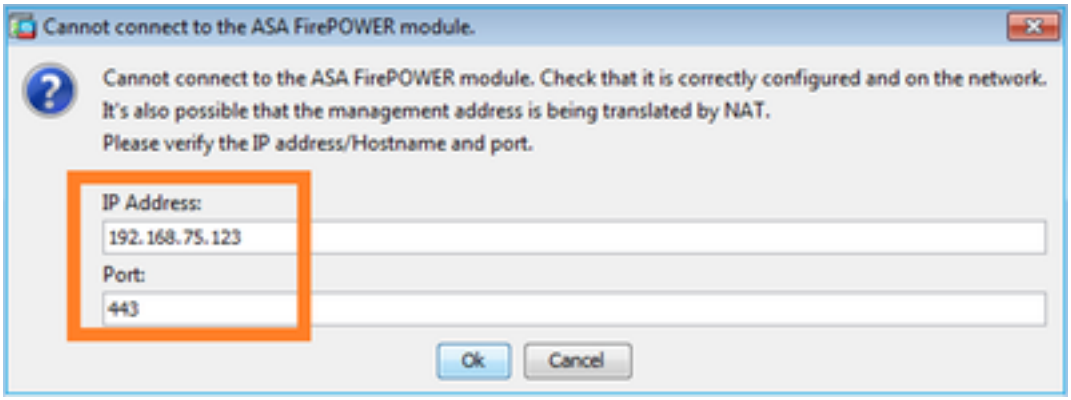
確認 7

ASDM ユーザは特権レベル 15 があることを確認して下さい。 これを確認する 1 つの方法は**デバッグ http 255 の**実行によって ASDM によって接続している間行います:

```
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]
```

確認 8

ASDM ホストと FirePOWER モジュール間に Firepower 管理 IP のための NAT がそしてネットワークアドレス交換された IP を規定 する必要あれば:



確認 9

FirePOWER が ASDM に記録するそのケースで抜けていて下さいので FirePOWER モジュールが Firepower Management Center （ FMC ）によってまだ管理されていないことを確かめて下さい:

```
ASA5525# session sfr console
Opening console session with module sfr.
```

```
Connected to module sfr. Escape character sequence is 'CTRL-^X'.
> show managers
Managed locally.

>
```

別の方法:

```
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
```

確認 10

ASA/ASDM イメージが互換性があることを ASA 互換性ガイドで確認して下さい:

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

確認 11

FirePOWER デバイスが ASDM バージョンと互換性があることを Firepower 互換性ガイドで確認して下さい:

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

関連資料

Cisco ASA FirePOWER モジュール クイック スタート ガイド

FirePOWER サービス ローカル管理 コンフィギュレーション ガイドが付いている ASA、バージョン 6.1.0

ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X および ASA5516-X のための ASA FirePOWER モジュール ユーザガイド、バージョン 5.4.1