

Usando o ASDM para controlar um módulo de FirePOWER no ASA

Índice

[Introdução](#)

[Componentes usados](#)

[Pré-requisitos](#)

[Arquitetura](#)

[Operação de fundo quando um usuário conectar ao ASA através do ASDM](#)

[Etapa 1 – O usuário inicia a conexão ASDM](#)

[Etapa 2 – O ASDM descobre a configuração ASA e o IP do módulo de FirePOWER](#)

[Etapa 3 – O ASDM inicia uma comunicação para o módulo de FirePOWER](#)

[Etapa 4 – O ASDM recupera os itens de menu de FirePOWER](#)

[Troubleshooting](#)

[Ações recomendadas](#)

[Documentos relacionados](#)

Introdução

Um módulo de FirePOWER que seja instalado no ASA pode ser controlado por qualquer um:

- Centro de gerenciamento de FirePOWER (FMC) – Esta é a solução de gerenciamento da fora-caixa
- Security Device Manager adaptável (ASDM) – Esta é a solução de gerenciamento da em-caixa

O objetivo deste documento é explicar como o software ASDM se comunica com o ASA e um módulo de software de FirePOWER instalados nele.

Componentes usados

- Um host de Windows 7
- ASA5525-X que executa o código ASA 9.6.2-3
- Software ASDM 7.6.2.150
- Módulo de software 6.1.0-330 de FirePOWER

Pré-requisitos

Configuração ASA para permitir o Gerenciamento 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

```

Adicionalmente, no ASA a licença 3DES/AES deve ser permitida:

```

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

```

Arquitetura

O ASA tem 3 interfaces internas:

- **asa_dataplane** = é usado para reorientar pacotes do trajeto de dados ASA ao módulo de software de FirePOWER
- **asa_mgmt_plane** = é usado para permitir que a interface de gerenciamento de FirePOWER comunique-se com a rede
- **cplane** = relação plana do controle que é usada para transferir o Keepalives entre o ASA e o módulo de FirePOWER

Você pode capturar o tráfego em todas as interfaces internas:

```

ASA5525# capture CAP interface ?

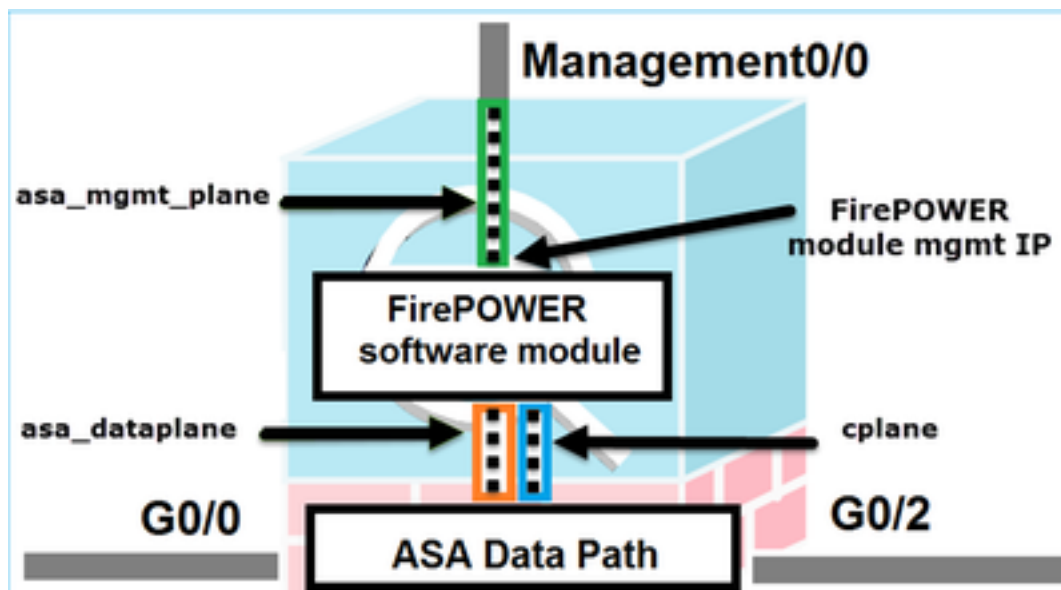
```

```

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

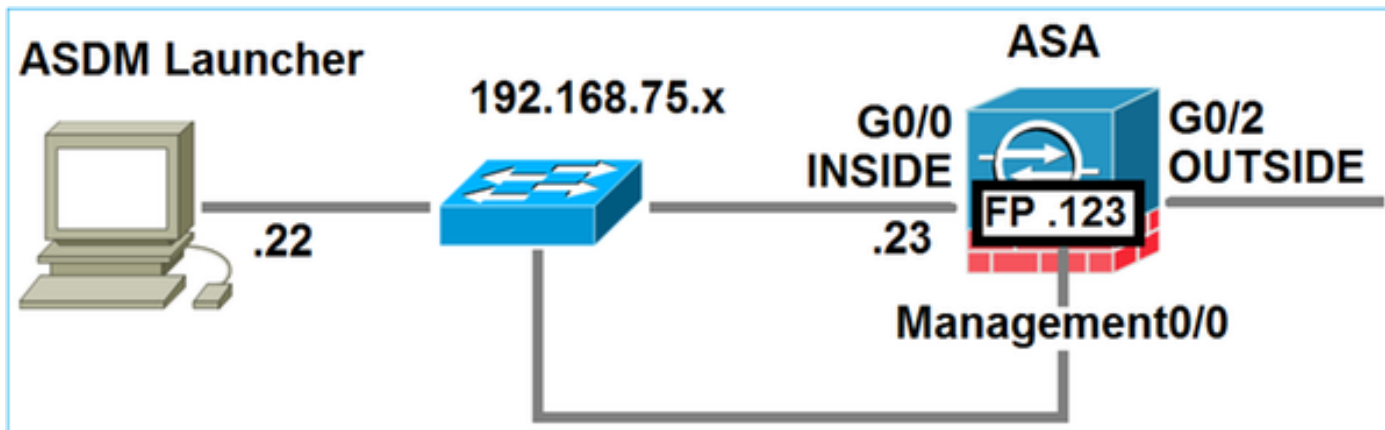
```

O acima pode ser visualizado como segue:



Operação de fundo quando um usuário conectar ao ASA através do ASDM

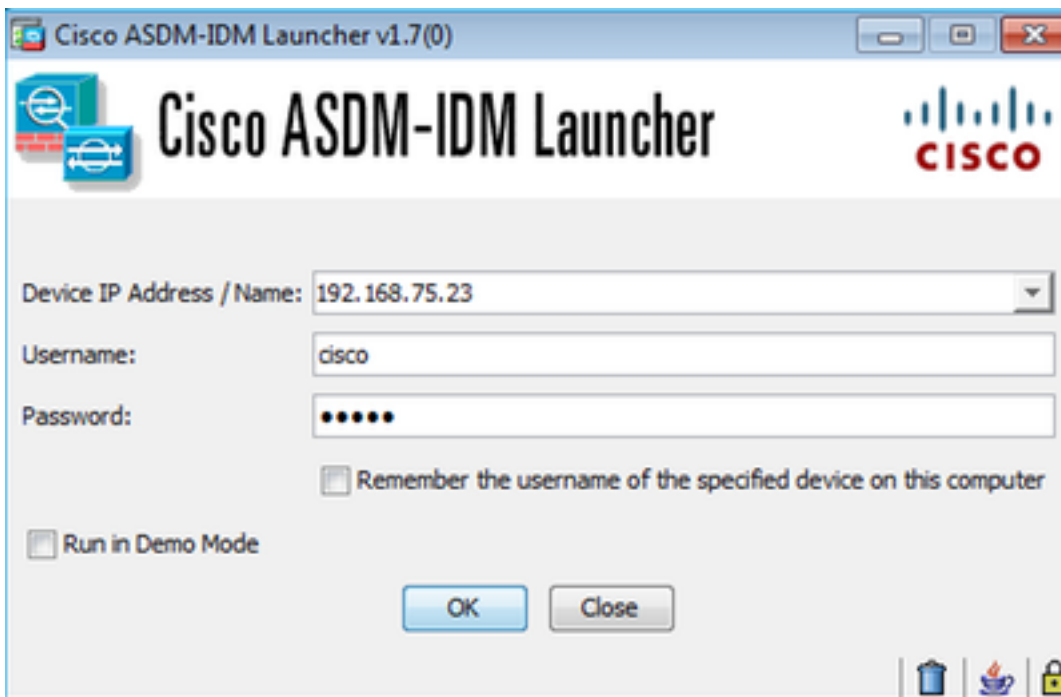
Considere a seguinte topologia



Quando um usuário inicia uma conexão ASDM ao ASA os seguintes eventos ocorrerão:

Etapa 1 – O usuário inicia a conexão ASDM

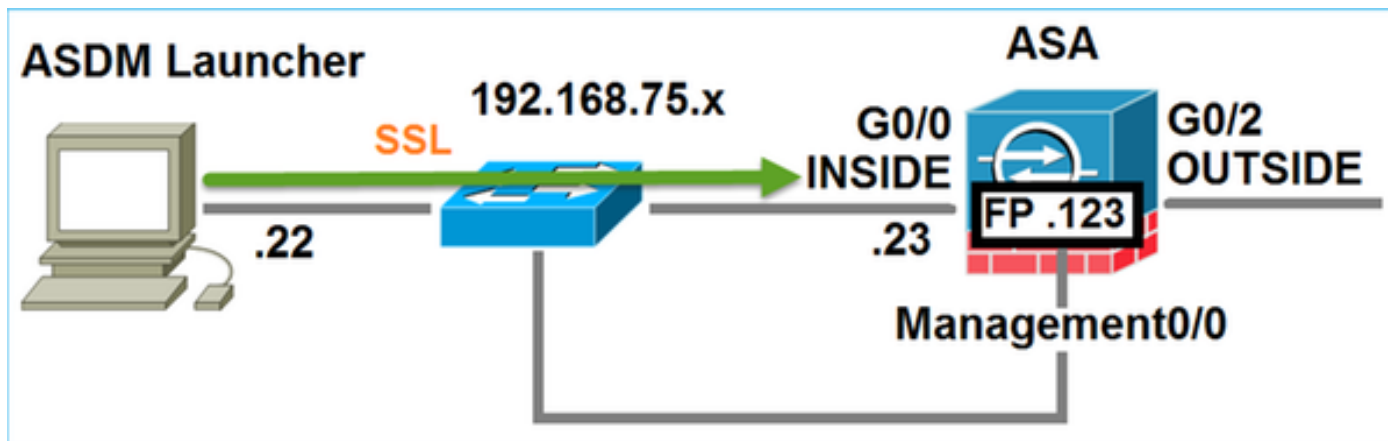
O usuário especifica o IP ASA usado para o Gerenciamento HTTP, incorpora as credenciais e inicia uma conexão para o ASA:



No fundo um túnel SSL entre o ASDM e o ASA é estabelecido:

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

Isto pode ser visualizado como segue:



Etapa 2 – O ASDM descobre a configuração ASA e o IP do módulo de FirePOWER

Permitir **debuga HTTP 255** no ASA mostrará todas as verificações que estão feitas no fundo quando o ASDM conecta ao 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
```

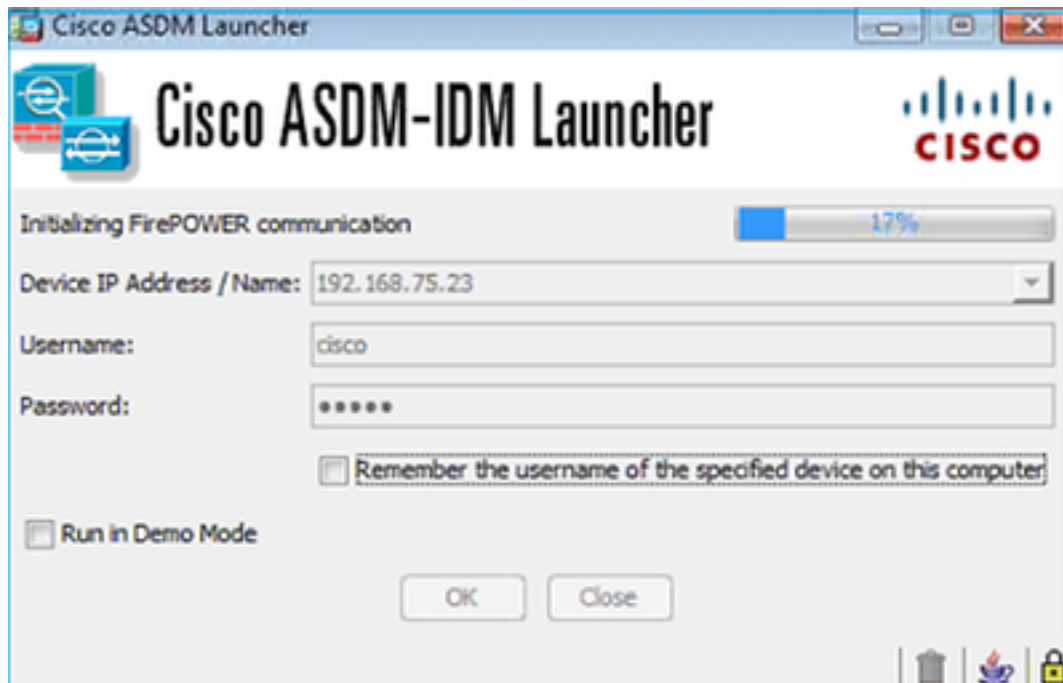
- o módulo show = O ASDM descobre os módulos ASA
- os detalhes do sfr do módulo show = O ASDM descobrem os detalhes do módulo que incluem o IP de gerenciamento de FirePOWER

O acima será visto no fundo como uma série de conexões SSL do PC para o 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	192.168.75.123	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

Etapa 3 – O ASDM inicia uma comunicação para o módulo de FirePOWER

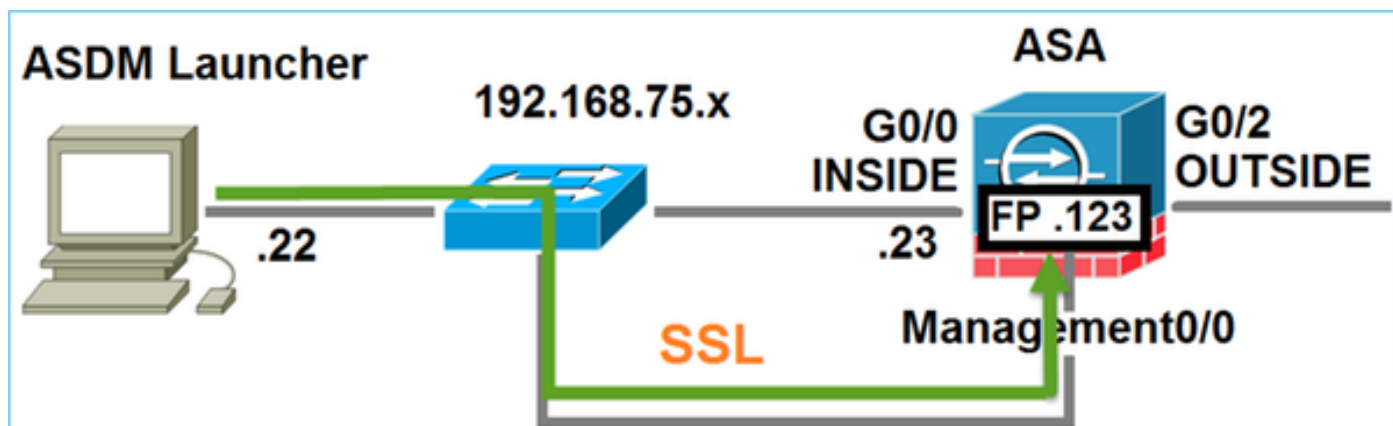
Desde que o ASDM conhece o IP de gerenciamento de FirePOWER inicia sessões de SSL para o módulo:



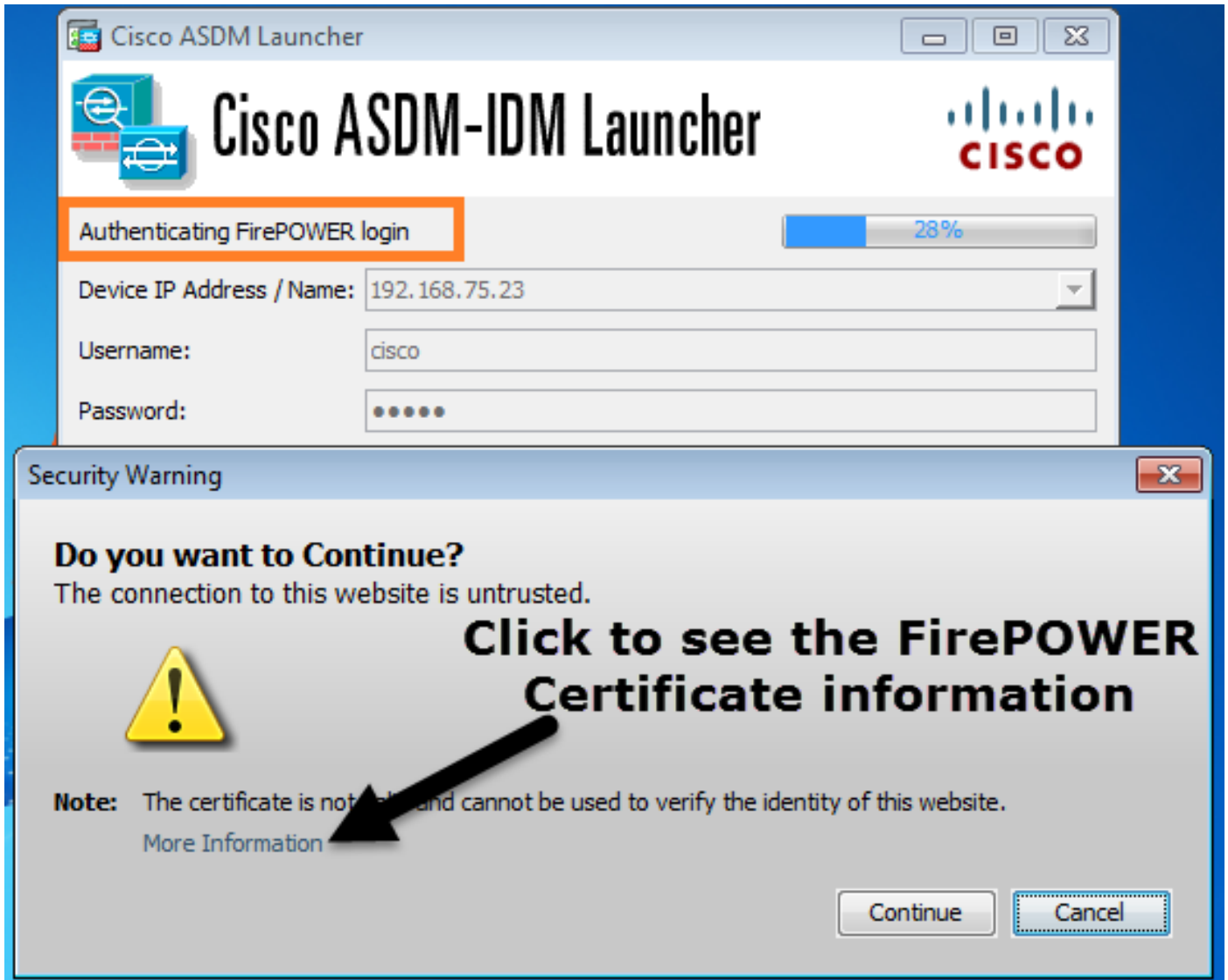
O acima será visto no fundo como conexões SSL do host ASDM para o IP de gerenciamento de FirePOWER:

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	

Isto pode ser visualizado como segue:

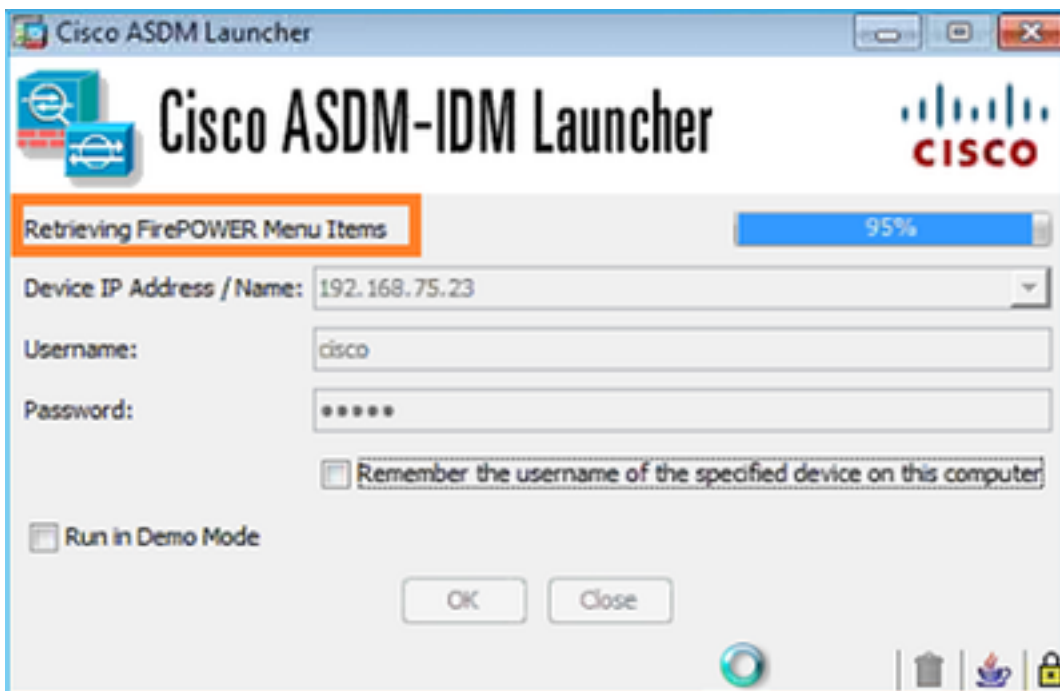


O ASDM autentica FirePOWER e um aviso da Segurança é mostrado desde que o certificado de FirePOWER auto-é assinado:

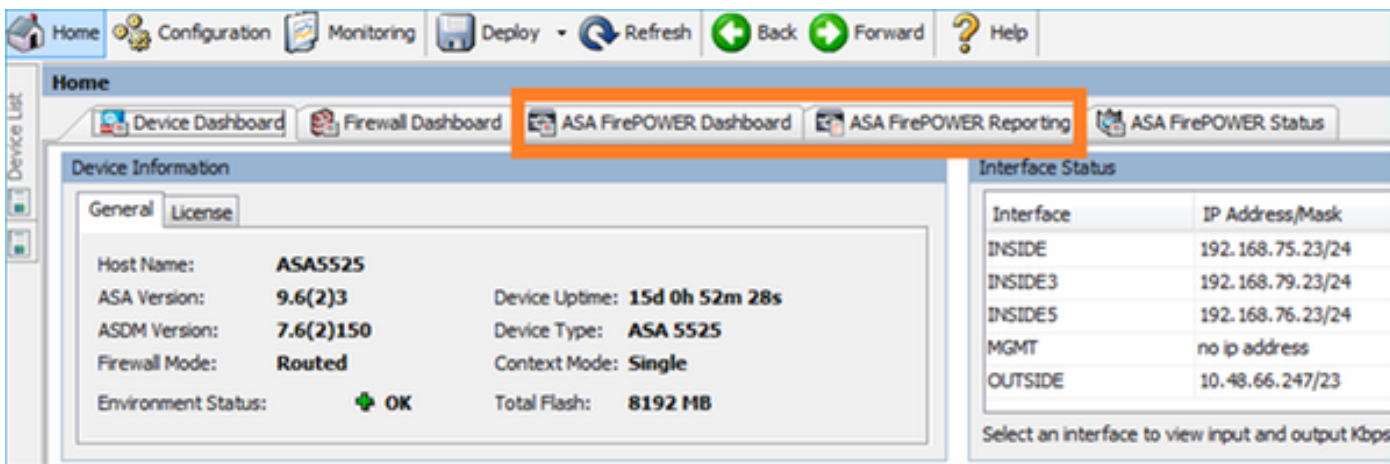


Etapa 4 – O ASDM recupera os itens de menu de FirePOWER

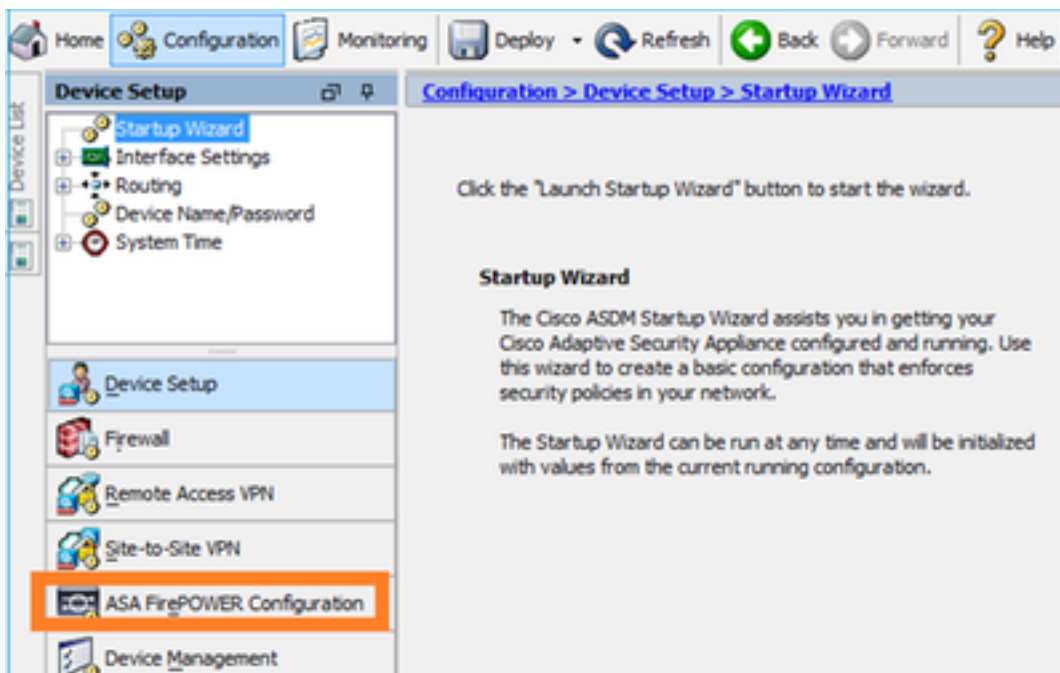
Após a autenticação bem sucedida o ASDM recupera de FirePOWER os itens de menu:



As abas recuperadas:

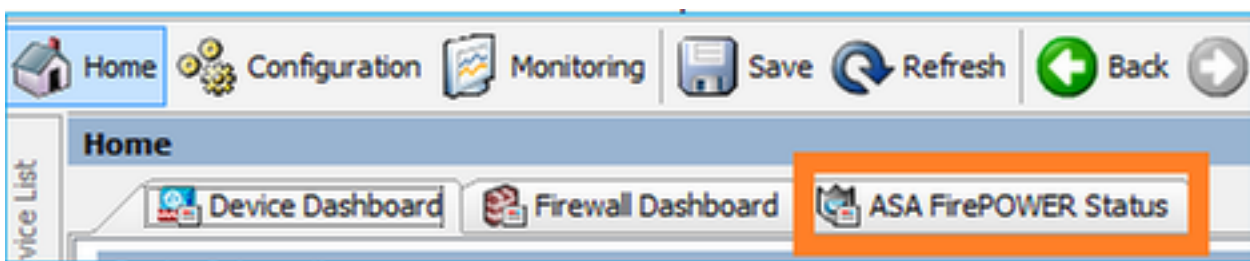


Igualmente recupera o artigo de menu de configuração ASA FirePOWER:

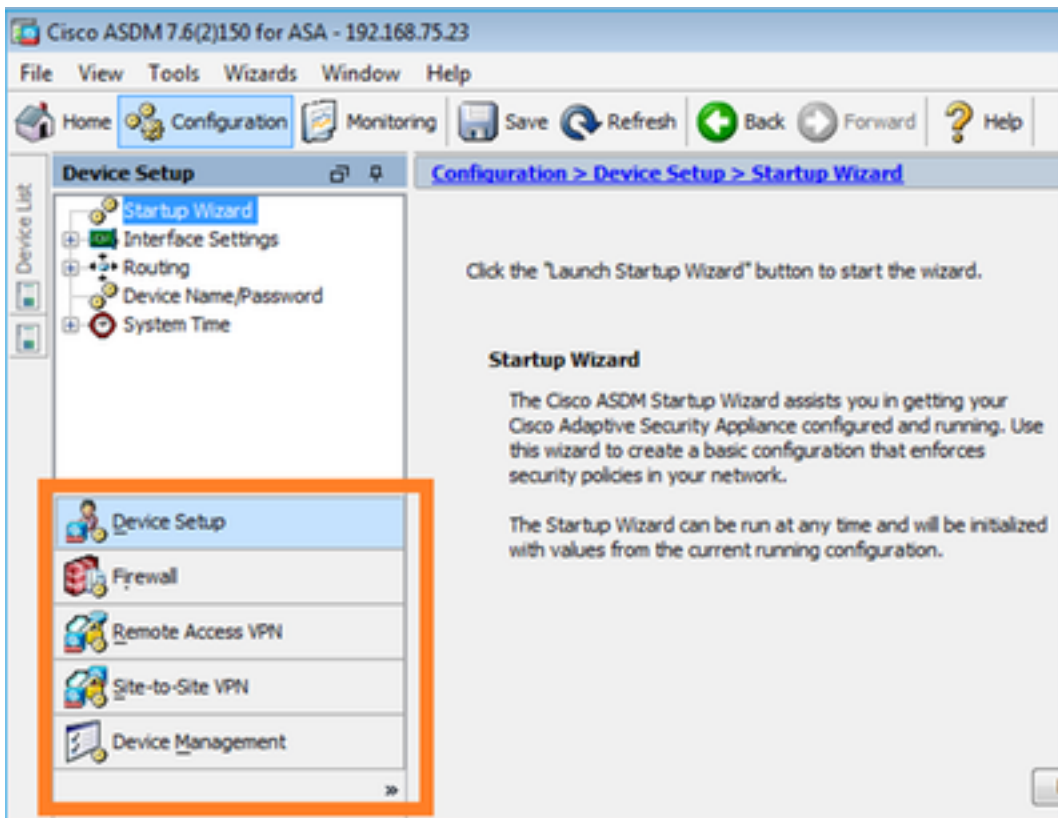


Troubleshooting

Caso que o ASDM não pode estabelecer um túnel SSL com o IP de gerenciamento FP então carregará somente o seguinte item de menu de FirePOWER:



O item de configuração ASA FirePOWER faltará também:



Ações recomendadas

Verificação 1

Certifique-se de que a interface de gerenciamento ASA é ASCENDENTE e o switchport conectado a ele está no VLAN apropriado:

```
ASA5525# show interface ip brief | include Interface|Management0/0
```

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

Verificação 2

Certifique-se de que o módulo de FirePOWER está inicializado inteiramente, em serviço:

```
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
-----
```

```
>
```

Verificação 3

Verifique a conectividade básica entre o host ASDM e o IP de gerenciamento do módulo de FirePOWER usando ferramentas como o **sibilo** e o **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.
```

Verificação 4

Se o host ASDM e o IP de gerenciamento de FirePOWER são na mesma verificação da rede L3 a tabela ARP no 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
```

Verificação 5

Permita a captação no dispositivo ASDM quando você conectar através do ASDM para ver se há uma comunicação TCP apropriada entre o host e o módulo de FirePOWER. No mínimo você deve ver:

- Aperto de mão da 3-maneira TCP entre o host ASDM e o ASA
- Túnel SSL estabelecido entre o host ASDM e o ASA
- Aperto de mão da 3-maneira TCP entre o host ASDM e o IP de gerenciamento do módulo de FirePOWER
- Túnel SSL estabelecido entre o host ASDM e o IP de gerenciamento do módulo de FirePOWER

Verificação 6

Para verificar o tráfego a e do módulo de FirePOWER você pode permitir a captação na relação do asa_mgmt_plane. Na captação abaixo dela pode ser visto:

- Requisição ARP do host ASDM (pacote 42)
- Resposta ARP do módulo de FirePOWER (pacote 43)
- Aperto de mão da 3-maneira TCP entre o host ASDM e o módulo de FirePOWER (pacotes 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
```

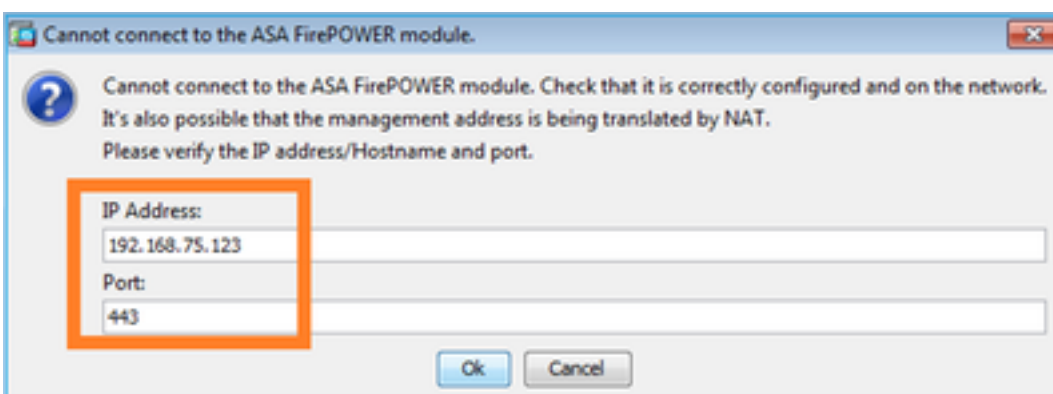
Verificação 7

Verifique que o usuário ASDM tem o nível de privilégio 15. Uma maneira de confirmar isto é sendo executado **debug HTTP 255** ao conectar através do 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]
```

Verificação 8

Se entre o host ASDM e o módulo de FirePOWER há NAT para o IP de gerenciamento de FirePOWER então você necessidade de especificar o IP do NATed:



Verificação 9

Certifique-se de que o módulo de FirePOWER não está controlado já pelo centro de gerenciamento de FirePOWER (FMC) porque nesse caso que FirePOWER cataloga no ASDM

falte:

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

>
```

Uma outra maneira:

```
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
```

Verificação 10

Verifique no guia da compatibilidade ASA que as imagens ASA/ASDM são compatíveis:

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

Verificação 11

Verifique no guia da compatibilidade de FirePOWER que o dispositivo de FirePOWER é compatível com a versão ASDM:

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

Documentos relacionados

[Guia de início rápido do módulo de Cisco ASA FirePOWER](#)

[ASA com o manual de configuração do gerenciamento local dos serviços de FirePOWER, versão 6.1.0](#)

[Guia do Usuário do módulo ASA FirePOWER para o ASA5506-X, o ASA5506H-X, o ASA5506W-X, o ASA5508-X, e o ASA5516-X, versão 5.4.1](#)