Usando o ASDM para controlar um módulo da potência de fogo no ASA

Índice

Introdução

Um módulo da potência de fogo que seja instalado no ASA pode ser controlado por qualquer um:

- Centro de gerenciamento da potência de fogo (FMC)? Esta é a solução de gerenciamento da fora-caixa
- Security Device Manager adaptável (ADSM)? 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 da potência de fogo 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 da potência de fogo

Pré-requisitos

Configuração ASA para permitir o Gerenciamento 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
```

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

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

Arquitetura

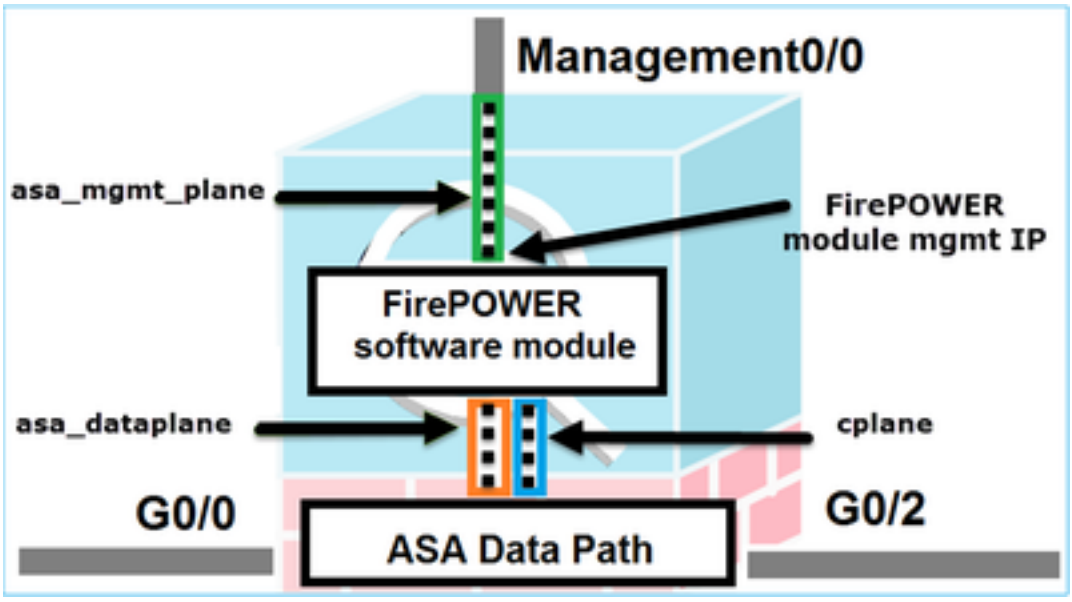
O ASA tem 3 interfaces internas:

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

Você pode capturar o tráfego em todas as interfaces internas:

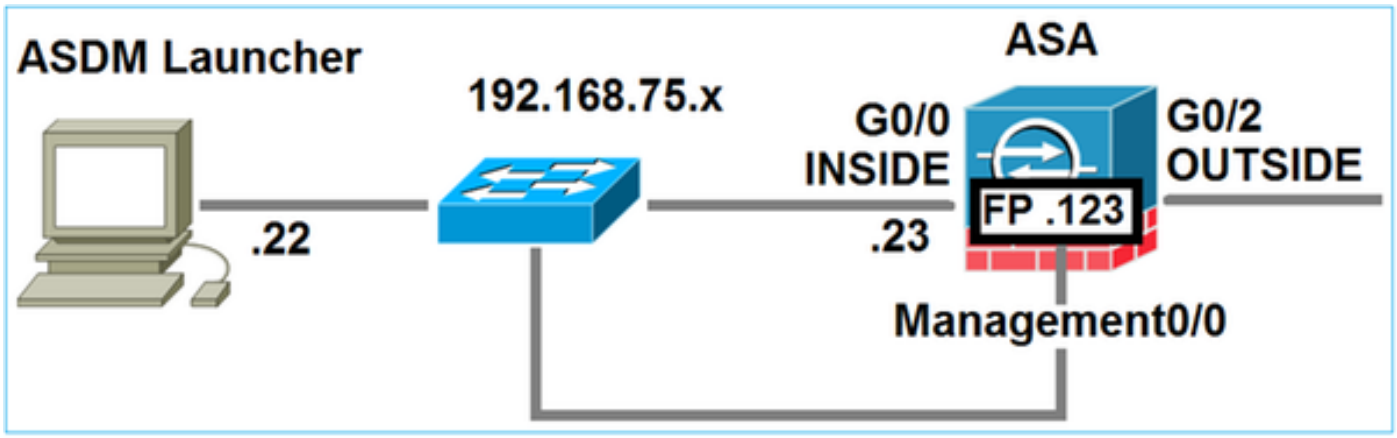
```
ASA5525# capture CAP interface ? asa_dataplane Capture packets on dataplane interface
asa_mgmt_plane Capture packets on managementplane interface cplane Capture packets on
controlplane interface
```

O acima pode ser visualizado como segue:



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

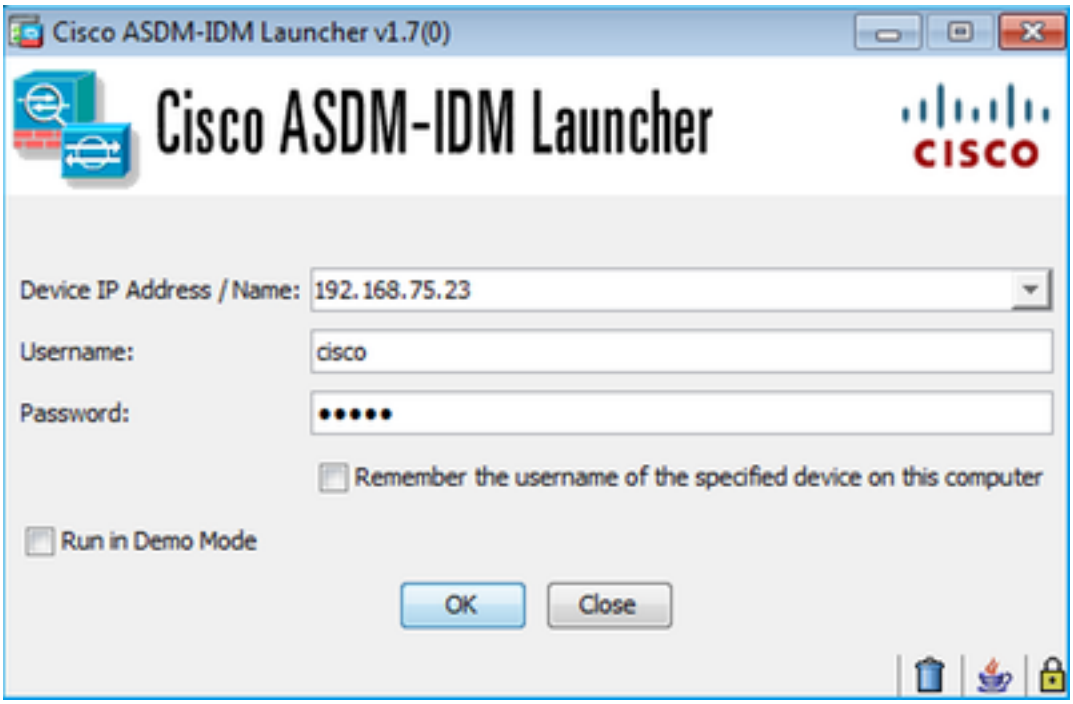
Considere a seguinte topologia



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

Etapa 1? O usuário inicia a conexão ASDM

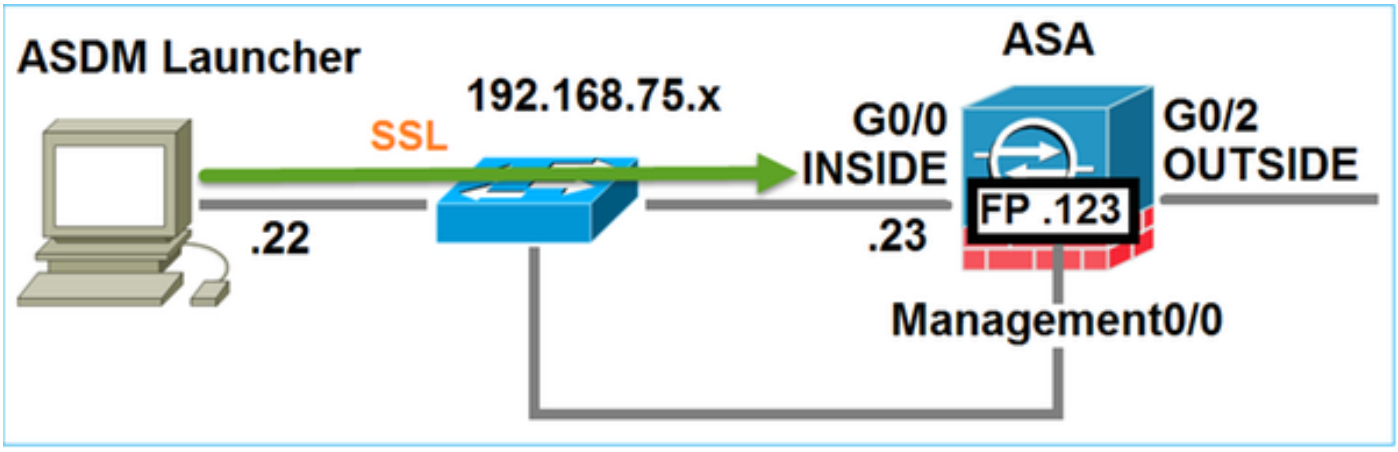
O usuário especifica o IP ASA usado para o Gerenciamento HTTP, incorpora as credenciais e inicia uma conexão para o ASA:



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 da potência de fogo

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
192.168.75.22HTTP: 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
```

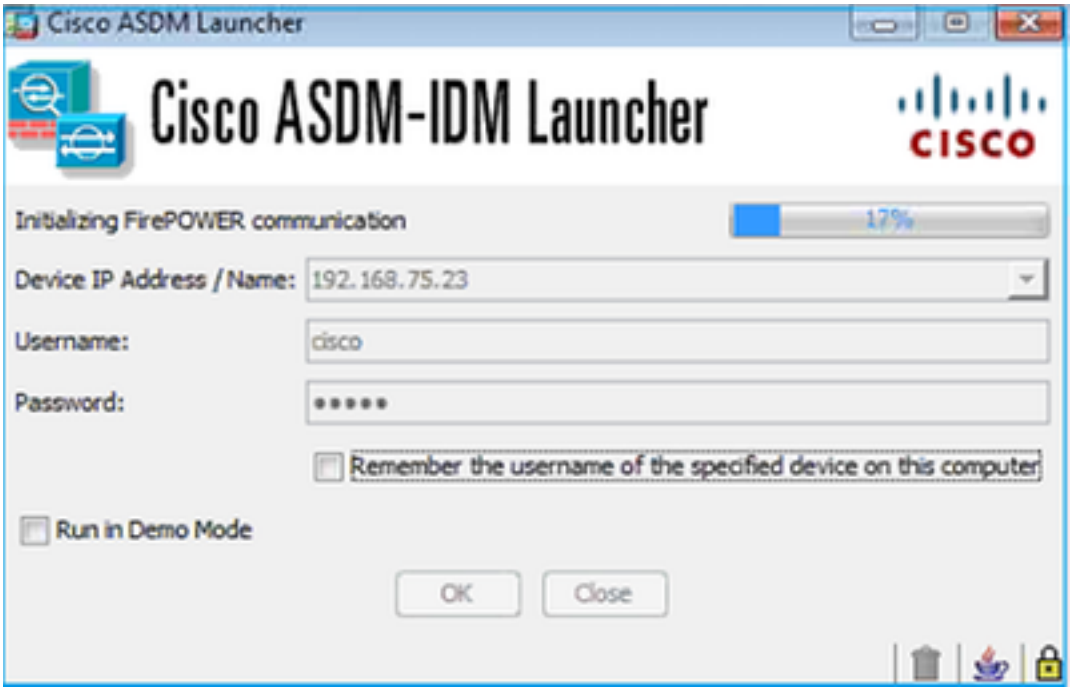
- o módulo show = O ASDM descobre os módulos ASA
- os detalhes do sfr do módulo show = O ASDM descobrem os detalhes do módulo que incluem o IP de gerenciamento da potência de fogo

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	192.168.75.23	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 da potência de fogo

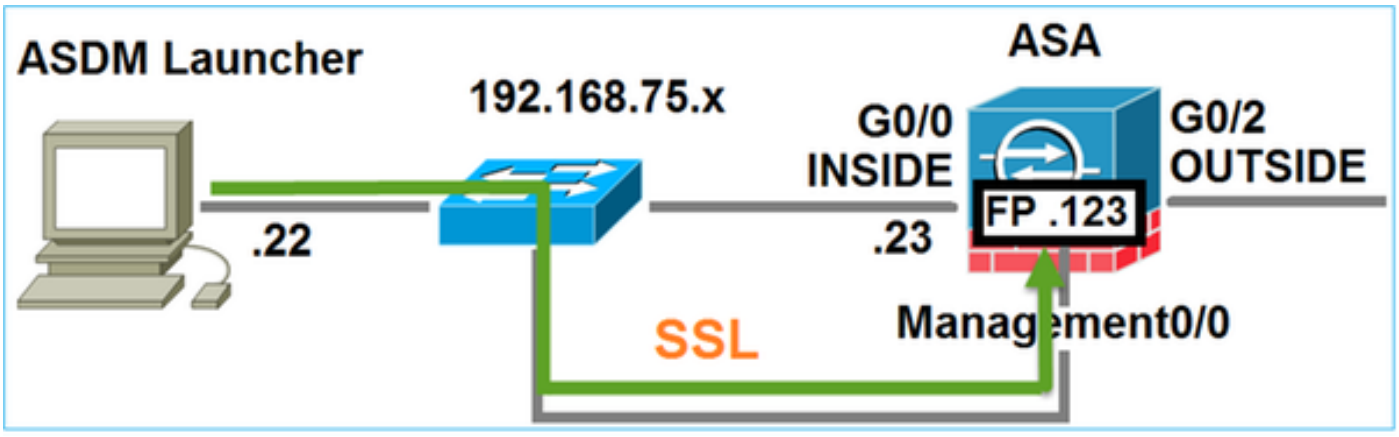
Desde que o ASDM conhece o IP de gerenciamento da potência de fogo inicia sessões de SSL para o módulo:



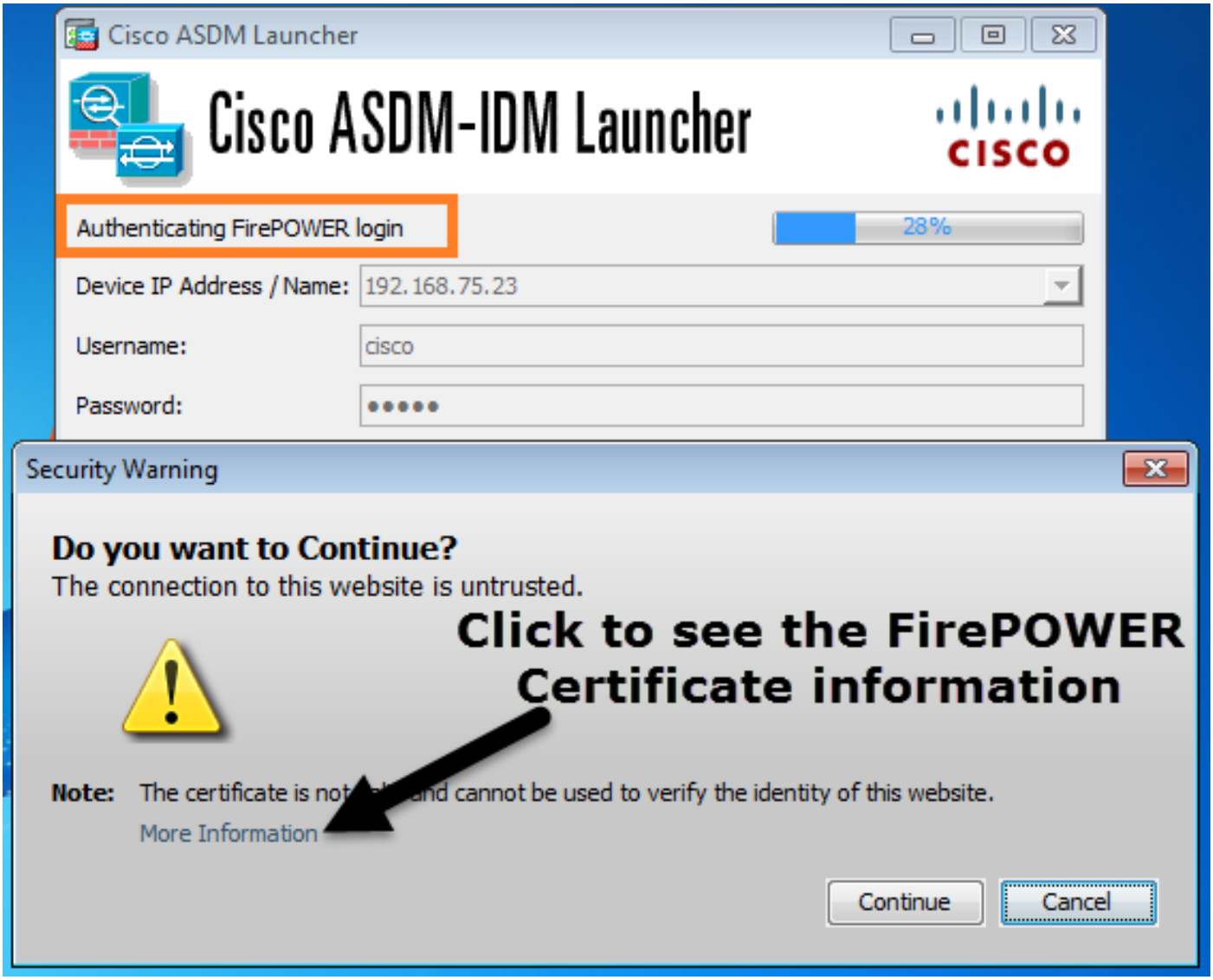
O acima será visto no fundo como conexões SSL do host ASDM para o IP de gerenciamento da potência de fogo:

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:

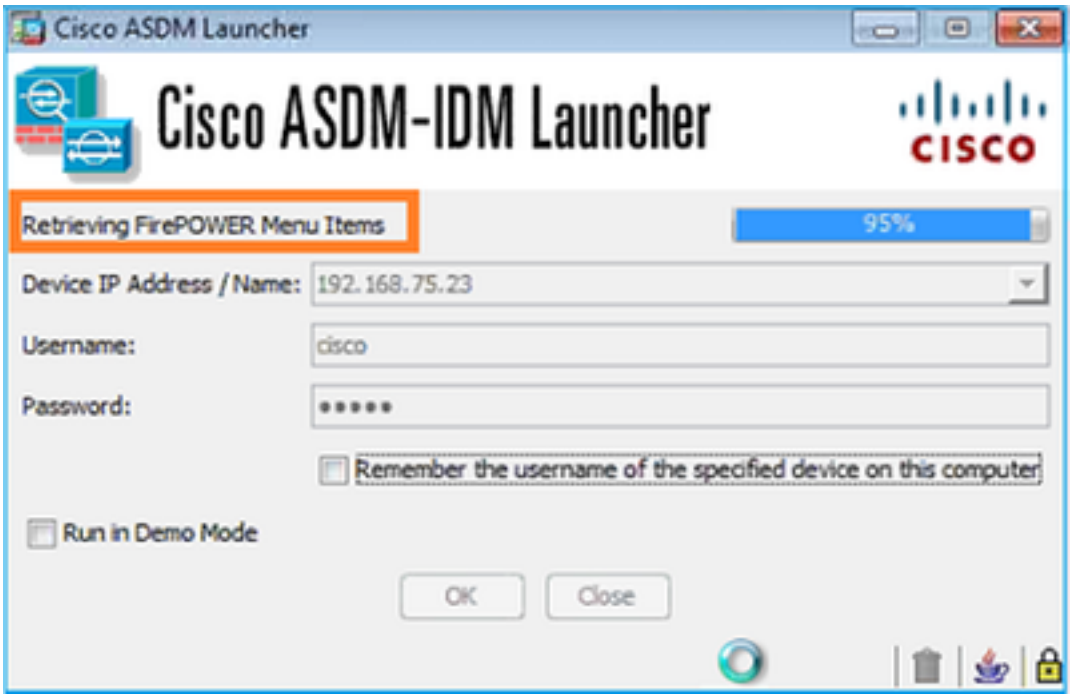


O ASDM autentica a potência de fogo e um aviso da Segurança é mostrado desde que o certificado da potência de fogo auto-é assinado:

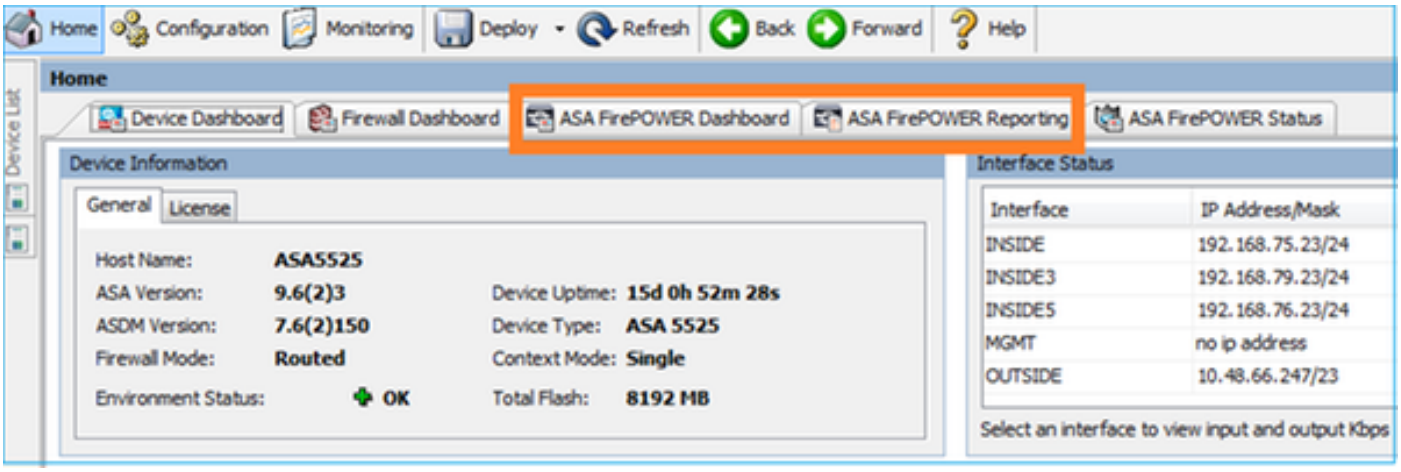


Etapa 4? O ASDM recupera os itens de menu da potência de fogo

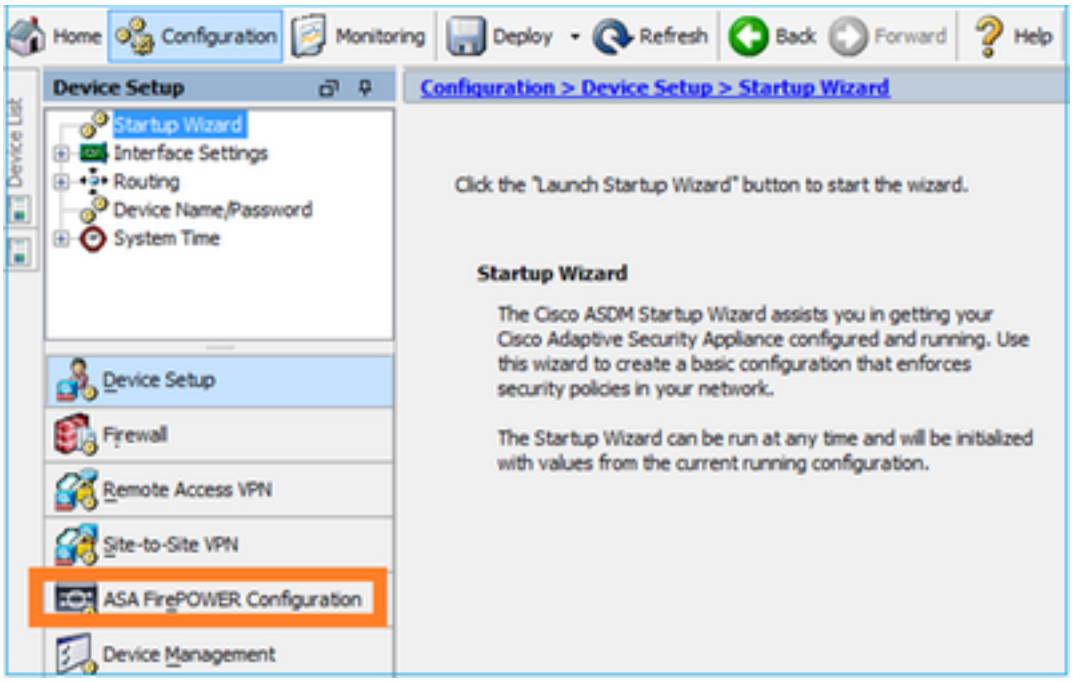
Após a autenticação bem sucedida o ASDM recupera da potência de fogo os itens de menu:



As abas recuperadas:

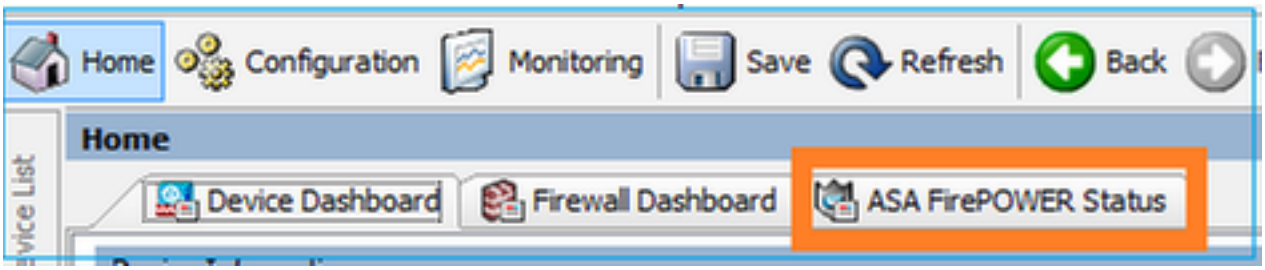


Igualmente recupera o artigo de menu de configuração da potência de fogo ASA:

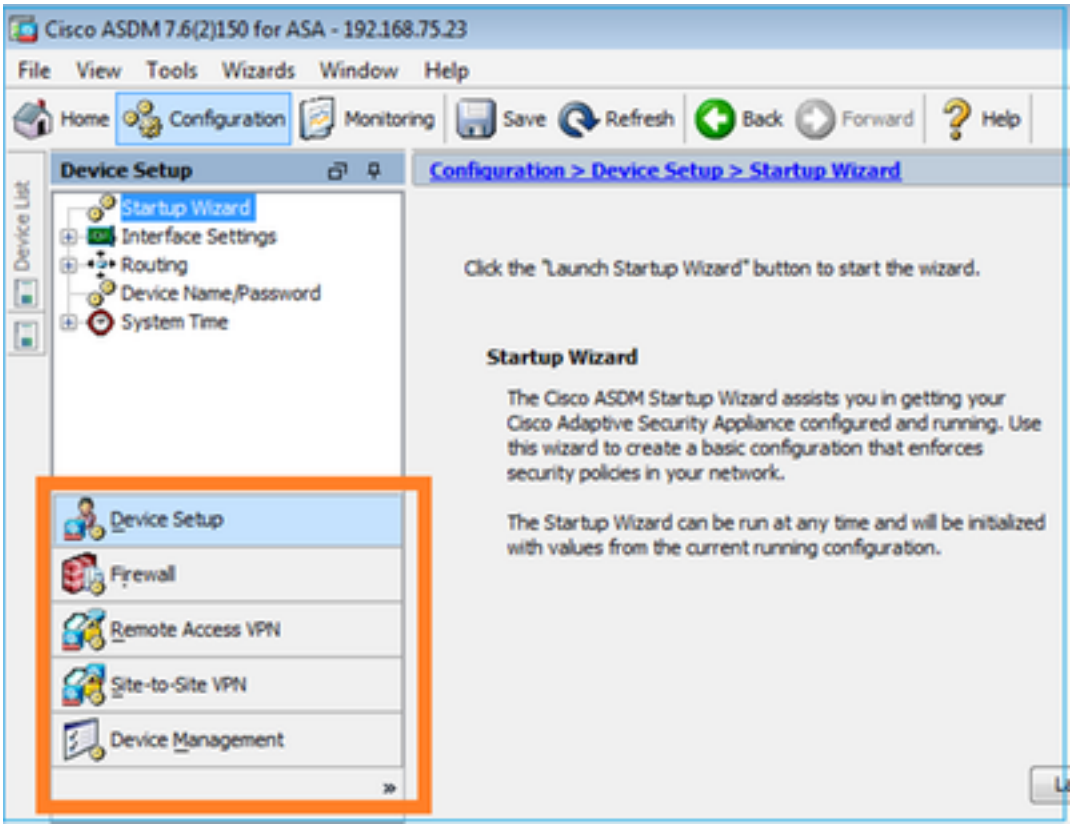


Troubleshooting

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



O item de configuração da potência de fogo ASA 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|Management0/0Interface IP-Address OK?
Method Status ProtocolManagement0/0 unassigned YES unset up up
```

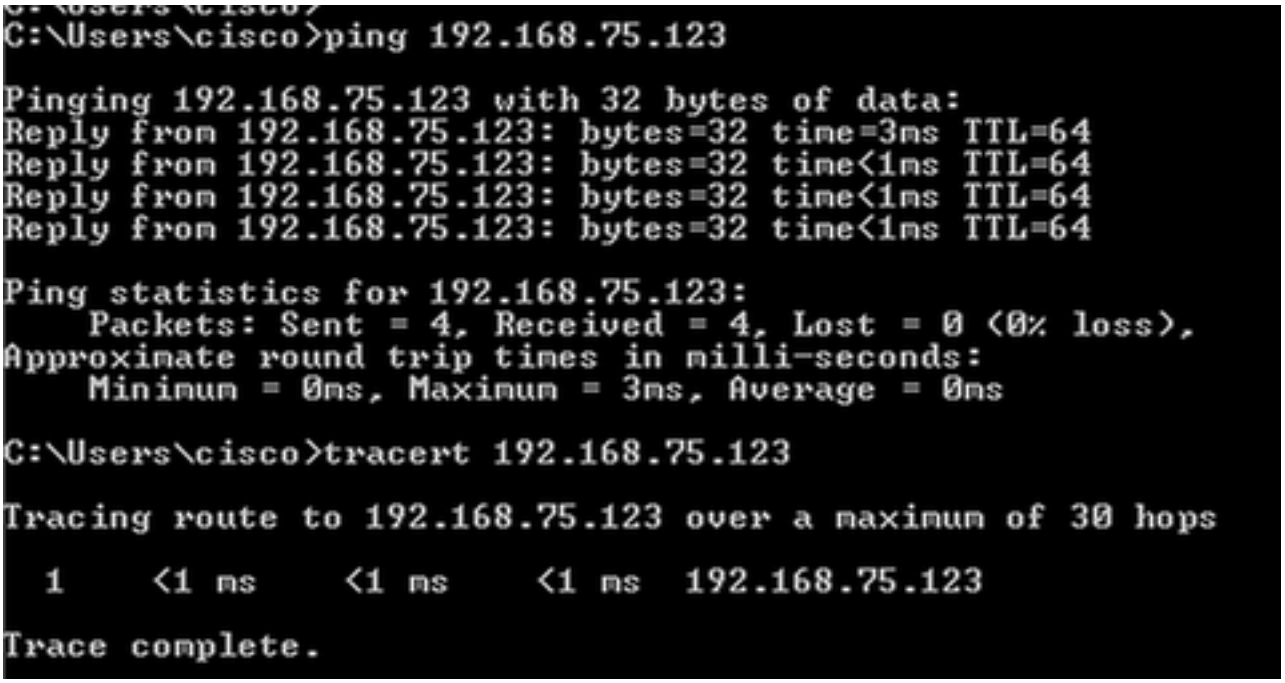
Verificação 2

Certifique-se de que o módulo da potência de fogo está inicializado inteiramente, em serviço:

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

Verificação 3

Verifique a conectividade básica entre o host ASDM e o IP de gerenciamento do módulo da potência de fogo usando ferramentas como o **sibilo** e o **tracert/traceroute:**



Verificação 4

Se o host ASDM e o IP de gerenciamento da potência de fogo 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 da potência de fogo. 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 da potência de fogo
- Túnel SSL estabelecido entre o host ASDM e o IP de gerenciamento do módulo da potência de fogo

Verificação 6

Para verificar o tráfego a e do módulo da potência de fogo 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 da potência de fogo (pacote 43)
- Aperto de mão da 3-maneira TCP entre o host ASDM e o módulo da potência de fogo (pacotes 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
```

Verificação 7

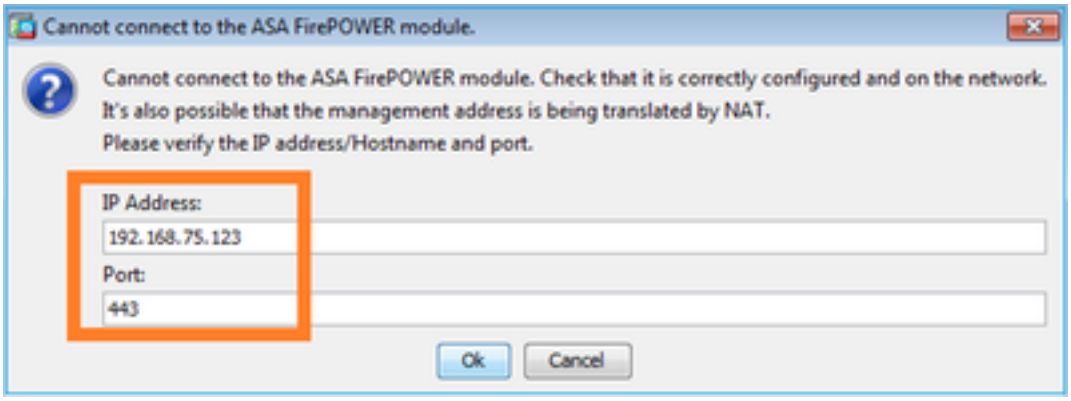
Verifique que o usuário ASDM tem o nível de privilégio 15. Uma maneira de confirmar isto é

sendo executado **debuga HTTP 255** ao conectar através do 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]
```

Verificação 8

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



Verificação 9

Certifique-se de que o módulo da potência de fogo não está controlado já pelo centro de gerenciamento da potência de fogo (FMC) porque nesse caso que a potência de fogo cataloga no ASDM falte:

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

Uma outra maneira:

```
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
```

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/asamatrx.html

Verificação 11

Verifique no guia da compatibilidade da potência de fogo que o dispositivo da potência de fogo 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 da potência de fogo de Cisco ASA

O ASA com potência de fogo presta serviços de manutenção ao manual de configuração do gerenciamento local, versão 6.1.0

Guia do Usuário do módulo da potência de fogo ASA para o ASA5506-X, o ASA5506H-X, o ASA5506W-X, o ASA5508-X, e o ASA5516-X, versão 5.4.1