Usar o ASDM para gerenciar um módulo FirePOWER em um ASA

Contents

Introduction

Este documento descreve como o software Adaptive Security Device Manager (ASDM) se comunica com o Adaptive Security Appliance (ASA) e com um módulo de software FirePOWER instalado nele.

Um módulo FirePOWER instalado em um ASA pode ser gerenciado por:

- Firepower Management Center (FMC) - Esta é a solução de gerenciamento externa.
- ASDM - esta é a solução de gerenciamento integrada.

Prerequisites

Requirements

Uma 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
```

Verifique a compatibilidade entre o módulo ASA/SFR; caso contrário, as guias do FirePOWER não serão vistas.

Além disso, no ASA, a licença 3DES/AES deve ser habilitada:

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

Verifique se o sistema cliente ASDM executa uma versão compatível do Java JRE.

Componentes Utilizados

- Um host do Microsoft Windows 7
- ASA5525-X que executa o ASA versão 9.6(2.3)
- ASDM versão 7.6.2.150
- Módulo de software 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Arquitetura

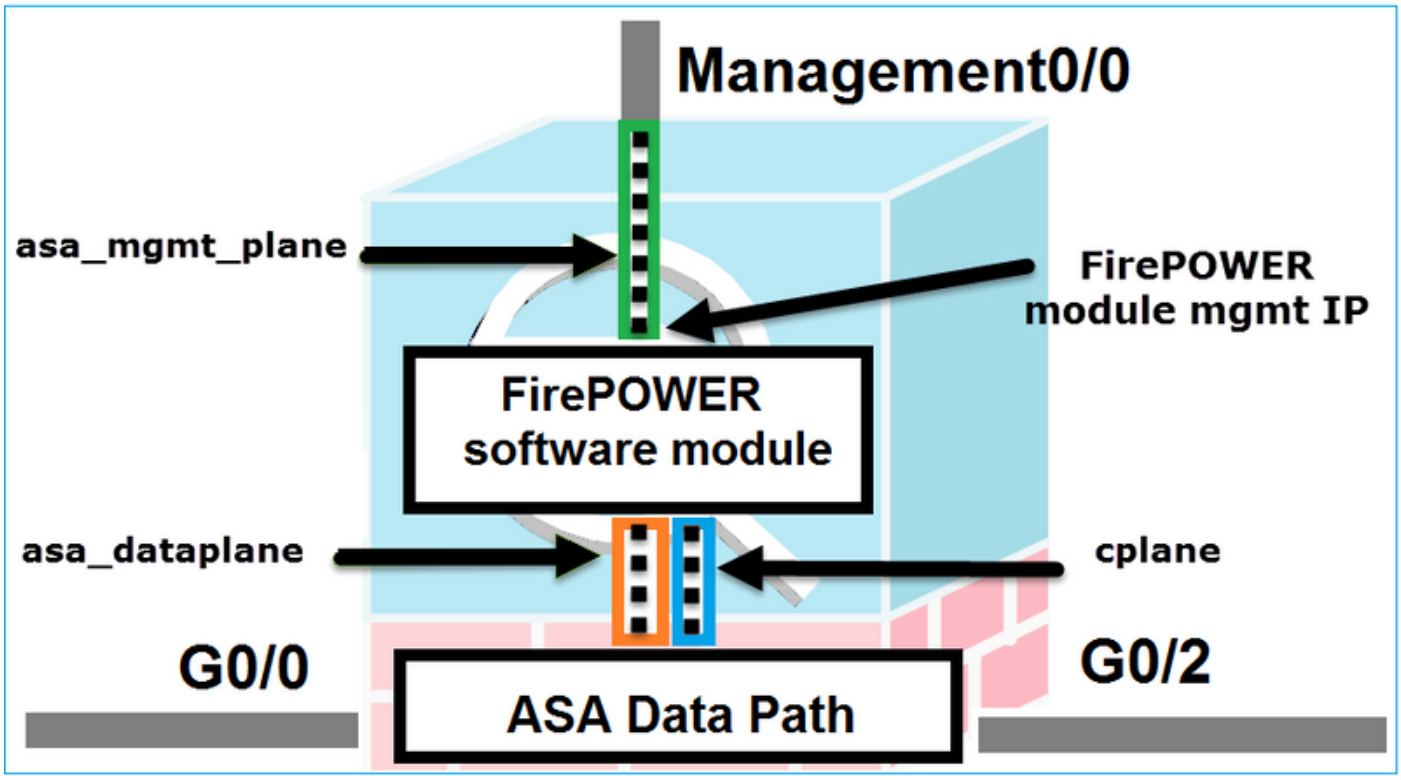
O ASA tem três interfaces internas:

- asa_dataplane - É usado para redirecionar pacotes do caminho de dados do ASA para o módulo do software FirePOWER.
- asa_mgmt_plane - É usado para permitir que a interface de gerenciamento do FirePOWER se comunique com a rede.
- cplane - Interface do plano de controle usada para transferir keepalives entre o ASA e o módulo FirePOWER.

Você pode capturar o tráfego em todas as interfaces internas:

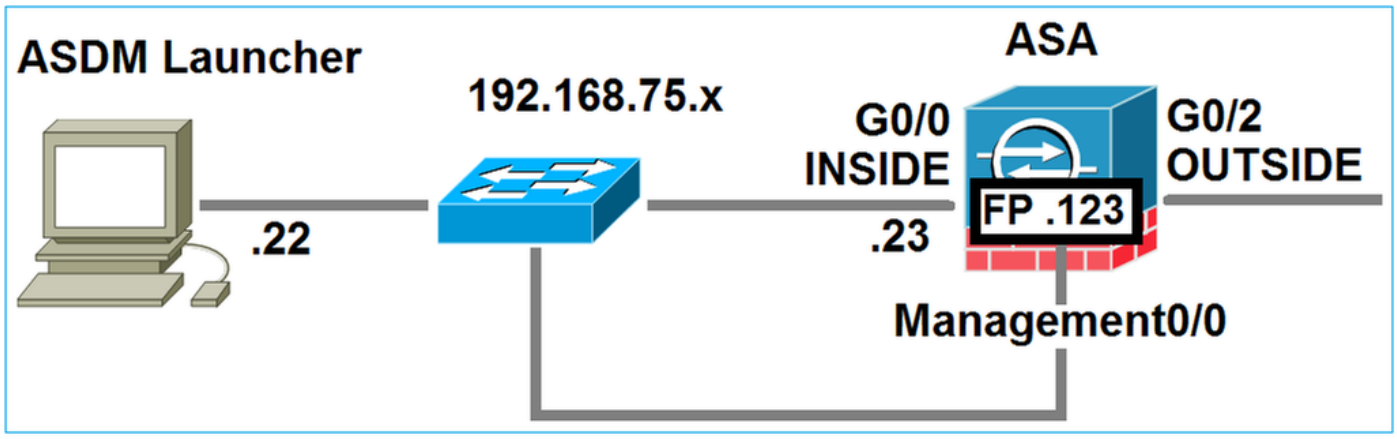
```
ASA5525# capture CAP interface ?

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

Isso pode ser visualizado da seguinte forma:



Operação em segundo plano quando um usuário se conecta a um ASA via ASDM

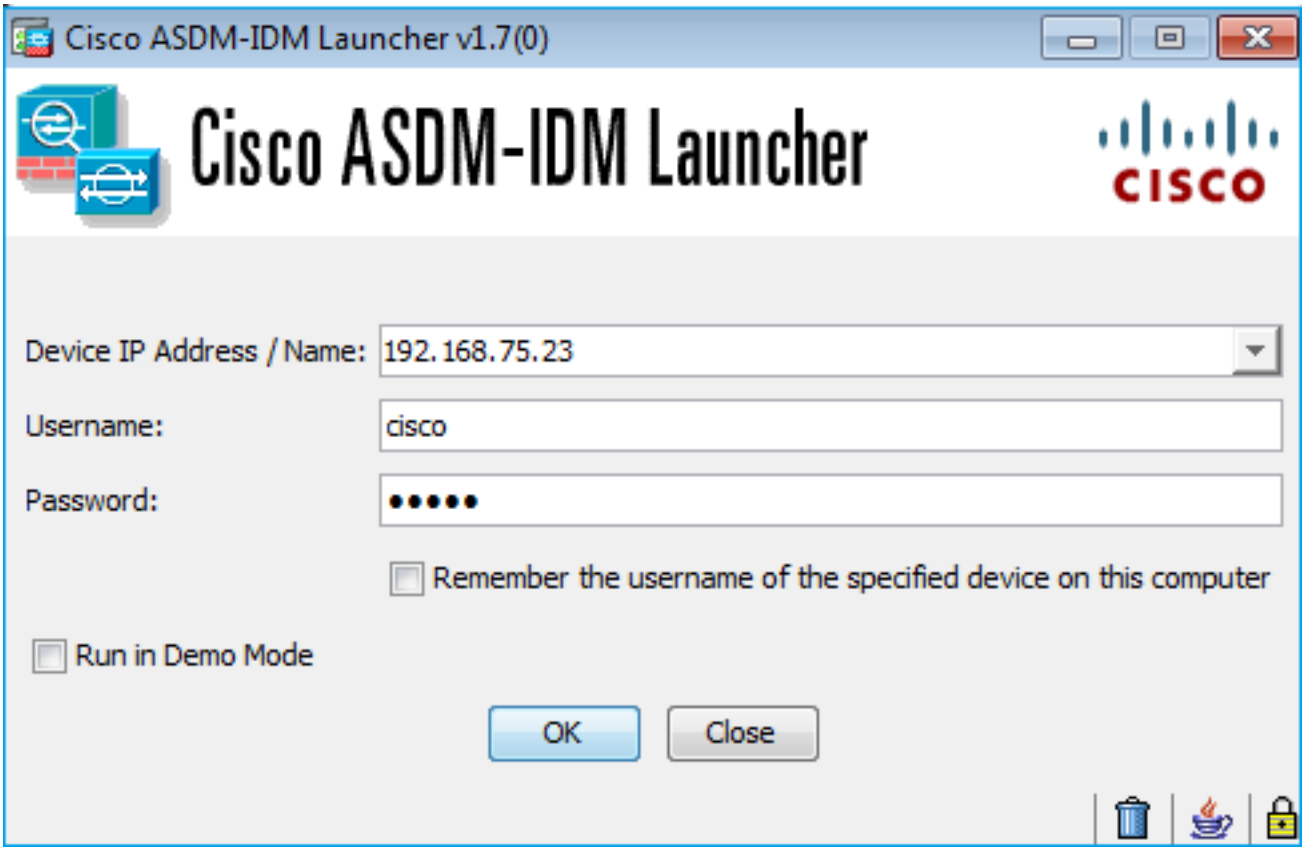
Considere esta topologia:



Quando um usuário inicia uma conexão ASDM com o ASA, estes eventos ocorrem:

Etapa 1 - O usuário inicia a conexão ASDM

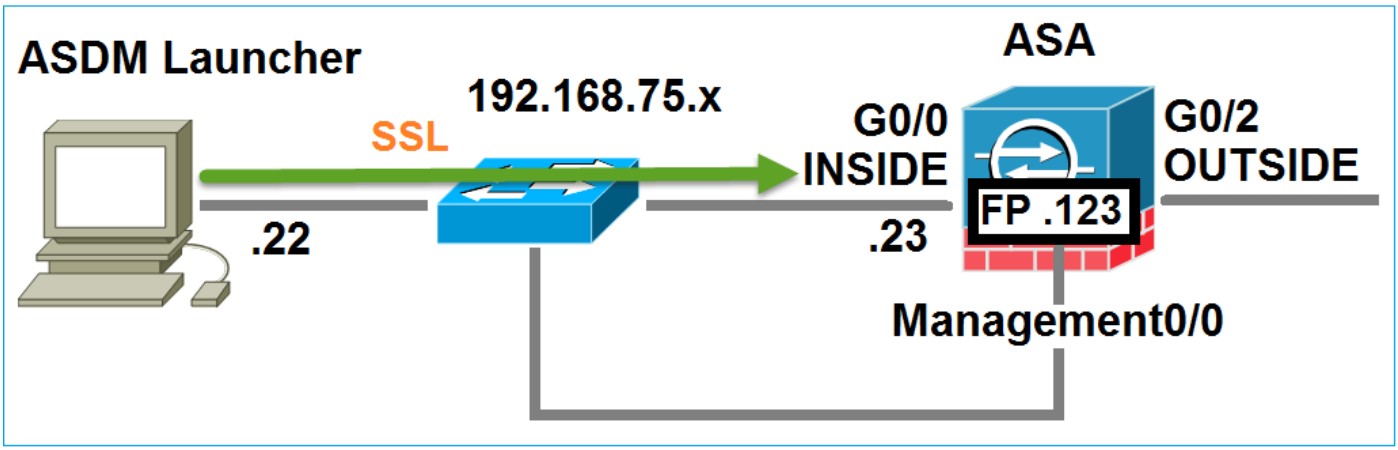
O usuário especifica o endereço IP do ASA usado para o gerenciamento HTTP, insere as credenciais e inicia uma conexão com o ASA:



Em segundo plano, 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

Isso pode ser visualizado da seguinte forma:



Etapa 2 - O ASDM descobre a configuração do ASA e o endereço IP do módulo FirePOWER

Insira o comando **debug http 255** no ASA para mostrar todas as verificações feitas em segundo plano quando o ASDM se 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
```

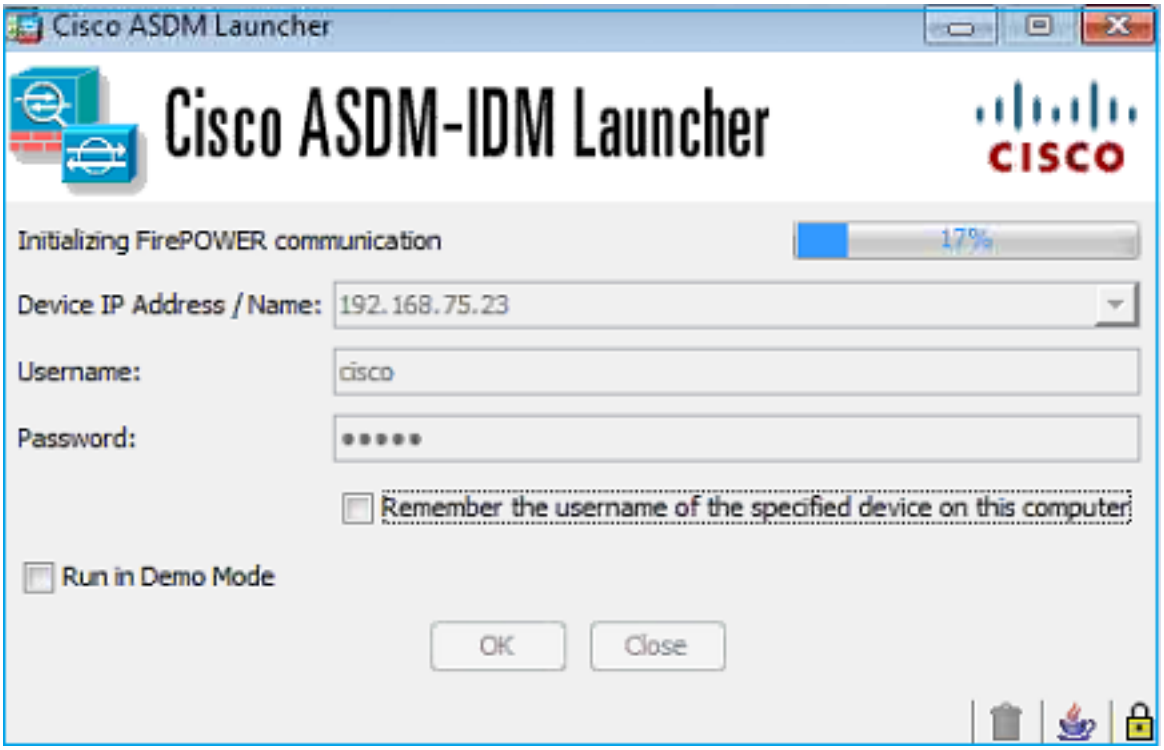
- show module - O ASDM descobre os módulos ASA.
- show module sfr details - O ASDM descobre os detalhes do módulo, que incluem o endereço IP de gerenciamento do FirePOWER.

Eles serão vistos em segundo plano como uma série de conexões SSL do PC para o endereço IP do 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 a comunicação em direção ao módulo FirePOWER

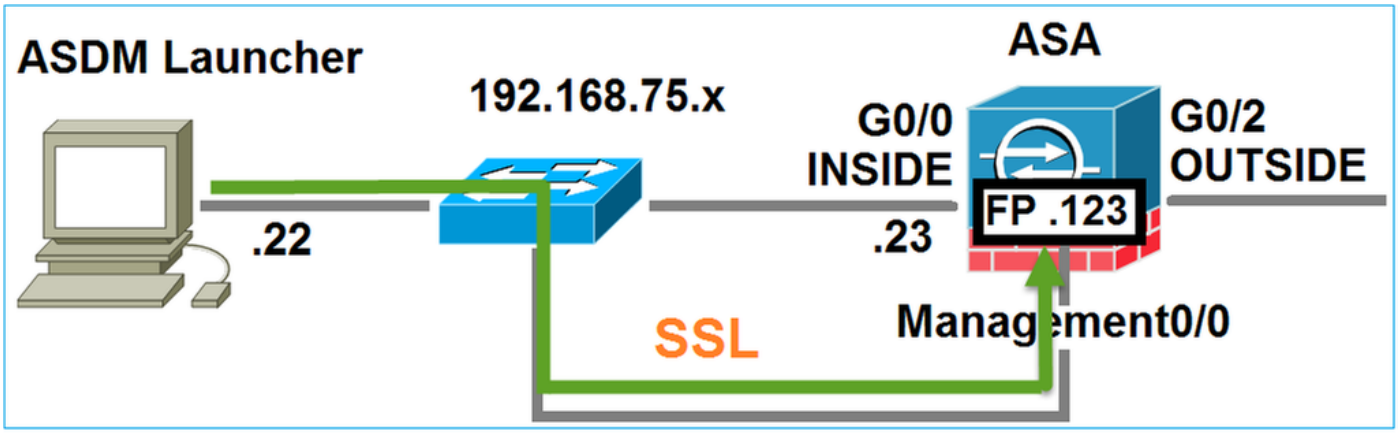
Como o ASDM conhece o endereço IP de gerenciamento do FirePOWER, ele inicia sessões SSL para o módulo:



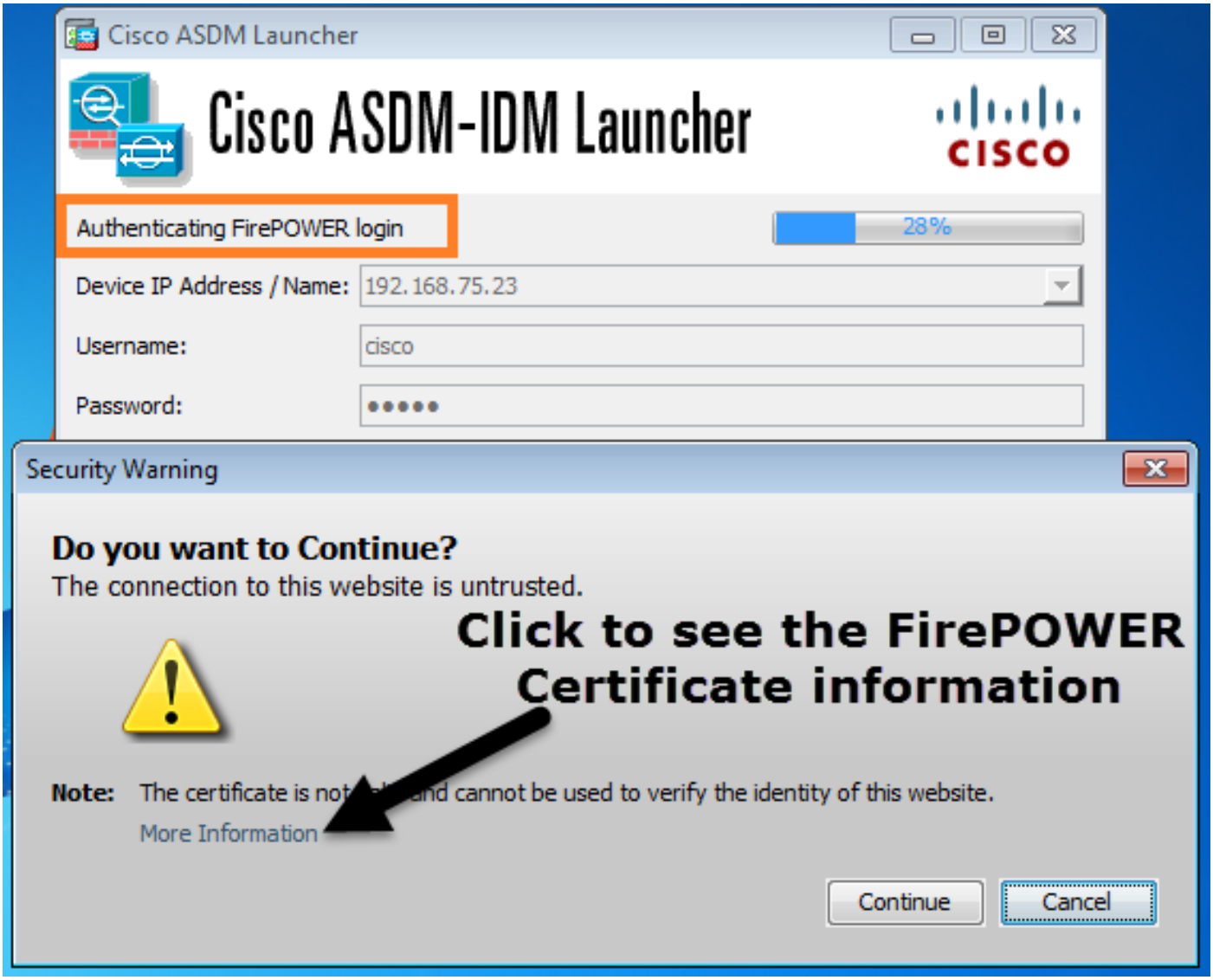
Isso será visto em segundo plano como conexões SSL do host ASDM para o endereço IP de gerenciamento do FirePOWER:

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

Isso pode ser visualizado da seguinte forma:

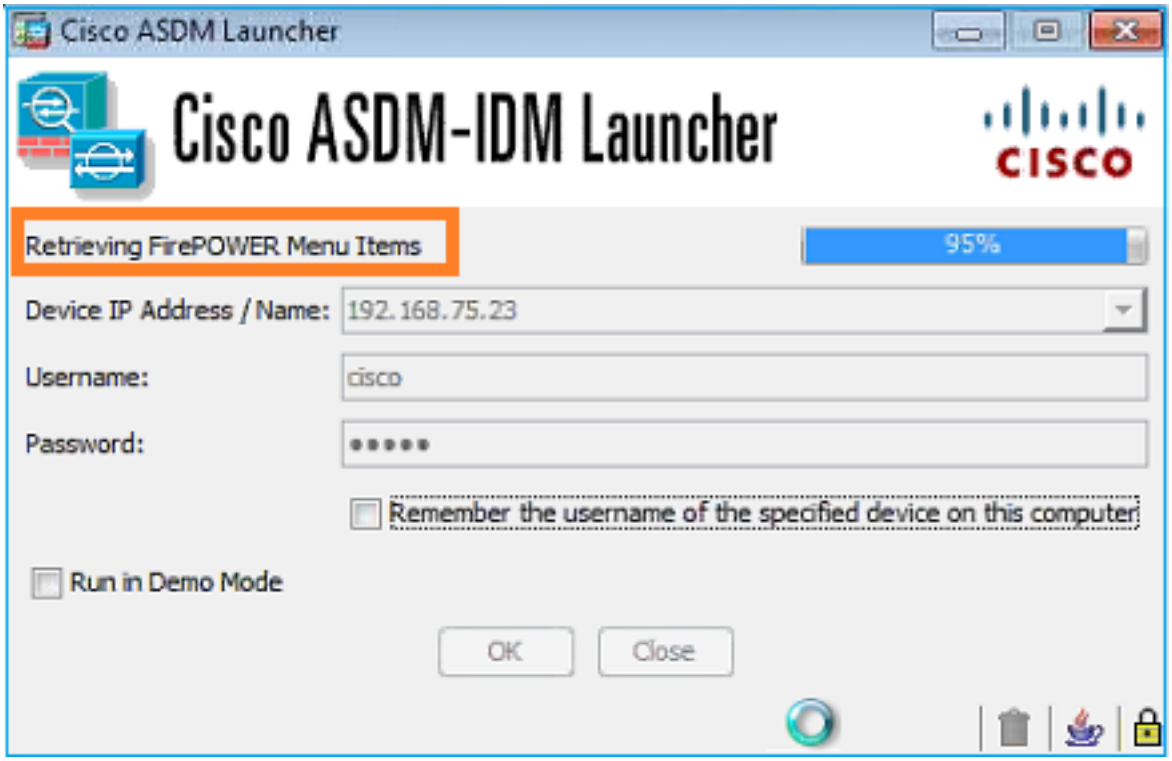


O ASDM autentica o FirePOWER e um aviso de segurança é mostrado, pois o certificado do FirePOWER é autoassinado:

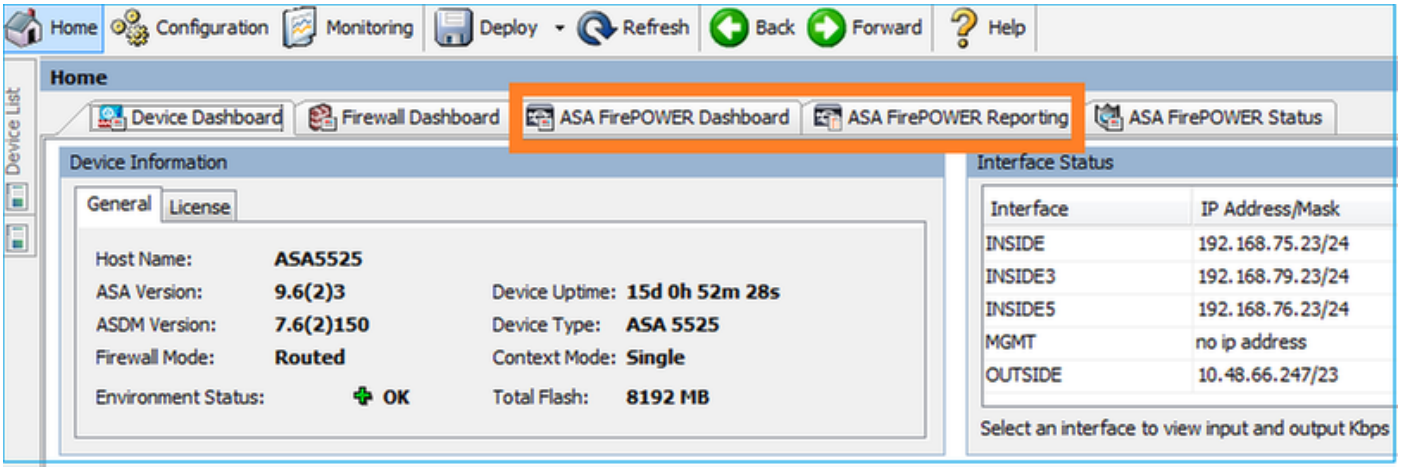


Etapa 4 - O ASDM recupera os itens do menu do FirePOWER

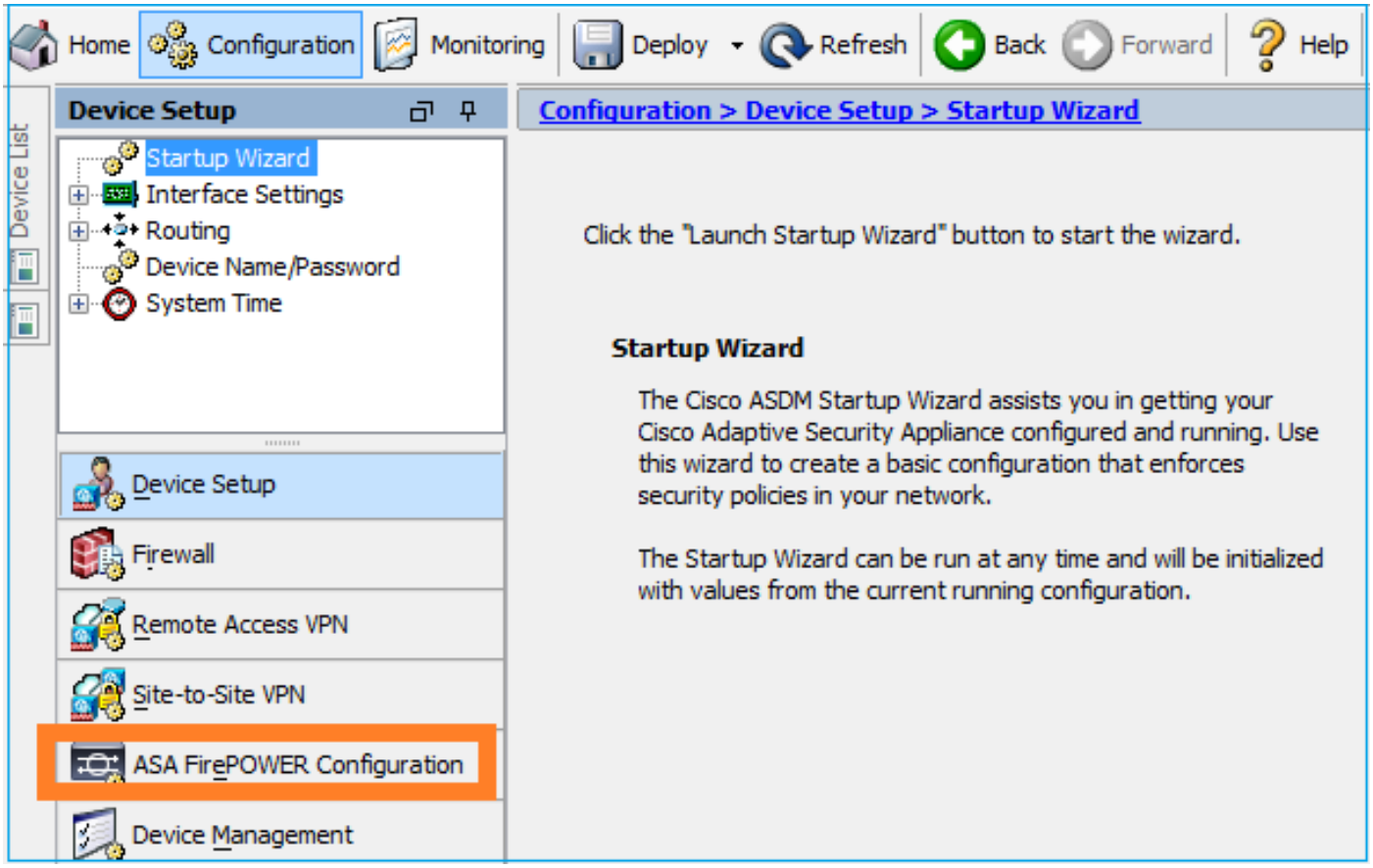
Após a autenticação bem-sucedida, o ASDM recupera os itens de menu do dispositivo FirePOWER:



As guias recuperadas são mostradas neste exemplo:

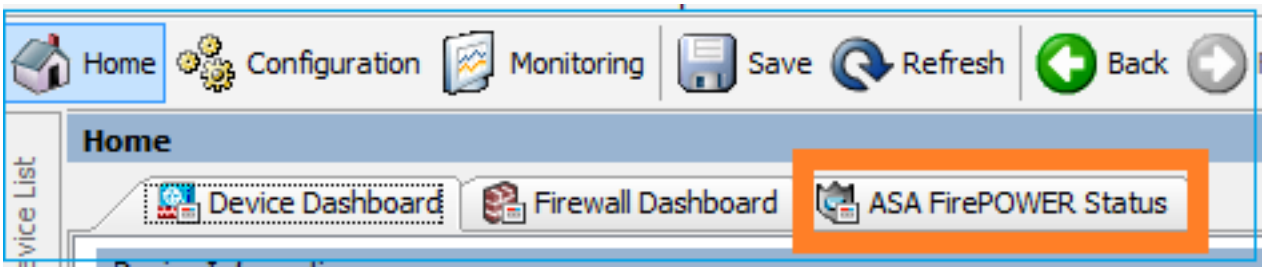


Ele também recupera o item do menu de configuração do ASA FirePOWER:

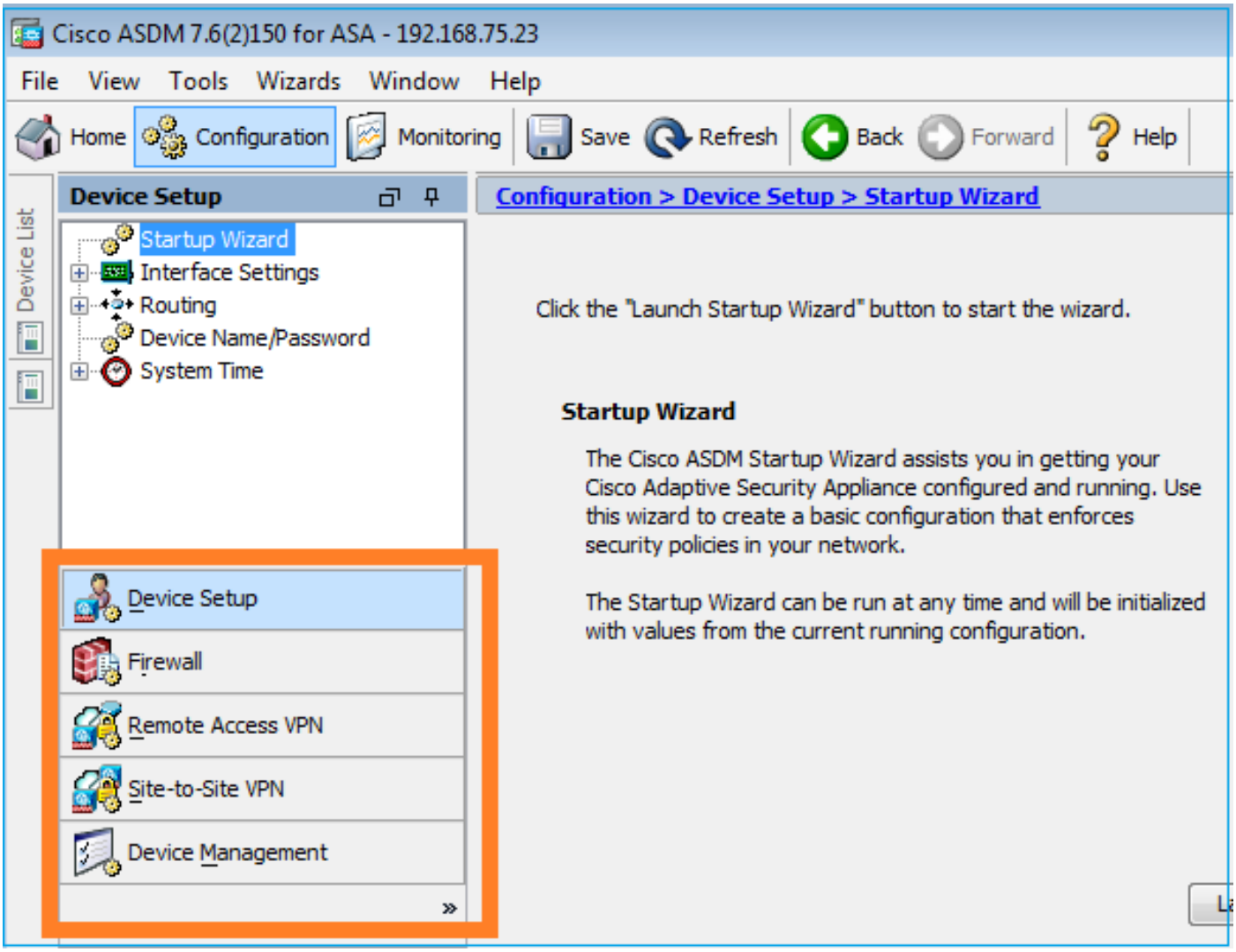


Troubleshoot

Caso o ASDM não consiga estabelecer um túnel SSL com o endereço IP do FirePOWER Management, ele carregará somente este item do menu do FirePOWER:



O item de configuração do ASA FirePOWER também está ausente:



Verificação 1

Certifique-se de que a interface de gerenciamento ASA esteja UP e que a porta do switch conectada a ela esteja na VLAN apropriada:

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

Solução de problemas recomendada

- Defina a VLAN apropriada.
- Ative a porta (verifique o cabo, verifique a configuração da porta do switch (velocidade/duplex/fechamento).

Verificação 2

Verifique se o módulo FirePOWER está totalmente inicializado, ATIVO e em execução:

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

>
```

Solução de problemas recomendada

- Verifique se há erros ou falhas na saída do comando **show module sfr log console**.

Verificação 3

Verifique a conectividade básica entre o host ASDM e o IP de gerenciamento do módulo FirePOWER com comandos como **ping** e **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.
```

Solução de problemas recomendada

- Verifique o roteamento ao longo do caminho.
- Verifique se não há dispositivos no caminho que bloqueiem o tráfego.

Verificação 4

Se o host ASDM e o endereço IP de gerenciamento do FirePOWER estiverem na mesma rede da camada 3, verifique a tabela ARP (Address Resolution Protocol) 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
```

Solução de problemas recomendada

- Se não houver entradas ARP, use o Wireshark para verificar a comunicação ARP. Verifique se os endereços MAC dos pacotes estão corretos.
- Se houver entradas ARP, verifique se elas estão corretas.

Verificação 5

Ative a captura no dispositivo ASDM enquanto você se conecta via ASDM para ver se há comunicação TCP adequada entre o host e o módulo FirePOWER. No mínimo, você deve ver:

- Handshake triplo TCP entre o host ASDM e o ASA.
- Túnel SSL estabelecido entre o host ASDM e o ASA.
- Handshake triplo TCP entre o host ASDM e o endereço IP de gerenciamento do módulo FirePOWER.

- Túnel SSL estabelecido entre o host ASDM e o endereço IP de gerenciamento do módulo FirePOWER.

Solução de problemas recomendada

- Se o handshake triplo do TCP falhar, certifique-se de que não haja tráfego assimétrico ou dispositivos no caminho que bloqueie os pacotes TCP.
- Se o SSL falhar, verifique se não há nenhum dispositivo no caminho que faça o man-in-the-middle (MITM) (o Emissor do certificado do servidor dará uma dica para isso).

Verificação 6

Para verificar o tráfego de e para o módulo FirePOWER, habilite a captura na interface asa_mgmt_plane. Na captura, você pode ver:

- Solicitação ARP do host ASDM (pacote 42).
- Resposta ARP do módulo FirePOWER (pacote 43).
- Handshake triplo TCP entre o host ASDM e o módulo 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
Sack
ack
```

Solução de problemas recomendada

- Igual à da Verificação 5.

Verificação 7

Verifique se o usuário ASDM tem o nível de privilégio 15. Uma forma de confirmar isso é inserir o comando **debug http 255** enquanto ele se conecta via ASDM:

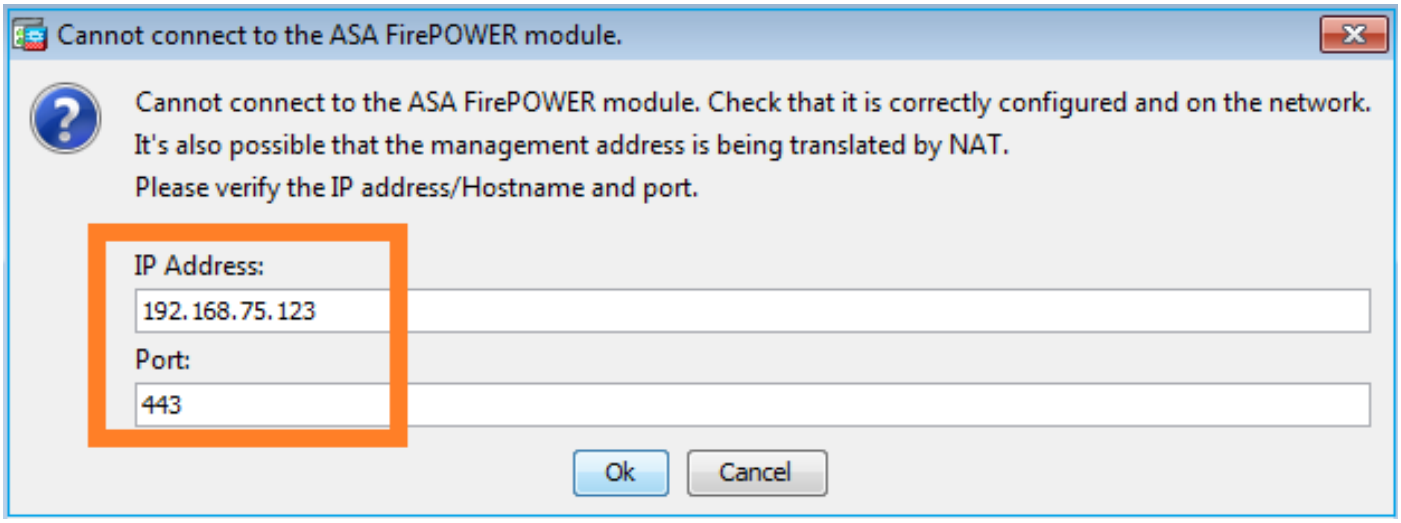
```
ASA5525# debug http 255
debug http enabled at level 255.
HTTP: processing ASDM request [/admin/asdm_banner] with cookie-based authentication
(aware_webvpn_conf.re2c:444)
HTTP: check admin session. Cookie index [2][c8a06c50]
HTTP: Admin session cookie [A27614B@20480@78CF@58989AACB80CE5159544A1B3EE62661F99D475DC]
HTTP: Admin session idle-timeout reset
HTTP: admin session verified =  [1]
HTTP: username = [user1], privilege = [14]
```

Solução de problemas recomendada

- Se o nível de privilégio não for 15, tente com um usuário que tenha o nível 15.

Verificação 8

Se entre o host ASDM e o módulo FirePOWER houver uma conversão de endereço de rede (NAT) para o endereço IP do FirePOWER Management, você precisará especificar o endereço IP do NAT:



Solução de problemas recomendada

- Capturas nos endpoints (ASA/SFR e host final) confirmarão isso.

Verificação 9

Certifique-se de que o módulo FirePOWER ainda não esteja gerenciado pelo FMC, pois nesse caso as guias do FirePOWER no ASDM estarão ausentes:

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

>
```

Outro método é com o comando **show module sfr details**:

```
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
```

Solução de problemas recomendada

- Se o dispositivo já for gerenciado, você precisará cancelar o registro antes de gerenciá-lo do ASDM. Consulte o Guia de Configuração do Firepower Management Center.

Verificação 10

Verifique a captura do Wireshark para garantir que o cliente ASDM se conecte com uma versão TLS adequada (por exemplo, TLSv1.2).

Solução de problemas recomendada

- Ajuste as configurações SSL do navegador.
- Tente com outro navegador.
- Tente de outro host final.

Verificação 11

Verifique no guia de compatibilidade do Cisco ASA se as imagens do ASA/ASDM são compatíveis.

Solução de problemas recomendada

- Usar uma imagem ASDM compatível.

Verificação 12

Verifique no guia de compatibilidade do Cisco ASA se o dispositivo FirePOWER é compatível com a versão ASDM.

Solução de problemas recomendada

- Usar uma imagem ASDM compatível.

Informações Relacionadas

- Guia de início rápido do módulo Cisco ASA FirePOWER
- Guia de configuração de gerenciamento local do ASA com FirePOWER Services, versão 6.1.0
- Guia do usuário do módulo ASA FirePOWER para ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X e ASA5516-X, versão 5.4.1
- Suporte Técnico e Documentação - Cisco Systems