ASDMを使用したASA上のFirepowerモジュールの管理

内容

はじめに

このドキュメントでは、ASDMソフトウェアが適応型セキュリティアプライアンス(ASA)およびそれにインストールされているFirepowerソフトウェアモジュールと通信する方法について説明します。

背景説明

ASAにインストールされたFirepowerモジュールは、次のいずれかによって管理できます。

- Firepower Management Center(FMC)：オフボックスの管理ソリューションです。
- Adaptive Security Device Manager(ASDM)：これはオンボックスの管理ソリューションです。

前提条件

要件

ASDM管理を有効にするASA設定：

```
<#root>

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
```

ASA/SFRモジュール間の互換性を確認します。互換性がない場合は、Firepowerタブが表示されません。

さらに、ASAで3DES/AESライセンスを有効にする必要があります。

<#root>

```
ASA5525#

show version | in 3DES

Encryption-3DES-AES

               :

Enabled

 perpetual
```

ASDMクライアントシステムで、サポートされているバージョンのJava JREが稼働していること

を確認します。

使用するコンポーネント

- Microsoft Windows 7ホスト
- ASAバージョン9.6(2.3)が稼働するASA5525-X
- ASDM バージョン 7.6.2.150
- FirePOWER ソフトウェア モジュール 6.1.0-330

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

アーキテクチャ

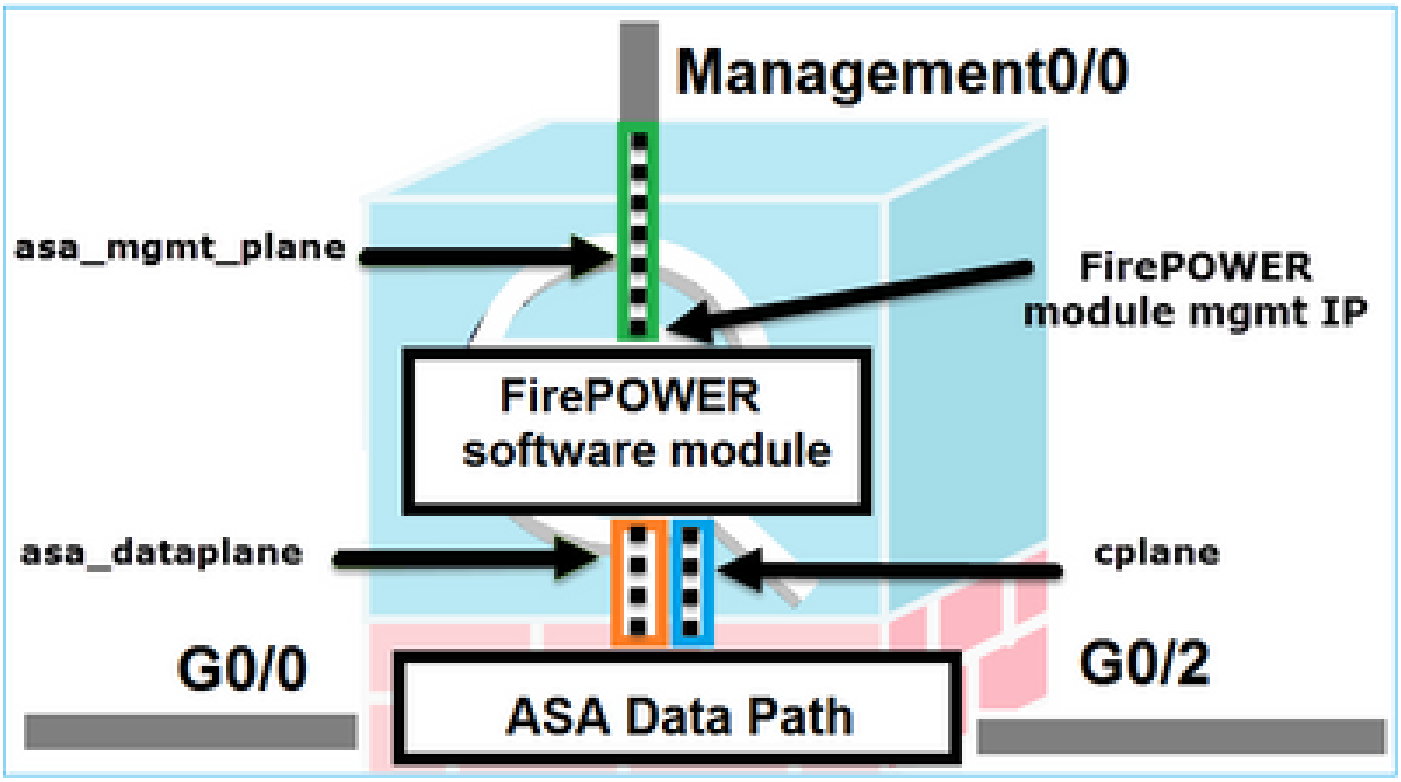
ASAには3つの内部インターフェイスがあります。

- asa_dataplane:ASAデータパスからFirepowerソフトウェアモジュールにパケットをリダイレクトするために使用されます。
- asa_mgmt_plane：ネットワーク管理インターフェイスがFirepowerと通信できるようにするために使用されます。
- cplane:ASAとFirepowerモジュール間でキープアライブを転送するために使用され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イスでトラフィックをキャプチャできます。

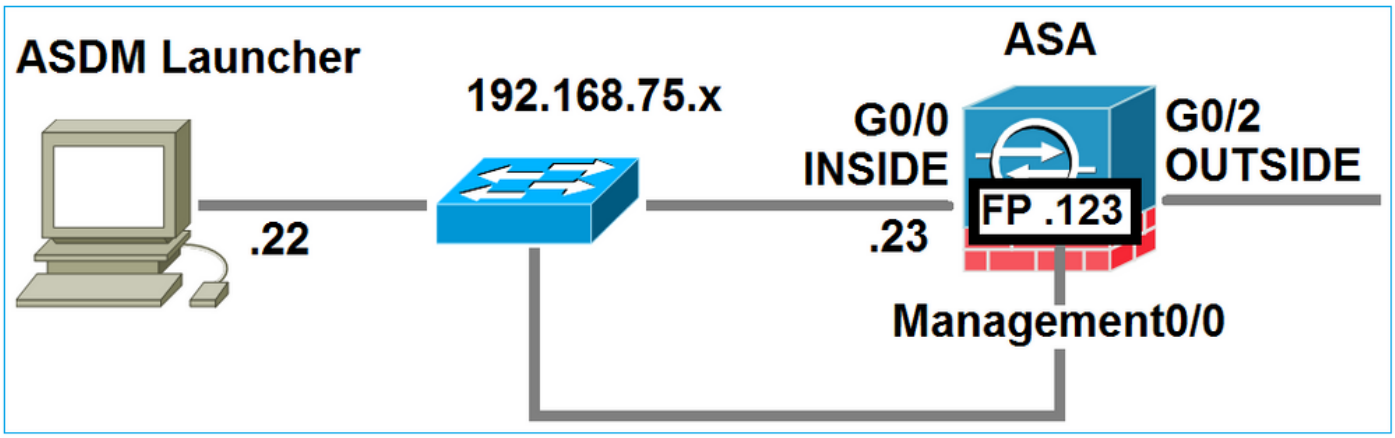
```
<#root>

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
```

これは次のように視覚化できます。



ユーザがASDMを介してASAに接続する場合のバックグラウンド動作

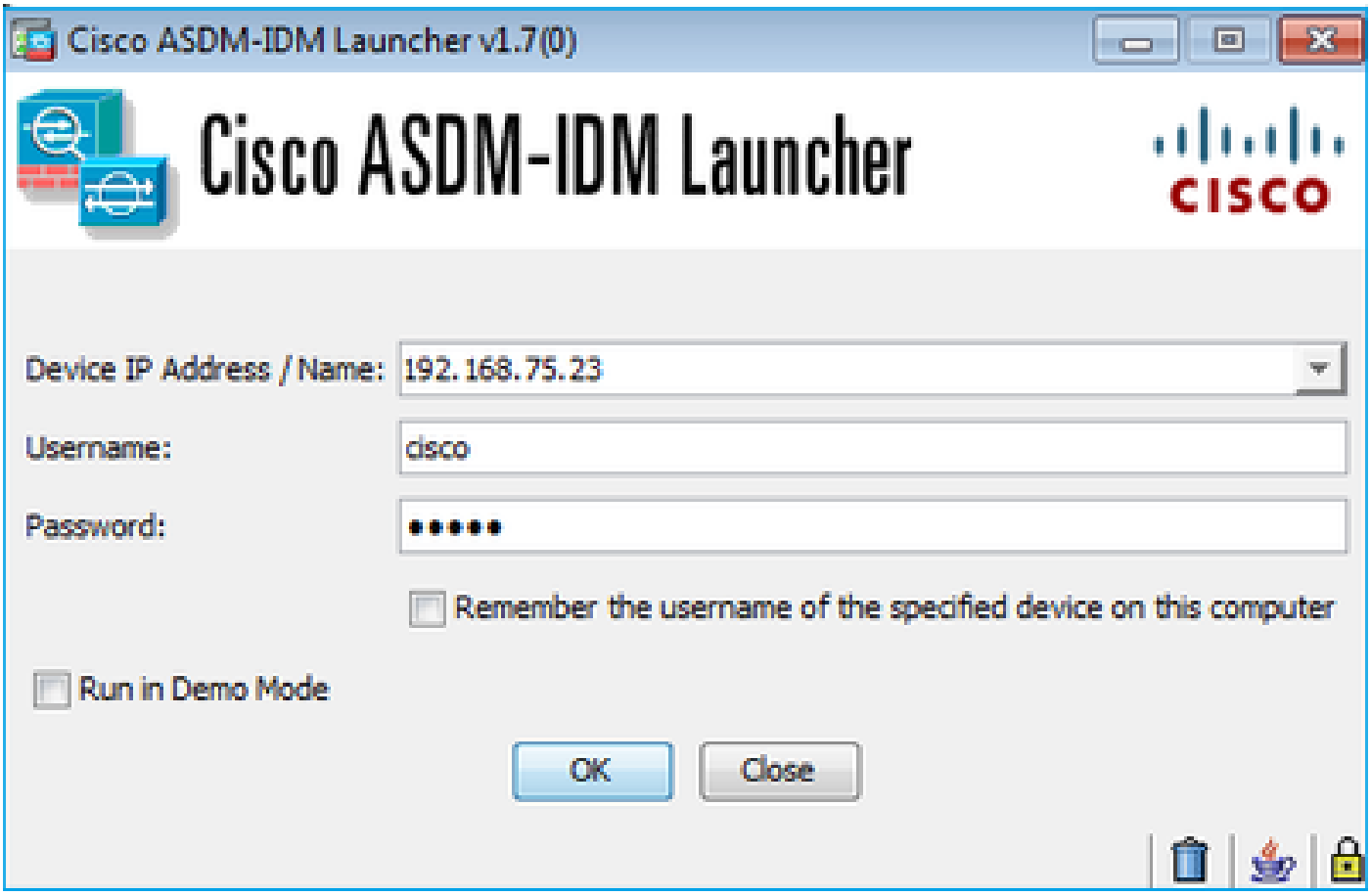
このトポロジを参照してください。



ユーザがASAへのASDM接続を開始すると、次のイベントが発生します。

ステップ1：ユーザによるASDM接続の開始

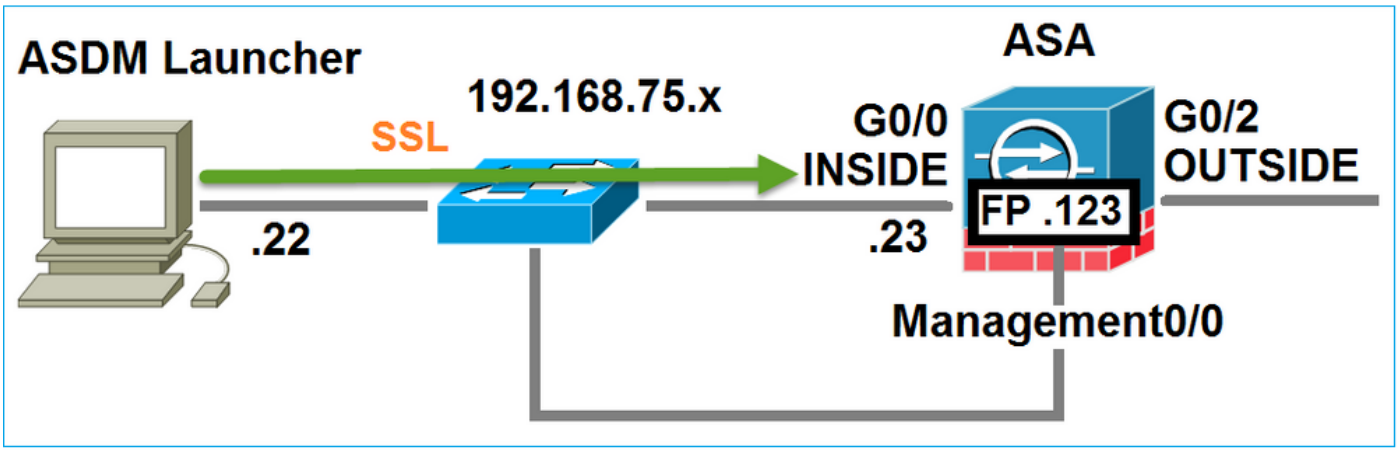
ユーザはHTTP管理に使用するASA IPアドレスを指定し、クレデンシャルを入力して、ASAへの接続を開始します。



バックグラウンドで、ASDMとASAの間にSSLトンネルが確立されます。

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

これは次のように視覚化できます。



ステップ2:ASDMがASA設定とFirepowerモジュールのIPアドレスを検出する

ASDMがASAに接続するときにバックグラウンドで実行されるすべてのチェックを表示するには、ASAでdebug http 255コマンドを入力します。

```
<#root>

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 authenticatio
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/s

how+module+sfr+details

] with cookie-based authentication
HTTP: processing GET URL '/admin/exec/show+module+sfr+details' from host 192.168.75.22
```

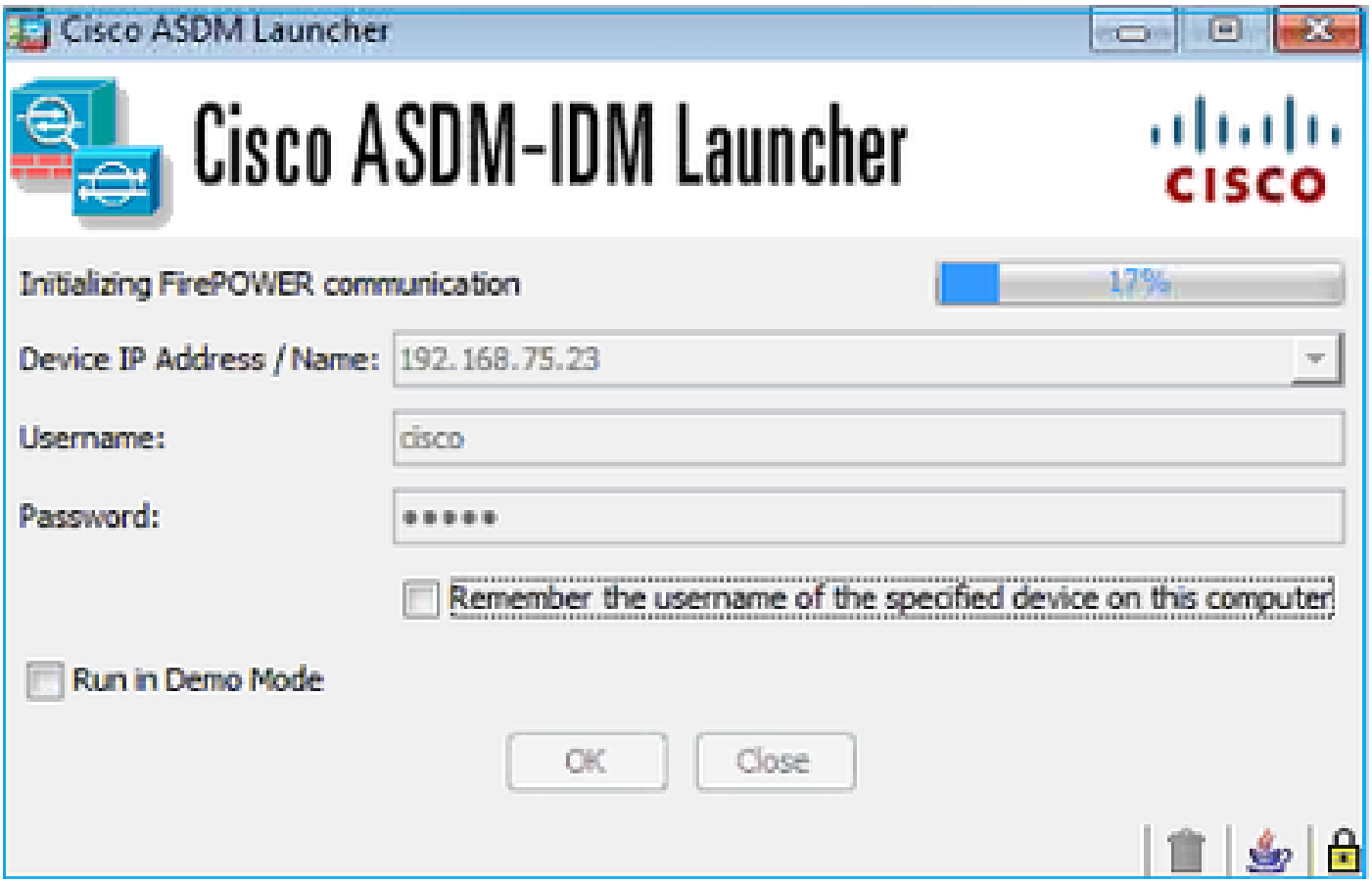
- show module:ASDMがASAモジュールを検出します。
- show module sfr details:ASDMは、Firepower管理IPアドレスを含むモジュールの詳細を検出します。

これらは、PCからASA IPアドレスへの一連のSSL接続としてバックグラウンドで表示されます。

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がFirepowerモジュールへの通信を開始します

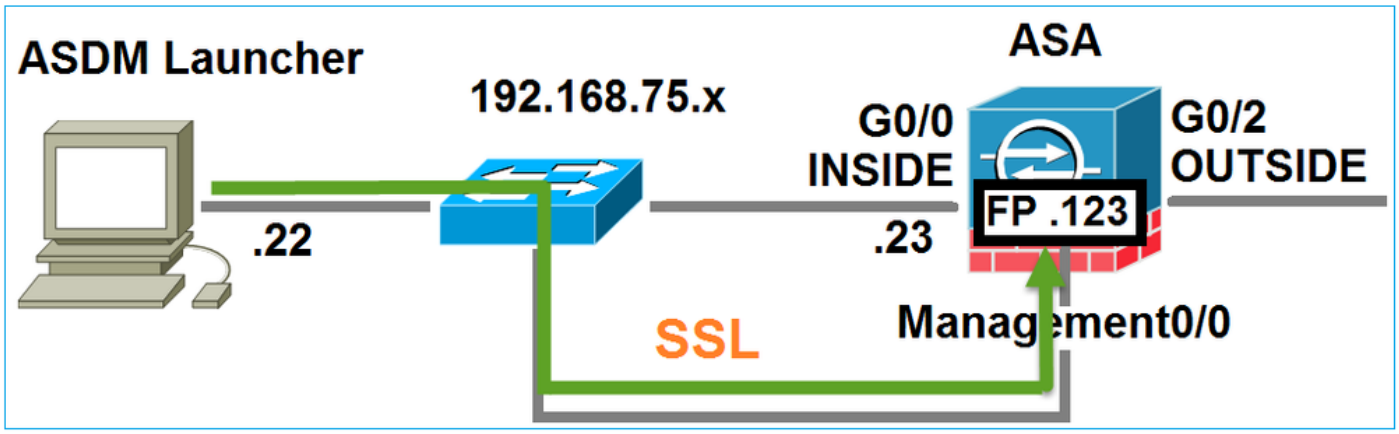
ASDMはモジュール管理IPアドレスを認識しているため、FirepowerへのSSLセッションを開始します。



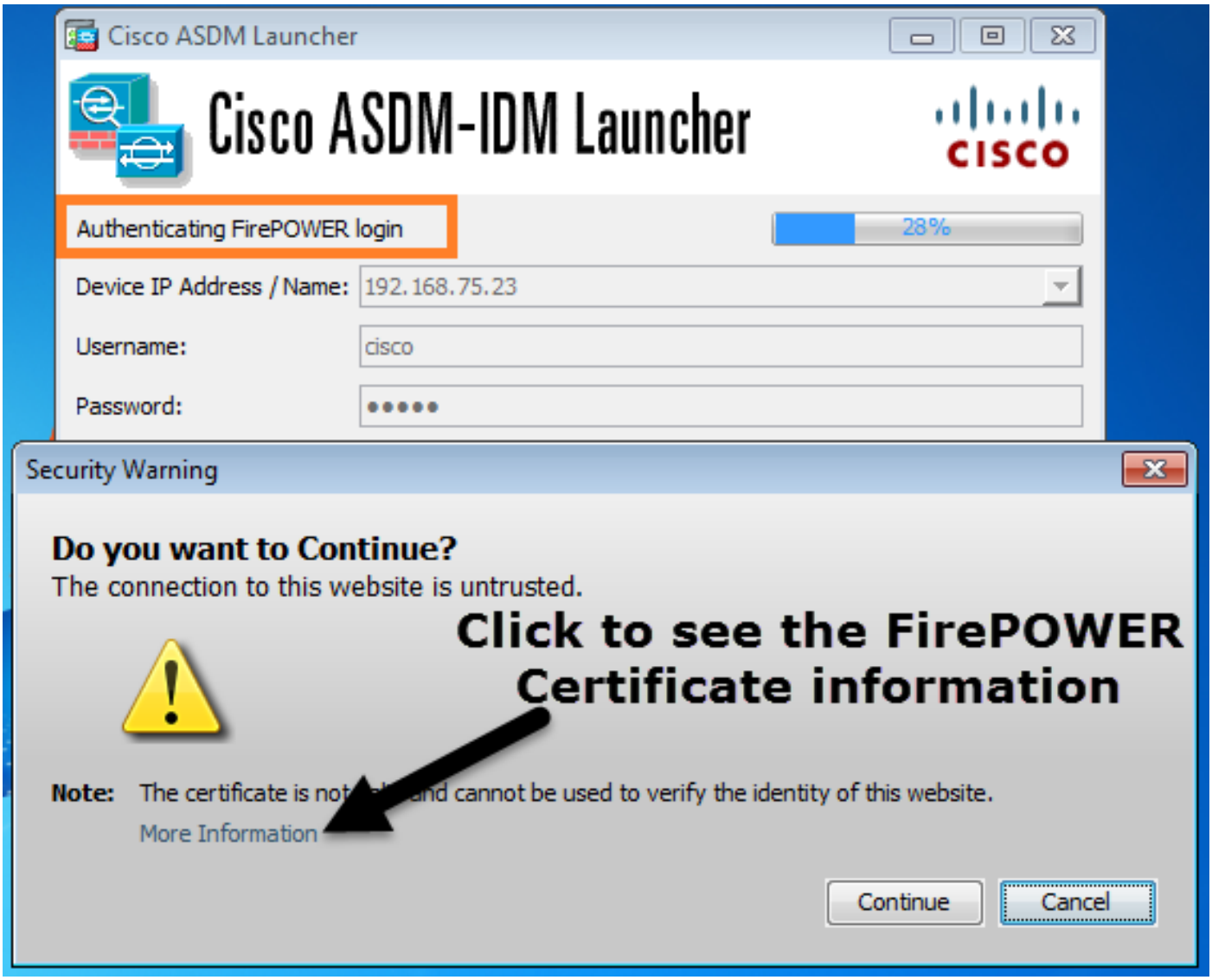
これは、ASDMホストからFirepower管理IPアドレスへのSSL接続としてバックグラウンドで表示されます。

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

これは次のように視覚化できます。

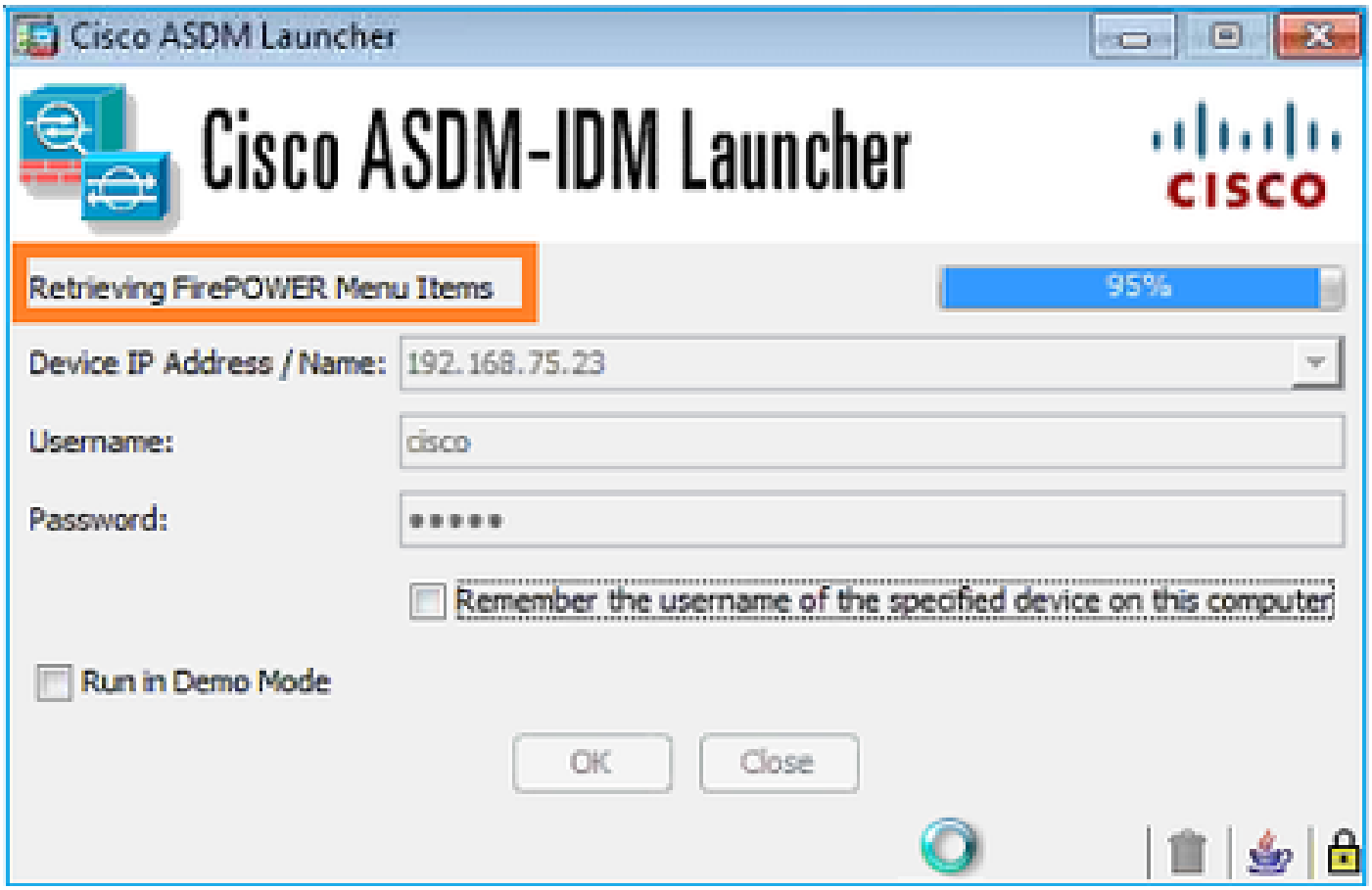


ASDMがFirepowerを認証し、Firepower証明書が自己署名されているため、セキュリティ警告が表示されます。

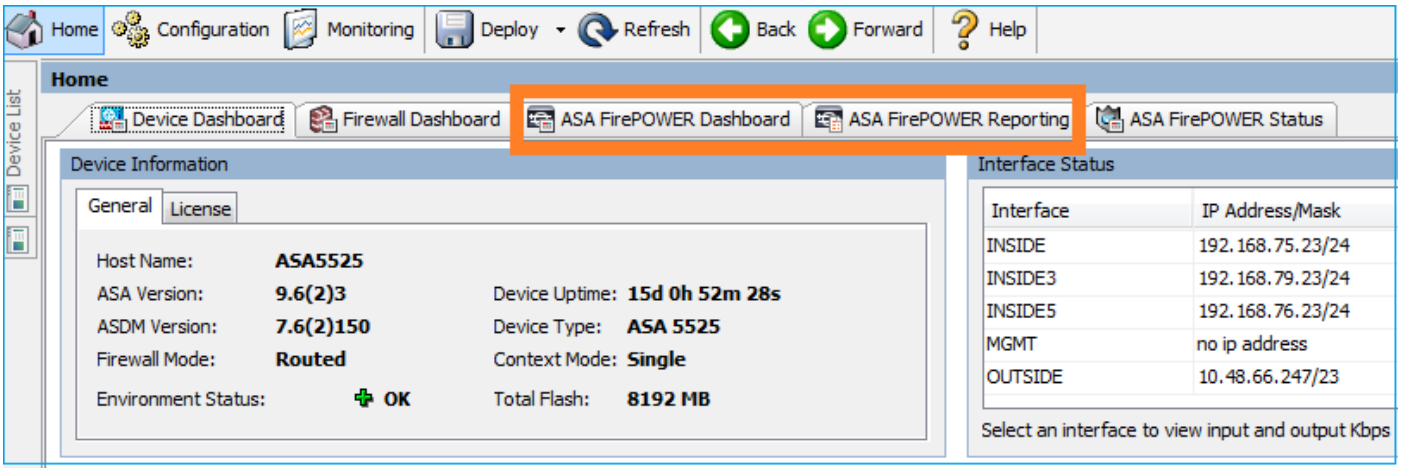


ステップ4:ASDMがFirepowerメニュー項目を取得する

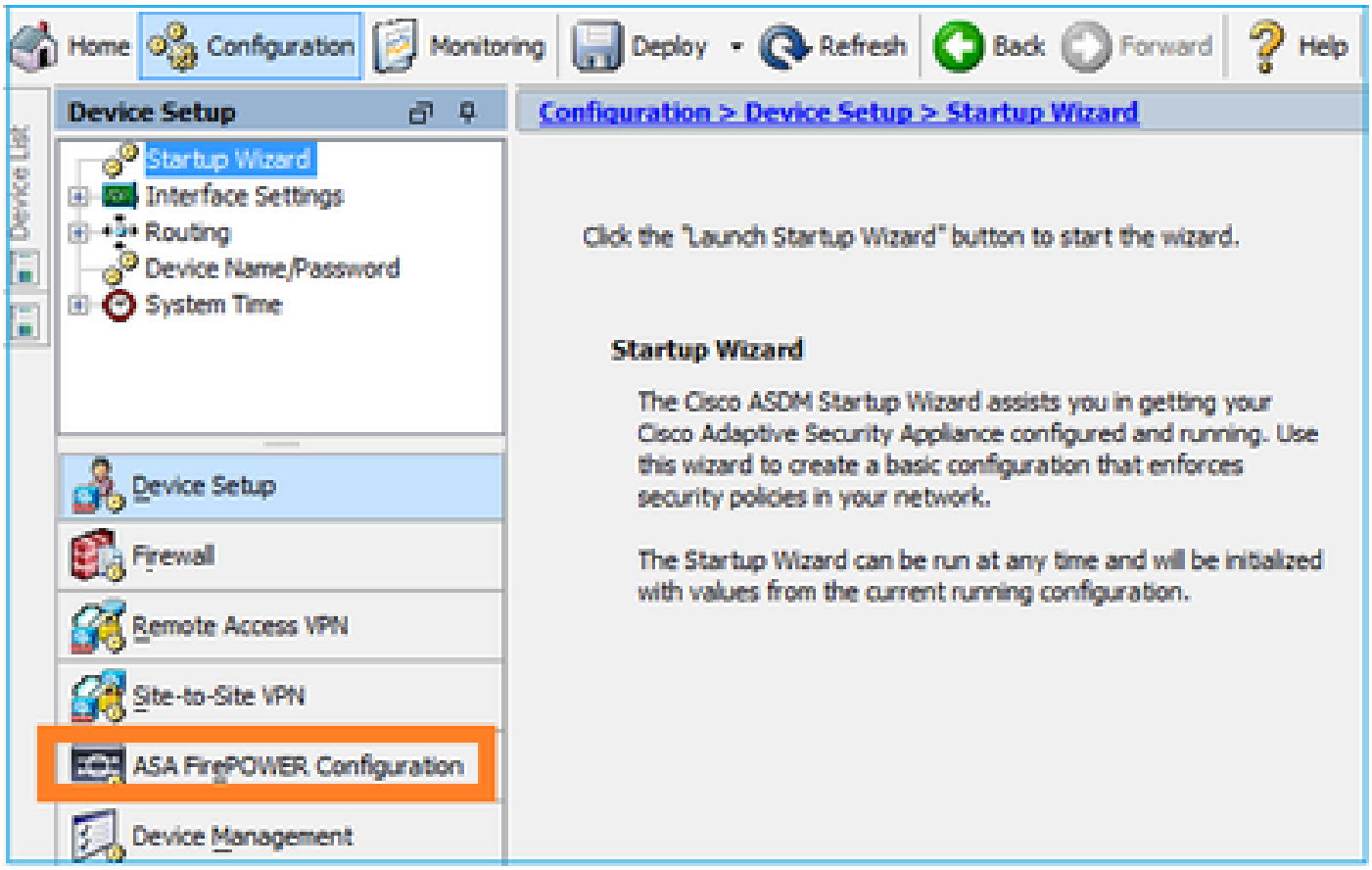
認証に成功すると、ASDMはFirepowerデバイスからMenu Itemsを取得します。



取得したタブを次の例に示します。

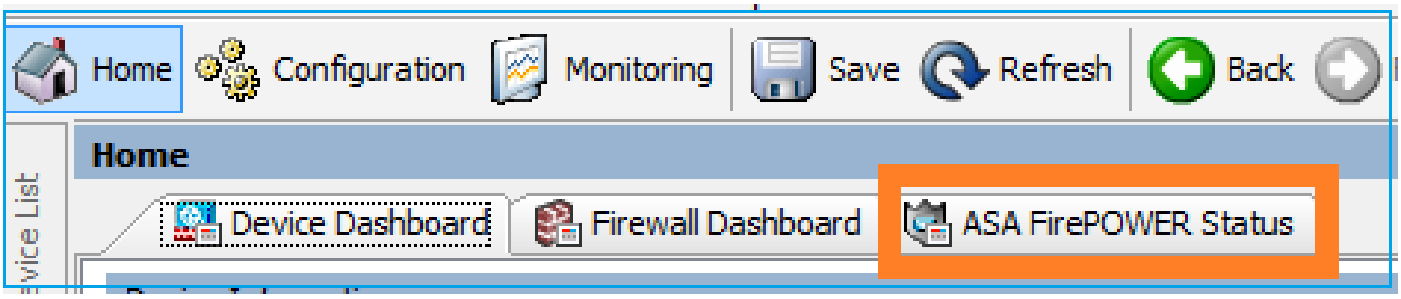


また、ASA FirePOWER 設定メニュー項目も取得します。

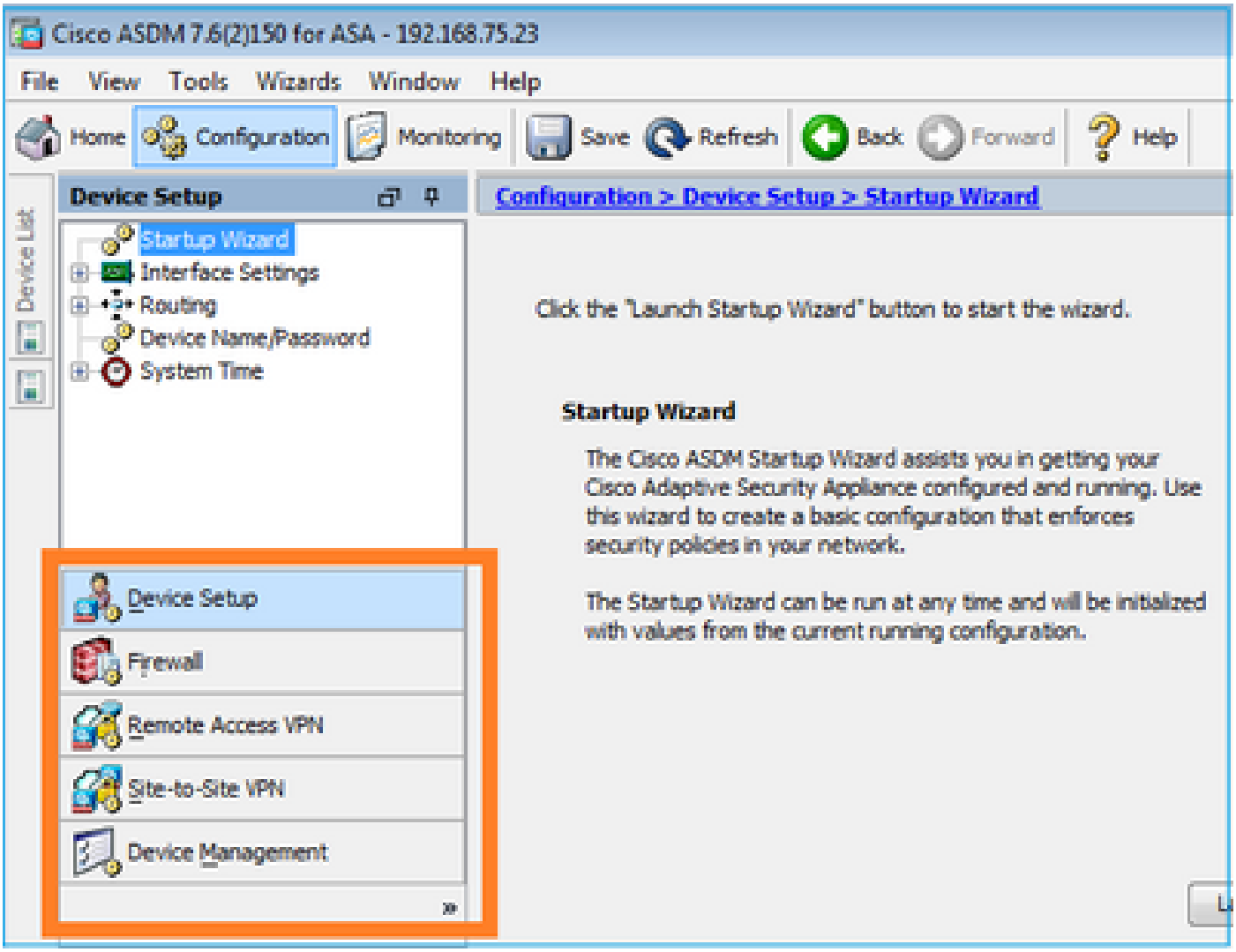


トラブルシュート

ASDMがFirepower管理IPアドレスを使用してSSLトンネルを確立できない場合、次のFirepowerメニュー項目のみがロードされます。



ASAFirepowerの設定項目も欠落しています。



検証 1

ASA 管理インターフェイスが稼働していて、そのインターフェイスに接続されているスイッチポートが適切な VLAN にあることを確認します。

```
<#root>

ASA5525#

show interface  ip brief | include Interface|Management0/0

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

up                    up
```

推奨されるトラブルシューティング

- 適切なVLANを設定します。
- ポートをアップにします(ケーブルをチェックし、スイッチポートの設定（速度/デュプレックス/シャットダウン）をチェックします)。

検証 2

firepowerモジュールが完全に初期化され、起動し、実行中であることを確認します。

<#root>

```
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
```

<#root>

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

>
```

推奨されるトラブルシューティング

- エラーや障害がないか、show module sfr log consoleコマンドの出力をチェックします。

検証 3

pingやtracert/tracerouteなどのコマンドを使用して、ASDMホストとFirepowerモジュール管理IP間の基本的な接続性を確認します。

```
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.
```

推奨されるトラブルシューティング

- パスに沿ったルーティングをチェックします。
- パス内にトラフィックをブロックするデバイスがないことを確認します。

検証 4

ASDMホストとFirepower管理IPアドレスが同じレイヤ3ネットワークにある場合は、ASDMホストのAddress Resolution Protocol（ARP；アドレス解決プロトコル）テーブルを確認します。

```
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
```

推奨されるトラブルシューティング

- ARPエントリがない場合は、Wiresharkを使用してARP通信を確認します。パケットのMACアドレスが正しいことを確認します。
- ARPエントリがある場合は、正しいことを確認します。

検証 5

ホストとFirepowerモジュールの間に適切なTCP通信があるかどうかを確認するには、ASDM経由で接続しているときにASDMデバイスでキャプチャを有効にします。少なくとも、次のように表示されます。

- ASDM ホストと ASA との間の TCP 3 ウェイ ハンドシェイク.
- ASDM ホストと ASA との間で確立された SSL トンネル.
- ASDMホストとFirepowerモジュール管理IPアドレス間のTCP 3ウェイハンドシェイク。
- ASDMホストとFirepowerモジュールの管理IPアドレスの間にSSLトンネルが確立されました。

推奨されるトラブルシューティング

- TCP 3ウェイハンドシェイクが失敗した場合は、パス内に非対称のトラフィックやデバイスが存在せず、TCPパケットがブロックされていないことを確認します。
- SSLに障害が発生した場合は、man-in-the-middle(MITM)を実行しているパスにデバイスが存在しないか確認します（サーバ証明書の発行者からヒントが提供されます）。

検証 6

firepowerモジュールとの間のトラフィックを確認するには、asa_mgmt_planeインターフェイスでキャプチャを有効にします。キャプチャで、次の内容を確認できます。

- ASDMホストからのARP要求（パケット42）。
- firepowerモジュール（パケット43）からのARP応答。
- ASDMホストとFirepowerモジュール間のTCP 3ウェイハンドシェイク（パケット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

45: 20:27:28.532549 192.168.75.123.443 > 192.168.75.22.48391:

S 1324352332:1324352332(0)

ack 2861923943 win 14600

46: 20:27:28.532839 192.168.75.22.48391 > 192.168.75.123.443: .

ack 1324352333 win 16695

推奨されるトラブルシューティング

- 検証5と同じです。

検証 7

ASDM ユーザに特権レベル 15 があることを確認します。これを確認する方法の1つは、ASDM経由で接続しているときにdebug http 255コマンドを入力することです。

<#root>

ASA5525#

debug http 255

```
debug http enabled at level 255.
HTTP: processing ASDM request [/admin/asdm_banner] with cookie-based authentication (aware_webvpn_conf.
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],
```

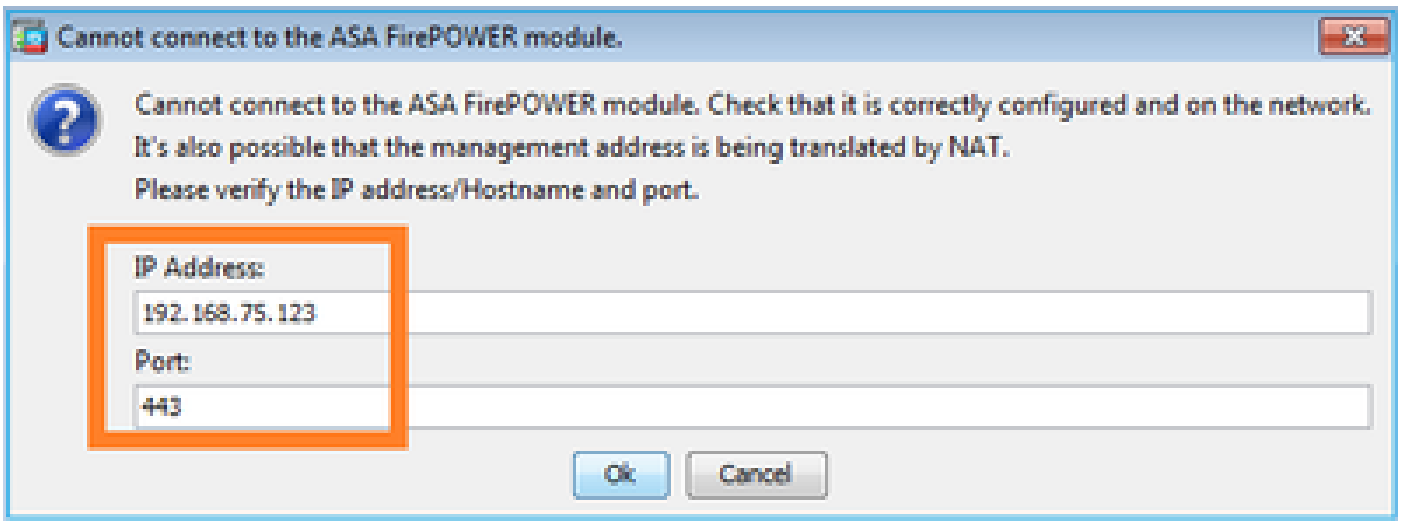
privilege = [14]

推奨されるトラブルシューティング

- 特権レベルが15でない場合は、レベル15のユーザで試してください。

検証 8

ASDMホストとFirepowerモジュールの間に、Firepower管理IPアドレスのネットワークアドレス変換(NAT)がある場合は、NAT変換されたIPアドレスを指定する必要があります。



推奨されるトラブルシューティング

- エンドポイント（ASA/SFRおよびエンドホスト）でのキャプチャがこれを確認します。

検証 9

firepowerモジュールがFMCによってまだ管理されていないことを確認します。管理されている場合は、ASDMのFirepowerタブが表示されません。

```
<#root>

ASA5525#

session sfr console

Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.
>

show managers

Managed locally.


>
```

もう1つの方法は、show module sfr detailsコマンドを使用する方法です。

```
<#root>

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
```

推奨されるトラブルシューティング

- デバイスがすでに管理されている場合は、ASDMから管理する前に登録解除する必要があります。『Firepower Management Center Configuration Guide』を参照してください。

検証 10

Wiresharkキャプチャをチェックして、ASDMクライアントが適切なTLSバージョン（TLSv1.2など）で接続することを確認します。

推奨されるトラブルシューティング

- ブラウザのSSL設定を調整します。
- 別のブラウザで試します。
- 別のエンドホストから試行します。

検証 11

Cisco ASA互換性ガイドで、ASA/ASDMイメージに互換性があることを確認します。

推奨されるトラブルシューティング

- 互換性のあるASDMイメージを使用します。

検証 12

firepowerデバイスがASDMバージョンと互換性があることを『Cisco ASA Compatibility』ガイドで確認します。

推奨されるトラブルシューティング

- 互換性のあるASDMイメージを使用します。

関連情報

- Cisco ASA FirePOWER モジュール クイック スタート ガイド
- ASA with FirePOWER Services バージョン 6.1.0 ローカル管理設定ガイド
- ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、および ASA5516-X 向けバージョン 5.4.1 ASA FirePOWER モジュール ユーザ ガイド
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。