ASDM을 사용하여 ASA에서 Firepower 모듈 관리

목차

소개

이 문서에서는 ASDM 소프트웨어가 ASA(Adaptive Security Appliance) 및 이에 설치된 Firepower 소프트웨어 모듈과 통신하는 방법에 대해 설명합니다.

배경 정보

ASA에 설치된 Firepower 모듈은 다음 중 하나로 관리할 수 있습니다.

- FMC(firepower 관리 센터) - 오프박스(off-box) 관리 솔루션입니다.
- ASDM(Adaptive Security Device Manager) - 온박스(on-box) 관리 솔루션입니다.

사전 요구 사항

요구 사항

ASDM 관리를 활성화하는 ASA 컨피그레이션:

```
<#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 모듈 간의 호환성을 확인하십시오. 그렇지 않으면 Firepower 탭이 표시되지 않습니다.

또한 ASA에서 3DES/AES 라이센스를 활성화해야 합니다.

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

ASDM 클라이언트 시스템에서 지원되는 버전의 Java JRE가 실행되는지 확인합니다.

사용되는 구성 요소

- Microsoft Windows 7 호스트
- ASA 버전 9.6(2.3)을 실행하는 ASA5525-X

- ASDM 버전 7.6.2.150
- Firepower 소프트웨어 모듈 6.1.0-330

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

아키텍처

ASA에는 3개의 내부 인터페이스가 있습니다.

- asa_dataplane - ASA 데이터 경로에서 Firepower 소프트웨어 모듈로 패킷을 리디렉션하는 데 사용됩니다.
- asa_mgmt_plane - Firepower 관리 인터페이스가 네트워크와 통신할 수 있도록 하는 데 사용됩니다.
- cplane - ASA와 Firepower 모듈 간에 킵얼라이브를 전송하는 데 사용되는 컨트롤 플레인 인터페이스입니다.

모든 내부 인터페이스에서 트래픽을 캡처할 수 있습니다.

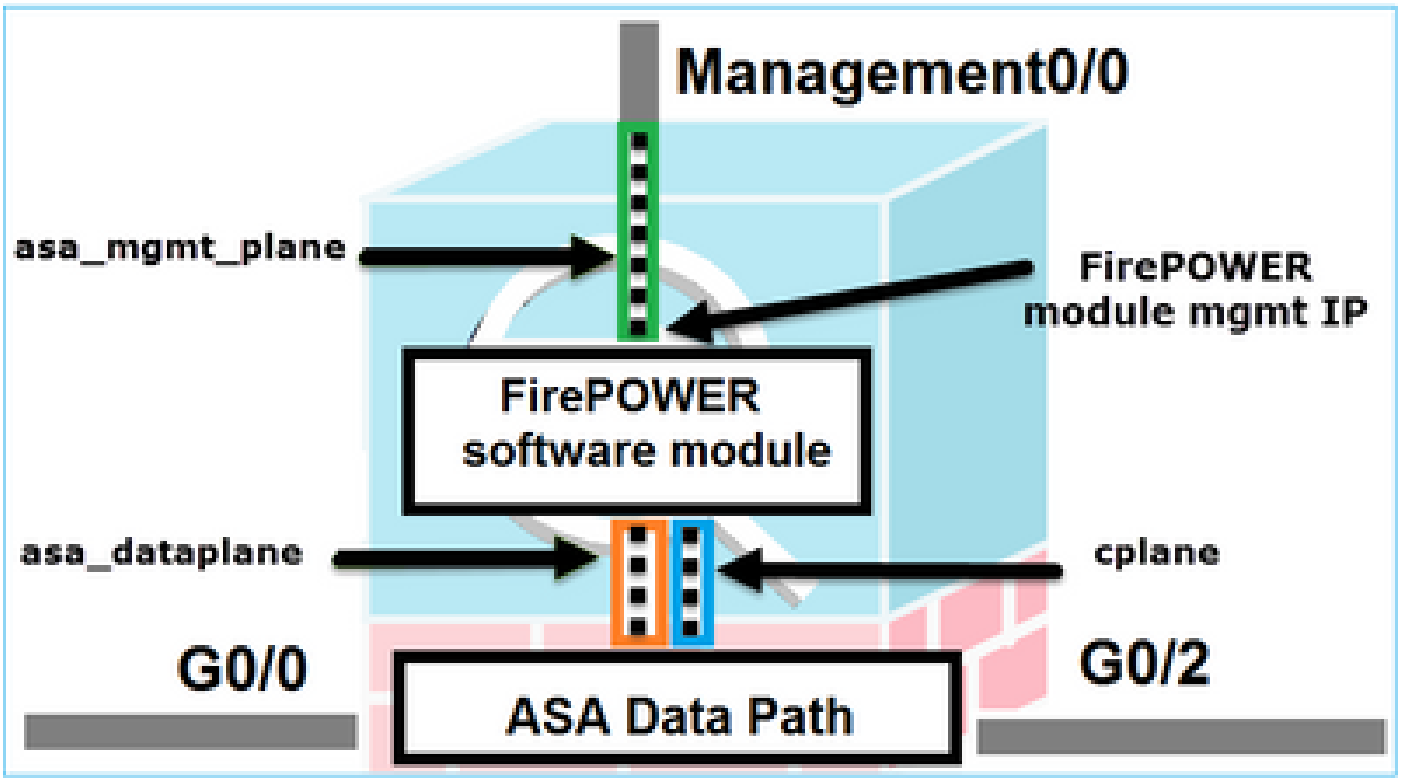
<#root>

ASA5525#

capture CAP interface ?

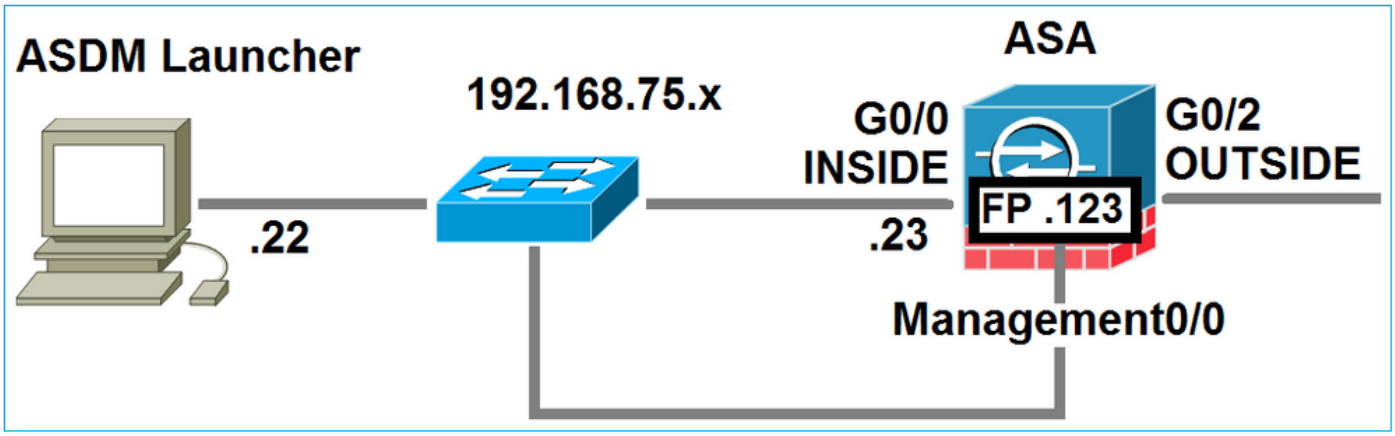
```
  asa_dataplane   Capture packets on dataplane interface
  asa_mgmt_plane  Capture packets on managementplane interface
  cplane          Capture packets on controlplane interface
```

이는 다음과 같이 시각화할 수 있습니다.



사용자가 ASDM을 통해 ASA에 연결할 때 백그라운드 작업

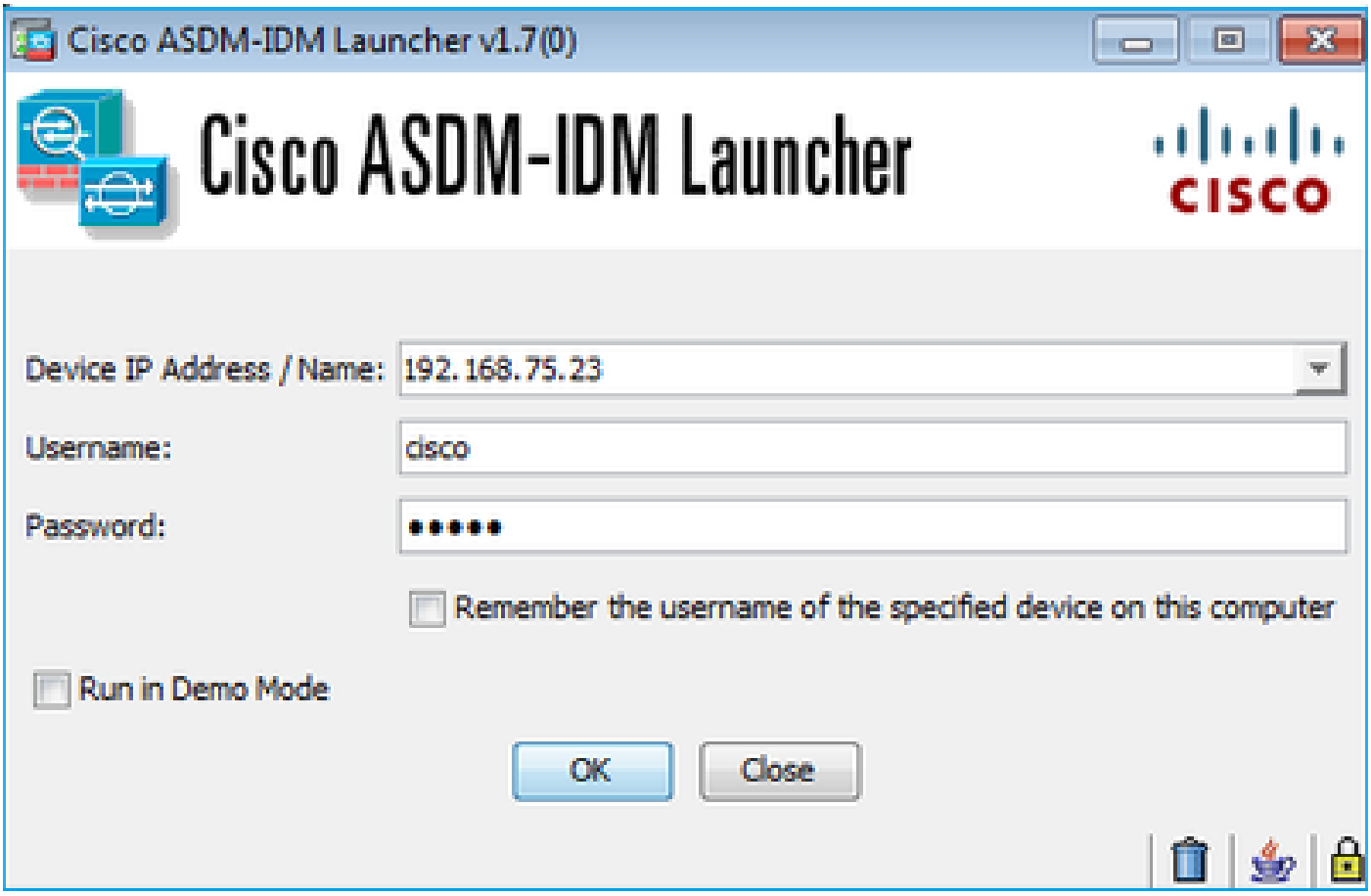
다음 토폴로지를 고려하십시오.



사용자가 ASA에 대한 ASDM 연결을 시작하면 다음과 같은 이벤트가 발생합니다.

1단계 - 사용자가 ASDM 연결을 시작합니다.

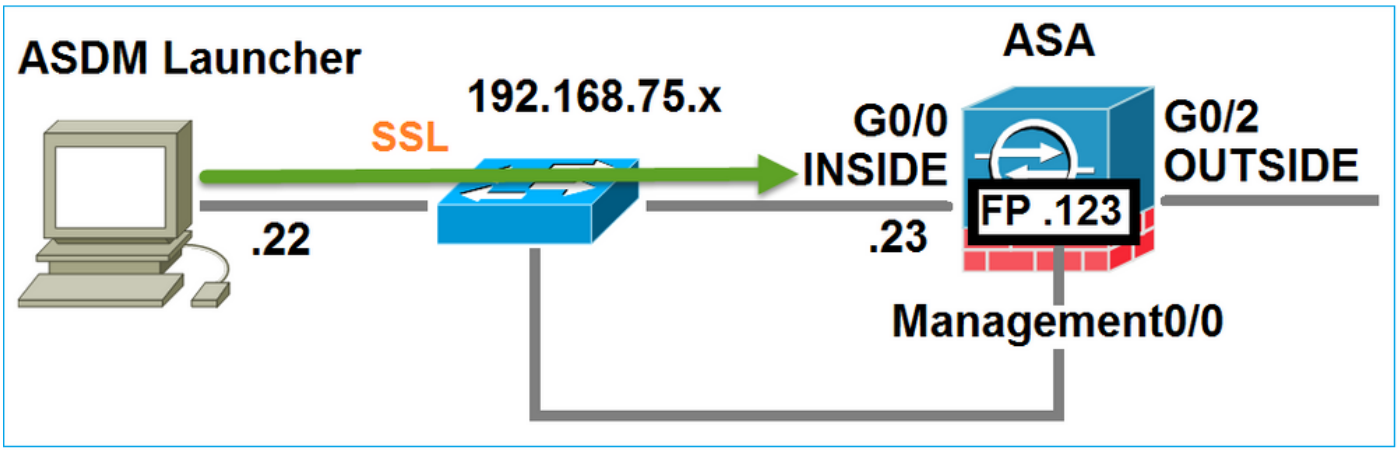
사용자는 HTTP 관리에 사용되는 ASA IP 주소를 지정하고, 자격 증명을 입력하고, ASA에 대한 연결을 시작합니다.



백그라운드에서 ASDM과 ASA 간의 SSL 터널이 설정됩니다.

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

이는 다음과 같이 시각화할 수 있습니다.



2단계 - ASDM에서 ASA 컨피그레이션 및 Firepower 모듈 IP 주소를 검색합니다.

ASDM이 ASA에 연결될 때 백그라운드에서 수행되는 모든 검사를 표시하려면 ASA에서 debug http 255 명령을 입력합니다.

<#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
```

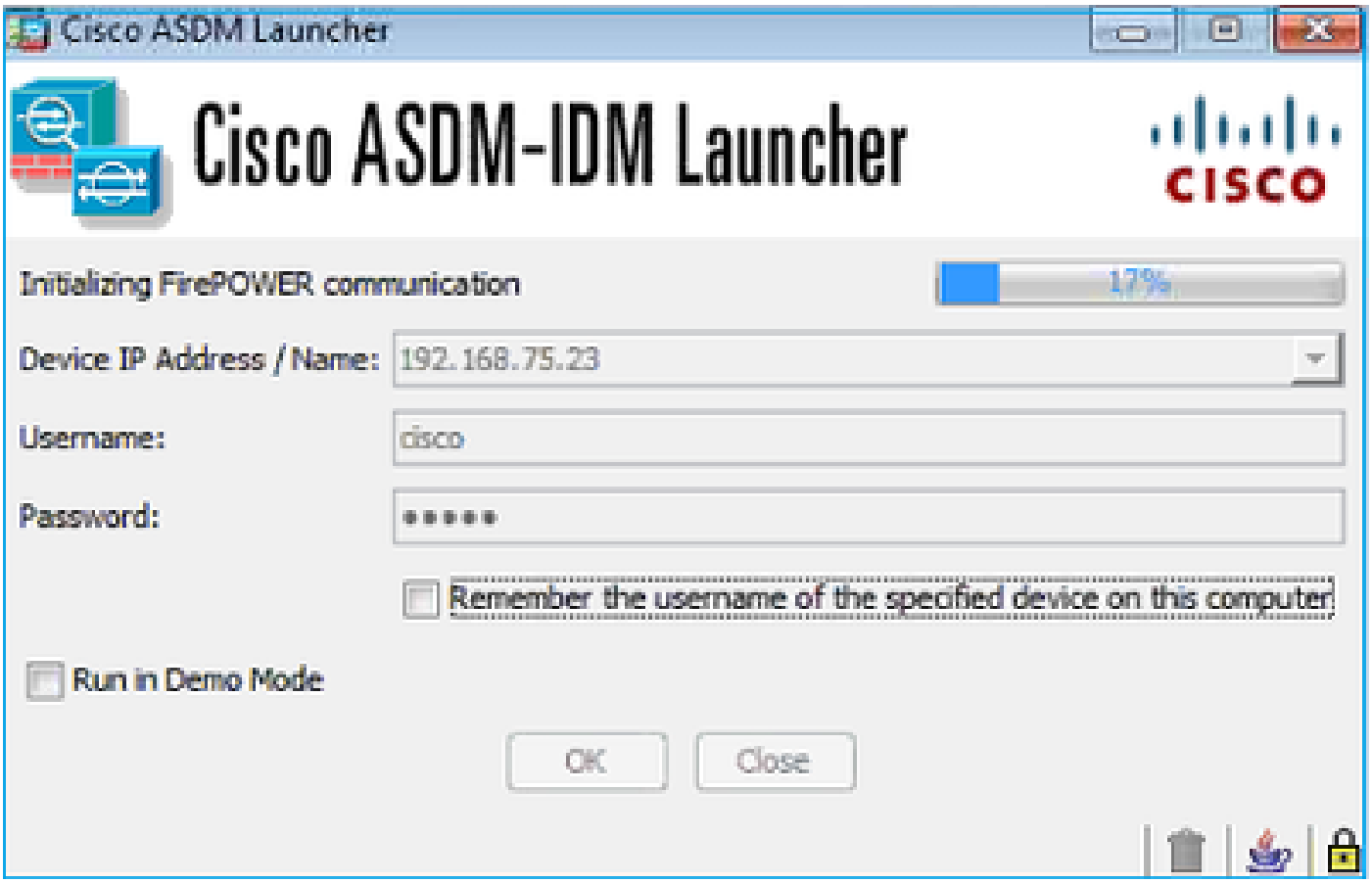
- show module - ASDM에서 ASA 모듈을 검색합니다.
- show module sfr details(모듈 sfr 세부사항 표시) - ASDM은 Firepower 관리 IP 주소를 포함하는 모듈 세부사항을 검색합니다.

이러한 연결은 PC에서 ASA IP 주소로 연결되는 일련의 SSL 연결로 백그라운드에서 표시됩니다.

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

3단계 - ASDM이 Firepower 모듈을 향해 통신을 시작합니다.

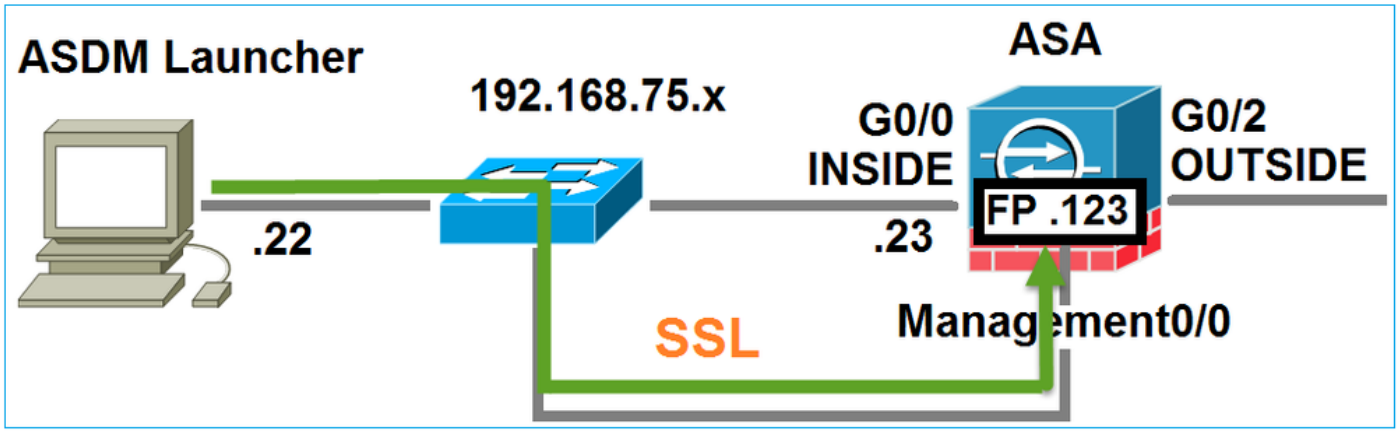
ASDM은 Firepower 관리 IP 주소를 알고 있으므로 모듈에 대해 SSL 세션을 시작합니다.



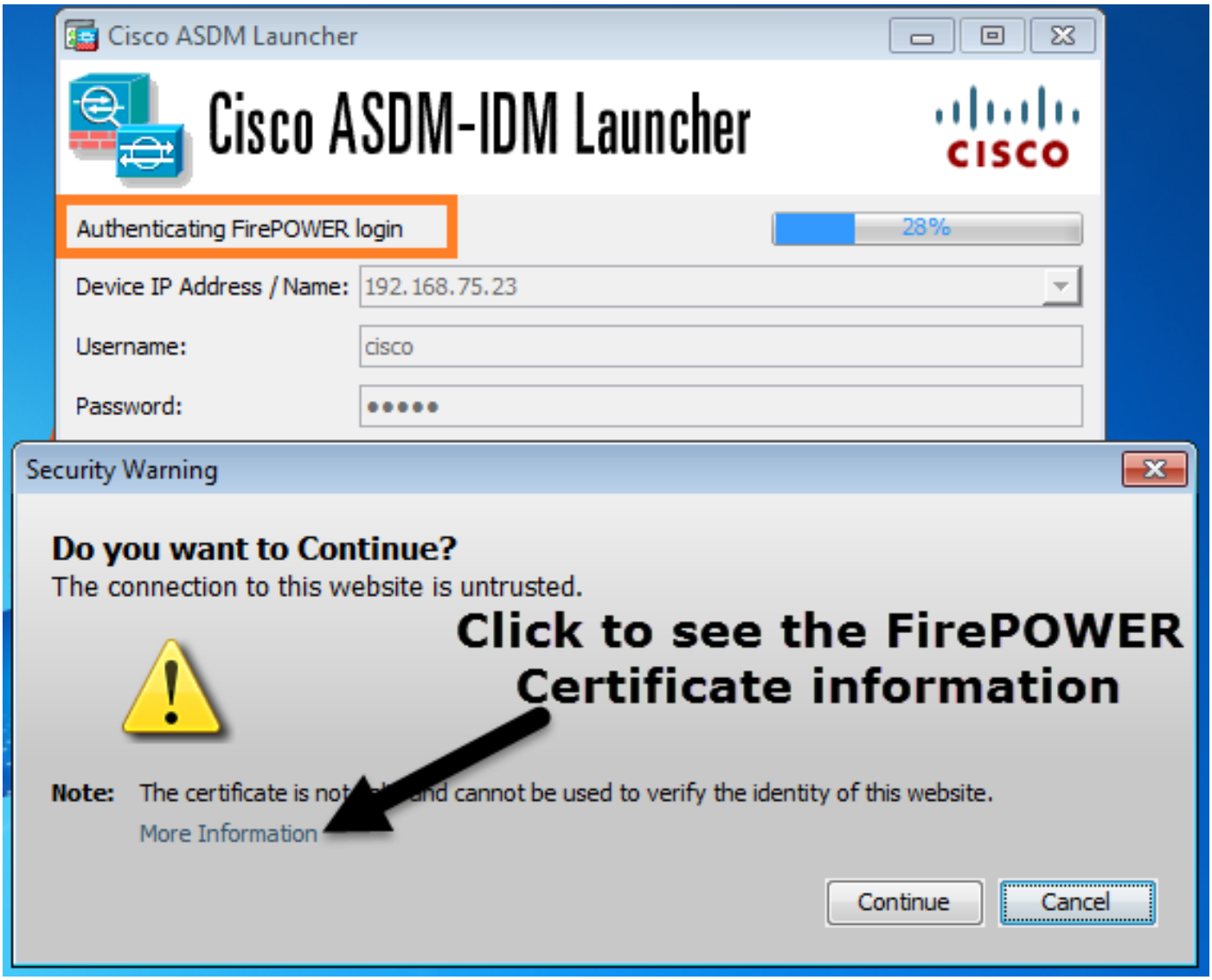
이는 백그라운드에서 ASDM 호스트에서 Firepower 관리 IP 주소로의 SSL 연결로 표시됩니다.

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

이는 다음과 같이 시각화할 수 있습니다.

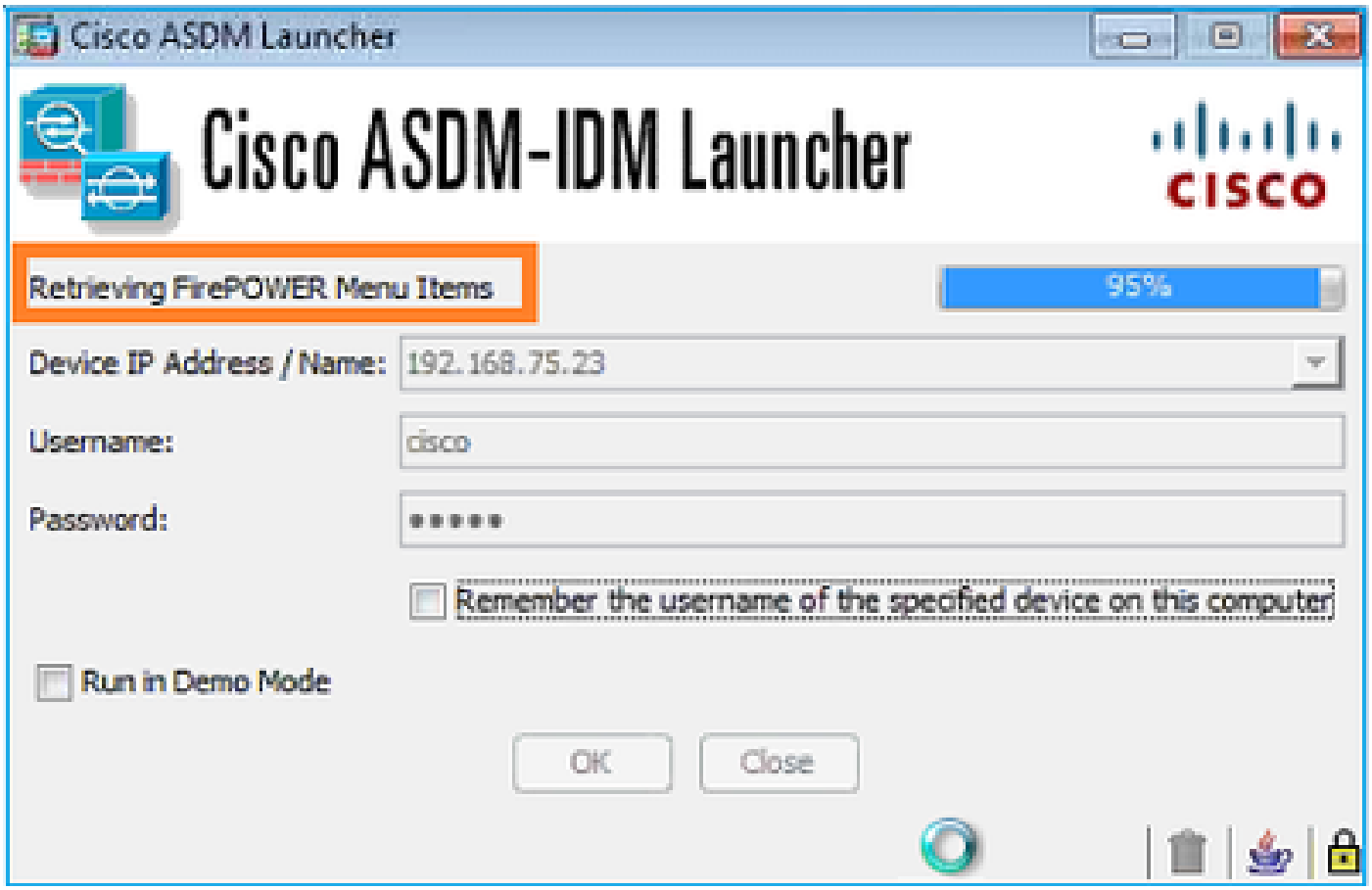


ASDM에서 Firepower을 인증하며 Firepower 인증서가 자체 서명되었으므로 보안 경고가 표시됩니다.

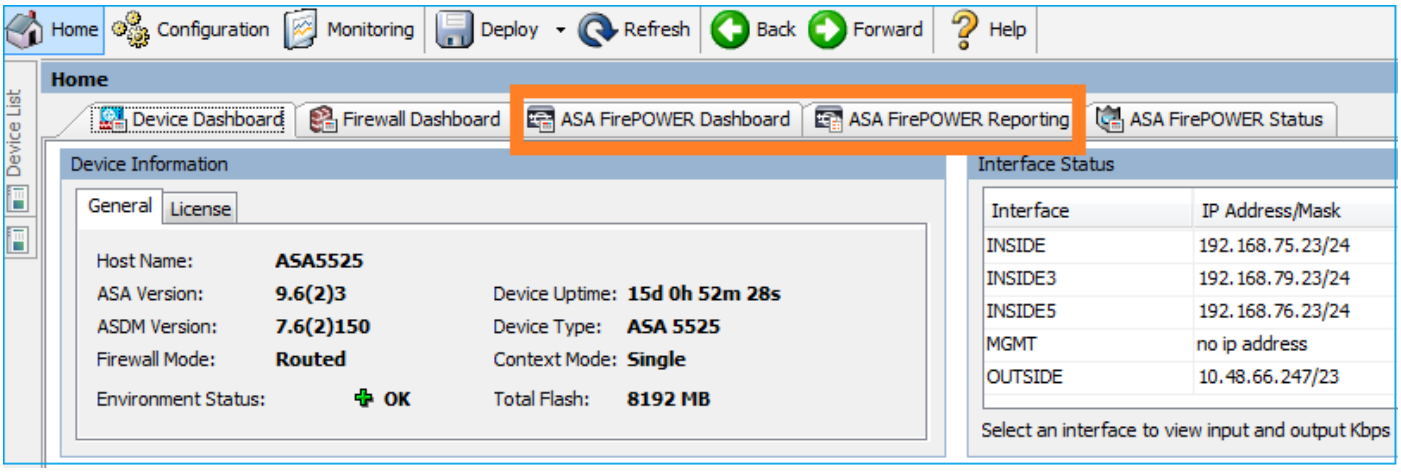


4단계 - ASDM에서 Firepower 메뉴 항목을 검색합니다.

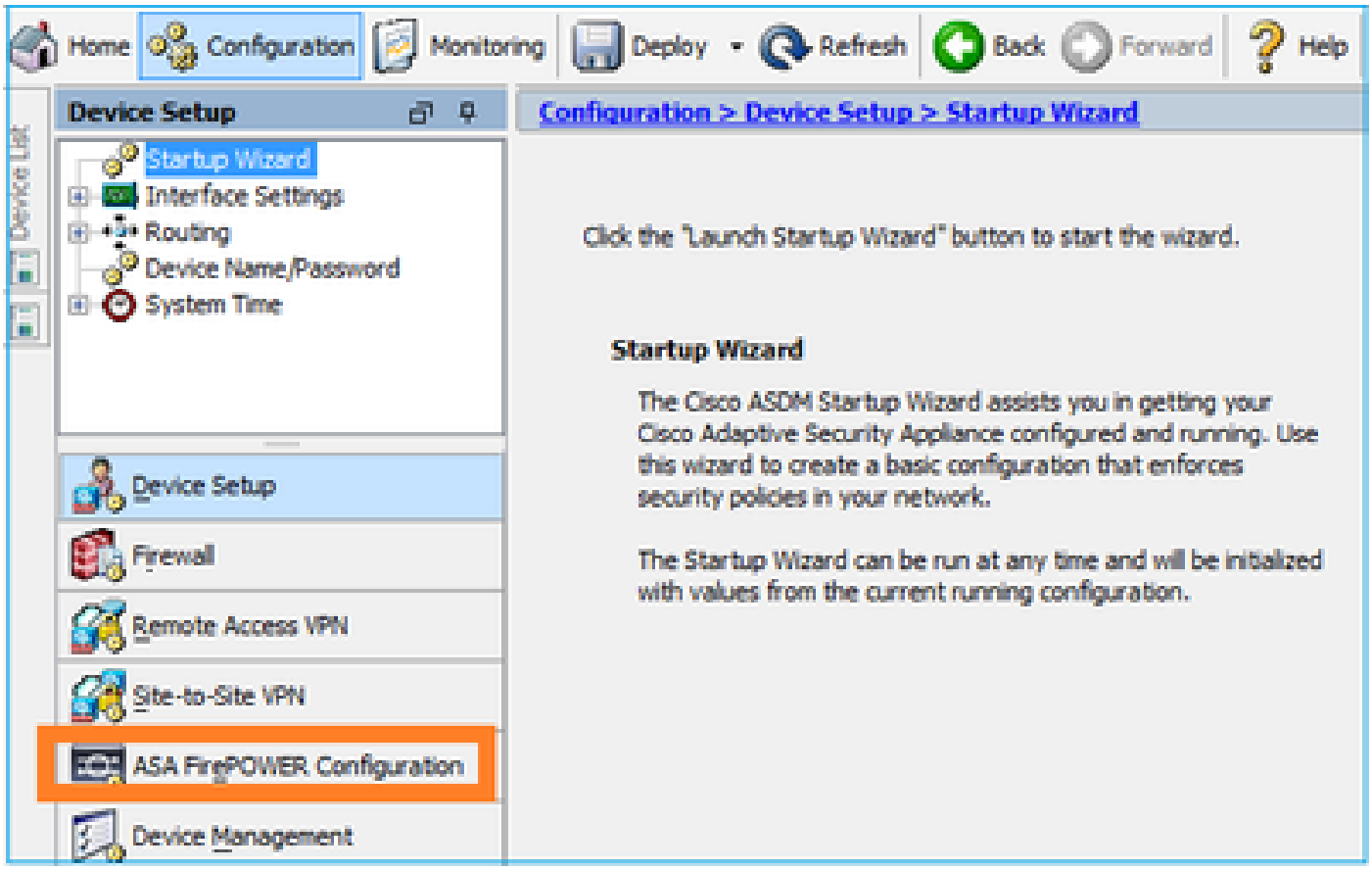
인증에 성공하면 ASDM은 Firepower 디바이스에서 메뉴 항목을 검색합니다.



검색된 탭은 다음 예에 나와 있습니다.

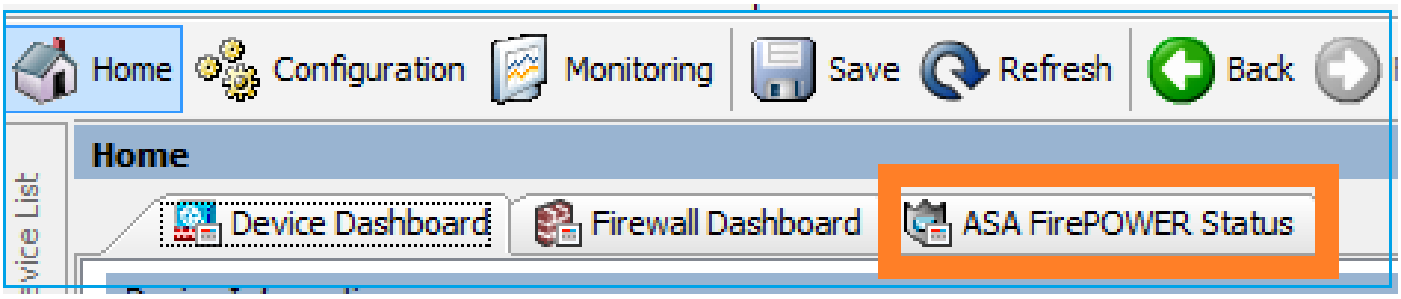


또한 ASA Firepower 컨피그레이션 메뉴 항목을 검색합니다.

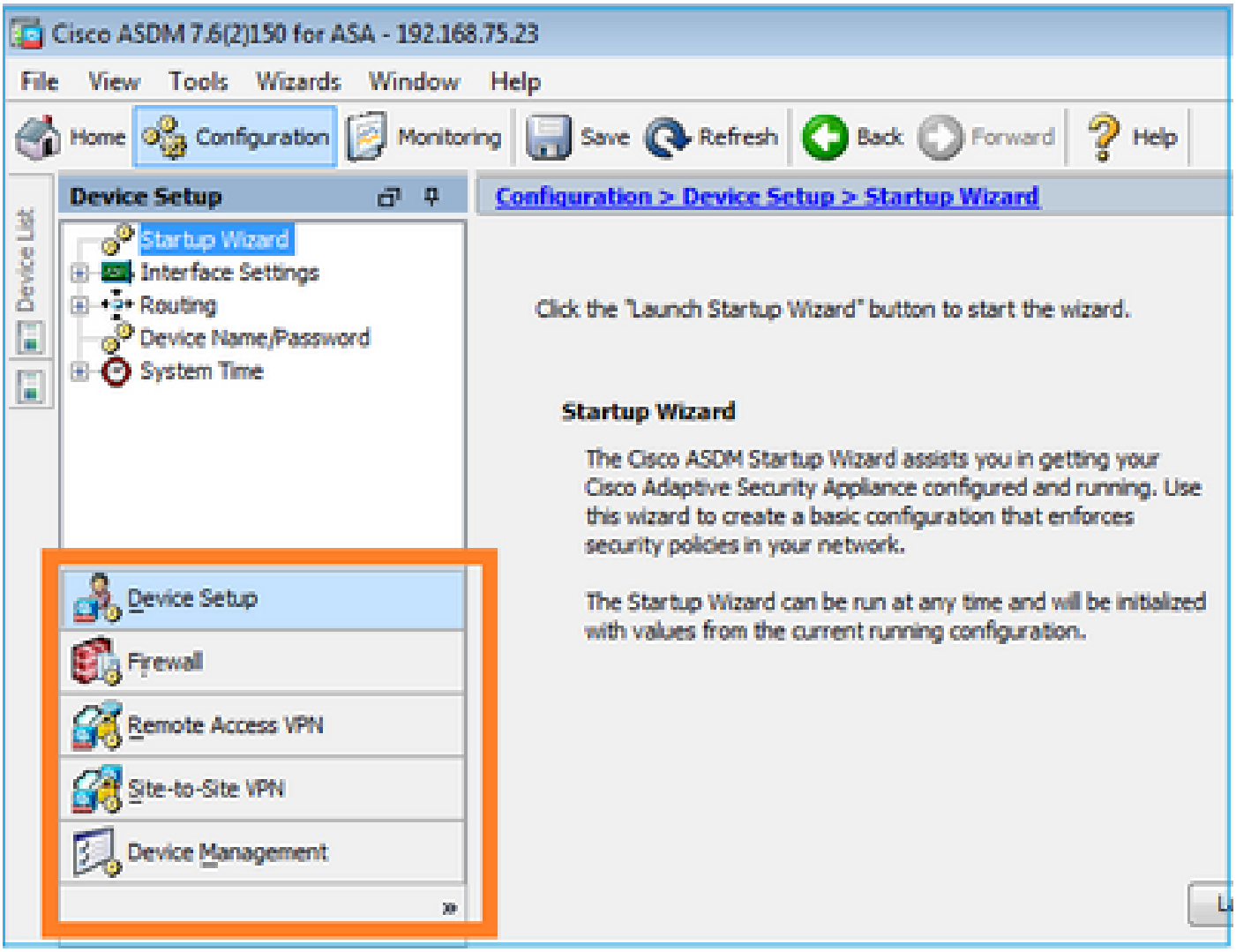


문제 해결

ASDM에서 Firepower 관리 IP 주소로 SSL 터널을 설정할 수 없는 경우 이 Firepower 메뉴 항목만 로드됩니다.



ASA Firepower 구성 항목도 없습니다.



확인 1

ASA 관리 인터페이스가 UP이고 여기에 연결된 스위치 포트가 올바른 VLAN에 있는지 확인합니다.

```
<#root>

ASA5525#

show interface  ip brief | include Interface|Management0/0

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

up                    up
```

권장 문제 해결

- 적절한 VLAN을 설정합니다.
- 포트를 가동합니다(케이블 확인, 스위치 포트 구성(속도/이중/차단) 확인).

확인 2

firepower 모듈이 완전히 초기화, 작동 및 실행 중인지 확인합니다.

<#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
----------------------------------------------------

>
```

권장 문제 해결

- show module sfr log console 명령의 출력에서 오류 또는 오류를 확인합니다.

확인 3

ping 및 tracert/traceroute와 같은 명령을 사용하여 ASDM 호스트와 Firepower 모듈 관리 IP 간의 기본 연결을 확인합니다.

```
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.
```

권장 문제 해결

- 경로를 따라 라우팅을 확인합니다.
- 경로에 트래픽을 차단하는 디바이스가 없는지 확인합니다.

확인 4

ASDM 호스트와 Firepower 관리 IP 주소가 동일한 레이어 3 네트워크에 있는 경우 ASDM 호스트에서 ARP(Address Resolution Protocol) 테이블을 확인합니다.

```
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
```

권장 문제 해결

- ARP 항목이 없는 경우 Wireshark를 사용하여 ARP 통신을 확인합니다. 패킷의 MAC 주소가 올바른지 확인합니다.
- ARP 항목이 있는 경우 해당 항목이 올바른지 확인합니다.

확인 5

호스트와 Firepower 모듈 사이에 적절한 TCP 통신이 있는지 확인하기 위해 ASDM을 통해 연결하는 동안 ASDM 디바이스에서 캡처를 활성화합니다. 최소한 다음 사항을 확인할 수 있습니다.

- ASDM 호스트와 ASA 간의 TCP 3-way 핸드셰이크.
- ASDM 호스트와 ASA 간에 설정된 SSL 터널입니다.
- ASDM 호스트와 Firepower 모듈 관리 IP 주소 간의 TCP 3-way 핸드셰이크.
- ASDM 호스트와 Firepower 모듈 관리 IP 주소 간에 설정된 SSL 터널.

권장 문제 해결

- TCP 3-way 핸드셰이크가 실패할 경우 TCP 패킷을 차단하는 경로에 비대칭 트래픽 또는 디바이스가 없는지 확인합니다.
- SSL이 실패할 경우 경로에 MITM(man-in-the-middle)을 수행하는 디바이스가 없는지 확인합니다(서버 인증서 발급자가 이에 대한 힌트를 제공함).

확인 6

firepower 모듈을 오가는 트래픽을 확인하려면 asa_mgmt_plane 인터페이스에서 capture를 활성화합니다. 캡처에서 다음을 볼 수 있습니다.

- ASDM 호스트의 ARP 요청(패킷 42).
- firepower 모듈의 ARP 응답(패킷 43).
- ASDM 호스트와 Firepower 모듈 간의 TCP 3-way 핸드셰이크(패킷 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

권장 문제 해결

- 확인 5와 동일합니다.

확인 7

ASDM 사용자에게 권한 레벨 15가 있는지 확인합니다. 이를 확인하는 한 가지 방법은 debug http 255 명령이 ASDM을 통해 연결되는 동안 이 명령을 입력하는 것입니다.

<#root>

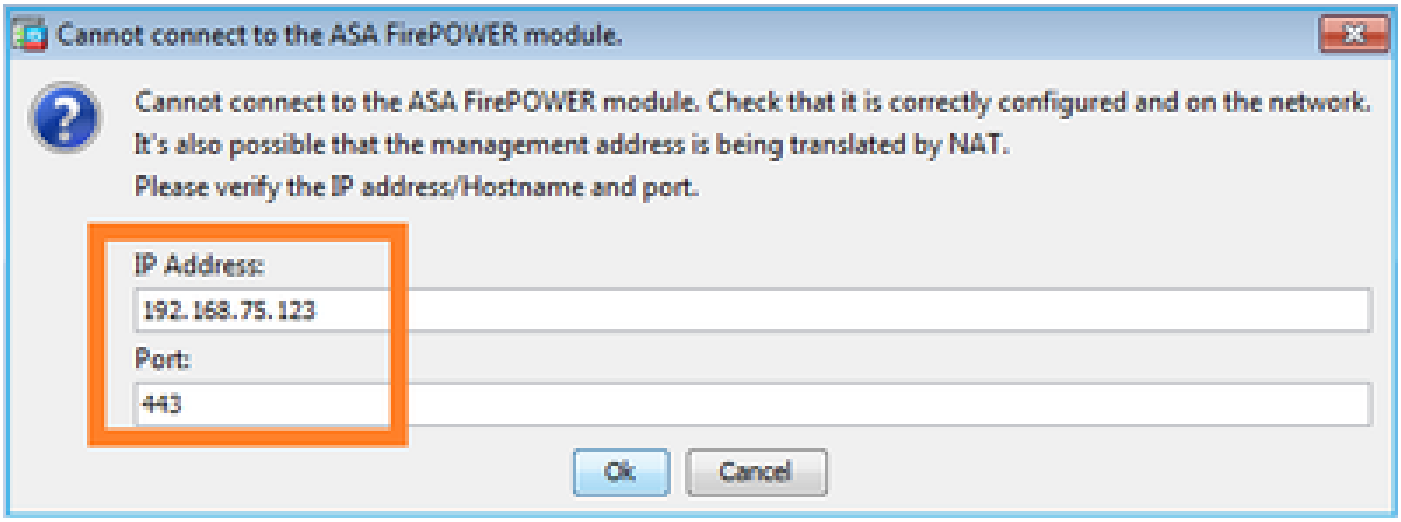
```
ASA5525#

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]
```

권장 문제 해결

- 권한 수준이 15가 아닌 경우 15가 있는 사용자로 시도합니다.

확인 8

ASDM 호스트와 Firepower 모듈 사이에 Firepower 관리 IP 주소에 대한 NAT(Network Address Translation)가 있는 경우 NATed IP 주소를 지정해야 합니다.



권장 문제 해결

- 엔드포인트(ASA/SFR 및 엔드 호스트)에서 이를 확인합니다.

확인 9

firepower 모듈이 FMC에서 아직 관리되지 않았는지 확인합니다. 이 경우 ASDM의 Firepower 탭이 누락되기 때문입니다.

<#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.


>
```

또 다른 방법은 show module sfr details 명령입니다.

<#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
```

권장 문제 해결

- 디바이스가 이미 관리되고 있는 경우 ASDM에서 관리하려면 먼저 등록을 취소해야 합니다. Firepower Management Center 컨피그레이션 가이드를 참조하십시오.

확인 10

ASDM 클라이언트가 적절한 TLS 버전(예: TLSv1.2)과 연결되는지 확인하려면 wireshark 캡처를 확인합니다.

권장 문제 해결

- 브라우저 SSL 설정을 조정합니다.
- 다른 브라우저를 사용해 보십시오.
- 다른 최종 호스트에서 시도하십시오.

확인 11

Cisco ASA 호환성 가이드에서 ASA/ASDM 이미지가 호환되는지 확인합니다.

권장 문제 해결

- 호환되는 ASDM 이미지를 사용합니다.

확인 12

Cisco ASA 호환성 가이드에서 Firepower 디바이스가 ASDM 버전과 호환되는지 확인합니다.

권장 문제 해결

- 호환되는 ASDM 이미지를 사용합니다.

관련 정보

- Cisco ASA Firepower 모듈 빠른 시작 설명서
- ASA with Firepower Services Local Management 컨피그레이션 가이드, 버전 6.1.0
- ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X 및 ASA5516-X 버전 5.4.1용 ASA Firepower 모듈 사용 설명서
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.