Introduction

This document describes how Adaptive Security Device Manager (ASDM) software communicates with the Adaptive Security Appliance (ASA) and a FirePOWER software module installed on it.

A FirePOWER module that is installed on an ASA can be managed by either:

- Firepower Management Center (FMC) - This is the off-box management solution.
- ASDM - This is the on-box management solution.

Prerequisites

Requirements

An ASA configuration to enable ASDM management:

```
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-if)#
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
```
Check the **compatibility** between the ASA/SFR module, otherwise the FirePOWER tabs will not be seen.

Additionally, on the ASA the 3DES/AES license should be enabled:

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

Ensure the ASDM client system runs a supported version of Java JRE.

**Components Used**

- A Microsoft Windows 7 host
- ASA5525-X that runs ASA Version 9.6(2.3)
- ASDM Version 7.6.2.150
- FirePOWER software module 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. If your network is live, ensure that you understand the potential impact of any command.

**Architecture**

The ASA has three internal interfaces:

- `asa_dataplane` - It is used to redirect packets from the ASA Data Path to the FirePOWER software module.
- `asa_mgmt_plane` - It is used to allow the FirePOWER management interface to communicate with the network.
- `cplane` - Control Plane interface that is used to transfer keepalives between the ASA and the FirePOWER module.

You can capture traffic in all internal interfaces:

```
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
```

This can be visualized as follows:
Background Operation When a User Connects to an ASA via ASDM

Consider this topology:

When a user initiates an ASDM connection to the ASA, these events will occur:

**Step 1 - The User Initiates the ASDM Connection**

The user specifies the ASA IP address used for HTTP management, enters the credentials, and initiates a connection towards the ASA:
In the background, an SSL tunnel between the ASDM and the ASA is established:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Data</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.75.22</td>
<td>192.168.75.23</td>
<td>TLSv1.2</td>
<td>252</td>
<td></td>
<td>Client Hello</td>
</tr>
</tbody>
</table>

This can be visualized as follows:

Step 2 - The ASDM Discovers the ASA Configuration and the FirePOWER Module IP Address

Enter the `debug http 255` command on the ASA in order to show all the checks that are done in the background when the ASDM connects to the 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+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 - The ASDM discovers the ASA modules.
- show module sfr details - The ASDM discovers the module details, which include the FirePOWER management IP address.

These will be seen in the background as a series of SSL connections from the PC towards the ASA IP address:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Data</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.75.22</td>
<td>192.168.75.23</td>
<td>TLSv1.2</td>
<td>252</td>
<td>Client Hello</td>
<td></td>
</tr>
<tr>
<td>192.168.75.22</td>
<td>192.168.75.23</td>
<td>TLSv1.2</td>
<td>284</td>
<td>Client Hello</td>
<td></td>
</tr>
<tr>
<td>192.168.75.22</td>
<td>192.168.75.23</td>
<td>TLSv1.2</td>
<td>284</td>
<td>Client Hello</td>
<td></td>
</tr>
<tr>
<td>192.168.75.22</td>
<td>192.168.75.23</td>
<td>TLSv1.2</td>
<td>284</td>
<td>Client Hello</td>
<td></td>
</tr>
<tr>
<td>192.168.75.22</td>
<td>192.168.75.23</td>
<td>TLSv1.2</td>
<td>284</td>
<td>Client Hello</td>
<td></td>
</tr>
<tr>
<td>192.168.75.22</td>
<td>192.168.75.23</td>
<td>TLSv1.2</td>
<td>284</td>
<td>Client Hello</td>
<td></td>
</tr>
<tr>
<td>192.168.75.22</td>
<td>192.168.75.23</td>
<td>TLSv1.2</td>
<td>284</td>
<td>Client Hello</td>
<td></td>
</tr>
<tr>
<td>192.168.75.22</td>
<td>192.168.75.23</td>
<td>TLSv1.2</td>
<td>284</td>
<td>Client Hello</td>
<td></td>
</tr>
<tr>
<td>192.168.75.22</td>
<td>192.168.75.23</td>
<td>TLSv1.2</td>
<td>284</td>
<td>Client Hello</td>
<td></td>
</tr>
<tr>
<td>192.168.75.22</td>
<td>192.168.75.23</td>
<td>TLSv1.2</td>
<td>284</td>
<td>Client Hello</td>
<td></td>
</tr>
<tr>
<td>192.168.75.22</td>
<td>192.168.75.23</td>
<td>TLSv1.2</td>
<td>284</td>
<td>Client Hello</td>
<td></td>
</tr>
</tbody>
</table>

**Step 3 - The ASDM Initiates Communication Towards the FirePOWER Module**

Since the ASDM knows the FirePOWER management IP address, it initiates SSL sessions towards the module:
This will be seen in the background as SSL connections from the ASDM host towards the FirePOWER management IP address:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Data</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.75.22</td>
<td>192.168.75.123</td>
<td>TLSv1.2</td>
<td>252</td>
<td>Client Hello</td>
<td></td>
</tr>
<tr>
<td>192.168.75.22</td>
<td>192.168.75.123</td>
<td>TLSv1.2</td>
<td>220</td>
<td>Client Hello</td>
<td></td>
</tr>
</tbody>
</table>

This can be visualized as follows:

The ASDM authenticates the FirePOWER and a security warning is shown since the FirePOWER Certificate is self-signed:
Step 4 - The ASDM Retrieves the FirePOWER Menu Items

After the successful authentication, the ASDM retrieves the Menu Items from the FirePOWER device:
The retrieved tabs are shown in this example:

It also retrieves the ASA FirePOWER Configuration Menu Item:
Troubleshoot

In case ASDM cannot establish an SSL tunnel with the FirePOWER Management IP address, then it will only load this FirePOWER Menu Item:

The ASA FirePOWER Configuration Item will be missing as well:
Verification 1

Make sure that the ASA management interface is UP and the switchport connected to it is in the proper VLAN:

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

**Recommended Troubleshooting**

- Set the proper VLAN.
- Bring the port UP (check the cable, check the switchport configuration (speed/duplex/shut)).

Verification 2

Make sure that the FirePOWER module is fully initialized, UP, and running:

```
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
```
Recommended Troubleshooting

- Check the output of the `show module sfr log console` command for errors or failures.

Verification 3

Check basic connectivity between the ASDM host and the FirePOWER module management IP with commands such as `ping` and `tracert/traceroute`:
Recommended Troubleshooting

- Check routing along the path.
- Verify that there are no devices in the path that block the traffic.

Verification 4

If the ASDM host and the FirePOWER management IP address are in the same Layer 3 network, check the Address Resolution Protocol (ARP) table on the ASDM host:

![ARP Table](image.jpg)

Recommended Troubleshooting

- If there are no ARP entries, use Wireshark in order to check the ARP communication. Ensure the MAC addresses of the packets are correct.
- If there are ARP entries, ensure they are correct.

Verification 5

Enable capture on the ASDM device while you connect via ASDM in order to see if there is proper TCP communication between the host and the FirePOWER module. At a minimum, you should see:

- TCP 3-way handshake between the ASDM host and the ASA.
- SSL tunnel established between the ASDM host and the ASA.
- TCP 3-way handshake between the ASDM host and the FirePOWER module management IP address.
- SSL tunnel established between the ASDM host and the FirePOWER module management IP address.

Recommended Troubleshooting

- If the TCP 3-way handshake fails, ensure that there is not asymmetric traffic or devices in the path that block the TCP packets.
- If SSL fails, check if there is no device in the path doing man-in-the-middle (MITM) (the Server Certificate Issuer will give a hint for this).

Verification 6

In order to check the traffic to and from the FirePOWER module, enable capture on the asa_mgmt_plane interface. In the capture, you can see the:

- ARP request from the ASDM host (packet 42).
- ARP reply from the FirePOWER module (packet 43).
- TCP 3-way handshake between the ASDM host and the FirePOWER module (packets 44-46).

ASA5525# capture FP_MGMT interface asa_mgmt_plane
Recommended Troubleshooting

- Same as in Verification 5.

Verification 7

Verify that the ASDM user has privilege level 15. One way to confirm this is to enter the `debug http 255` command while it connects 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 [A27614B0204B0078CF058989AAC80CE5159544A1B3EE62661F99D475DC]
HTTP: Admin session idle-timeout reset
HTTP: admin session verified = [1]
HTTP: username = [user1], privilege = [14]
```

Recommended Troubleshooting

- If the privilege level is not 15, then try with a user that has level 15.

Verification 8

If between the ASDM host and the FirePOWER module there is network address translation (NAT) for the FirePOWER Management IP address, then you need to specify the NATed IP address:

```
Cannot connect to the ASA FirePOWER module.

Cannot connect to the ASA FirePOWER module. Check that it is correctly configured and on the network. It's also possible that the management address is being translated by NAT. Please verify the IP address/Hostname and port.

IP Address: 192.168.75.123
Port: 443
```

Recommended Troubleshooting

- Captures at the end points (ASA/SFR and end-host) will confirm this.
Verification 9

Make sure that the FirePOWER module is not already managed by FMC, because in that case the FirePOWER tabs in ASDM will be missing:

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

Another method is with the **show module sfr details** command:

ASA5525# show module sfr details
Getting details from the Service Module, please wait...

<table>
<thead>
<tr>
<th>Card Type</th>
<th>FirePOWER Services Software Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>ASA5525</td>
</tr>
<tr>
<td>Hardware version</td>
<td>N/A</td>
</tr>
<tr>
<td>Serial Number</td>
<td>FCH1719J54R</td>
</tr>
<tr>
<td>Firmware version</td>
<td>N/A</td>
</tr>
<tr>
<td>Software version</td>
<td>6.1.0-330</td>
</tr>
<tr>
<td>MAC Address Range</td>
<td>6c41.6aa1.2bf2 to 6c41.6aa1.2bf2</td>
</tr>
<tr>
<td>App. name</td>
<td>ASA FirePOWER</td>
</tr>
<tr>
<td>App. Status</td>
<td>Up</td>
</tr>
<tr>
<td>App. Status Desc</td>
<td>Normal Operation</td>
</tr>
<tr>
<td>App. version</td>
<td>6.1.0-330</td>
</tr>
<tr>
<td>Data Plane Status</td>
<td>Up</td>
</tr>
<tr>
<td>Console session</td>
<td>Ready</td>
</tr>
<tr>
<td>Status</td>
<td>Up</td>
</tr>
<tr>
<td>DC addr</td>
<td>No DC Configured</td>
</tr>
<tr>
<td>Mgmt IP addr</td>
<td>192.168.75.123</td>
</tr>
<tr>
<td>Mgmt Network mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Mgmt Gateway</td>
<td>192.168.75.23</td>
</tr>
<tr>
<td>Mgmt web ports</td>
<td>443</td>
</tr>
<tr>
<td>Mgmt TLS enabled</td>
<td>true</td>
</tr>
</tbody>
</table>

**Recommended Troubleshooting**

- If the device is already managed, you need to unregister it before you manage it from ASDM. See the [Firepower Management Center Configuration Guide](#).

Verification 10

Check the wireshark capture in order to ensure the ASDM client connects with a proper TLS version (for example, TLSv1.2).

**Recommended Troubleshooting**

- Tune the browser SSL settings.
- Try with another browser.
- Try from another end-host.

Verification 11
Verify in the Cisco ASA Compatibility guide that the ASA/ASDM images are compatible.

**Recommended Troubleshooting**

- Use a compatible ASDM image.

**Verification 12**

Verify in the Cisco ASA Compatibility guide that the FirePOWER device is compatible with the ASDM version.

**Recommended Troubleshooting**

- Use a compatible ASDM image.

**Related Information**

- Cisco ASA FirePOWER Module Quick Start Guide
- ASA with FirePOWER Services Local Management Configuration Guide, Version 6.1.0
- Technical Support & Documentation - Cisco Systems