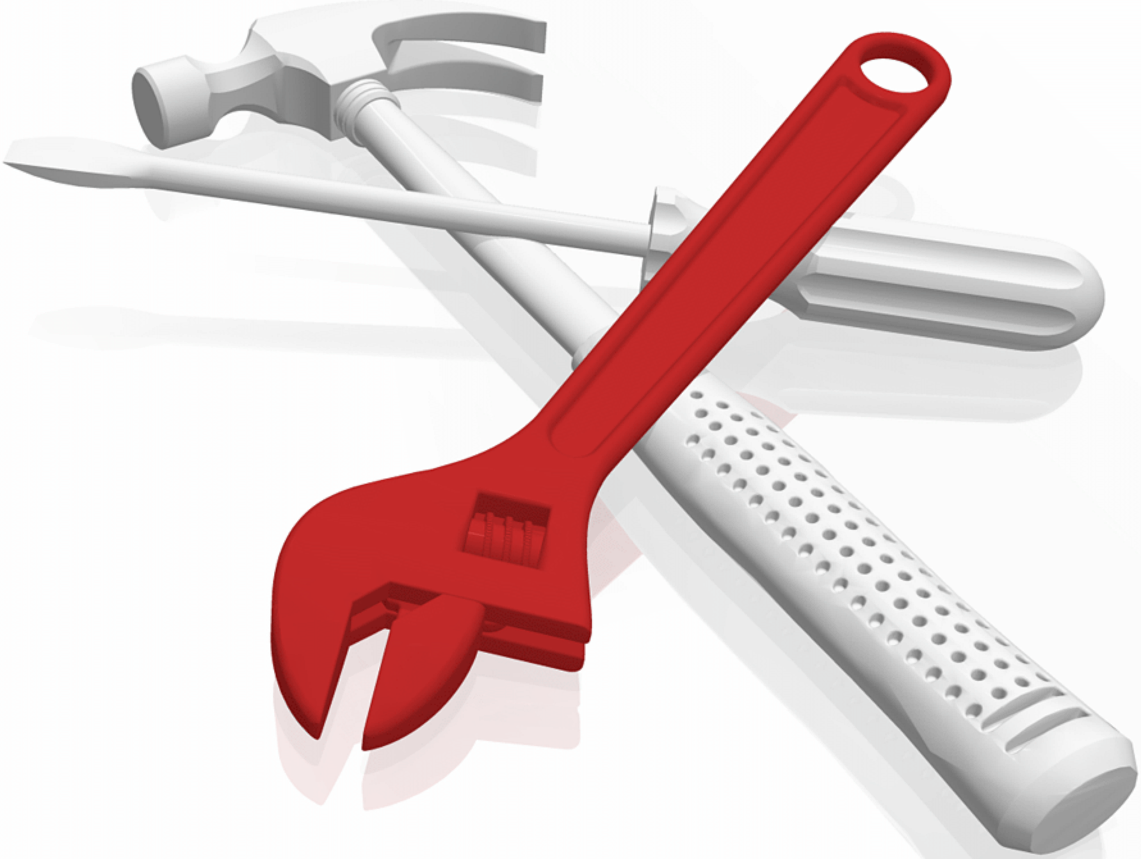
Redbooks

ibm.com/redbooks

Experiences Installing Firepower Services on an ASA-5525 X

Technical Enablement Series

Aaron Lewis



IBM Systems Worldwide Client Experience Centers

Redpaper

Experiences Installing Firepower Services on an ASA-5525 X

This IBM® Redpaper describes a case study that involves software and hardware from Cisco Systems, Inc. Specifically, a Cisco FirePOWER module — also known as a SourceFire (SFR) module — was installed on a Cisco Adaptive Security Appliance (ASA). The case study reveals the steps, issues, and decision points of such an installation.

The scope of this case study is as follows:
FirePOWER 6.2.0 on an ASA 5525-X running code level 9.6.2 from the Command Line Interface (CLI). We do not discuss the ASDM installation method.

This document addresses the needs of Network Administrators, Security Administrators, and other staff who install and manage Intrusion Prevention or Intrusion Detection systems (IPS / IDS).

The reader should have a basic understanding of computer networking and be familiar with basic networking terms such as Interface, Access Control Lists (ACL), Domain Name Service (DNS), and Internet Protocol (IP) address.

Introduction

This case study reviews the installation process for Cisco FirePOWER Services on a Cisco ASA 5525-X Series firewall. The sequence of activities in the installation is as follows:

- "Obtain the installation images"
- "Install the SFR module"
- "Activate the SFR module"
- "Add a device"

The study includes relevant details from the following sources:

- *Install and Configure a FirePOWER Services Module on an ASA Platform*
  http://www.cisco.com/c/en/us/support/docs/security/asa-firepower-services/118644-configure-firepower-00.html
- *Register a Device with a FireSIGHT Management Center*
  http://www.cisco.com/c/en/us/support/docs/security/firesight-management-center/118596-configure-firesight-00.html
- Observations of the author.

You must know the prerequisites and compatibility matrix for your specific hardware and software versions from Cisco before you attempt this installation in your system.

This document assumes that you do not have a previous IPS or SFR module installed on your ASA and that you have one of the following situations:

- You have purchased a Firepower enabled ASA or
- You have subsequently purchased and installed an SSD for each ASA, essentially making it "Firepower enabled"

The steps in this document result in a *FirePOWER-enabled* firewall for both of these scenarios.

During an installation, be prepared to choose one of the following installation modes for your environment:

- **Passive:** A copy of the traffic is sent to the module for inspection, alerting and logging but no action is taken while the original packet is sent to its destination. This mode is typically chosen for an initial system like the one described in this IBM Redpaper.
- **In-Line:** Traffic is sent to the module for inspection and acted upon before being forwarded. This mode is required for a true Intrusion Prevention system.

Obtain the installation images

To obtain the installation images, you must have a Cisco CCO login account.

To perform the installation, you need two files. The boot loader file (.img) and the service install package (.pkg). The standard sources for the software are as follows:

- FirePOWER Management Center (FMC)
  https://software.cisco.com/download/home/286261232/type/286271056
- Image and Package installers
  https://software.cisco.com/download/home/286271172/type/286277393/

EXAMPLE:

- `asasfr-5500x-boot-6.2.0-2.img`
- `asasfr-sys-6.2.0-362.pkg`

Newer versions are available

Install the SFR module

> **Note:** It is best practice to place the SourceFire (FirePOWER) sensor as close as possible to the assets that you are trying to protect.

The installation steps are as follows:

1. Copy the boot loader file (**.img**) and ONLY the boot loader file to the ASA through normal means, usually File Transfer Protocol (FTP), as in this example:

   ```
   ciscoasa# copy ftp://<FTP_SERVER>/asasfr-5500x-boot-6.2.0-2.img
   disk0:/asasfr-5500x-boot-6.2.0-2.img
   ```

2. Specify the location of the boot loader image to the ASA.

   ```
   ciscoasa# sw-module module sfr recover configure image
   disk0:/asasfr-5500x-boot-6.2.0-2.img
   ```

> **Note:** If you want to see what happens during the next step, you can activate **`debug module-boot`** at this time.

3. Load the boot image and create the environment where the SFR module runs.

   ```
   ciscoasa# sw-module module sfr recover boot
   ```

   If you turned on debugging you'll see some output like this:

   ```
   Mod-sfr 788> *** EVENT: Creating the Disk Image...
   Mod-sfr 789> *** TIME: 05:50:26 UTC Jul 1 2014
   Mod-sfr 790> ***
   Mod-sfr 791> ***
   Mod-sfr 792> *** EVENT: The module is being recovered.
   Mod-sfr 793> *** TIME: 05:50:26 UTC Jul 1 2014
   Mod-sfr 794> ***
   ...
   Mod-sfr 795> ***
   Mod-sfr 796> *** EVENT: Disk Image created successfully.
   Mod-sfr 797> *** TIME: 05:53:06 UTC Jul 1 2014
   Mod-sfr 798> ***
   Mod-sfr 799> ***
   Mod-sfr 800> *** EVENT: Start Parameters: Image: /mnt/disk0/vm/vm_3.img,
    ISO: -cdrom /mnt/disk0
   <DETAILS REMOVED TO CONSERVE SPACE>

   Mod-sfr 239> Starting Advanced Configuration and Power Interface daemon:
    acpid.
   Mod-sfr 240> acpid: starting up with proc fs
   Mod-sfr 241> acpid: opendir(/etc/acpi/events): No such file or directory
   Mod-sfr 242> starting Busybox inetd: inetd... done.
   Mod-sfr 243> Starting ntpd: done
   Mod-sfr 244> Starting syslogd/klogd: done
   Mod-sfr 245>
   ```

```
Cisco ASA SFR Boot Image 6.2.0
```

In this case study and others that we conducted, this step required 2 to 3 minutes.

At this point, if all goes well, you have something similar to a ROM Monitor (ROMMON) environment where you can install the actual SFR software, which is the **.PKG** file that you downloaded. So, you are ready to access the environment through the console. First, you set basic parameters that get the system on the network so that you can install the SFR software.

Now that the environment is running, you must set some parameters on the SFR Boot image to facilitate the installation of the **.PKG** file.

4. Console into the Boot Image, as in this example code:

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.
Cisco ASA SFR Boot Image 5.3.1
asasfr login: admin
Password: Admin123
```

5. Open the setup menu.

```
asasfr-boot> setup
                        Welcome to SFR Setup
                          [hit Ctrl-C to abort]
                       Default values are inside []
```

Here, you'll be prompted to set the required parameters such as hostname, IP address, netmask, gateway, Domain Name Servers (DNS), and so on. It's OK to use the IP information that you intend to use for the management interface of the module.

6. Ping the gateway to confirm the setup.
7. Run the system install command.
   You are installing the actual firepower SFR module OS (the **.PKG** file), as in the following example:

```
asasfr-boot >system install ftp://<FTP_SERVER>/asasfr-sys-6.2.0-362.pkg
Verifying
Downloading
Extracting
```

A message like the following example is displayed:

```
Package Detail
        Description: Cisco ASA-FirePOWER 5.3.1-152 System Install
        Requires reboot: Yes
Do you want to continue with upgrade? [y]: y
```

Note: Answer yes here. This reboot refers to the SFR module only, not to the ASA.

Here are the typical prompts that you see:

```
Warning: Please do not interrupt the process or turn off the system. Doing so
 might leave system in unusable state.
Upgrading
Starting upgrade process ...
Populating new system image
Reboot is required to complete the upgrade. Press 'Enter' to reboot the system.
(press Enter)
Broadcast message from root (ttyS1) (Mon Jun 23 09:28:38 2014):
The system is going down for reboot NOW!
Console session with module sfr terminated.
```

Again, this “reboot” is OK to do, because it affects only the SFR module.

8. Configure the SFR module with its network parameters.
   This configuration applies the IP information that we provided in the previous steps.

   a. Connect to the SFR

```
ciscoasa# session sfr
Opening command session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.
Sourcefire ASA5555 v5.3.1 (build 152)
Sourcefire3D login:
```

   b. Log in using the default credentials **`admin / Admin123`**.

   c. Read and accept the End User License Agreement (EULA).

   d. Change the **admin** password.

   e. Configure the management address and DNS settings, as prompted.

   Here are the typical prompts that you see:

```
System initialization in progress. Please stand by. You must change the password
 for 'admin' to continue. Enter new password: <new password>
Confirm new password: <repeat password>
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.0.2.24]:198.51.100.24
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.0
Enter the IPv4 default gateway for the management interface []: 198.51.100.24
Enter a fully qualified hostname for this system [Sourcefire3D]: asasfr.example.com
Enter a comma-separated list of DNS servers or 'none' []:
198.51.100.24, 198.51.100.24
Enter a comma-separated list of search domains or 'none' [example.net]: example.com
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
```

Activate the SFR module

Installation of the SFR module is complete! Now, you must activate the module as described here. The main requirements in this procedure are as follows:

- Register the SFR module with the FirePOWER Management Center
- Redirect traffic to the SFR module on the ASA.

Complete these steps to activate the SFR module:

1. Set up the SFR for registration.

   a. Run this command to log back in to the SFR: `ciscoasa#` **`session sfr`**

   b. Run this command to prepare to communicate with the management center:

```
configure manager add FMC_IP_Address my_key
```

EXAMPLE:

```
configure manager add 192.0.2.2 mykey
Manager successfully configured.
```

Note: Keep a record of this key. You need it to add the device to the management center.

2. Redirect ASA traffic to the SFR module for processing, as follows:

   a. Use the **access-list** command to specify which traffic that you are interested in.
   In this example, all of the traffic from all of the interfaces is redirected to the SFR. You can redirect specific traffic by writing the appropriate ACL to match traffic of interest.

```
ciscoasa(config)# access-list to-sfr-acl remark ***** Control traffic to SFR module *****
ciscoasa(config)# access-list to-sfr-acl extended permit ip any any
```

   b. Create a class-map to match the traffic on the new access list:

```
ciscoasa(config)# class-map SFR
ciscoasa(config-cmap)# match access-list to-sfr-acl
```

   c. Specify the deployment mode that manages traffic for the SFR module:
   passive (monitor-only) or inline (normal), as described in this step.
   At first, most users want passive (monitor-only) mode. Both modes are explained in the following table.

Table 1 Specifying deployment mode[1]

To specify passive deployment mode:	Use the **monitor-only** keyword, as in this example. `ciscoasa(config-pmap-c)# sfr fail-open monitor-only` If you do not include this keyword, the traffic is sent in inline mode. **Behavior of this mode:** A copy of the traffic is sent to the SFR service module, but it is not returned to the ASA. With passive mode you can view the actions that the SFR module would have completed for the traffic. It also allows you to evaluate the content of the traffic, without an impact to the network.

To specify inline deployment:	You create a policy map and configure the ASA SFR module as in this example:
	`ciscoasa(config)# policy-map global_policy`
	`ciscoasa(config-pmap)# class SFR`
	`ciscoasa(config-pmap-c)# sfr fail-open`
	Behavior of this mode: The undesired traffic is dropped and any other actions that are applied by policy are performed. Then, the traffic is returned to the ASA for further processing and ultimate transmission.

3. Confirm that the policy mapping is globally applied.

   Typically you add settings to a default policy map that is defined globally. So, you probably do not need to apply it again in any specific location.

   a. Run the following command to confirm:

```
ciscoasa(config-pmap-c)# sh run service-policy
service-policy global_policy global
```

   b. If you don't see that result (`service-policy global_policy global`), you must run the following command.

```
ciscoasa(config)# service-policy global_policy global
```

   The **global** keyword applies the policy map to all the interfaces, In contrast, the **interface** keyword applies the policy to one interface. Only one global policy is allowed.

[1] For more information on the behavior of each deployment mode see, "Install and Configure a FirePOWER Services Module on an ASA Platform," Nazmul Rajib, Cisco Systems, Inc., December 12, 2016.
https://www.cisco.com/c/en/us/support/docs/security/asa-firepower-services/118644-configure-firepower-00.html

The basic setup on the ASA is complete. Next, we add the firewall device to the FirePOWER Management Center.

Add a device

1. Use a browser to log into the FirePOWER Management Center by using its URL.
   Example: `https://fmc.mydomain.com`
2. Click the Devices tab in the top menu. Then, click **Add Device**.
3. In the Host field, enter the IP address that is assigned to the SFR module (the device that you want to manage).
4. In the Registration Key field, enter the registration key that you assigned above (**mykey**)
5. Set the rest of the options to your preference.
6. Click **Register**.
   After a few moments, you see the device that is listed in the Devices tab.

General information for your installation

Adding the FMC to TACACS or RADIUS for authentication

For information, see the *Integration of FireSIGHT System with ACS 5.x for RADIUS User Authentication* webpage:
http://www.cisco.com/c/en/us/support/docs/security/firesight-management-center/200204-Integration-of-FireSIGHT-System-with-ACS.html

Rejoining a disconnected SFR

The SFR module might become disassociated from the FirePower Management Center. To rejoin a device that was previously managed by this management center, you must delete and redefine the manager on the SFR module, as follows:

1. Log into the SFR module.
2. Run this command: `manager delete`
3. Run this command to redefine the manager:
   ```
   manager add <IP of the FMC> 'yourkey'
   ```

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

Redbooks (logo) ®

IBM®

The following terms are trademarks of other companies:

Other company, product, or service names may be trademarks or service marks of others.

REDP-5562-00

ISBN 0738458066

Printed in U.S.A.