Install and Configure a FirePOWER Services Module on an ASA Platform

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

- Before You Begin

Install

- Install the SFR Module on the ASA
- Set Up the ASA SFR Boot Image

Configure

- Configure the FirePOWER Software
- Configure the FireSIGHT Management Center
- Redirect Traffic to the SFR Module

Verify

Troubleshoot

Related Information

Introduction

This document describes how to install and configure a Cisco FirePOWER (SFR) module on a Cisco ASA and register the SFR module with Cisco FireSIGHT.

Prerequisites

Requirements

Cisco recommends that your system meet these requirements before you attempt the procedures that are described in this document:

- Ensure that you have at least 3GB of free space on the flash drive (disk0), in addition to the size of the boot software.
- Ensure that you have access to the privileged EXEC mode. In order to access the privileged EXEC mode, enter the **enable** command into the CLI. If a password was not set, then press **Enter**:

  <#root>

  ```
  ciscoasa>
  ```

  enable

  ```
  Password:
  ciscoasa#
  ```

Components Used

In order to install the FirePOWER Services on a Cisco ASA, these components are required:

- Cisco ASA software Version 9.2.2 or later
- Cisco ASA platforms 5512-X through 5555-X
- FirePOWER Software Version 5.3.1 or later

Note: If you want to install FirePOWER (SFR) Services on an ASA 5585-X Hardware Module, refer to Install a SFR Module on an ASA 5585-X Hardware Module.

These components are required on the Cisco FireSIGHT Management Center:

- FirePOWER Software Version 5.3.1 or later
- FireSIGHT Management Center FS2000, FS4000 or virtual appliance

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.

Background Information

The Cisco ASA FirePOWER module (also known as the ASA SFR) provides next-generation Firewall services, such as:

- Next Generation Intrusion Prevention System (NGIPS)
- Application Visibility and Control (AVC)
- Filter URLs
- Advanced Malware Protection (AMP)

Note: You can use the ASA SFR module in Single or Multiple context mode, and in Routed or Transparent mode.

Before You Begin

Consider this important information before you attempt the procedures that are described in this document:

- If you have an active service policy that redirects traffic to an Intrusion Prevention System (IPS)/Context Aware (CX) module (that you replaced with the ASA SFR), you must remove it before you configure the ASA SFR service policy.
- You must shut down any other software modules that currently run. A device can run a single software module at a time. You must do this from the ASA CLI. For example, these commands shut down and uninstall the IPS software module, and then reload the ASA:

  <#root>

  ```
  ciscoasa#
  ```

  sw-module module ips shutdown

```
ciscoasa#
sw-module module ips uninstall

ciscoasa#
reload
```

- The commands that are used in order to remove the CX module are the same, except the **cxsc** keyword is used instead of **ips**:
<#root>

```
ciscoasa#
sw-module module cxsc shutdown

ciscoasa#
sw-module module cxsc uninstall

ciscoasa#
reload
```

- When you reimage a module, use the same **shutdown** and **uninstall** commands that are used in order to remove an old SFR image. Here is an example:

<#root>

```
ciscoasa#
sw-module module sfr uninstall
```

- If the ASA SFR module is used in Multiple context mode, perform the procedures that are described in this document within the system execution space.

Tip: In order to determine the status of a module on the ASA, enter the **show module** command.

Install

This section describes how to install the SFR module on the ASA and how to set up the ASA SFR boot image.

Install the SFR Module on the ASA

Complete these steps in order to install the SFR module on the ASA:

1. Download the ASA SFR system software from Cisco.com to an HTTP, HTTPS, or FTP server that is accessible from the ASA SFR management interface.
2. Download the boot image to the device. You can use either the Cisco Adaptive Security Device Manager (ASDM) or the ASA CLI in order to download the boot image to the device.

Note: Do not transfer the system software; it is downloaded later to the Solid State Drive (SSD).

Complete these steps in order to download the boot image via the ASDM:

a. Download the boot image to your workstation, or place it on an FTP, TFTP, HTTP, HTTPS, Server Message Block (SMB), or Secure Copy (SCP) server.
b. Choose **Tools > File Management** in the ASDM.
c. Choose the appropriate File Transfer command, either *Between Local PC and Flash* or *Between Remote Server and Flash*.
d. Transfer the boot software to the flash drive (disk0) on the ASA.

Complete these steps in order to download the boot image via the ASA CLI:

a. Download the boot image on an FTP, TFTP, HTTP, or HTTPS server.
b. Enter the **copy** command into the CLI in order to download the boot image to the flash drive.

Here is an example that uses HTTP protocol (replace the **<HTTP_Server>** with your server IP address or hostname). For FTP Server, the URL looks like this:**ftp://username:password@server-ip/asasfr-5500x-boot-5.3.1-152.img .**

```
<#root>

ciscoasa#

copy http://<HTTP_SERVER>/asasfr-5500x-boot-5.3.1-152.img
 disk0:/asasfr-5500x-boot-5.3.1-152.img
```

3. Enter this command in order to configure the ASA SFR boot image location in the ASA flash drive:

```
<#root>

ciscoasa#

 sw-module module sfr recover configure image disk0:/file_path
```

Here is an example:

```
<#root>

ciscoasa#

sw-module module sfr recover configure image disk0:
 /asasfr-5500x-boot-5.3.1-152.img
```

4. Enter this command in order to load the ASA SFR boot image:

```
<#root>

ciscoasa#

sw-module module sfr recover boot
```

During this time, if you enable **debug module-boot** on the ASA, these debugs are printed:

```
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
Mod-sfr 801> /asasfr-5500x-boot-5.3.1-152.img, Num CPUs: 6, RAM: 7659MB,
 Mgmt MAC: A4:4C:11:29:
Mod-sfr 802> CC:FB, CP MAC: 00:00:00:04:00:01, HDD: -drive file=/dev/md0,
 cache=none,if=virtio,
Mod-sfr 803> Dev
Mod-sfr 804> ***
Mod-sfr 805> *** EVENT: Start Parameters Continued: RegEx Shared Mem:
 32MB, Cmd Op: r, Shared M
Mod-sfr 806> em Key: 8061, Shared Mem Size: 64, Log Pipe: /dev/ttyS0_vm3,
 Sock: /dev/ttyS1_vm3,
Mod-sfr 807>  Mem-Path: -mem-path /hugepages
Mod-sfr 808> *** TIME: 05:53:06 UTC Jul 1 2014
Mod-sfr 809> ***
Mod-sfr 810> IVSHMEM: optarg is key=8061,64,unix:/tmp/nahanni, name is,
 key is 8061, size is 6
...
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 5.3.1
```

5. Wait approximately 5 to 15 minutes for the ASA SFR module to boot up, and then open a console session to the operational ASA SFR boot image.

Set Up the ASA SFR Boot Image

Complete these steps in order to set up the newly installed ASA SFR boot image:

1. Press **Enter** after you open a session in order to reach the login prompt.



Note: The default username is **admin**. The password differs based upon software release:**Adm!n123** for 7.0.1 (new device from the factory only), **Admin123** for 6.0, and later, **Sourcefire** for pre-6.0.

Here is an example:

<#root>

```
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
```

Tip: If the ASA SFR module boot has not been completed, the session command fails and a message appears to indicate that the system is unable to connect over TTYS1. If this occurs, wait for the module boot to complete and try again.

2. Enter the **setup** command in order to configure the system so that you can install the system software package:

<#root>

```
asasfr-boot>
```

setup

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

You are then prompted for this information:

- **Host name** - The hostname can be up to 65 alphanumeric characters, with no spaces. The use of hyphens is allowed.
- **Network address** - The network address can be either static IPv4 or IPv6 addresses. You can also use DHCP for IPv4, or IPv6 stateless auto-configuration.
- **DNS information** - You must identify at least one Domain Name System (DNS) server, and you can also set the domain name and search domain.
- **NTP information** - You can enable Network Time Protocol (NTP) and configure the NTP servers in order to set the system time.

3. Enter the **system install** command in order to install the system software image:

<#root>

```
asasfr-boot >
```

system install [noconfirm] ***url***

Include the **noconfirm** option if you do not want to respond to confirmation messages. Replace the **url** keyword with the location of the **.pkg** file. Again, you can use an FTP, HTTP, or HTTPS server. Here is an example:

```
<#root>

asasfr-boot >

system install http://<HTTP_SERVER>/asasfr-sys-5.3.1-152.pkg


Verifying
Downloading
Extracting


Package Detail
        Description: Cisco ASA-FirePOWER 5.3.1-152 System Install
        Requires reboot: Yes

Do you want to continue with upgrade? [y]: y
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.
```

For FTP Server, the URL looks like this:**ftp://username:password@server-ip/asasfr-sys-5.3.1-152.pkg.**

Note The SFR is in a "**Recover**" state during the installation process. It can take up to an hour or so to complete the installation of the SFR module. When the installation is complete, the system reboots. Allow ten or more minutes for the application component installation and for the ASA SFR services to start. The output of the **show module sfr** command indicates that all processes are **Up**.

Configure

This section describes how to configure the FirePOWER software and the FireSIGHT Management Center, and how to redirect traffic to the SFR module.

Configure the FirePOWER Software

Complete these steps in order to configure the FirePOWER software:

1. Open a session to the ASA SFR module.

Note: A different login prompt now appears because the login occurs on a fully-functional module.

Here is an example:

```
<#root>

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:
```

2. Log in with the username **admin** and the password differs based on software release:**Adm!n123** for 7.0.1 (new device from the factory only), **Admin123** for 6.0, and later,**Sourcefire** for pre-6.0.
3. Complete the system configuration as prompted, which occurs in this order:
   a. Read and accept the End User License Agreement (EULA).
   b. Change the admin password.
   c. Configure the management address and DNS settings, as prompted.

Note: You can configure both IPv4 and IPv6 management addresses.

Here is an example:

```
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 [192.168.45.45]:198.51.100.3
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 []: 198.51.100.1
Enter a fully qualified hostname for this system [Sourcefire3D]: asasfr.example.com
Enter a comma-separated list of DNS servers or 'none' []:
 198.51.100.15, 198.51.100.14
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'
```

4. Wait for the system to reconfigure itself.

Configure the FireSIGHT Management Center

In order to manage an ASA SFR module and security policy, you must register it with a FireSIGHT Management Center. Refer to Register a Device with a FireSIGHT Management Center for more information. You cannot perform these actions with a FireSIGHT Management Center:

- Configure the ASA SFR module interfaces
- Shut down, restart, or otherwise manage the ASA SFR module processes
- Create backups from, or restore backups to, the ASA SFR module devices
- Write access control rules in order to match traffic with the use of VLAN tag conditions

Redirect Traffic to the SFR Module

In order to redirect traffic to the ASA SFR module, you must create a service policy that identifies specific traffic. Complete these steps in order to redirect traffic to an ASA SFR module:

1. Select the traffic that must be identified with the **access-list** command. In this example, all of the traffic from all of the interfaces is redirected. You can do this for specific traffic as well.

   ```
   <#root>

   ciscoasa(config)#

   access-list sfr_redirect extended permit ip any any
   ```

2. Create a class-map in order to match the traffic on an access list:

   ```
   <#root>

   ciscoasa(config)#

   class-map sfr


   ciscoasa(config-cmap)#

   match access-list sfr_redirect
   ```

3. Specify the deployment mode. You can configure your device in either a passive (monitor-only) or inline (normal) deployment mode.

   Note: You cannot configure both a passive mode and inline mode at the same time on the ASA. Only one type of security policy is allowed.

   - In an inline deployment, the SFR Module inspects the traffic based upon the Access Control Policy and provides the verdict to the ASA to take the appropriate action (Allow, Deny, and so on) on the traffic flow. This example shows how to create a policy-map and configure the ASA SFR module in the inline mode.
   - Please verify that the current **global_policy** is configured with another module configuration**(show run policy-map global_policy, show run service-policy)**, then first reset/remove the global_policy for other module configuration and then re-configure the **global_policy**.

     ```
     <#root>

     ciscoasa(config)#

     policy-map global_policy
     ```

```
ciscoasa(config-pmap)#
class sfr

ciscoasa(config-pmap-c)#
sfr fail-open
```

- In a passive deployment, a copy of the traffic is sent to the SFR service module, but it is not returned to the ASA. Passive mode allows you to view the actions that the SFR module would have completed in regards to the traffic. It also allows you to evaluate the content of the traffic, without an impact to the network.

  If you want to configure the SFR module in passive mode, use the **monitor-only** keyword (as shown in the next example). If you do not include the keyword, the traffic is sent in inline mode.

```
<#root>
ciscoasa(config-pmap-c)#
sfr fail-open monitor-only
```



Warning: The **monitor-only** mode does not allow the SFR service module to deny or block malicious traffic.



Caution: It can be possible to configure an ASA in *monitor-only* mode with the use of the interface-level **traffic-forward sfr monitor-only** command; however, this configuration is purely for demonstration functionality and must not be used on a production ASA. Any issues that are found in this demonstration feature are not supported by the Cisco Technical Assistance Center (TAC). If you desire to deploy the ASA SFR service in passive mode, configure it with the use of a *policy-map*.

4. Specify a location and apply the policy. You can apply a policy globally or on an interface. In order to override the global policy on an interface, you can apply a service policy to that interface.

   The **global** keyword applies the policy map to all of the interfaces, and the **interface** keyword applies the policy to one interface. Only one global policy is allowed. In this example, the policy is applied globally:

```
<#root>
ciscoasa(config)#
service-policy global_policy global
```



Caution: The policy map **global_policy** is a default policy. If you use this policy and want to remove it on your device to troubleshoot, ensure that you understand its implication.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

- You can run this command (**debug module-boot**) to enable the debug at the start of the installation of the SFR boot image.
- If ASA got stuck in Recover mode and the console did not come up, then you try this command (**sw-module module sfr recover stop**).
- If the SFR Module was not able to come out of the recovery state, then you can try to reload the ASA **(reload quick)**. (If the traffic passes through, then it can cause network disturbance). If Still SFR is stuck in the recovery state, you can shut down the ASA and **unplug the SSD** card & start the ASA. Check the status of the module and it must be INIT state. Again, shut down the ASA, **insert the SSD** card & start the ASA. you can start re-image of the ASA SFR module.

Related Information

- Cisco Secure IPS - Cisco NGIPS Features
- Register a Device with a FireSIGHT Management Center

- Cisco ASA FirePOWER Module Quick Start Guide

- Deployment of FireSIGHT Management Center on VMware ESXi
- Technical Support & Documentation - Cisco Systems