在ASA平台上安装和配置FirePOWER服务模块

目录

简介

本文档介绍如何在Cisco ASA上安装和配置Cisco FirePOWER(SFR)模块并向Cisco FireSIGHT注册SFR模块。

先决条件

要求

Cisco建议您在尝试本文档中所述的步骤之前，系统应满足以下要求：

- 除了启动软件的大小外，请确保闪存驱动器(disk0)上至少有3 GB的可用空间。
- 确保您有权访问特权执行模式。要访问特权执行模式，请输入 **enable** 命令到CLI。如果未设置密码，请按 **Enter**：

```
<#root>

ciscoasa>

enable

Password:
ciscoasa#
```

使用的组件

要在Cisco ASA上安装FirePOWER服务，需要以下组件：

- Cisco ASA 软件版本 9.2.2 或更高版本
- Cisco ASA平台5512-X至5555-X
- FirePOWER软件5.3.1版或更高版本

注：如果要在ASA 5585-X硬件模块上安装FirePOWER(SFR)服务，请参阅在ASA 5585-X硬件模块上安装SFR模块。

Cisco FireSIGHT管理中心需要以下组件：

- FirePOWER软件5.3.1版或更高版本
- FireSIGHT管理中心FS2000、FS4000或虚拟设备

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

Cisco ASA FirePOWER模块（也称为ASA SFR）提供下一代防火墙服务，例如：

- 下一代入侵防御系统(NGIPS)
- 应用可视性与可控性(AVC)
- 过滤URL
- 高级恶意软件保护 (AMP)

注意：您可以在单情景或多情景模式以及路由或透明模式下使用ASA SFR模块。

开始使用前

在尝试本文档中介绍的步骤之前，请考虑以下重要信息：

- 如果具有将流量重定向到入侵防御系统(IPS)/情景感知(CX)模块（已替换为ASA SFR）的活动服务策略，则必须在配置ASA SFR服务策略之前将其删除。
- 您必须关闭当前运行的任何其他软件模块。设备一次可以运行一个软件模块。您必须从ASA CLI执行此操作。例如，以下命令关闭并卸载IPS软件模块，然后重新加载ASA:

  <#root>

  ciscoasa#

  sw-module module ips shutdown

```
ciscoasa#
sw-module module ips uninstall

ciscoasa#
reload
```

- 用于删除CX模块的命令是相同的，除了 **cxsc** 使用关键字而不是 **ips**:
  <#root>

```
ciscoasa#
sw-module module cxsc shutdown

ciscoasa#
sw-module module cxsc uninstall

ciscoasa#
reload
```

- 重新映像模块时，请使用相同 **shutdown** 和 **uninstall** 用于删除旧SFR映像的命令。例如：

  <#root>

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

- 如果ASA SFR模块用于多情景模式，请在系统执行空间中执行本文档中介绍的过程。

提示：要确定ASA上模块的状态，请输入 **show module** 命令。

Install（安装）

本节介绍如何在ASA上安装SFR模块以及如何设置ASA SFR引导映像。

在ASA上安装SFR模块

要在ASA上安装SFR模块，请完成以下步骤：

1. 从Cisco.com将ASA SFR系统软件下载到可从ASA SFR管理接口访问的HTTP、HTTPS或FTP服务器。
2. 将启动映像下载到设备。您可以使用思科自适应安全设备管理器(ASDM)或ASA CLI将引导映像下载到设备。

注：请勿传输系统软件；稍后会将其下载到固态驱动器(SSD)。

要通过ASDM下载启动映像，请完成以下步骤：

a. 将启动映像下载到您的工作站，或将其置于FTP、TFTP、HTTP、HTTPS、服务器消息块(SMB)或安全复制(SCP)服务器上。
b. 选择**Tools > File Management** 在ASDM中。
c. 选择适当的File Transfer命令，Between Local PC and Flash或Between Remote Server and Flash。
d. 将启动软件传输到ASA上的闪存驱动器(disk0)。

要通过ASA CLI下载启动映像，请完成以下步骤：

a. 在FTP、TFTP、HTTP或HTTPS服务器上下载启动映像。
b. 输入 **copy** 命令，以便将引导映像下载到闪存驱动器。

以下是使用HTTP协议的示例(替换
服务器IP地址或主机名)。对于FTP服务器，URL如下所示：**ftp://username:password@server-ip/asasfr-5500x-boot-5.3.1-152.img .**

```
<#root>

ciscoasa#

copy http://

            /asasfr-5500x-boot-5.3.1-152.img
 disk0:/asasfr-5500x-boot-5.3.1-152.img
```

3. 输入以下命令以在ASA闪存驱动器中配置ASA SFR引导映像位置：

```
<#root>

ciscoasa#

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

例如：

```
<#root>

ciscoasa#

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

4. 输入以下命令以加载ASA SFR引导映像：

<#root>

ciscoasa#

sw-module module sfr recover boot

在此期间，如果启用 **debug module-boot** 在ASA上，会打印以下调试：

```
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. 等待大约5到15分钟以启动ASA SFR模块，然后打开可操作的ASA SFR启动映像的控制台会话。

设置ASA SFR引导映像

要设置新安装的ASA SFR引导映像，请完成以下步骤：

1. 按 **Enter** 打开会话以进入登录提示符后。

   注：默认用户名是 **admin**.密码因软件版本而异：**Adm!n123** 对于7.0.1（仅限工厂的新设备），**Admin123** 用于6.0及更高版本，**Sourcefire** 适用于6.0之前的版本。

   例如：

   <#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
   ```

   提示：如果ASA SFR模块引导尚未完成，会话命令将失败，并显示一条消息，指示系统无法通过TTYS1进行连接。如果发生这种情况，请等待模块启动完成，然后重试。

2. 输入 **setup** 命令配置系统，以便安装系统软件包：

   <#root>

   ```
   asasfr-boot>
   setup


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

   然后系统将提示您输入以下信息：

   - **Host name** — 主机名最多可以包含65个字母数字字符，不含空格。允许使用连字符。
   - **Network address** — 网络地址可以是静态IPv4或IPv6地址。您也可以使用DHCP进行IPv4或IPv6无状态自动配置。
   - **DNS information** — 必须识别至少一个域名系统(DNS)服务器，而且还可以设置域名和搜索域。
   - **NTP information** — 可以启用网络时间协议(NTP)并配置NTP服务器以设置系统时间。

3. 输入 **system install** 命令安装系统软件映像：

```
<#root>

asasfr-boot >

system install [noconfirm] url
```

包括 **noconfirm** 选项，如果您不想回应确认消息。更换 **url** 关键字，以及位置 **.pkg** 文件.同样，您可以使用FTP、HTTP或HTTPS服务器。例如：

```
<#root>

asasfr-boot >

system install http://

          /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.
```

对于FTP服务器，URL如下所示：**ftp://username:password@server-ip/asasfr-sys-5.3.1-152.pkg**.

注意SFR位于“**Recover**"状态。完成SFR模块的安装最多可能需要一个小时左右的时间。 安装完成后，系统重新启动。等待十分钟或更长时间，以便安装应用组件并启动ASA SFR服务。的输出 **show module sfr** 命令表示所有进程都处于 **Up**.

配置

本节介绍如何配置FirePOWER软件和FireSIGHT管理中心，以及如何将流量重定向至SFR模块。

配置FirePOWER

要配置FirePOWER软件，请完成以下步骤：

1. 打开与ASA SFR模块的会话。

   注意：现在显示不同的登录提示，因为登录发生在全功能模块上。

   例如：

   <#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. 使用用户名登录 **admin** 密码因软件版本而异：**Adm!n123** 对于7.0.1（仅限工厂的新设备），**Admin123** 用于6.0及更高版本，**Sourcefire** 适用于6.0之前的版本。
3. 按照提示完成系统配置，按以下顺序执行：
   a. 阅读并接受最终用户许可协议(EULA)。
   b. 更改管理员密码。
   c. 根据提示配置管理地址和DNS设置。

   注意：您可以同时配置IPv4和IPv6管理地址。

   例如：

   ```
   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. 等待系统重新配置自身。

配置FireSIGHT管理中心

要管理ASA SFR模块和安全策略，您必须向FireSIGHT管理中心注册该模块。有关详细信息，请参阅向FireSIGHT管理中心注册设备。您不能使用FireSIGHT管理中心执行这些操作：

- 配置ASA SFR模块接口
- 关闭、重新启动或以其他方式管理ASA SFR模块进程
- 从ASA SFR模块设备创建备份或将备份还原到
- 编写访问控制规则，使流量与使用VLAN标记条件相匹配

将流量重定向至SFR模块

要将流量重定向至ASA SFR模块，您必须创建识别特定流量的服务策略。完成以下步骤以将流量重定向至ASA SFR模块：

1. 选择必须使用 access-list 命令。在本示例中，来自所有接口的所有流量都会被重定向。您也可以对特定流量执行此操作。

<#root>

```
ciscoasa(config)#
access-list sfr_redirect extended permit ip any any
```

2. 创建类映射以匹配访问列表中的流量：

<#root>

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

ciscoasa(config-cmap)#
match access-list sfr_redirect
```

3. 指定部署模式。您可以在被动（仅监控）或内联（正常）部署模式下配置设备。

> 注：您不能在ASA上同时配置被动模式和内联模式。只允许一种安全策略。

- 在内联部署中，SFR模块根据访问控制策略检查流量并向ASA提供判定以对流量流采取相应操作（允许、拒绝等）。此示例显示如何创建策略映射并在内联模式下配置ASA SFR模块。
- 请验证当前的 **global_policy** 配置了另一个模块配置**(show run policy-map global_policy, show run service-policy)**，然后首先重置/删除其他模块配置的global_policy，然后重新配置 **global_policy**.

  <#root>

  ```
  ciscoasa(config)#
  policy-map global_policy

  ciscoasa(config-pmap)#
  class sfr

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

- 在被动部署中，流量的副本发送到SFR服务模块，但不返回到ASA。被动模式允许您查看SFR模块针对流量应完成的操作。它还允许您评估流量的内容，而不影响网络。

  如果要将SFR模块配置为被动模式，请在执行模式下使用 **monitor-only** 关键字（如下例所示）。如果不包含关键字，流量将以内联模式发送。

  <#root>

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

警告： **monitor-only** 模式不允许SFR服务模块拒绝或阻止恶意流量。

注意：可以使用接口级别在仅监控模式下配置ASA **traffic-forward sfr monitor-only** 命令；但是，此配置仅用于演示功能，不能在生产ASA上使用。思科技术支持中心(TAC)不支持此演示功能中发现的任何问题。如果您希望在被动模式下部署ASA SFR服务，请使用policy-map对其进行配置。

4. 指定位置并应用策略。您可以全局应用策略，也可以在接口上应用策略。要覆盖接口上的全局策略，可以将服务策略应用于该接口。

   此 **global** 关键字将策略映射应用于所有接口，并且 **interface** 关键字将策略应用于一个接口。仅允许有一个全局策略。在本示例中，策略全局应用：

   <#root>

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

⚠ 注意：策略映射 **global_policy** 是默认策略。如果使用此策略并要在设备上删除它以进行故障排除，请确保您了解其含义。

验证

当前没有可用于此配置的验证过程。

故障排除

- 您可以运行此命令(**debug module-boot**)以在安装SFR引导映像开始时启用调试。
- 如果ASA陷入恢复模式且控制台未启动，则尝试此命令(**sw-module module sfr recover stop**影响。
- 如果SFR模块无法退出恢复状态，则可以尝试重新加载ASA **(reload quick)**.（如果流量通过，则可能导致网络干扰）。如果Still SFR处于恢复状态，您可以关闭ASA并 **unplug the SSD** 卡并启动ASA。检查模块的状态，它必须是INIT状态。再次关闭ASA， **insert the SSD** 卡并启动ASA。您可以开始重新映像ASA SFR模块。

相关信息

- Cisco Secure IPS - Cisco NGIPS功能
- 向FireSIGHT管理中心注册设备
- Cisco ASA FirePOWER模块快速入门指南
- 在VMware ESXi上部署FireSIGHT管理中心
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。