在ASA 5585-X硬件模块上安装SFR模块

目录

简介

ASA FirePOWER模块（也称为ASA SFR）提供下一代防火墙服务，包括下一代IPS(NGIPS)、应用可视性与可控性(AVC)、URL过滤和高级恶意软件防护(AMP)。 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模块。本文档介绍ASA 5585-X硬件模块上FirePOWER(SFR)模块的必备条件和安装过程。它还提供了向FireSIGHT管理中心注册SFR模块的步骤。

> **注意**：FirePOWER(SFR)服务驻留在ASA 5585-X的硬件模块上，而ASA 5512-X至5555-X系列设备上的FirePOWER服务安装在软件模块上，因此在安装过程中会有所差异。

先决条件

要求

本文档中的说明要求访问特权EXEC模式。要访问特权EXEC模式，请输入enable命令。如果未设置密码，只需按Enter。

```
ciscoasa> enable
Password:
ciscoasa#
```

要在ASA上安装FirePOWER服务，需要以下组件：

- ASA软件9.2.2版或更高版本
- ASA 5585-X平台
- 可通过FirePOWER模块的管理接口访问的TFTP服务器
- 带5.3.1或更高版本的FireSIGHT管理中心

注意：本文档中的信息是从特定实验环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

开始使用前

如果ASA SSM始终占用ASA 5585-X机箱中两个插槽中的一个，则您拥有除FirePOWER(SFR)服务SSP(如SSP-CX（情景感知）或AIP-SSM（高级检测和防御安全）之外的硬件模块必须卸载模块以为SSP-SFR腾出空间。在删除硬件模块之前，请运行以下命令关闭模块：

```
ciscoasa# hw-module module 1 shutdown
```

布线和管理

- 您无法通过ASA 5585-X上的ASA控制台访问SFR模块的串行端口。
- 调配SFR模块后，您可以使用“session 1”命令与刀片会话。
- 要在ASA 5585-X上完全重新映像SFR模块，必须在串行管理端口上使用管理以太网接口和控制台会话，这些端口位于SFR模块上，与ASA的管理接口和控制台分开。

提示：要查找ASA上模块的状态，请运行“show module 1 details”命令，该命令检索SFR模块的管理IP和关联的防御中心。

在ASA上安装FirePOWER(SFR)模块

1.将ASA FirePOWER SFR模块初始引导程序映像从Cisco.com下载到可从ASA FirePOWER管理接口访问的TFTP服务器。映像名称类似于“asasfr-boot-5.3.1-152.img”

2.将ASA FirePOWER系统软件从Cisco.com下载到可从ASA FirePOWER管理接口访问的HTTP、HTTPS或FTP服务器。

3.重新启动SFR模块

选项 1：如果您没有SFR模块的口令，可以从ASA发出以下命令以重新启动模块。

```
ciscoasa# hw-module module 1 reload
Reload module 1? [confirm]
Reload issued for module 1
```

选项 2：如果您有SFR模块的口令，则可以直接从其命令行重新启动传感器。

```
Sourcefire3D login: admin
Password:

Sourcefire Linux OS v5.3.1 (build 43)
Sourcefire ASA5585-SSP-10 v5.3.1 (build 152)

>system reboot
```

4.使用ESCAPE或终端会话软件的中断序列中断SFR模块的启动过程，以将模块放入ROMMON中。

```
The system is restarting...
CISCO SYSTEMS
Embedded BIOS Version 2.0(14)1 15:16:31 01/25/14



Cisco Systems ROMMON Version (2.0(14)1) #0: Sat Jan 25 16:44:38 CST 2014

Platform ASA 5585-X FirePOWER SSP-10, 8GE

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot in 8 seconds.

Boot interrupted.

Management0/0
Link is UP
MAC Address: xxxx.xxxx.xxxx

Use ? for help.

rommon #0>
```

5.使用IP地址配置SFR模块管理接口，并指示TFTP服务器的位置和引导程序映像的TFTP路径。输入以下命令，在接口上设置IP地址并检索TFTP映像：

-
- ADDRESS= Your_IP_Address
- GATEWAY= Your_Gateway
- SERVER= Your_TFTP_Server
- IMAGE= Your_TFTP_Filepath
-
- `tftp`

!使用的IP地址信息示例。更新您的环境。

```
rommon #1> ADDRESS=198.51.100.3
rommon #2> GATEWAY=198.51.100.1
rommon #3> SERVER=198.51.100.100
rommon #4> IMAGE=/tftpboot/asasfr-boot-5.3.1-152.img
rommon #5> sync

Updating NVRAM Parameters...

rommon #6> tftp
ROMMON Variable Settings:
ADDRESS=198.51.100.3
SERVER=198.51.100.100
GATEWAY=198.51.100.1
PORT=Management0/0
VLAN=untagged
IMAGE=/tftpboot/asasfr-boot-5.3.1-152.img
CONFIG=
LINKTIMEOUT=20
PKTTIMEOUT=4
RETRY=20

tftp /tftpboot/asasfr-boot-5.3.1-152.img@198.51.100.100 via 198.51.100.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<truncated output>

Received 41235627 bytes

Launching TFTP Image...

Execute image at 0x14000
```

6.登录初始启动映像。以管理员身份登录，密码为Admin123

```
Cisco ASA SFR Boot Image 5.3.1

asasfr login: admin
Password:

Cisco ASA SFR Boot 5.3.1 (152)
Type ? for list of commands
```

7.使用初始引导映像在模块的管理接口上配置IP地址。输入setup命令以进入向导。系统将提示您输入以下信息：

- **主机名:**最多65个字母数字字符，无空格。允许连字符。
- **网络地址：**您可以设置静态IPv4或IPv6地址，或者使用DHCP（用于IPv4）或IPv6无状态自动配置。
- **DNS 信息:**您必须至少标识一个DNS服务器，还可以设置域名和搜索域。
- **NTP信息**:您可以启用NTP并配置NTP服务器，以设置系统时间。

!使用的示例信息。更新您的环境。

```
asasfr-boot>setup

Welcome to SFR Setup
[hit Ctrl-C to abort]
```

```
Default values are inside []

Enter a hostname [asasfr]: sfr-module-5585
Do you want to configure IPv4 address on management interface?(y/n) [Y]: Y
Do you want to enable DHCP for IPv4 address on management interface?(y/n) [N]: N
Enter an IPv4 address [192.168.8.8]: 198.51.100.3
Enter the netmask [255.255.255.0]: 255.255.255.0
Enter the gateway [192.168.8.1]: 198.51.100.1
Do you want to configure static IPv6 address on management interface?(y/n) [N]: N
Stateless autoconfiguration will be enabled for IPv6 addresses.
Enter the primary DNS server IP address: 198.51.100.15
Do you want to configure Secondary DNS Server? (y/n) [n]: N
Do you want to configure Local Domain Name? (y/n) [n]: N
Do you want to configure Search domains? (y/n) [n]: N
Do you want to enable the NTP service? [Y]: N

Please review the final configuration:
Hostname: sfr-module-5585
Management Interface Configuration

IPv4 Configuration: static
IP Address: 198.51.100.3
Netmask: 255.255.255.0
Gateway: 198.51.100.1

IPv6 Configuration: Stateless autoconfiguration

DNS Configuration:
DNS Server: 198.51.100.15

Apply the changes?(y,n) [Y]: Y
Configuration saved successfully!
Applying...
Restarting network services...
Restarting NTP service...
Done.
```

8.使用system install命令使用引导映像拉取和安装系统**软件映**像。如果不想响应确认消息，请包括noconfirm选项。将url关*键字*替换为.pkg文件的位置。

```
asasfr-boot> system install [noconfirm] url
```

例如，

```
> system install http://Server_IP_Address/asasfr-sys-5.3.1-152.pkg

Verifying
Downloading
Extracting

Package Detail
Description: Cisco ASA-SFR 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 ...
```

注意：在20到30分钟内完成安装后，系统将提示您按Enter键重新启动。为应用组件安装和ASA FirePOWER服务启动提供10分钟或更长时间。show module 1 details输出应将所有进程显示为Up。

安装期间的模块状态

```
ciscoasa# show module 1 details

Getting details from the Service Module, please wait...
Unable to read details from module 1

Card Type: ASA 5585-X FirePOWER SSP-10, 8GE
Model: ASA5585-SSP-SFR10
Hardware version: 1.0
Serial Number: JAD18400028
Firmware version: 2.0(14)1
Software version: 5.3.1-152
MAC Address Range: 58f3.9ca0.1190 to 58f3.9ca0.119b
App. name: ASA FirePOWER
App. Status: Not Applicable
App. Status Desc: Not Applicable
App. version: 5.3.1-152
Data Plane Status: Not Applicable
Console session: Not ready
Status: Unresponsive
```

成功安装后的模块状态

```
ciscoasa# show module 1 details

Getting details from the Service Module, please wait...

Card Type: ASA 5585-X FirePOWER SSP-10, 8GE
Model: ASA5585-SSP-SFR10
Hardware version: 1.0
Serial Number: JAD18400028
Firmware version: 2.0(14)1
Software version: 5.3.1-152
MAC Address Range: 58f3.9ca0.1190 to 58f3.9ca0.119b
App. name: ASA FirePOWER
App. Status: Up
App. Status Desc: Normal Operation
App. version: 5.3.1-152
Data Plane Status: Up
Console session: Ready
Status: Up
DC addr: No DC Configured
Mgmt IP addr: 192.168.45.45
Mgmt Network mask: 255.255.255.0
Mgmt Gateway: 0.0.0.0
Mgmt web ports: 443
Mgmt TLS enabled: true
```

配置

配置FirePOWER软件

1.您可以通过以下外部端口之一连接到ASA 5585-X FirePOWER模块：

- ASA FirePOWER控制台端口
- 使用SSH的ASA FirePOWER管理1/0接口

注意：您无法使用session sfr命令通过ASA背板访问ASA FirePOWER硬件模块CLI。

2.通过控制台访问FirePOWER模块后，使用用户名admin和密码Sourcefire登录。

```
Sourcefire3D login: admin
Password:

Last login: Fri Jan 30 14:00:51 UTC 2015 on ttyS0

Copyright 2001-2013, Sourcefire, Inc. All rights reserved. Sourcefire is a registered
trademark of Sourcefire, Inc. All other trademarks are property of their respective
owners.

Sourcefire Linux OS v5.3.1 (build 43)
Sourcefire ASA5585-SSP-10 v5.3.1 (build 152)

Last login: Wed Feb 18 14:22:19 on ttyS0

System initialization in progress.  Please stand by.
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]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]: dhcp
If your networking information has changed, you will need to reconnect.
[1640209.830367] ADDRCONF(NETDEV_UP): eth0: link is not ready
[1640212.873978] e1000e: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
[1640212.966250] ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
For HTTP Proxy configuration, run 'configure network http-proxy'

This sensor must be managed by a Defense Center.  A unique alphanumeric registration
key is always required.  In most cases, to register a sensor to a Defense Center,
you must provide the hostname or the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Defense Center are separated by a NAT device, you
must enter a unique NAT ID, along with the unique registration key. 'configure
manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Defense Center, you must use the same
registration key and, if necessary, the same NAT ID when you add this
sensor to the Defense Center.

>
```

配置FireSIGHT管理中心

要管理ASA FirePOWER模块和安全策略，您**必须**向FireSIGHT管理中心注册。您不能使用

FireSIGHT管理中心执行以下操作：

- 无法配置ASA FirePOWER接口。
- 无法关闭、重新启动或以其他方式管理ASA FirePOWER进程。
- 无法从ASA FirePOWER设备创建备份或将备份还原到ASA FirePOWER设备。
- 无法写入访问控制规则以匹配使用VLAN标记条件的流量。

将流量重定向到SFR模块

通过创建识别特定流量的服务策略，可将流量重定向到ASA FirePOWER模块。要将流量重定向到FirePOWER模块，请执行以下步骤：

步骤 1：选择通信

首先，使用access-list命令选择流量。在以下示例中，我们重定向来自所有接口的所有流量。您也可以针对特定流量执行此操作。

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

步骤 2：匹配流量

以下示例显示如何创建类映射并匹配访问列表上的流量：

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

步骤 3：指定操作

您可以在被动（“仅监控”）或内联部署中配置设备。您不能在ASA上同时配置仅监控模式和普通内联模式。只允许一种安全策略。

内联模式

在内联部署中，在丢弃不需要的流量并采取策略应用的任何其他操作后，流量将返回ASA以进行进一步处理和最终传输。以下示例展示如何创建策略映射并在内联模式下配置FirePOWER模块：

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class sfr
ciscoasa(config-pmap-c)# sfr fail-open
```

被动模式

在被动部署中，

- 流量的副本将发送到设备，但不会返回到ASA。
- 被动模式让您可以查看设备对流量将执行什么操作，并让您评估流量的内容，而不影响网络。

如果要在被动模式下配置FirePOWER模块，请使用monitor-only关键字，如下所示。如果不包含关键字，则流量在内联模式下发送。

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

步骤 4：指定位置

最后一步是应用策略。您可以全局应用策略或在接口上应用策略。您可以通过对接口应用服务策略以覆盖此接口的全局策略。

global关键字将策略映射应用于所有接口，而interface将策略应用于一个接口。只允许一个全局策略。在以下示例中，策略全局应用：

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

> **警告**：策略映射global_policy是默认策略。如果使用此策略并想在设备上删除此策略以排除故障，请确保了解其含义。

相关文档

- 向FireSIGHT管理中心注册设备
- 在VMware ESXi上部署FireSIGHT管理中心
- 5500-X IPS模块上的IPS管理配置方案