安装并且配置在ASA平台的一FirePOWER服务模块

目录

简介

本文描述如何安装和配置在思科可适应安全工具的思科FirePOWER (SFR)模块(ASA)运行和如何注册有思科FireSIGHT管理中心的SFR模块。

先决条件

要求

思科建议您的系统满足这些需求，在您尝试在本文描述的步骤前：

- 保证您有可用空间至少3GB在闪存驱动器(disk0)的，除引导程序软件的大小之外。
- 保证您访问特权EXEC模式。为了访问特权EXEC模式，请输入**enable命令**到CLI。如果密码未设置，则请按回车：

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

使用的组件

为了安装在思科ASA的FirePOWER服务，这些组件要求：

- Cisco ASA软件版本9.2.2或以上

- 思科ASA平台5512-X通过5555-X
- FirePOWER软件版本5.3.1或以上

  注意：如果要安装在ASA 5585-X硬件模块的FirePOWER (SFR)服务，请读FirePOWER (SFR)服务的安装在ASA 5585-X硬件模块。

这些组件在思科FireSIGHT管理中心要求：

- FirePOWER软件版本5.3.1或以上
- FireSIGHT管理中心FS2000、FS4000或者虚拟设备

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。

背景信息

思科ASA FirePOWER模块，亦称ASA SFR，提供下一代防火墙服务，例如：

- 下一代入侵防御系统(NGIPS)
- 应用程序可见性和控制(AVC)
- URL 过滤
- 先进的恶意软件保护(安培)

  注意：您能使用ASA SFR模块在单个或多个上下文模式和在已路由或透明模式。

开始使用前

请考虑此重要信息，在您尝试在本文描述的步骤前：

- 如果有重定向流量到入侵防御系统(IPS) /Context意识的活动服务服务策略(CX)模块(该用ASA SFR)替换的您，您必须删除它，在您配置ASA SFR服务策略前。

- 您必须关闭当前运行的所有其它软件模块。设备能每次运行单个软件模块。您必须从ASA CLI执行此。例如，这些命令关闭并且卸载IPS软件模块，然后重新加载ASA ：
  ```
  ciscoasa# sw-module module ips shutdown
  ciscoasa# sw-module module ips uninstall
  ciscoasa# reload
  ```
  使用为了去除CX模块的命令是相同的，除了**cxsc**关键字使用而不是**ips** ：
  ```
  ciscoasa# sw-module module cxsc shutdown
  ciscoasa# sw-module module cxsc uninstall
  ciscoasa# reload
  ```
- 当您再镜像模块时，请使用同一**关闭**并且**卸载**使用为了删除一旧有SFR镜像的命令。示例如下：
  ```
  ciscoasa# sw-module module sfr uninstall
  ```
- 如果ASA SFR模块用于多个上下文模式，请执行在系统最多执行空间内的本文描述的步骤。

  提示：为了确定一个模块的状况在ASA的，请输入**show module命令**。

安装

此部分描述如何安装在ASA的SFR模块和如何设置ASA SFR启动镜像。

安装在ASA的SFR模块

完成这些步骤为了安装在ASA的SFR模块：

1. 下载从Cisco.com的ASA SFR系统软件到从ASA SFR管理接口是可访问的HTTP、HTTPS或者FTP服务器。
2. 下载启动镜像到设备。您能使用Cisco Adaptive Security Device Manager (ASDM)或ASA CLI为了下载启动镜像到设备。 **注意**：请勿转接系统软件;它下载的以后对固体驱动(SSD)。完成这些步骤为了通过ASDM下载启动镜像： 下载启动镜像到您的工作站或者放置它在FTP、TFTP、HTTP、HTTPS、服务器消息块(SMB)或者思科安全复制(SCP)服务器。选择在ASDM的**Tools>文件管理**。选择适当的文件传输命令，*在本地PC和闪存之间*或者*在远程服务器和闪存之间*。转接引导程序软件到闪存驱动器(disk0)在ASA。完成这些步骤为了通过ASA CLI下载启动镜像：下载在FTP、TFTP、HTTP或者HTTPS服务器的启动镜像。输入**copy命令**到CLI为了下载启动镜像到闪存驱动器。 这是使用HTTP协议的示例(请用您的服务器IP地址或主机名替换**<HTTP_Server>**)：`ciscoasa# copy http://<HTTP_SERVER>/asasfr-5500x-boot-5.3.1-152.img disk0:/asasfr-5500x-boot-5.3.1-152.img`
3. 输入此命令为了配置ASA闪存驱动器的ASA SFR启动镜像位置：
   `ciscoasa# sw-module module sfr recover configure image disk0:/file_path`
   示例如下：
   ```
   ciscoasa# sw-module module sfr recover configure image disk0:
    /asasfr-5500x-boot-5.3.1-152.img
   ```
4. 输入此命令为了装载ASA SFR启动镜像：
   `ciscoasa# sw-module module sfr recover boot`
   在此时间，如果启用在ASA的**调试模块引导**，这些调试打印：
   `ciscoasa# sw-module module sfr recover boot`
5. 等大约5到15分钟为了ASA SFR模块能启动，然后开始控制台会话对可操作的ASA SFR启动镜像。

设置ASA SFR启动镜像

完成这些步骤为了设置最近安装的ASA SFR启动镜像：

1. 在您开始会话为了到达登录提示后，请按回车。 **注意**：默认用户名是**admin**，并且默认密码是**Admin123**。示例如下：
   ```
   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模块引导未完成， session命令发生故障，并且消息看上去表明系统无法在TTYS1连接。如果这发生，请等待模块引导完成和再试一次。
2. 输入**setup命令**为了配置系统，以便您能安装系统软件软件包：
   ```
   asasfr-boot> setup
   Welcome to SFR Setup
   [hit Ctrl-C to abort]
   Default values are inside []
   ```
   然后提示对于此信息：**主机名**-主机名可以是65字母数字字符，没有空间。使用连字符允许。**网络地址**-网络地址可以是静态IPv4或IPv6地址。您能也使用DHCP IPv4或者IPv6无状态的自

动配置。**DNS信息**-您必须识别至少一个域名系统(DNS)服务器，并且您能也设置域名和搜索域。**NTP信息**-您能启用网络时间协议(NTP)和配置NTP服务器为了设置系统时间。

3. 输入**install命令的系统**为了配置系统软件镜像：
   ```
   asasfr-boot >system install [noconfirm] url
   ```
   如果不要响应到确认消息，请包括**noconfirm**选项。用**.pkg**文件的位置替换**URL**关键字。示例如下：
   ```
   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.
   ```
   注意：当安装完成时，系统重新启动。允许十或更多分钟应用程序组件安装的和ASA SFR服务的能开始。**show module sfr** should命令的输出表明所有进程是UP。

配置

此部分描述如何配置FirePOWER软件和FireSIGHT管理中心和如何重定向流量到SFR模块。

配置FirePOWER软件

完成这些步骤为了配置FirePOWER软件：

1. 开始会话到ASA SFR模块。
   注意：因为登录在一个功能完备的模块，发生一个不同的登录提示当前出现。示例如下：
   ```
   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. 用用户名**admin**和密码**Admin123**登陆。
3. 完成系统配置如被提示，按此顺序发生： 读并且接受终端用户许可权协定(EULA)。更改管理员密码。配置管理地址和DNS设置，如被提示。 **注意**：您能配置IPv4和IPv6管理地址。示例如下：
   ```
   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:
   ```

4. 等待系统重新配置自己。

配置FireSIGHT管理中心

为了管理ASA SFR模块和安全策略，您必须注册它与FireSIGHT管理中心。您不可进行这些操作与FireSIGHT管理中心：

- 配置ASA SFR模块接口
- 关闭，重新启动或者管理ASA SFR模块进程
- 创建备份从或者恢复备份对， ASA SFR模块设备
- 写入访问控制规则为了匹配与使用的流量VLAN标记情况

重定向流量到SFR模块

为了重定向流量到ASA SFR模块，您必须创建识别特定的流量的服务策略。完成这些步骤为了重定向流量到ASA SFR模块：

1. 选择应该用**访问列表命令**识别的流量。在本例中，所有从所有的流量接口重定向。您能为特定的流量执行此。
   ```
   ciscoasa(config)# access-list sfr_redirect extended permit ip any any
   ```
2. 创建类映射为了匹配在访问列表的流量：
   ```
   ciscoasa(config)# class-map sfr
   ciscoasa(config-cmap)# match access-list sfr_redirect
   ```
3. 指定部署模式。您能配置您的在被动(只监控的)或轴向(正常)部署模式的设备。
   注意：您不能同时配置一个被动模式和轴向模式在ASA。仅安全策略的一种类型允许。在一轴向部署，在不期望的流量丢弃后，并且由策略应用的所有其他操作进行，流量返回对进一步处理和最终发射的ASA。此示例显示如何创建策略映射和配置在轴向模式的ASA SFR模块：
   ```
   ciscoasa(config)# policy-map global_policy
   ciscoasa(config-pmap)# class sfr
   ciscoasa(config-pmap-c)# sfr fail-open
   ```

   在一被动部署，流量的复制被发送到SFR服务模块，但是没有返回对ASA。被动模式允许您查看SFR模块关于流量将完成的操作。它也允许您评估流量的内容，不用影响到网络。

   如果要配置在被动模式的SFR模块，请使用**只监控的**关键字(如下一个示例所显示)。如果不包括关键字，流量在轴向模式发送。
   ```
   ciscoasa(config-pmap-c)# sfr fail-open monitor-only
   ```
   警告：**只监控的**模式不允许SFR服务模块否决或阻塞恶意流量。**警告：**配置在*只监控的*模式的ASA与使用interface-level流量**转发sfr只监控的**命令也许是可能的;然而，此配置纯粹地是为演示功能，并且不应该使用在制作ASA。在此演示功能被找到Cisco技术支持中心(TAC)不支持的任何问题。如果希望部署在被动模式的ASA SFR服务，请用使用*策略映射*配置它。
4. 指定位置并且运用策略。您能运用策略全局或在接口。为了改写在接口的全局策略，您能运用服务策略到该接口。

   全局关键字应用策略映射对所有接口，并且**接口**关键字运用策略对一个接口。 仅允许有一个全局策略。在本例中，策略应用全局：
   ```
   ciscoasa(config)# service-policy global_policy global
   ```
   警告：策略映射global_policy是默认策略。如果在为了实现故障排除目的您的设备使用此策略并且要取消它，请保证您了解其暗示。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 注册有FireSIGHT管理中心的一个设备
- FireSIGHT管理中心的部署在VMware ESXi的
- 在5500-X IPS模块的IPS管理配置情形
- 技术支持和文档 - Cisco Systems