Firepower (SFR)服务的安装在ASA 5585-X硬件模块的

目录

简介

亦称ASA Firepower模块， ASA SFR，用品下一代防火墙服务，包括下一代IPS (NGIPS)，应用程序可见性和控制(AVC)， URL过滤和预先的恶意软件保护(AMP)。您能使用模块在单个或多个上下文模式和在已路由或透明模式。本文描述一个Firepower (SFR)模块的前提条件和安装过程在ASA 5585-X硬件模块的。它也提供步骤注册有FireSIGHT管理中心的一个SFR模块。

> **Note**:Firepower (SFR)服务在硬件模块位于在ASA 5585-X，而，在ASA 5512-X的Firepower服务通过5555-X系列设备在软件模块安装，发生的差异安装过程。

先决条件

要求

关于本文的说明要求对特权EXEC模式的访问。为了访问特权EXEC模式，请输入`enable`。如果密码未设置，请按回车。

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

为了安装在ASA的Firepower服务，以下组件是必要的：

- ASA软件版本9.2.2或更加极大
- ASA 5585-X平台
- TFTP server可及的由Firepower模块管理接口
- 与版本5.3.1或以上的FireSIGHT管理中心

Note:本文档中的信息从在特定实验室环境的设备创建。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

给ASA SSM总是占用在ASA 5585-X机箱的两slot之一，如果有一个硬件模块除Firepower (SFR)服务SSP之外例如SSP-CX (意识的上下文)或AIP-SSM (先进的检查和预防安全)，另一个模块必须卸载做SSP-SFR的空间。在您去除硬件模块前，请运行以下命令关闭模块：

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

布线和管理

- 您不能通过ASA的5585-X ASA的控制台访问SFR模块的串行端口。
- 一旦SFR模块设置，使用“1"命令，您能会话到刀片。
- 为了完全再镜像在ASA 5585-X的SFR模块，您必须使用管理以太网接口和一个控制台会话序列管理端口的，是在SFR模块和分别于ASA的管理接口并且控制。

  提示：为了查找一个模块的状况在ASA的，请运行“`show module 1`”发出命令哪些获取SFR模块的管理IP和相关的防御中心。

安装在ASA的Firepower (SFR)模块

1. 下载从Cisco.com的ASA Firepower SFR模块初始Bootstrap镜像到TFTP server可访问从ASA Firepower管理接口。镜像名称看起来象“asasfr `BOOT5.3.1 152.img`"

2. 下载从Cisco.com的ASA Firepower系统软件到HTTP、HTTPS或者FTP服务器可访问从ASA Firepower管理接口。

3. 重新启动SFR模块

选项 1：如果没有密码到SFR模块，您能发出从ASA的以下命令重新启动模块。

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

选项 2：如果有密码到SFR模块，您能重新启动传感器直接地从其line命令。

```
Sourcefire3D login: admin
Password:

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

>system reboot
```

4. 中断SFR模块使用ESCAPE或您的终端会话软件中断序列的启动程序放置模块到ROMMON。

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

<truncated output>

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. 配置与IP地址的SFR模块管理接口并且指示TFTP server的位置并且TFTP路径到Bootstrap镜像。输入以下命令设置在接口的一个IP地址和检索TFTP镜像：

-
- ADDRESS= Your_IP_Address
- = Your_Gateway
- = Your_TFTP_Server
- IMAGE = Your_TFTP_Filepath
-
- tftp

!示例使用的IP地址信息。为您的环境的更新。

```
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. 对初始引导程序镜像的登录。登录作为admin和用密码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. 请使用初始引导程序镜像配置在模块的管理接口的一个IP地址。输入setup命令输入向导。提示对于以下信息：

- **主机名**：65字母数字字符，没有空间。连字符允许。
- 网络地址：您能设置静态IPv4或IPv6地址，或者请使用DHCP (IPv4)或IPv6无状态的自动配置。
- **DNS信息**：您必须识别至少一个DNS服务器，并且您能也设置域名和搜索域。
- **NTP信息**：您能启用NTP和配置NTP服务器，设置的系统时间。

!使用的示例信息。为您的环境的更新。

```
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. 请使用启动镜像请求和配置系统软件镜像使用**install**。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。

```
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 ...
```

Note:当安装在20到30分钟之内完成，将提示您按回车密钥重新启动。允许10或更多分钟应用程序组件安装的和ASA Firepower服务的能开始。show module 1详细信息输出应该显示所有进程作为。

在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
```

在成功的安装以后的模块状态

```
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.You能连接到ASA 5585-X Firepower模块通过任一个下列的外部端口：

- ASA Firepower控制台端口
- ASA Firepower管理1/0接口使用SSH

Note:使用`sfr`命令，您不能访问在ASA背板的ASA Firepower硬件模块CLI。

2. 在您通过控制台后访问Firepower模块，请用用户名**admin**和密码**Sourcefire**登陆。

```
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

为了管理ASA Firepower模块和安全策略，您**必须**注册它与FireSIGHT管理中心。您不能执行以下与

FireSIGHT管理中心：

- 不能配置ASA Firepower接口。
- 不能关闭，重新启动或者管理ASA Firepower进程。
- 不能创建备份从或恢复备份到ASA Firepower设备。
- 使用VLAN标记情况，不能写入访问控制规则匹配流量。

重定向流量到SFR模块

您重定向流量到ASA Firepower模块通过创建识别特定的流量的服务策略。为了重定向流量到Firepower模块，请遵从下面步骤：

步骤 1：选择通信

首先，挑选流量使用。在以下示例中，我们重定向从所有的所有流量接口。您可能为特定的流量执行它。

```
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和匹配在访问列表的流量：

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

步骤 3：指定操作

您能配置您的在一被动(“只监控的”)或轴向部署的设备。您不能同时配置只监控的模式和正常轴向模式在ASA。仅安全策略的一种类型允许。

轴向模式

在一轴向部署，在降低不期望的流量和采取策略应用的任何其他行动以后，流量返回对进一步处理和最终发射的ASA。以下示例显示如何创建策略映射和配置在轴向模式的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

在一被动部署，

- 流量的复制被发送到设备，但是没有返回对ASA。
- 被动模式让您发现什么设备将执行对流量，并且让您评估流量的内容，无需影响网络。

如果要配置在被动模式的Firepower模块，请使用关键字作为下面。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
```

步骤 4：指定位置

最后一步是运用策略。您能运用策略全局或在接口。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。

关键字应用策略映射对所有接口，并且运用策略对一个接口。 仅允许有一个全局策略。在以下示例中，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。如果使用此策略并且要取消在您的设备的此策略故障排除目的，请确保您了解其暗示。

相关文档

- 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