快速入门指南

Cisco ASA FirePOWER 模块

修订日期：2014 年 10 月 1 日

1 ASA FirePOWER 模块

ASA FirePOWER 模块提供下一代防火墙服务，包括下一代入侵防御系统 (NGIPS)、应用可视性与可控性 (AVC)、 URL 过滤和高级恶意软件防护 (AMP)。您可在单个或多情景模式以及路由模式或透明模式中使用本模块。

本模块也称为 ASA SFR。

虽然本模块具有用于初始配置和故障排除的基本命令行界面 (CLI)，您也可使用单独的应用 - FireSIGHT 管理中心，来配置设备的安全策略。该应用可托管在单独的 FireSIGHT 管理中心设备或作为虚拟设备运行在 VMware 服务器上。（FireSIGHT 管理中心也称为防御中心。）

ASA FirePOWER 模块与 ASA 的配合方式

ASA FirePOWER 模块运行 ASA 提供的单独应用。本模块可以是一个硬件模块 （仅在 ASA 5585-X 上），也可以是一个软件模块 （其他型号）。作为一个硬件模块时，设备包括单独的管理和控制台端口，以及由 ASA 直接使用而非模块自身使用的额外数据接口。

您可以在被动部署 （“仅监控”）或内联部署中配置设备。

- 在被动部署中，流量副本将会被发送到设备，但不会被返回到 ASA。通过被动模式，您可以知道设备可能完成的流量处理，并能在不影响网络的情况下评估流量内容。
- 在内联部署中，实际流量将会被发送至设备，并且设备策略影响对流量的处理。在丢弃不需要的流量并采取策略应用的任何其他操作后，流量将会返回至 ASA，以进行进一步处理和最终传输。

以下各节详细地说明了这些模式。

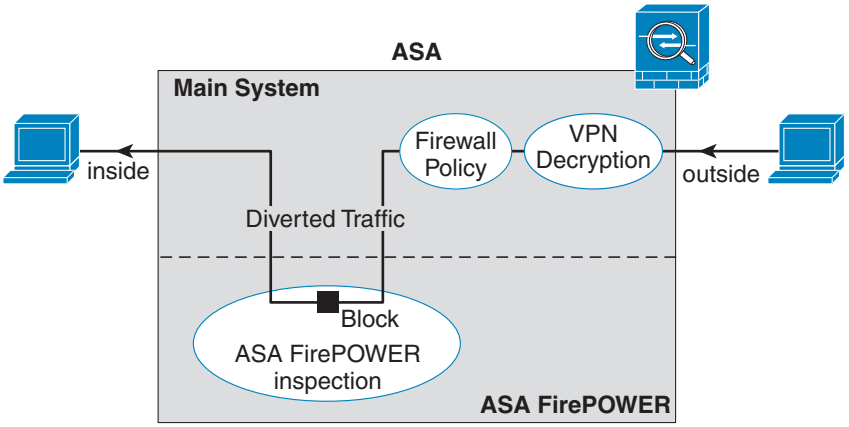
ASA FirePOWER 内联模式

在内联模式中，流量在被转发到 ASA FirePOWER 模块之前会通过防火墙检查。当在 ASA 上识别流量以进行 ASA FirePOWER 检查时，流量按以下顺序流经 ASA 和本模块：

1. 流量进入 ASA。
2. 解密流入 VPN 的流量。
3. 应用防火墙策略。
4. 流量被发送至 ASA FirePOWER 模块。
5. ASA FirePOWER 模块将安全策略应用至流量，并执行适当的操作。
6. 有效流量被返回到 ASA；ASA FirePOWER 模块可能根据其安全策略阻止某些流量，这些流量将不会被传送。
7. 加密流出 VPN 的流量。
8. 流量退出 ASA。

下图显示在内联模式中使用 ASA FirePOWER 模块时的流量。在本示例中，模块阻止了某个应用所不允许的流量。所有其他流量都是通过 ASA 转发。

图 1　　ASA 中的 ASA FirePOWER 模块流量



注　如果主机之间通过两个 ASA 接口连接，并且只有一个接口配置了 ASA FirePOWER 服务策略，则这些主机之间的所有流量都将发送到 ASA FirePOWER 模块，包括来自非 ASA FirePOWER 接口的流量（因为此功能是双向的）。

ASA FirePOWER 被动（仅监控）模式

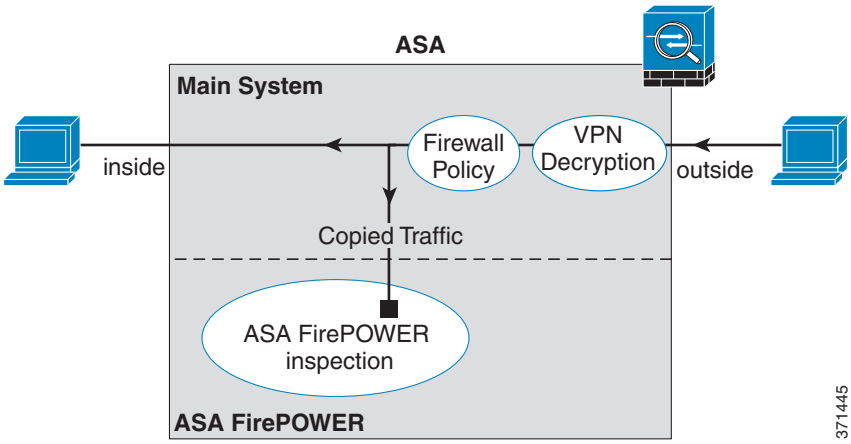
仅监控模式的流量与内联模式的流量基本相同，唯一的区别是 ASA FirePOWER 模块不向 ASA 回传流量。相反，本模块将安全策略应用至流量，并告知您其在内联模式中运行时将会做出的处理，例如流量可能在事件中被标记为“应丢弃”。您可以利用此信息进行流量分析并决定是否需要内联模式。

要配置被动模式，您需将仅监控指示添加至重定向流量至本模块的服务策略。

注　在 ASA 上，您无法同时配置仅监控模式和正常内联模式。只允许一种安全策略。在多情景模式下，您无法为某些情景配置仅监控模式并为其他情景配置常规内联模式。

下图显示此模块在被动模式中运行时的流量。

图 2　　ASA FirePOWER 被动（仅监控）模式



ASA FirePOWER 管理访问

共有两个用于管理 ASA FirePOWER 模块的单独访问层：初始配置 （以及后续的故障排除）和策略管理。

进行初始配置时，您必须使用 ASA FirePOWER 模块的 CLI。要访问 CLI，您可以使用以下方法：

- ASA 5585-X （硬件模块）：
  - ASA FirePOWER 控制台端口 - 模块上的控制台端口是一个单独的外部控制台端口。
  - 使用 SSH 的 ASA FirePOWER 管理 1/0 接口 - 您可以连接至默认的 IP 地址 (192.168.45.45/24)，也可以在使用 ASDM 更改管理 IP 地址后使用 SSH 进行连接。模块上的管理接口是一个单独的外部千兆位以太网接口。

注 您无法使用 **session** 命令来访问 ASA 背板上的 ASA FirePOWER 硬件模块 CLI。

- 所有其他型号 （软件模块）：
  - 背板上的 ASA 会话 — 如果您有权通过 CLI 访问 ASA，则可以与模块会话并访问模块 CLI。
  - 使用 SSH 的 ASA FirePOWER 管理 0/0 接口 - 您可以连接至默认的 IP 地址 (192.168.45.45/24)，也可以在使用 ASDM 更改管理 IP 地址后使用 SSH 进行连接。ASA FirePOWER 管理接口与 ASA 共用管理接口。ASA 和 ASA FirePOWER 模块支持单独的 MAC 地址和 IP 地址。您必须在 ASA FirePOWER 操作系统内 （使用 CLI 或 ASDM）配置 ASA FirePOWER IP 地址。但是，物理特性 （例如启用接口）在 ASA 配置。您可以移除 ASA 接口配置 （尤其是接口名称），将此接口指定为一个 ASA FirePOWER 接口。此接口仅用于管理。

完成初始配置后，请使用 FireSIGHT 管理中心 ASA FirePOWER 配置安全策略。然后，配置 ASA 策略，以使用 CLI、 ASDM 或 Cisco Security Manager 将流量发送至 ASA FirePOWER 模块。

与 ASA 功能的兼容性

ASA 带有诸多高级应用检查功能，其中包括 HTTP 检查。但是，ASA FirePOWER 模块比ASA 提供了更高级的 HTTP 检查，以及适用于其他应用的其他功能，包括监测和控制应用的使用情况。

要充分利用 ASA FirePOWER 模块的功能，请按照以下原则处理发送至 ASA FirePOWER 模块的流量：

- 请勿对 HTTP 流量配置 ASA 检查。
- 请勿配置云网络安全 (ScanSafe) 检查。如果对同一流量同时配置 ASA FirePOWER 检查和云网络安全检查， ASA 只执行 ASA FirePOWER 检查。
- ASA 的其他应用检查 （包括默认检查）与 ASA FirePOWER 模块兼容。
- 请勿启用移动用户安全 (MUS) 服务器；此服务器与 ASA FirePOWER 模块不兼容。

2 ASA FirePOWER 指导原则

故障转移指导原则

不直接支持故障转移；在 ASA 进行故障转移时，所有现有 ASA FirePOWER 流量会被传输到新 ASA。新 ASA 的 ASA FirePOWER 模块开始从该点向前检查流量；不会传输旧的检查状态。

您需将高可用性 ASA 对中 ASA FirePOWER 模块上的策略保持一致 （使用 FireSIGHT 管理中心），确保故障转移行为的一致性。

ASA 集群指导原则

不支持直接集群，但可在集群中使用这些模块。您需使用 FireSIGHT 管理中心将集群内 ASA FirePOWER 模块上的策略保持一致。请勿对集群内设备使用不同的基于 ASA 接口的区域定义。

型号指导原则

- 对于 5512-X 至 5585-X 型号，最低软件要求为 ASA 软件 9.2 (2.4) 和 ASA FirePOWER 5.3.1。
- 以下型号支持 ASA FirePOWER 模块。对于 ASA 5585-X，本模块是一个硬件模块，但对于其他所有型号，本模块是一个软件模块。有关详细信息，请参阅 《*思科 ASA 兼容性矩阵*》(http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html)。
  - 5585-X （硬件模块）
  - 5555-X
  - 5545-X
  - 5515-X
  - 5512-X
- 对于 5512-X 到 ASA 5555-X，您必须安装思科固态硬盘 (SSD)。有关详细信息，请参阅 《ASA 5500 - X 硬件指南》。

其他指导原则和限制

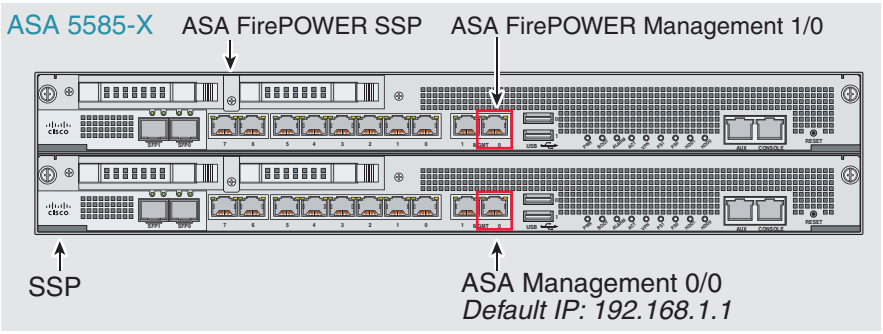
- 请参阅第 4 页上的与 ASA 功能的兼容性。
- 您无法更改安装在硬件模块的上软件类型；如果您购买了 ASA FirePOWER 模块，您日后无法在模块上安装其他软件。
- 在 ASA 上，您无法同时配置仅监控模式和正常内联模式。只允许一种安全策略。在多情景模式下，您无法为某些情景配置仅监控模式或为其他情景配置常规内联模式。

3 连接 ASA FirePOWER 管理接口

除了提供对 ASA FirePOWER 模块的管理访问以外， ASA FirePOWER 管理接口需要访问 HTTP 代理服务器或 DNS 服务器及互联网，以获取更新签名和更多信息。本节描述的仅为推荐的网络配置。本节里的网络可能与您的网络不同。

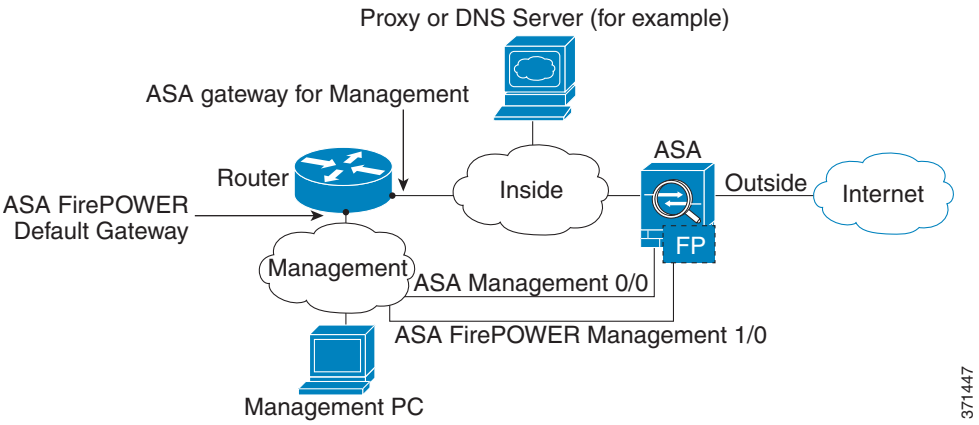
ASA 5585-X （硬件模块）

ASA FirePOWER 模块带有一个 ASA 提供的单独管理和控制台接口。对于初始设置，可以使用默认的 IP 地址，通过 SSH 连接到 ASA FirePOWER 管理 1/0 接口。如果无法使用默认的 IP 地址，可以使用控制台端口或使用 ASDM 更改管理 IP 地址，以使用 SSH。（请参阅第 11 页上的更改 ASA FirePOWER 管理 IP 地址。）



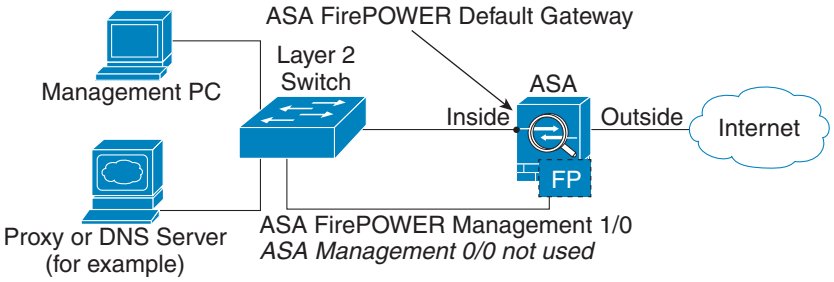
如果有内部路由器

如果有内部路由器，您可以在包括 ASA 管理 0/0 和 ASA FirePOWER 管理 1/0 接口的管理网络和 ASA 内部网络之间建立路由，以访问互联网。此外，请务必在 ASA 上添加一个路由，以通过内部路由器访问管理网络。



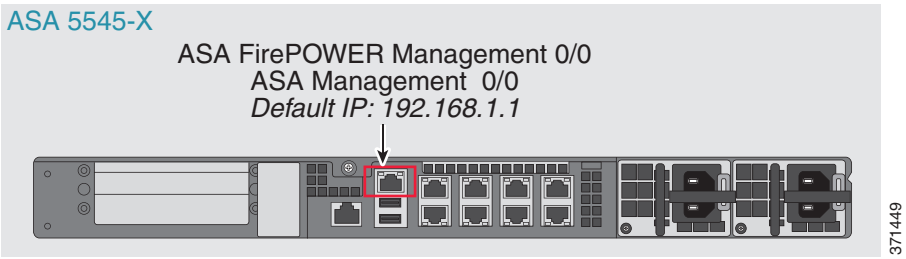
如果没有内部路由器

如果只有一个内部网络，您就无法拥有一个单独管理网络，这需要内部路由器实现网络之间的路由。在这种情况下，您可以从内部接口而非 0/0 接口来管理 ASA。由于 ASA FirePOWER 模块是 ASA 提供的单独设备，您可以将 ASA FirePOWER 管理 1/0 地址配置到与内部接口相同的网络。



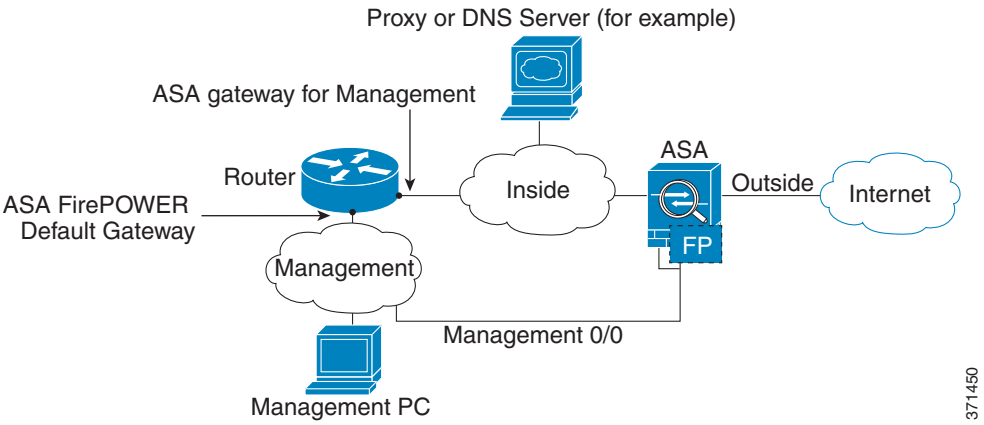
ASA5512-X 到 ASA 5555-X （软件模块）

ASA FirePOWER 模块在这些型号中作为一个软件模块运行， ASA FirePOWER 管理接口与 ASA 共用管理 0/0 接口。对于初始设置，可以使用 SSH 连接到 ASA FirePOWER 默认的 IP 地址。如果无法使用默认的 IP 地址，可以与背板上的 ASA FirePOWER 会话或使用 ASDM 更改管理 IP 地址，以使用 SSH。



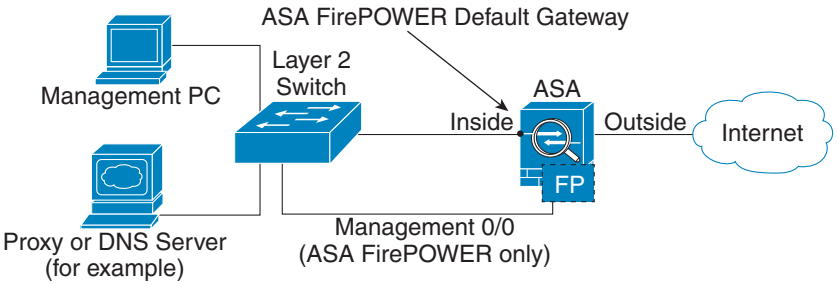
如果有内部路由器

如果有内部路由器，您可以在包括 ASA 和 ASA FirePOWER 管理 IP 地址的管理 0/0 网络与内部网络之间实现路由，以访问互联网。此外，请务必在 ASA 上添加一个路由，以通过内部路由器访问管理网络。



如果没有内部路由器

如果只有一个内部网络，您就无法拥有一个单独的管理网络。在这种情况下，可以从内部接口而非 0/0 接口来管理 ASA。如果从管理 0/0 接口移除 ASA 配置的名称，您仍可以配置该接口的 ASA FirePOWER IP 地址。由于 ASA FirePOWER 模块实质上是 ASA 提供的单独设备，您 *可以* 将 ASA FirePOWER 管理地址配置到与内部接口相同的网络。



注 您必须移除管理 0/0 的 ASA 配置名称。如果在 ASA 已配置该名称，则 ASA FirePOWER 地址必须与 ASA 在同一网络，并且排除所有已在其他 ASA 接口上配置的网络。如果该名称未配置，则 ASA FirePOWER 地址可在任何网络，例如，ASA 内部网络。

4 启动 ASA 上的自适应安全设备管理器 (ASDM)

可使用默认 ASA 配置连接到默认的管理 IP 地址 (192.168.1.1)。根据不同的网络，您可能需要更改 ASA 管理 IP 地址，或为 ASDM 访问配置其他的 ASA 接口 （请参阅第 5 页上的连接 ASA FirePOWER 管理接口）。

对于 ASA 5512-X 到 ASA 5555-X，如果您没有单独的管理网络 （请参阅第 7 页上的如果没有内部路由器），就需要为管理配置一个内部接口，*并且*从 0/0 接口移除名称。要更改接口和管理设置，请参阅 《ASA 配置指南》。

步骤 1 在管理计算机上，启动网络浏览器。

步骤 2 在地址栏中，输入以下 URL：**https://***ASA_IP_address*/**admin**。默认的 ASA 管理 IP 地址为 192.168.1.1。

步骤 3 点击 **Run ASDM** 运行 Java Web Start 应用。或者，从该页面下载 ASDM 启动程序。

步骤 4 根据系统显示的对话框接受所有证书。系统将显示 **Cisco ASDM-IDM Launcher** 对话框。

步骤 5 不填写用户名和密码字段，并点击 **OK**。系统将显示 ASDM 主窗口。

5 安装或重新映像 ASA FirePOWER 软件模块

如果您购买了含有 ASA FirePOWER 模块的 ASA，模块软件和所需的固态硬盘 (SSD) 已经预装，您随时可以进行配置。如果要向现有 ASA 添加一个 ASA FirePOWER 软件模块 或需要更换 SSD，您需要安装 ASA FirePOWER 启动软件，将 SSD 分区，并根据此程序安装系统软件。

重新映像模块的步骤与此类似，不同之处在于您首先要卸载 ASA FirePOWER 模块。如果更换 SSD，需要重新映像系统。

有关如何物理安装 SSD 的信息，请参阅 《ASA 硬件指南》。

先决条件

- 闪存 (disk0) 的可用空间至少应为 3 GB 加上启动软件的大小。
- 在多情景模式下，请在系统执行空间中执行此步骤。
- 设备一次只能运行一个软件模块，因此必须先关闭所有可能正在运行的其他软件模块。此操作必须从 ASA CLI 执行。例如，执行以下命令关闭并卸载 IPS 软件模块，然后重新加载 ASA；移除 CX 模块的命令与此相同，但使用 **cxsc** 关键字而非 **ips**。

  ```
  hostname# sw-module module ips shutdown
  hostname# sw-module module ips uninstall
  hostname# reload
  ```

- 如果有主动服务策略将流量重定向至 IPS 或 CX 模块，您必须移除该策略。例如，如果策略为全局策略，则使用 no service-policy *ips_policy* global。如果服务策略包括想要维护的其他规则，您则只从相关的策略映射移除重定向命令，或者，如果定向是类的唯一操作，则从整个流量类别移除。可以使用 CLI 或 ASDM 移除策略。
- 当重新映像模块时，使用相同的关闭和卸载命令移除旧映像。例如， **sw-module module sfr uninstall**。
- 从 Cisco.com 获取 ASA FirePOWER 启动映像和系统软件包。

操作步骤

步骤 1 将启动映像下载到设备。请勿传输系统软件；系统软件稍后会下载到 SSD。您有以下选项：

- ASDM：首先将启动映像下载到工作站，或者将其放置在 FTP、TFTP、HTTP、HTTPS、SMB 或 SCP 服务器上。然后，在 ASDM 中，选择 **Tools > File Management**，然后选择适当的 **File Transfer** 命令，**Between Local PC and Flash** 或 **Between Remote Server and Flash**。将启动软件传输至 ASA 上的 disk0。
- ASA CLI：首先将启动映像放置在 TFTP、 FTP、 HTTP 或 HTTPS 服务器，然后使用 **copy** 命令将其下载到闪存。以下示例使用 TFTP；请使用服务器的 IP 地址或主机名替换 <TFTP Server>。

  ```
  ciscoasa# copy tftp://<TFTP SERVER>/asasfr-5500x-boot-5.3.1-58.img
  disk0:/asasfr-5500x-boot-5.3.1-58.img
  ```

步骤 2 从 Cisco.com 将 ASA FirePOWER 系统软件下载到可以通过 ASA FirePOWER 管理接口访问的 HTTP、HTTPS 或 FTP 服务器。

步骤 3 输入以下命令，在 ASA disk0 中设置 ASA FirePOWER 模块启动映像位置：

```
hostname# sw-module module sfr recover configure image disk0:file_path
```

如果收到类似“ERROR: Another service (cxsc) is running, only one service is allowed to run at any time”的信息，表明您已经配置了不同的软件模块。如上面的先决条件一节所述，必须将其停止并移除，然后安装新模块。

例如：

```
hostname# sw-module module sfr recover configure image
disk0:asasfr-5500x-boot-5.3.1-58.img
```

步骤 4 输入下列命令加载 ASA FirePOWER 启动映像：

```
hostname# sw-module module sfr recover boot
```

步骤 5 等待 5 到 15 分钟左右，ASA FirePOWER 模块启动完成后，打开与正在运行的 ASA FirePOWER 启动映像之间的控制台会话。打开会话后，您可能需要按 Enter 键显示登录提示。默认用户名是 **admin**，默认密码是 **Admin123**。

```
hostname# 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
```

如果模块启动未完成，**session** 命令将失败并提示无法通过 ttyS1 进行连接。请稍后重试。

步骤 6 使用 **setup** 命令配置系统后，您可以安装系统软件包。

```
asasfr-boot> setup


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

系统提示您输入以下内容。请注意，管理地址和网关以及 DNS 信息是配置的主要设置。

- Host name - 最多 65 个字母数字的字符，不能含有空格。允许含有连字符。
- Network address - 可以设置为静态 IPv4 或 IPv6 地址，或者使用 DHCP（适用于 IPv4）或 IPv6 无状态自动配置。
- DNS information - 必须确定至少一个 DNS 服务器；您也可以设置域名和搜索域。
- NTP information - 可以启用 NTP 并配置 NTP 服务器来设置系统时间。

步骤 7 使用 **system install** 命令安装系统软件映像：

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

如果不想回复确认消息，请在命令中添加 **noconfirm** 选项。使用 HTTP、 HTTPS 或 FTP URL；如果需要用户名和密码，系统将提示您输入用户名和密码。

安装完成后，系统重启。应用组件安装以及 ASA FirePOWER 服务启动需要 10 分钟或更长的时间。（**show module sfr** 输出应将所有流程显示为 Up。）

例如：

```
asasfr-boot> system install http://asasfr-sys-5.3.1-44.pkg
Verifying
Downloading
Extracting
Package Detail
        Description:                    Cisco ASA-FirePOWER 5.3.1-44 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 Feb 17 19:28:38 2014):

The system is going down for reboot NOW!
Console session with module sfr terminated.
```

步骤 8 打开与 ASA FirePOWER 模块的会话。因为登录的是全功能模块，系统将会显示不同的登录提示。

```
asa3# session sfr
Opening command session with module sfr.
Connected to module sfr.Escape character sequence is 'CTRL-^X'.

Sourcefire ASA5555 v5.3.1 (build 44)
Sourcefire3D login:
```

步骤 9 使用用户名 **admin** 和密码 **Sourcefire** 登录。

步骤 10 按提示完成系统配置。

您必须先阅读并接受最终用户许可协议 (EULA)。然后按提示更改管理员密码，配置管理地址和 DNS 设置。您可以配置 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]: 10.86.118.3
Enter an IPv4 address for the management interface [255.255.255.0]: 255.255.252.0
Enter the IPv4 default gateway for the management interface []: 10.86.116.1
Enter a fully qualified hostname for this system [Sourcefire3D]: asasfr.example.com
Enter a comma-separated list of DNS servers or 'none' []: 10.100.10.15,
10.120.10.14
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'
(Wait for the system to reconfigure itself.)

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.
```

步骤 11 使用 **configure manager add** 命令识别将管理此设备的 FireSIGHT 管理中心设备。

系统将提供一个注册密钥，您将在向设备库存添加设备时于 FireSIGHT 管理中心中使用。以下示例给出一个简单案例。当存在 NAT 边界时，命令会有所不同；请参阅第 12 页上的向 FireSIGHT 管理中心添加 ASA FirePOWER。

```
> configure manager add 10.89.133.202 123456
Manager successfully configured.
```

步骤 12 在浏览器中，使用 HTTPS 连接以及上面输入的主机名和地址登录 FireSIGHT 管理中心。例如，https://DC.example.com。

使用 Device Management (**Devices > Device Management**) 页面添加设备。有关详细信息，请参阅联机帮助或《*FireSIGHT 系统用户指南*》中的“管理设备”章节。

提示 也可以通过 FireSIGHT 管理中心配置 NTP 和时间设置。在通过 **System > Local > System Policy** 页面编辑本地策略时，请使用时间同步设置。

6 更改 ASA FirePOWER 管理 IP 地址

如果无法使用默认的管理 IP 地址，可以从 ASA 设置管理 IP 地址。设置管理 IP 地址后，可以使用 SSH 访问 ASA FirePOWER 模块执行其他设置。

如果已经在初始系统设置时通过 ASA FirePOWER CLI 配置了管理地址，如第 11 页上的在 ASA FirePOWER CLI 配置基本 ASA FirePOWER 设置所述，则不需要通过 ASA CLI 或 ASDM 配置管理地址。

注 对于软件模块，可以访问 ASA FirePOWER CLI，通过从 ASA CLI 发起会话来执行设置；然后在设置过程中设置 ASA FirePOWER 管理 IP 地址。对于硬件模块，您可以通过控制台端口完成初始设置。

在多情景模式下，请在系统执行空间中执行此步骤。

步骤 1 在 ASDM 中，选择 **Wizards > Startup Wizard**。

步骤 2 点击 **Next** 从初始屏幕向前浏览，直至显示出 ASA FirePOWER Basic Configuration 屏幕。

步骤 3 输入新的管理 IP 地址、子网掩码和默认网关。

您还必须接受最终用户许可协议。

步骤 4 点击 **Finish** 跳过其余屏幕，或者点击 **Next** 向前浏览剩余屏幕，完成向导。

7 在 ASA FirePOWER CLI 配置基本 ASA FirePOWER 设置

配置安全策略之前，您必须在 ASA FirePOWER 模块配置基本网络设置和其他参数。该步骤假设您已安装了完整的系统软件（而不仅仅是启动映像）；要么是在直接安装软件后，购买了已预安装模块的设备，或者是硬件模块中已安装了软件。

此步骤还假设您正在执行初始配置。在初始配置期间，系统会提示您执行这些设置。如果以后需要更改这些设置，请运行 **configure network** 命令更改单个设置。有关 **configure network** 命令的详细信息，请使用 **?** 命令获取帮助，并参阅《*FireSIGHT 系统用户指南*》或 FireSIGHT 管理中心内的联机帮助。

步骤 1 执行以下操作之一：

- （适用于所有型号）使用 SSH 连接至 ASA FirePOWER 管理 IP 地址。
- （仅适用于软件模块）从 ASA CLI 打开与模块的会话 （请参阅常规操作配置指南中的“入门”章节访问 ASA CLI）。在多情景模式，请从系统执行空间打开会话。

```
hostname# session sfr
```

步骤 2 使用用户名 **admin** 和密码 **Sourcefire** 登录。

步骤 3 按提示完成系统配置。

您必须先阅读并接受最终用户许可协议 (EULA)。然后按提示更改管理员密码，配置管理地址和 DNS 设置。您可以配置 IPv4 和 IPv6 管理地址。当系统显示传感器必须通过 FireSIGHT 管理中心进行管理的消息时，配置完成。

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]: 10.86.118.3
Enter an IPv4 address for the management interface [255.255.255.0]: 255.255.252.0
Enter the IPv4 default gateway for the management interface []: 10.86.116.1
Enter a fully qualified hostname for this system [Sourcefire3D]: asasfr.example.com
Enter a comma-separated list of DNS servers or 'none' []: 10.100.10.15,
```

```
10.120.10.14
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'
(Wait for the system to reconfigure itself.)

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.
```

步骤 4 现在必须按照第 12 页上的向 FireSIGHT 管理中心添加 ASA FirePOWER 的说明，确定管理此设备的 FireSIGHT 管理中心。

8 向 FireSIGHT 管理中心添加 ASA FirePOWER

FireSIGHT 管理中心也称为防御中心，是管理相同或不同型号的多个 FirePOWER 设备的单独服务器。 FireSIGHT 管理中心可以保证跨设备配置的一致性和流量分析的效率，是管理大型部署的理想之选。

对于 ASA 5512-X 到 5585-X，必须将模块注册至 FireSIGHT 管理中心。您无法通过其他方式配置模块。

要注册具有 FireSIGHT 管理中心的设备，请使用 **configure manager add** 命令。将设备注册至 FireSIGHT 管理中心时，通常需要一个字母数字注册密钥。这是一个指定的简单密钥，与许可证密钥不同。

在大多数情况下，除注册密钥外，还必须提供 FireSIGHT 管理中心的主机名或 IP 地址，例如：

```
configure manager add DC.example.com my_reg_key
```

但是，如果设备与 FireSIGHT 管理中心由 一台 NAT 设备分开，请与注册密钥一起输入唯一的 NAT ID，并指定 DONTRESOLVE 而非主机名，例如：

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

步骤 1 执行以下操作之一：

- （适用于所有型号）使用 SSH 连接至 ASA FirePOWER 管理 IP 地址。
- （仅适用于软件模块）从 ASA CLI 打开与模块的会话 （请参阅常规操作配置指南中的“入门”章节访问ASA CLI）。在多情景模式，请从系统执行空间打开会话。

  ```
  hostname# session sfr
  ```

步骤 2 使用用户名 **admin** 或具有 CLI 配置 （管理员）访问权限级别的其他用户名登录。

步骤 3 在提示符位置，使用 **configure manager add** 命令将设备注册至 FireSIGHT 管理中心。语法如下：

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

其中：

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} 指定 FireSIGHT 管理中心的完全限定主机名或 IP 地址。如果 FireSIGHT 管理中心不可直接寻址，请使用 DONTRESOLVE。
- *reg_key* 是向 FireSIGHT 管理中心注册设备需要的唯一字母数字注册密钥。
- *nat_id* 是在 FireSIGHT 管理中心与设备之间的注册过程中使用的可选字母数字字符串。如果主机名设置为 DONTRESOLVE，此项为必填项。

步骤 4 在浏览器中，使用 HTTPS 连接以及上面输入的主机名和地址登录 FireSIGHT 管理中心。例如，https://DC.example.com。

使用 Device Management (**Devices > Device Management**) 页面添加设备。有关详细信息，请参阅联机帮助或《*FireSIGHT 系统用户指南*》中的“管理设备”章节。

9 配置 ASA FirePOWER 模块安全策略

安全策略对模块提供的服务进行控制，例如下一代 IPS 过滤和应用过滤。

可使用 FireSIGHT 管理中心配置模块上的安全策略。

没有用于配置安全策略的 CLI。

使用 FireSIGHT 管理中心配置安全策略

要打开 FireSIGHT 管理中心，请执行以下操作之一：

- 使用网络浏览器打开 **https://***DC_address*，其中 *DC_address* 是在第 12 页上的向 FireSIGHT 管理中心添加 ASA FirePOWER 中定义的管理器 DNS 名称或 IP 地址。例如， https://dc.example.com。
- 在 ASDM 中，选择 **Home > ASA FirePOWER Status** 并点击控制面板底部的链接。

有关如何配置安全策略的信息，请参阅 《*FireSIGHT 系统用户指南*》或 FireSIGHT 管理中心中的联机帮助。

10 向 ASA FirePOWER 模块重定向流量

您可创建识别特定流量的服务策略，向 ASA FirePOWER 模块重定向流量。

您可以在被动部署 （“仅监控”）或内联部署中配置设备。

- 在被动部署中，流量副本将会被发送到设备，但不会被返回到 ASA。通过被动模式，您可以知道设备可能完成的流量处理，并能在不影响网络的情况下评估流量内容。
- 在内联部署中，实际流量将会被发送至设备，并且设备策略影响对流量的处理。在丢弃不需要的流量并采取策略应用的任何其他操作后，流量将会返回至 ASA，以进行进一步处理和最终传输。

在 ASA 上，您无法同时配置仅监控模式和正常内联模式。只允许一种安全策略。在多情景模式下，您无法为某些情景配置仅监控模式并为其他情景配置常规内联模式。

准备工作

- 如果有主动服务策略将流量重定向至 IPS 或 CX 模块 （已用 ASA FirePOWER 替换），您必须移除该策略，然后才能配置 ASA FirePOWER 服务策略。
- 请确保在 ASA 和 ASA FirePOWER 上配置的策略一致。两个策略应该反映流量的被动或内联模式。
- 在多情景模式下，请在每个安全情景中执行此步骤。

操作步骤

步骤 1 在 ASDM 中，选择 **Configuration > Firewall > Service Policy Rules**。

步骤 2 选择 **Add > Add Service Policy Rule**。

步骤 3 选择是否向特定接口应用策略或全局应用此策略，并点击 **Next**。

步骤 4 配置流量匹配。例如，您可以匹配 **Any Traffic**，这样通过入站访问规则的所有流量都将被重定向至模块。或者，您也可以定义基于端口、 ACL （源和目标条件），或现有流量类，定义更严格的条件。其他选项对于此策略的用处不大。完成流量类定义后，点击 **Next**。

步骤 5 在 Rule Actions 页面，点击 **ASA FirePOWER Inspection** 选项卡。

步骤 6 选择 **Enable ASA FirePOWER for this traffic flow** 复选框。

步骤 7 在 If ASA FirePOWER Card Fails 区域，请点击以下任一内容：

- **Permit traffic** - 如果模块不可用，则设置 ASA 允许所有流量不经检测即可通过。
- **Close traffic** - 如果模块不可用，则设置 ASA 阻止所有流量。

步骤 8 （可选）选中 **Monitor-only** 向模块发送流量只读副本，即被动模式。如果选择此选项，流量将以内联模式发送。有关详细信息，请参阅第 3 页上的ASA FirePOWER 被动 （仅监控）模式。

步骤 9 点击 **Finish**，然后点击 **Apply**。

根据需要重复此步骤，以配置其他流量。

11 更多信息指南

- 有关 ASA FirePOWER 模块的详细信息，请参阅 《ASA/ASDM 防火墙配置指南》的 “ASA FirePOWER 模块”章节或 ASDM 联机帮助。您可以从以下网址中获取所有 ASA/ASDM 文档的链接：

  http://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asaroadmap.html
- 有关 FireSIGHT 管理中心 （也称为防御中心）的详细信息，请参阅应用的联机帮助或 《*FireSIGHT 系统用户指南*》。

  http://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html

美洲总部
Cisco Systems, Inc.
加州圣荷西

亚太总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。思科网站 **www.cisco.com/go/offices** 上提供各办事处的地址、电话和传真。