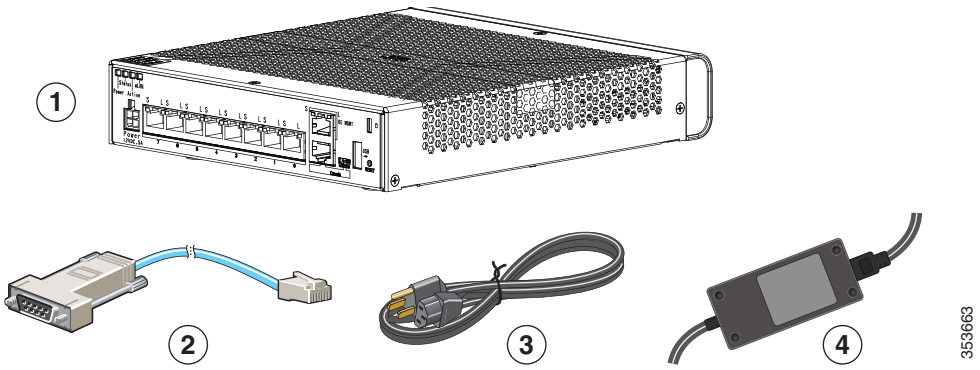
思科 ASA 5506-X 快速入门指南

发布日期：2015 年 3 月 2 日

1. 装箱清单

本节列出了机箱装箱清单中的配件。请注意，装箱清单可能有所变动，实际配件的数量可能多于或少于装箱清单上所列。



1	ASA 5506-X 机箱	2	蓝色控制台电缆和串行 PC 终端适配器（DB-9 转 RJ-45）
3	电源电缆	4	电源

2. 启动 ASA

1. 将电源电缆连接到 ASA 并将其连接到电源插座。

   插上电源电缆插头时，自动接通电源。没有电源按钮。

2. 检查 ASA 背面的电源 LED；如果该 LED 呈绿色稳定亮起，表示设备已接通电源。
3. 检查 ASA 背面的状态 LED；其呈绿色稳定亮起之后，系统已通过通电诊断。

3. 修改 ASA FirePOWER 模块

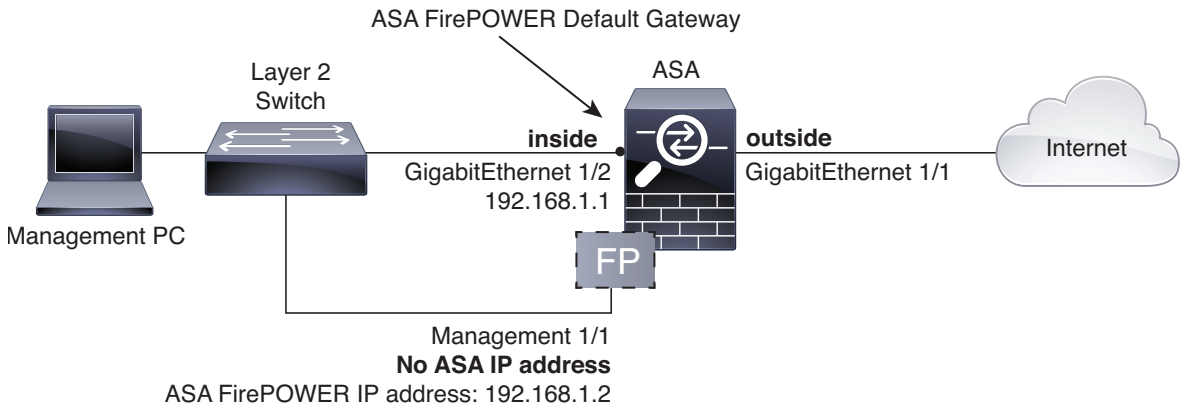
ASA 采用出厂默认配置，支持将自适应安全设备管理器 (ASDM) 连接到 **管理 1/1** 接口。当使用 ASA FirePOWER 模块，我们建议您*不要*使用默认配置。本节介绍如何应用新配置，以便您可以使用以下：

- ASA FirePOWER 模块 - 需要访问互联网进行更新。

此配置还可为内部 和外部网络启用基本可用配置。

下图显示具有 ASA FirePOWER 模块的 ASA 5506-X 的建议网络部署：

3. 修改 ASA FirePOWER 模块



可通过此操作步骤连接到 ASA 控制台端口，并粘贴在配置以下行为的新配置中：

- 内部 --> 外部流量
- 从 DHCP 的外部 IP 地址
- 内部 中客户端的 DHCP
- 管理 1/1 接口启用，但未进行其他配置。然后， ASA FirePOWER 模块可以使用此接口访问 ASA 内部网络并将此内部接口用作互联网网关。
- 内部接口上的 ASDM 访问

要实现上述配置，请执行以下步骤。

操作步骤

1. 使用所提供的控制台电缆或迷你 USB 电缆，将您的计算机连接到 ASA 控制台端口
2. 启动终端仿真程序并连接到 ASA。有关使用 USB 控制台端口的说明，请参阅硬件指南。
3. 按 **Enter** 键查看以下提示符：

   ```
   ciscoasa>
   ```

4. 访问特权 EXEC 模式：

   ```
   enable
   ```

   系统将显示以下提示符：

   ```
   Password:
   ```

5. 按 **Enter** 键。默认情况下，密码为空。
6. 访问全局配置模式：

   ```
   configure terminal
   ```

7. 清除配置：

   ```
   clear configure all
   ```

8. 在提示符处，复制并粘贴以下配置：

   ```
   interface gigabitethernet1/1
     nameif outside
     ip address dhcp setroute
     no shutdown
   interface gigabitethernet1/2
     nameif inside
     ip address 192.168.1.1 255.255.255.0
   ```

```
  security-level 100
  no shutdown
interface management1/1
  no shutdown
object network obj_any
  subnet 0 0
  nat (any,outside) dynamic interface
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
```

9. 保存新配置：

```
write memory
```

10. 将以下各项布线到第 2 层以太网交换机：
    - 内部千兆以太网 1/2 接口 （内部）
    - 管理 1/1 接口
    - 计算机
11. 将千兆以太网 1/1 （外部）接口连接到广域网设备，例如，电缆调制解调器。

4. 启动 ASDM

ASDM 可供您使用网络浏览器管理 ASA。有关运行 ASDM 的要求，请参阅 Cisco.com 上的 ASDM 版本说明。

操作步骤

1. 在连接到 ASA 的计算机上，启动网络浏览器。如果您使用默认配置，未使用第 1 页上的 3.修改 ASA FirePOWER 模块，则需要连接到管理 1/1 接口。
2. 在 Address 字段中，输入以下 URL：**https://192.168.1.1/admin**。系统将显示 **Cisco ASDM** 网页。
3. 点击 **Run Startup Wizard**。

   注意：如果选择点击 **Install ASDM Launcher**，在某些情况下，您需要根据安装 ASDM 的身份证书安装 ASA 的身份证书以及 ASA FirePOWER 模块的单独证书。
4. 按照屏幕上的说明进行操作。系统将显示 **Cisco ASDM-IDM Launcher** 。
5. 将用户名和密码字段留空，然后点击 **OK**。系统将显示 ASDM Startup Wizard。

   注意：如果看到 **Cannot Connect to the ASA FirePOWER module** 对话框，这对新设备来说是正常的，因为尚未设置模块 IP 地址。点击 **Cancel**。
6. 根据需要配置启动向导屏幕。到达 **ASA FirePOWER Basic Configuration** 屏幕时，如果使用的是第 1 页上的 3.修改 ASA FirePOWER 模块中的配置，请使用 ASA FirePOWER 模块的以下网络设置：
   - 管理接口：192.168.1.2
   - 管理子网掩码：255.255.255.0
   - 网关 IP：192.168.1.1

   您还必须接受最终用户许可协议。
7. 点击 **Next** 向前浏览其余屏幕，并完成向导。

5. 运行其他 ASDM 向导和高级配置

ASDM 包括许多向导以配置安全策略。有关所有可用的向导，请参阅 **Wizards** 菜单。要继续配置 ASA，请参阅浏览思科 ASA 系列文档中适合您的软件版本的文档。

6. 配置 ASA FirePOWER 模块

使用 ASDM 配置模块安全策略并将流量发送到模块。

注意：或者，您可以使用 FireSIGHT 管理中心管理 ASA FirePOWER 模块。有关详细信息，请参阅 ASA 版本 ASA防火墙配置指南。

操作步骤

1. 使用 ASDM 中的 ASA FirePOWER 页面配置模块安全策略。可以点击任意页面内的 **Help**，或选择 **Help > ASA FirePOWER Help Topics** 了解有关如何配置策略的详细信息。
2. 要将流量发送到模块，请选择 **Configuration > Firewall > Service Policy Rules**。
3. 选择 **Add > Add Service Policy Rule**。
4. 选择是向特定接口应用此策略还是全局应用此策略，并点击 **Next**。
5. 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**。
6. 在 Rule Actions 页面，点击 **ASA FirePOWER Inspection** 选项卡。
7. 选中 **Enable ASA FirePOWER for this traffic flow** 复选框。
8. 在 If ASA FirePOWER Card Fails 区域中，点击以下选项之一：
   - **Permit traffic** - 将 ASA 设置为在模块不可用时允许所有流量未经检查即可通过。
   - **Close traffic** - 将 ASA 设置为在模块不可用时阻止所有流量。
9. （可选）选中 **Monitor-only** 向模块发送流量只读副本，即被动模式。
10. 点击 **Finish**，然后点击 **Apply**。

    请重复此操作步骤，以根据需要配置更多流量流。