

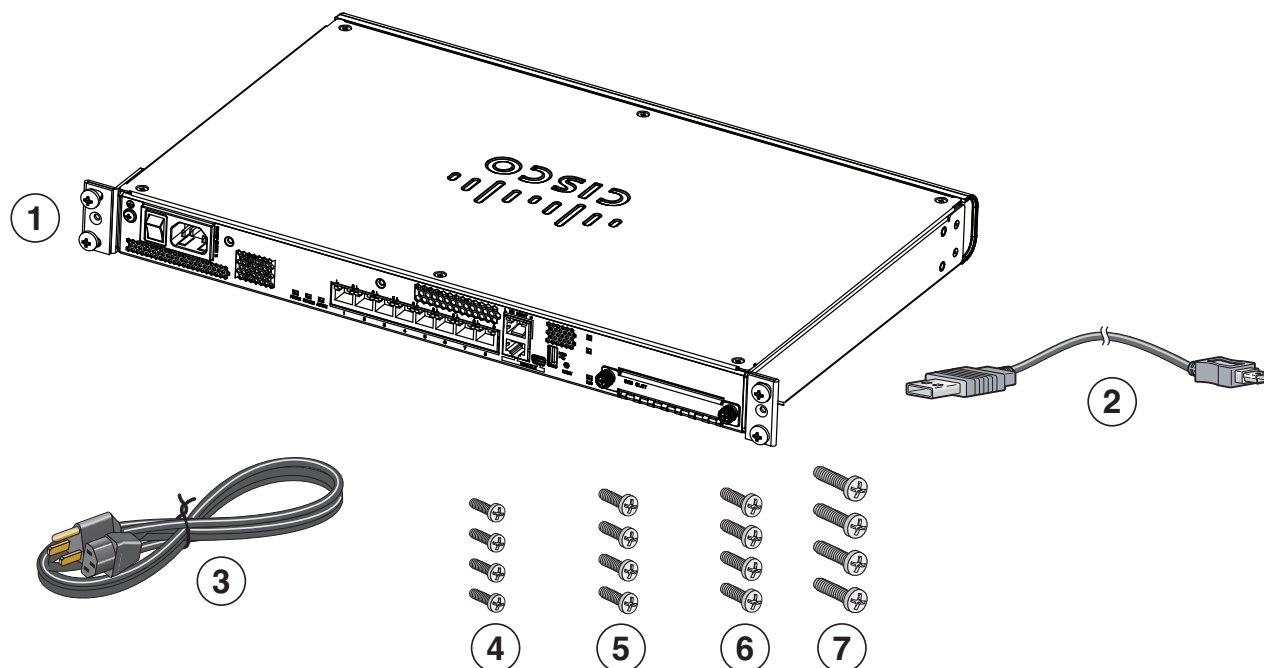


思科 ASA 5508-X 和 ASA 5516-X 快速入门指南

首次发布日期：2015 年 4 月 7 日
最后更新日期：2016 年 5 月 11 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，实际配件可能多于或少于装箱清单上列出的内容。



1	ASA 5508-X 或 ASA 5516-X 机箱	2	USB 控制台电缆（用于将 A 型端口连接到 B 型端口）
3	电源线	4	4 个用于机架安装的 10-32 十字头螺钉
5	4 个用于机架安装的 12-24 十字头螺钉	6	4 个用于机架安装的 M6 十字头螺钉
7	4 个用于机架安装的 M4 十字头螺钉		

3153664

2. 许可证要求

ASA 许可证

ASA 5508-X 或 ASA 5516-X 默认包含**基本许可证**，在符合条件的情况下，还会包含**强加密 (3DES/AES) 许可证**。您还可以购买下列许可证：

- **安全情景**
- **AnyConnect Plus 或 Apex 许可证**

如果您需要自行申请强加密许可证（免费提供），请参阅 <http://www.cisco.com/go/license>。

如果您需要从基本许可证升级到 Security Plus 许可证，或者需要购买 AnyConnect 许可证，请参阅 <http://www.cisco.com/go/ccw>。您稍后会收到一封包含产品授权密钥 (PAK) 的电子邮件，以这种方式获得许可证激活密钥。对于 AnyConnect 许可证，您会收到一个能够多次使用的 PAK，可用于激活同一用户会话池中的多个 ASA。

注意：许可使用的序列号与硬件铭牌上标示的机箱序列号不同。机箱序列号用于获取技术支持，而非获取许可。要查看许可序列号，请使用 `show version | grep Serial` 命令，或在 ASDM 上访问**配置 (Configuration) > 设备管理 (Device Management) > 许可激活密钥 (Licensing Activation Key)** 页面。

ASA FirePOWER许可证

ASA FirePOWER 模块使用不同于 ASA 的独立许可机制。该模块不预装任何许可证，但是可以通过系统输出信息提供一个 PAK，该 PAK 可用于获取下列功能的许可证激活密钥：

- **控制和保护功能** - 控制功能也称为“应用可视性与可控性 (AVC)”或“应用”；保护功能也称为“IPS”。除了这些许可证的激活密钥外，您还需要购买“使用权”订用，才能自动更新这些功能。

控制功能 (AVC) 的更新支持包含在思科支持合同中。

保护功能 (IPS) 的更新支持需要购买 IPS 订用 (<http://www.cisco.com/go/ccw>)。此订用可提供对“规则”、“引擎”、“漏洞”和“地理位置”等内容的更新。**注意：**此使用权订用不会生成（或不需要）用于 ASA FirePOWER 模块的 PAK/许可证激活密钥，而只是提供对更新的使用权。

您还可以购买用于以下功能的其他许可证：

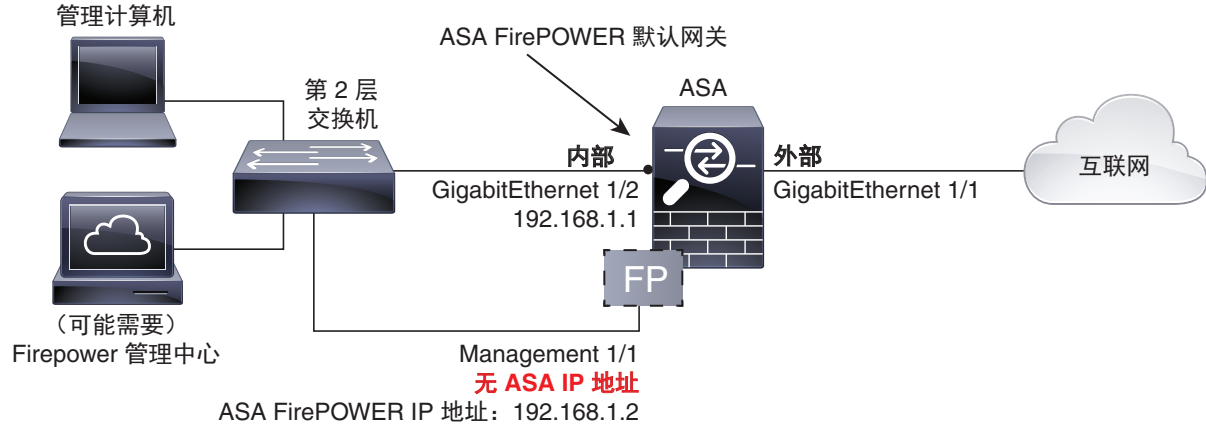
- **高级恶意软件防护 (AMP)**
- **URL 过滤**

这些许可证会生成用于 ASA FirePOWER 模块的 PAK/许可证激活密钥。有关订购信息，请参阅**具备 FirePOWER 服务的思科 ASA 订购指南**。您也可以参阅**思科 Firepower 系统功能许可证**。

要安装“控制和保护功能”许可证以及其他可选许可证，请参阅**安装许可证（第 6 页）**。

3. 在您的网络中部署 ASA 5508-X 或 ASA 5516-X

下图显示的是具有 ASA FirePOWER 模块的 ASA 5508-X 或 ASA 5516-X 的建议网络部署方式：



注意: 您必须在部署中使用独立的内部交换机。

默认配置通过如下行为实现上面的网络配置。

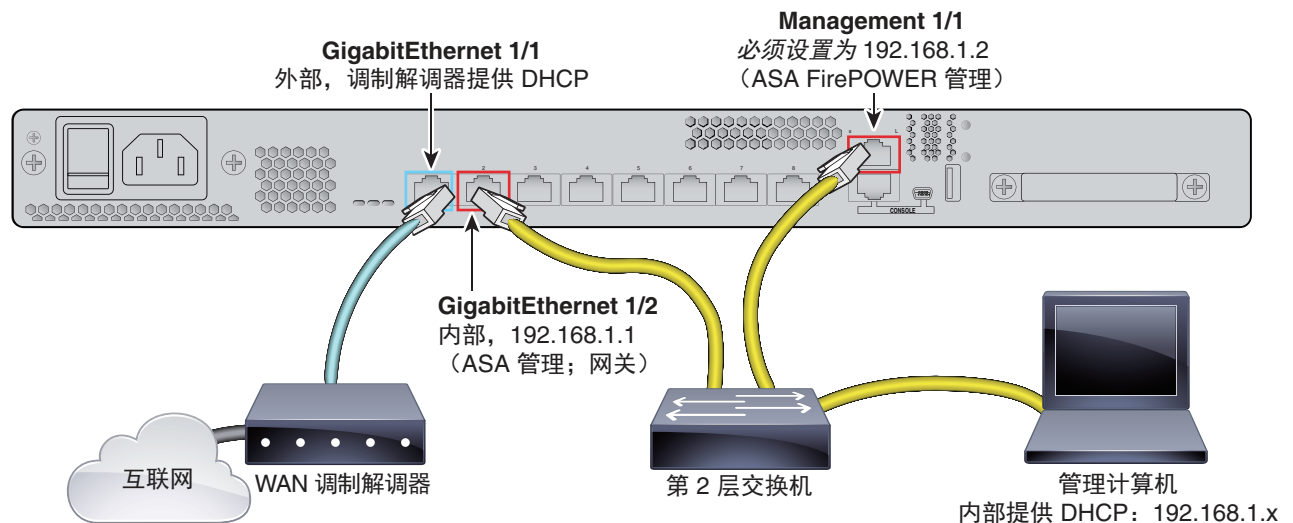
- 网络流量从**内部到外部**
- **外部 IP 地址**从 DHCP 获取
- 用于客户端的 **DHCP** 位于**内部**
- **Management 1/1** 属于 **ASA FirePOWER 模块**。接口为上行接口，*但是在 ASA 上不需要配置此接口*。ASA FirePOWER 模块可以使用此接口**访问 ASA 内部网络**，并使用内部接口作为**互联网网关**。

注意: 请勿在 ASA 配置中为此接口配置 IP 地址，仅在 Firepower 配置中配置 IP 地址。从路由的角度来看，应**将此接口视为完全独立于 ASA**。

- **ASDM 访问**在内部接口上进行

注意: 如果要在内部网络上部署单独的路由器，则可以在管理接口和内部接口之间进行路由。在这种情况下，您可以通过适当更改配置，在 Management 1/1 上同时管理 ASA 和 ASA FirePOWER 模块。

程序



1. 将以下各项布线到第 2 层以太网交换机：
 - GigabitEthernet 1/2 接口（内部）
 - Management 1/1 接口（用于 ASA FirePOWER 模块）
 - 计算机

注意：您可以在同一网络上连接内部接口和管理接口，因为管理接口的作用与仅属于 ASA FirePOWER 模块的独立设备相似。

2. 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。

注意：如果电缆调制解调器使用位于 192.168.1.0/24 范围内的外部地址，则必须更改 ASA 配置以使用不同 IP 地址。接口 IP 地址、HTTPS (ASDM) 访问和 DHCP 服务器设置都可以使用启动向导进行更改。如果将 IP 地址改为用于连接 ASDM 的 IP 地址，在完成向导后，您的设备会断开连接。您需要重新连接到新 IP 地址。

4. 启动 ASA

1. 将电源电缆连接到 ASA 并将其连接到电源插座。
2. 按下 ASA 背面的 Power（电源）按钮。
3. 检查 ASA 正面的电源 LED；如果绿灯常亮，表示设备已接通电源。
4. 检查 ASA 正面的状态 LED；绿灯常亮后，表示系统已通过通电诊断。

5. 启动 ASDM

请参阅 Cisco.com 上的 [ASDM 版本说明](#) 了解运行 ASDM 的要求。

注意：此过程假定您希望使用 ASDM 管理 ASA FirePOWER 模块。如果您希望使用 FireSIGHT 系统，则需连接至模块 CLI 并运行安装脚本；请参阅《[ASA FirePOWER 快速入门指南](#)》。

操作步骤

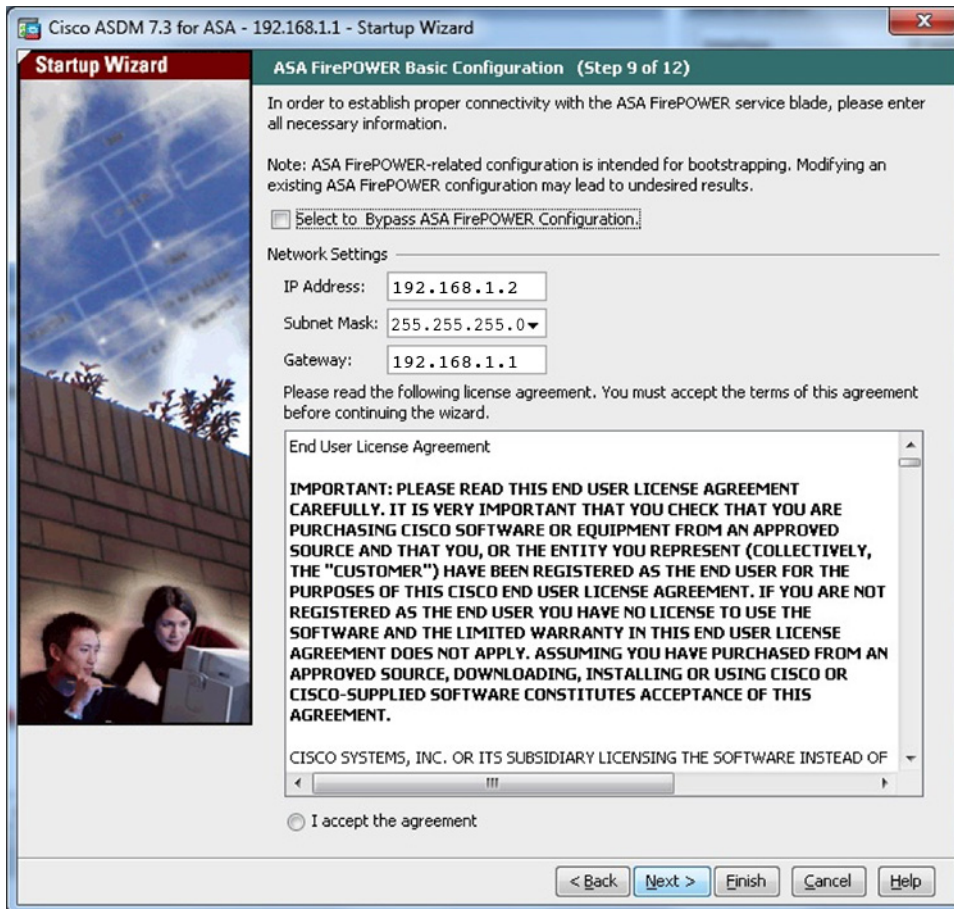
1. 在连接到 ASA 的计算机上，启动 Web 浏览器。
2. 在地址栏中输入以下 URL：<https://192.168.1.1/admin>。此时将显示思科 ASDM (Cisco ASDM) 网页。
3. 点击以下可用选项之一：**安装 ASDM 启动程序 (Install ASDM Launcher)**、**运行 ASDM (Run ASDM)** 或 **运行启动向导 (Run Startup Wizard)**。
4. 根据您选择的选项，按照屏幕上的说明启动 ASDM。系统将显示思科 ASDM-IDM 启动程序 (Cisco ASDM-IDM Launcher)。

如果点击**安装 ASDM 启动程序 (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 模块的独立证书。

5. 将用户名和密码字段留空，然后点击**确定 (OK)**。系统将显示 ASDM 主窗口。
6. 若系统提示您提供已安装 ASA FirePOWER 模块的 IP 地址，请取消对话框。您首先必须使用启动向导 (Startup Wizard) 设置正确的模块 IP 地址。

ASDM 可更改整个 ASA 背板的 ASA FirePOWER 模块 IP 地址设置；但是如果以后需要通过 ASDM 管理该模块，ASDM 必须能通过网络的 Management 1/1 接口访问该模块（及其新 IP 地址）。执行推荐部署后，可进行此访问，因模块 IP 地址位于内部网络上。若设置 IP 地址后 ASDM 无法到达网络上的该模块，则会看到一则错误消息。

7. 选择**向导 (Wizards) > 启动向导 (Startup Wizard)**。
8. 根据需要配置其他 ASA 设置，或跳过设置屏幕直接进入“ASA FirePOWER 基本配置”屏幕。



使用默认配置设置如下值：

- IP 地址 (IP Address) - 192.168.1.2
- 子网掩码 (Subnet Mask) - 255.255.255.0
- 网关 (Gateway) - 192.168.1.1

9. 点击我接受该协议 (I accept the agreement)，然后点击下一步 (Next) 或完成 (Finish) 结束向导。
10. 退出 ASDM，然后重新启动。在主页 (Home) 中，您会看到 ASA FirePOWER 选项卡。

6. 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。

7. 配置 ASA FirePOWER 模块

使用 ASDM 可以安装许可证，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 Firepower 管理中心管理 ASA FirePOWER 模块。请参阅《[ASA FirePOWER 模块快速入门指南](#)》了解更多信息。

安装许可证

设备默认随附“控制和保护功能”许可证，并通过系统输出信息提供产品授权密钥 (PAK)。如果需要订购其他许可证，您需要在邮件中提供 PAK，以便用于这些许可证。

程序

1. 依次选择**配置 (Configuration) > ASA FirePOWER 配置 (ASA FirePOWER Configuration) > 许可证 (Licenses)**，然后点击**添加新许可证 (Add New License)**，获得机箱的许可证密钥。
此许可证密钥将显示在靠近顶部的位置，例如 72:78:DA:6E:D9:93:35。
2. 点击**获取许可证 (Get License)** 打开许可门户。或者，您也可以在浏览器中输入 <http://www.cisco.com/go/license>。
3. 在**获取新许可证 (Get New Licenses)** 字段中，输入 PAK（多个 PAK 之间用逗号分隔），然后点击**执行 (Fulfill)**。
4. 系统将提示您输入许可证密钥和电子邮件等信息。
5. 复制系统生成的许可证激活密钥，您既可以复制网站上显示的信息，也可以从系统自动发送的许可电子邮件中随附的 zip 文件进行复制。
6. 在 ASDM 上，返回**配置 (Configuration) > ASA FirePOWER 配置 (ASA FirePOWER Configuration) > 许可证 (Licenses) > 添加新许可证 (Add New License)** 屏幕。
7. 将许可证激活密钥粘贴到**许可证 (License)** 文本框。
8. 点击**验证许可证 (Verify License)** 检查复制的文本是否正确，验证完成后，点击**提交许可证 (Submit License)**。
9. 点击 **Return to License Page**（返回许可证页面）。

配置 ASA FirePOWER 安全策略

程序

1. 选择**配置 (Configuration) > ASA FirePOWER 配置 (ASA FirePOWER Configuration)**，配置 ASA FirePOWER 安全策略。
如需了解详细信息，请参阅 ASDM 中的 ASA FirePOWER 页面。可以点击任意页面内的**帮助 (Help)**，或选择**帮助 (Help) > ASA FirePOWER 帮助主题 (Help Topics)** 了解有关如何配置策略的详细信息。
您还可以参阅《[ASA FirePOWER 模块用户指南](#)》。

配置 ASA 安全策略

程序

1. 要将流量发送到模块，请选择**配置 (Configuration) > 防火墙 (Firewall) > 服务策略规则 (Service Policy Rules)**。
2. 依次选择**添加 (Add) > 添加服务策略规则 (Add Service Policy Rule)**。
3. 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**下一步 (Next)**。
4. 配置流量匹配。例如，可以匹配**任何流量 (Any Traffic)**，以便将符合入站访问规则的所有流量重定向到模块。或者，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**下一步 (Next)**。
5. 在“规则操作” (Rule Actions) 页面，点击 **ASA FirePOWER 检查 (ASA FirePOWER Inspection)** 选项卡。
6. 选中**为此流量启用 ASA FirePOWER (Enable ASA FirePOWER for this traffic flow)** 复选框。

7. 在若 **ASA FirePOWER 卡故障 (If ASA FirePOWER Card Fails)** 区域中，点击以下选项之一：
 - **允许流量 (Permit traffic)** - 将 ASA 设置为在模块不可用时允许所有流量未经检测即可通过。
 - **关闭流量 (Close traffic)** - 将 ASA 设置为在模块不可用时阻止所有流量。
8. (可选) 选中**仅监控 (Monitor-only)** 以将流量的只读副本发送到模块，即被动模式。
9. 点击**完成 (Finish)**，然后点击**应用 (Apply)**。

请重复此操作步骤，以根据需要配置其他流量。

8. 后续步骤

- 有关 ASA FirePOWER 模块和 ASA 操作的详细信息，请参阅《ASA/ASDM 防火墙配置指南》中的“ASA FirePOWER 模块”章节或 ASDM 联机帮助。您可以在[思科 ASA 系列文档导航](#)页面中找到所有 ASA/ASDM 文档的相应链接。
- 有关 ASA FirePOWER 配置的详细信息，请参阅联机帮助或《[ASA FirePOWER 模块用户指南](#)》或《[FireSIGHT/Firepower 管理中心系统用户指南](#)》。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请转至此 URL：www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作关系。(1110R)

© 2016 思科系统公司。版权所有。

