思科 ASA 和 Firepower 威胁防御重新映像指南

首次发布日期: 2016 年 5 月 10 日

上次修改日期: 2018 年 4 月 17 日

思科 ASA 和 Firepower 威胁防御重新映像指南

需要访问控制台端口

要执行重新映像，您必须将计算机连接到控制台端口。

对于 Firepower 2100、ASA 5512-X、5515-X、5525-X、5545-X 和 5555-X，您可能需要使用第三方串行-USB 转换电缆建立连接。其他型号配备一个 Mini USB B 型控制台端口，因此您可以使用任意一种 Mini USB 电缆。对于 Windows，您可能需要安装从 software.cisco.com 下载的 USB-串行驱动程序。有关控制台端口选项和驱动程序要求的详细信息，请参阅以下网址提供的硬件指南：http://www.cisco.com/go/asa5500x-install

对终端仿真程序使用以下设置：9600 波特、8 个数据位、无奇偶校验、1 个停止位和无流量控制。

支持的型号

以下型号支持 ASA 软件或 Firepower 威胁防御软件。有关 ASA 和 Firepower 威胁防御版本支持，请参阅 ASA 兼容性指南或 Firepower 兼容性指南。

- ASA 5506-X
- ASA 5506W-X
- ASA 5506H-X
- ASA 5508-X
- ASA 5512-X
- ASA 5515-X
- ASA 5516-X
- ASA 5525-X
- ASA 5545-X
- ASA 5555-X

- ISA 3000
- Firepower 2100

注释 Firepower 4100 和 9300 还支持 ASA 或 Firepower 威胁防御，但它们将作为逻辑设备进行安装；有关详细信息，请参阅《FXOS 配置指南》。

注释 对于 ASA 5512-X 至 5555-X 上的 Firepower 威胁防御，必须安装思科固态驱动器 (SSD)。有关详细信息，请参阅《ASA 5500-X 硬件指南》。对于 ASA，使用 ASA FirePOWER 模块也需要 SSD。（SSD 是 ASA 5506-X、5508-X 和 5516-X 的标准配置。）

重新映像 ASA 5500-X 或 ISA 3000

ASA 5500-X 或 ISA 3000 系列中的许多型号都支持 Firepower 威胁防御软件或 ASA 软件。

- 支持的型号，第 1 页
- 下载软件，第 2 页
- 升级 ROMMON 映像（ASA 5506-X、5508-X 和 5516-X），第 5 页
- 从 ASA 重新映像到 Firepower 威胁防御，第 6 页
- 从 FirePOWER 威胁防御重新映像到 ASA，第 9 页

下载软件

获取 Firepower 威胁防御软件或 ASA、ASDM 和 ASA FirePOWER 模块软件。本文档中的程序要求将软件放在 TFTP 服务器上，供初始下载使用。其他映像可以通过其他类型服务器（例如 HTTP 或 FTP）下载。有关确切的软件包和服务器类型，请参阅相关程序。

注释 需要 Cisco.com 登录信息和思科服务合同。

表 *1: Firepower* 威胁防御软件

Firepower 威胁防御型号	下载位置	软件包
ASA 5506-X、ASA 5508-X 和 ASA 5516-X	请参阅：http://www.cisco.com/go/asa-firepower-sw。	注释 您还会看到后缀名为 **.sh** 的补丁文件；本文档不提供有关补丁升级流程的信息。
	启动映像 选择您的型号 > **Firepower 威胁防御软件** > 版本。	启动映像都有一个文件名，例如：ftd-boot-9.6.2.0.**lfbff**。
	系统软件安装包 选择您的型号 > **Firepower 威胁防御软件** > 版本。	系统软件安装包都有一个文件名，例如：ftd-6.1.0-330.**pkg**。
ASA 5512-X 至 ASA 5555-X	请参阅：http://www.cisco.com/go/asa-firepower-sw。	注释 您还会看到后缀名为 **.sh** 的补丁文件；本文档不提供有关补丁升级流程的信息。
	启动映像 选择您的型号 > **Firepower 威胁防御软件** > 版本。	启动映像都有一个文件名，例如：ftd-boot-9.6.2.0.**cdisk**。
	系统软件安装包 选择您的型号 > **Firepower 威胁防御软件** > 版本。	系统软件安装包都有一个文件名，例如：ftd-6.1.0-330.**pkg**。
ISA 3000	请参阅： http://www.cisco.com/go/isa3000-software	注释 您还会看到后缀名为 **.sh** 的补丁文件；本文档不提供有关补丁升级流程的信息。
	选择您的型号 > **Firepower 威胁防御软件** > 版本。	启动映像都有一个文件名，例如：ftd-boot-9.9.2.0.**lfbff**。
	选择您的型号 > **Firepower 威胁防御软件** > 版本。	系统软件安装包都有一个文件名，例如：ftd-6.2.3-330.**pkg**。

表 *2: ASA* 软件

ASA 型号	下载位置	软件包
ASA 5506-X、ASA 5508-X 和 ASA 5516-X	http://www.cisco.com/go/asa-firepower-sw	
	ASA 软件 选择您的型号 > **Adaptive Security Appliance (ASA) Software** > 版本。	ASA 软件文件都有一个文件名，例如：asa962-**lfbff-k8.SPA**。
	ASDM 软件 选择您的型号 > **Adaptive Security Appliance (ASA) Device Manager** > 版本。	ASDM 软件文件都有一个文件名，例如：asdm-762**.bin**。
	REST API 软件 选择您的型号 > **Adaptive Security Appliance REST API Plugin** > 版本。	API 软件文件的文件名类似于 asa-restapi-132-**lfbff-k8.SPA**。要安装 REST API，请参阅 API 快速启动指南。
	ROMMON 软件 选择您的型号 > **ASA Rommon Software** > 版本。	ROMMON 软件文件的文件名类似于 asa5500-firmware-1108**.SPA**。
ASA 5512-X 至 ASA 5555-X	http://www.cisco.com/go/asa-software	
	ASA 软件 选择您的型号 > **Software on Chassis** > **Adaptive Security Appliance (ASA) Software** > 版本。	ASA 软件文件都有一个文件名，例如：asa962-**smp-k8.bin**。
	ASDM 软件 选择您的型号 > **Software on Chassis** > **Adaptive Security Appliance (ASA) Device Manager** > 版本。	ASDM 软件文件都有一个文件名，例如：asdm-762**.bin**。
	REST API 软件 选择您的型号 > **Software on Chassis** > **Adaptive Security Appliance REST API Plugin** > 版本。	API 软件文件的文件名类似于 asa-restapi-132-**lfbff-k8.SPA**。要安装 REST API，请参阅 API 快速启动指南。
	适用于思科应用策略基础设施控制器 (APIC) 的 ASA 设备软件包 选择您的型号 > **Software on Chassis** > **ASA for Application Centric Infrastructure (ACI) Device Packages** > 版本。	对于 APIC 1.2(7) 及更高版本，请选择 Policy Orchestration with Fabric Insertion 或 Fabric Insertion-only 软件包。设备软件包软件文件的文件名类似于 asa-device-pkg-1.2.7.10**.zip**。要安装 ASA 设备软件包，请参阅思科 APIC 第 4 层至第 7 层服务部署指南中的“导入设备软件包”一章。

ASA 型号	下载位置	软件包
ISA 3000	http://www.cisco.com/go/isa3000-software	
	ASA 软件 选择您的型号 > **Adaptive Security Appliance (ASA) Software** > 版本。	ASA 软件文件都有一个文件名，例如：asa962-**lfbff-k8.SPA**。
	ASDM 软件 选择您的型号 > **Adaptive Security Appliance (ASA) Device Manager** > 版本。	ASDM 软件文件都有一个文件名，例如：asdm-762**.bin**。
	REST API 软件 选择您的型号 > **Adaptive Security Appliance REST API Plugin** > 版本。	API 软件文件的文件名类似于 asa-restapi-132-**lfbff-k8.SPA**。要安装 REST API，请参阅 API 快速启动指南。

升级 ROMMON 映像（ASA 5506-X、5508-X 和 5516-X）

按照这些步骤升级 ASA 5506-X、ASA 5508-X 和 ASA 5516-X 系列的 ROMMON 映像。系统中的 ROMMON 版本必须为 1.1.8 或更高版本。

注释 您无法在重新映像至 Firepower 威胁防御后升级 ROMMON 映像。

开始之前

您只能升级到新版本；但无法降级。要查看当前版本，请输入 **show module** 命令，并在输出中查看“MAC 地址范围”(MAC Address Range) 表内的 Mod 1 的“防火墙版本”(Fw Version)。

```
ciscoasa# show module
[...]
Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   1 7426.aceb.ccea to 7426.aceb.ccf2  0.3          1.1.5        9.4(1)
 sfr 7426.aceb.cce9 to 7426.aceb.cce9  N/A          N/A
```

过程

步骤 1 从 Cisco.com 获取新的 ROMMON 映像，并将其放在服务器上以复制到 ASA。此程序显示 TFTP 副本。

从以下网址下载映像：

https://software.cisco.com/download/type.html?mdfid=286283326&flowid=77251

步骤 2 将 ROMMON 映像复制到 ASA 闪存中：

copy tftp://*server_ip*/**asa5500-firmware-***xxxx*.SPA disk0:asa5500-firmware-*xxxx*.SPA**

步骤 3 升级 ROMMON 映像：

upgrade rommon disk0:asa5500-firmware-*xxxx*.SPA

示例：

```
ciscoasa# upgrade rommon disk0:asa5500-firmware-1108.SPA
Verifying file integrity of disk0:/asa5500-firmware-1108.SPA

Computed Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af

Embedded Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af


Digital signature successfully validated
File Name                     : disk0:/asa5500-firmware-1108.SPA
Image type                    : Release
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 553156F4
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
Verification successful.
Proceed with reload? [confirm]
```

步骤 4 当出现提示时，确认重新加载 ASA。

ASA 将升级 ROMMON 映像，然后重新加载 ASA OS。

从 ASA 重新映像到 Firepower 威胁防御

要从 ASA 重新映像到 FirePOWER 威胁防御软件，您必须调出 ROMMON 提示符。在 ROMMON 中，您必须在管理接口上使用 TFTP 下载 FirePOWER 威胁防御启动映像；仅支持 TFTP。启动映像随后可以使用 HTTP 或 FTP 下载 FirePOWER 威胁防御系统软件安装包。TFTP 下载可能需要较长时间；请确保在 ASA 与 TFTP 服务器之间建立了稳定的连接，避免丢包情况。

开始之前

要简化重新映像回 ASA 的流程，请执行以下操作：

1. 使用 **backup** 命令执行完整系统备份。

   有关详细信息和其他备份技术，请参阅《配置指南》。

2. 复制并保存当前激活密钥，以便您可以使用 **show activation-key** 命令重新安装许可证。

过程

步骤 1 将 Firepower 威胁防御启动映像（请参阅下载软件，第 2 页）下载到 ASA 可通过管理接口访问的 TFTP 服务器。

对于 ASA 5506-X、5508-X 和 5516-X、ISA 3000，您必须使用管理端口 1/1 下载映像。对于其他型号，您可以使用任意接口。

步骤 2 将 Firepower 威胁防御系统软件安装包（请参阅下载软件，第 2 页）下载到 ASA 可通过管理接口访问的 HTTP 或 FTP 服务器。

步骤 3 从控制台端口重新加载 ASA：

reload

示例：

```
ciscoasa# reload
```

步骤 4 当系统提示进入 ROMMON 提示符时，需要在启动期间按 **Esc** 键。

请密切注意显示器显示的内容。

示例：

```
[...]
Booting from ROMMON

Cisco Systems ROMMON Version (2.1(9)8) #1: Wed Oct 26 17:14:40 PDT 2011

Platform ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot in   7 seconds.
```

此时按 **Esc** 键。

如果系统显示以下信息，则表明等待时间过长，必须在 ASA 完成启动后进行重新加载：

```
Launching BootLoader...
Boot configuration file contains 2 entries.
[...]
```

步骤 5 使用以下 ROMMON 命令设置网络设置并加载启动映像：

a) **interface**-（仅限于 ASA 5512-X、5515-X、5525-X、5545-X 和 5555-X）管理接口 ID。其他型号始终使用管理接口 1/1。

b) **address**- 管理接口 IP 地址

c) **server**- TFTP 服务器 IP 地址

d) **gateway**- 如果服务器在同一网络上，将此 IP 地址设置为与 TFTP 服务器 IP 地址相同

e) **file**- TFTP 文件路径和名称

f) **set**-（可选）查看网络设置。您还可以使用 ping 命令验证与服务器的连接

g) **sync**-（可选）保存网络设置

h) **tftpdnld**- 加载启动映像

示例：

适用于 **ASA 5555-X** 的示例：

```
rommon #0> interface gigabitethernet0/0
rommon #1> address 10.86.118.4
rommon #2> server 10.86.118.21
rommon #3> gateway 10.86.118.21
rommon #4> file ftd-boot-latest.cdisk
rommon #5> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=ftd-boot-latest.cdisk
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

rommon #6> sync

Updating NVRAM Parameters...

rommon #7> tftpdnld
```

适用于 **ASA 5506-X** 的示例：

```
rommon #0> address 10.86.118.4
rommon #1> server 10.86.118.21
rommon #2> gateway 10.86.118.21
rommon #3> file ftd-boot-latest.lfbff
rommon #4> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  VLAN=untagged
  IMAGE=ftd-boot-latest.lfbff
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

rommon #5> sync

Updating NVRAM Parameters...

rommon #6> tftpdnld
```

FirePOWER 威胁防御启动映像随即下载并启动，进入引导 CLI。

步骤 6 键入 **setup**，并配置管理接口的网络设置，以建立与 HTTP 或 FTP 服务器的临时连接，从而使您可以下载并安装系统软件包。例如：

- 主机名：**ftd1**
- IPv4 地址：**10.86.118.4**
- 子网掩码：**255.255.252.0**
- 网关：**10.86.116.1**
- DNS 服务器：**10.86.116.5**
- NTP 服务器：**ntp.example.com**

步骤 7 下载 FirePOWER 威胁防御系统软件安装包。此步骤展示了如何执行 HTTP 安装。

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

示例：

```
> system install noconfirm http://10.86.118.21/ftd-6.0.1-949.pkg
```

如果您不想回复确认消息，请在命令中添加 **noconfirm** 选项。

步骤 8 安装完成后，请在显示设备重新启动选项时选择 **Yes**。

重新启动通常需要 30 分钟以上，但也可能需要更长时间。重新启动后，即可进入 FirePOWER 威胁防御 CLI。

步骤 9 您可以使用 Firepower 设备管理器或 Firepower 管理中心管理设备。请参阅与您的型号和管理器对应的《快速入门指南》，继续设置：http://www.cisco.com/go/ftd-asa-quick

从 FirePOWER 威胁防御重新映像到 ASA

要从 FirePOWER 威胁防御重新映像到 ASA 软件，您必须调出 ROMMON 提示符。在 ROMMON 中，您必须移除磁盘，然后在管理接口上使用 TFTP 下载 ASA 映像；仅支持 TFTP。在重新加载 ASA 后，您可以配置基本设置，然后加载 FirePOWER 模块软件。

开始之前

- 请确保在 ASA 与 TFTP 服务器之间建立了稳定的连接，避免丢包情况。

过程

步骤 1 如果从 Firepower 管理中心管理 Firepower 威胁防御设备，请从管理中心删除该设备。

步骤 2 如果您使用 Firepower 设备管理器管理 Firepower 威胁防御设备，无论是通过 Firepower 设备管理器还是通过智能软件许可服务器，请确保从智能软件许可服务器注销该设备。

步骤 3 将 ASA 映像（请参阅下载软件，第 2 页）下载到 Firepower 威胁防御设备可通过管理接口访问的 TFTP 服务器。

对于 ASA 5506-X、5508-X 和 5516-X、ISA 3000，您必须使用管理端口 1/1 下载映像。对于其他型号，您可以使用任意接口。

步骤 4 在控制台端口，重新启动 FirePOWER 威胁防御设备。

示例：

```
> reboot
This command will reboot the system.  Continue?
Please enter 'YES' or 'NO': yes
```

输入 **yes** 重新启动。

步骤 5 当系统提示进入 ROMMON 提示符时，需要在启动期间按 **Esc** 键。

请密切注意显示器显示的内容。

示例：

```
[...]
Booting from ROMMON

Cisco Systems ROMMON Version (2.1(9)8) #1: Wed Oct 26 17:14:40 PDT 2011

Platform ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot in   7 seconds.
```

此时按 **Esc** 键。

如果系统显示以下信息，则表明等待时间过长，必须在FirePOWER威胁防御设备完成启动后进行重新加载：

```
Launching BootLoader...
Boot configuration file contains 2 entries.
[...]
```

步骤 6 请移除 Firepower 威胁防御设备上的所有磁盘。内部闪存称为 disk0。如果有外部 USB 驱动器，则称为 disk1。

示例：

```
Example:
rommon #0> erase disk0:

About to erase the selected device, this will erase
all files including configuration, and images.
Continue with erase? y/n [n]: y

Erasing Disk0:
.........................
[...]
```

此步骤删除了 FirePOWER 威胁防御文件，使 ASA 不会尝试加载可引发多种错误的不正确的配置文件。

步骤 7 使用以下 ROMMON 命令设置网络设置并加载 ASA 映像。

interface *interface_id*

address *management_ip_address*

server *tftp_ip_address*

gateway *gateway_ip_address*

file*path*/*filename*

set

sync

tftpdnld

ASA 映像随即下载并启动，进入 CLI。

请参阅以下信息：

- **interface**-（仅限于 ASA 5512-X、5515-X、5525-X、5545-X 和 5555-X）指定接口 ID。其他型号始终使用管理接口 1/1。
- **gateway**- 如果此网关地址与服务器 IP 地址在同一网络上，请将二者设置为同一地址。
- **set**- 显示网络设置。您还可以使用 **ping** 命令验证与服务器的连接。
- **sync**- 保存网络设置。
- **tftpdnld**- 加载启动映像。

示例：

适用于 ASA 5555-X 的示例：

```
rommon #2> interface gigabitethernet0/0
rommon #3> address 10.86.118.4
rommon #4> server 10.86.118.21
rommon #5> gateway 10.86.118.21
rommon #6> file asalatest-smp-k8.bin
rommon #7> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asalatest-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

rommon #8> sync

Updating NVRAM Parameters...
```

```
rommon #9> tftpdnld
```

适用于 ASA 5506-X 的示例：

```
rommon #2> address 10.86.118.4
rommon #3> server 10.86.118.21
rommon #4> gateway 10.86.118.21
rommon #5> file asalatest-lfbff-k8.SPA
rommon #6> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  VLAN=untagged
  IMAGE=asalatest-lfbff-k8.SPA
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

rommon #7> sync

Updating NVRAM Parameters...

rommon #8> tftpdnld
```

步骤 8 配置网络设置并准备磁盘。

当 ASA 首次启动时，它上面没有任何配置。您可以按照交互式提示配置用于 ASDM 访问的管理接口，也可以粘贴保存的配置；或者，如果您没有保存的配置，可使用建议配置（如下所示）。

如果您没有保存的配置，但计划使用 ASA FirePOWER 模块，最佳做法是粘贴建议配置。ASA FirePOWER 模块可在管理接口上进行管理，并需要访问互联网进行更新。建议的简单网络部署包括一台内部交换机，通过该交换机，您可以将管理接口（仅用于FirePOWER管理）、内部接口（用于 ASA 管理和内部流量）和管理 PC 连接到同一内部网络。有关网络部署的详细信息，请参阅以下网址提供的《快速入门指南》：

- http://www.cisco.com/go/asa5506x-quick
- http://www.cisco.com/go/asa5508x-quick
- http://www.cisco.com/go/asa5500x-quick

a) 当出现 ASA 控制台提示符时，系统将提示您为管理接口提供某种配置。

```
Pre-configure Firewall now through interactive prompts [yes]?
```

如果要为简单网络部署粘贴配置或创建建议配置，请输入 **no** 并继续执行此程序。

如果要配置管理接口，以便可以连接到 ASDM，请输入 **yes**，并按照提示操作即可。

b) 当出现 ASA 控制台提示符时，进入特权 EXEC 模式。

enable

系统将显示以下提示：

```
Password:
```

c) 按 **Enter** 键。默认情况下，密码为空。

d) 访问全局配置模式。

configure terminal

e) 如果没有使用交互式提示，请在提示符后复制并粘贴您的配置。

如果没有保存的配置，但想要使用本快速入门指南中介绍的简单配置，请在提示符处复制以下配置，根据需要更改 IP 地址和接口 ID。如果使用的是交互式提示，但想要转用此配置，请先使用 **clear configure all** 命令清除该配置。

```
interface gigabitethernetn/n
   nameif outside
   ip address dhcp setroute
   no shutdown
interface gigabitethernetn/n
   nameif inside
   ip address ip_address netmask
   security-level 100
   no shutdown
interface managementn/n
   no shutdown
object network obj_any
   subnet 0 0
   nat (any,outside) dynamic interface
http server enable
http inside_network netmask inside
dhcpd address inside_ip_address_start-inside_ip_address_end inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
```

对于 ASA 5506W-X，为 WiFi 接口添加以下配置：

```
same-security-traffic permit inter-interface
interface GigabitEthernet 1/9
security-level 100
nameif wifi
ip address ip_address netmask
no shutdown
http wifi_network netmask wifi
dhcpd address wifi_ip_address_start-wifi_ip_address_end wifi
dhcpd enable wifi
```

f) 重新格式化磁盘：

format disk0:

format disk1:

内部闪存称为 disk0。如果有外部 USB 驱动器，则称为 disk1。如果不重新格式化磁盘，则尝试复制 ASA 映像时，系统会显示以下错误：

```
%Error copying ftp://10.86.89.125/asa971-smp-k8.bin (Not enough space on device)
```

g) 保存新配置：

write memory

步骤 9 安装 ASA 和 ASDM 映像。

从 ROMMON 模式启动 ASA 不会在重新加载时保留系统映像；您仍需将映像下载到闪存。您还需要将 ASDM 下载到闪存。

a) 将 ASA 和 ASDM 映像（请参阅下载软件，第 2 页）下载到 ASA 可访问的服务器。ASA 支持多种服务器类型。有关详细信息，请参阅以下网址中有关 **copy** 命令的说明：http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/A-H/cmdref1/c4.html#pgfId-2171368。

b) 将 ASA 映像复制到 ASA 闪存。此步骤展示了如何执行 FTP 复制。

copy ftp://*user***:***password***@***server_ip***/***asa_file***disk0:***asa_file*

示例：

```
ciscoasa# copy ftp://admin:test@10.86.118.21/asa961-smp-k8.bin disk0:asa961-smp-k8.bin
```

c) 将 ASDM 映像复制到 ASA 闪存。此步骤展示了如何执行 FTP 复制。

copy ftp://*user***:***password***@***server_ip***/***asdm_file***disk0:***asdm_file*

示例：

```
ciscoasa# copy ftp://admin:test@10.86.118.21/asdm-761.bin disk0:asdm-761.bin
```

d) 重新加载 ASA：

reload

ASA 使用 disk0 中的映像进行重新加载。

步骤 10 （可选）安装 ASA FirePOWER 模块软件。

您需要安装 ASA FirePOWER 启动映像，对 SSD 进行分区，并按照此程序安装系统软件。

a) 将启动映像复制到 ASA。请勿传输系统软件；系统软件稍后会下载到 SSD。此步骤展示了如何执行 FTP 复制。

copy ftp://*user***:***password***@***server_ip***/***firepower_boot_file***disk0:***firepower_boot_file*

示例：

```
ciscoasa# copy ftp://admin:test@10.86.118.21/asasfr-5500x-boot-6.0.1.img
disk0:/asasfr-5500x-boot-6.0.1.img
```

b) 从 Cisco.com 将 ASA FirePOWER 服务系统软件安装包下载到可通过管理接口访问的 HTTP、HTTPS 或 FTP 服务器。请勿将其下载到 ASA 上的 disk0。

c) 设置 ASA FirePOWER 模块启动映像在 ASA disk0 中的位置：

sw-module module sfr recover configure image disk0:*file_path*

示例：

```
ciscoasa# sw-module module sfr recover configure image disk0:asasfr-5500x-boot-6.0.1.img
```

d) 加载 ASA FirePOWER 启动映像：

sw-module module sfr recover boot

示例：

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

Module sfr will be recovered. This may erase all configuration and all data
on that device and attempt to download/install a new image for it. This may take
several minutes.

Recover module sfr? [confirm] y
Recover issued for module sfr.
```

e) 等待几分钟，以便 ASA FirePOWER 模块启动，然后向当前正在运行的 ASA FirePOWER 启动映像发起控制台会话。发起会话后，可能需要按 **Enter** 键显示登录提示符。默认用户名是 **admin**，默认密码是 **Admin123**。

示例：

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

asasfr login: admin
Password: Admin123
```

如果模块启动未完成，session 命令会失败，并显示一条消息说明无法通过 ttyS1 进行连接。请稍后重试。

a) 配置系统，以便您可以安装系统软件安装包。

setup

系统将提示输入以下信息。请注意，管理地址和网关以及 DNS 信息是要配置的主要设置。

- 主机名 - 最多可达 65 个字母数字字符，不能包含空格。允许使用连字符。
- 网络地址 - 可设置静态 IPv4 或 IPv6 地址，或使用 DHCP（适用于 IPv4）或 IPv6 无状态自动配置。
- DNS 信息 - 必须至少确定一个 DNS 服务器，还可设置域名和搜索域。
- NTP 信息 - 可启用 NTP 并配置 NTP 服务器，以便设置系统时间。

示例：

```
asasfr-boot> setup

               Welcome to Cisco FirePOWER Services Setup
                         [hit Ctrl-C to abort]
                   Default values are inside []
```

a) 安装系统软件安装包：

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

如果您不想回复确认消息，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，系统将提示您提供这些信息。此文件较大，下载可能需要较长时间，具体取决于您的网络。

安装完成后，系统将重新启动。安装应用组件所需的时间以及启动 ASA FirePOWER 服务所需的时间差别极为明显：高端平台可能需要 10 分钟或更长时间，但低端平台可能需要 60-80 分钟或更长时间。（**show module sfr** 输出应将所有进程显示为 Up。）

示例：

```
asasfr-boot> system install
http://admin:pa$$wd@upgrades.example.com/packages/asasfr-sys-6.0.1-58.pkg
Verifying
Downloading
Extracting
Package Detail
        Description:                    Cisco ASA-FirePOWER 6.0.1-58 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. [type
Enter]
Broadcast message from root (ttyS1) (Mon Feb 17 19:28:38 2016):

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

a) 如果您需要安装补丁版本，可以稍后请求 ASDM 或 FirePOWER 管理中心的管理员执行此操作。

步骤 11 如需为未保存激活密钥的现有 ASA 获取强加密许可证和其他许可证，请参阅 http://www.cisco.com/go/license。在**管理 (Manage)** > **许可证 (Licenses)** 部分，您可以重新下载许可证。

要使用 ASDM（和许多其他功能），您需要安装强加密 (3DES/AES) 许可证。如果您在早先重新映像至 FirePOWER 威胁防御设备之前保存了此 ASA 的许可激活密钥，则可以重新安装该激活密钥。如果您未保存激活密钥，但拥有此 ASA 的许可证，则可以重新下载该许可证。对于新的 ASA，您需要申请新的 ASA 许可证。

步骤 12 为新的 ASA 获取许可证。

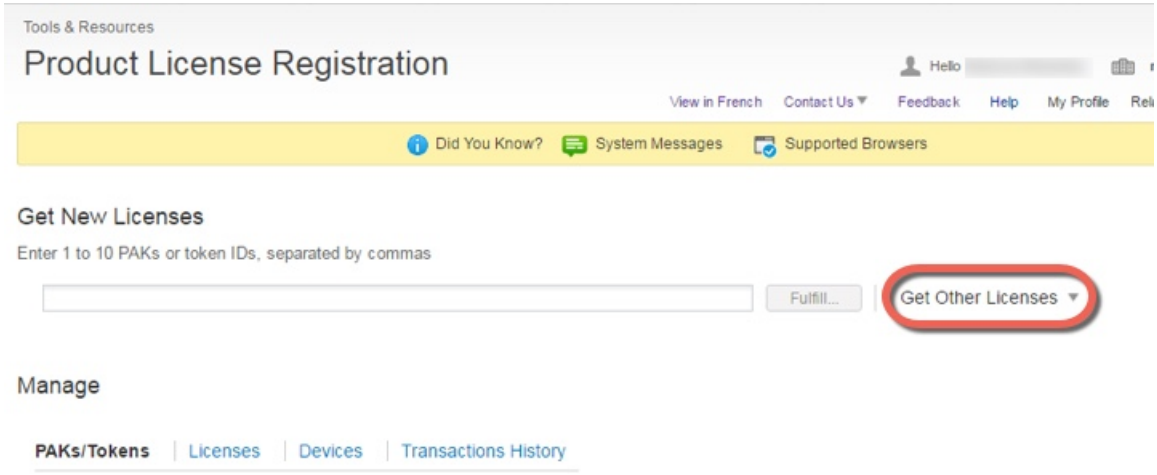
a) 通过输入以下命令获取 ASA 的序列号：

show version | grep Serial

此序列号与印制在硬件外部的机箱序列号不同。机箱序列号用于技术支持，但不用于许可。

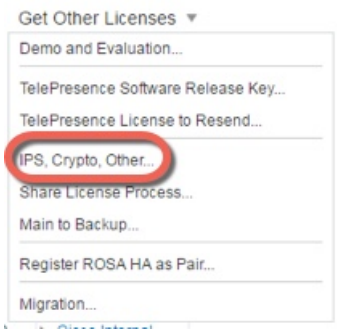
b) 访问 http://www.cisco.com/go/license，然后点击**获取其他许可证 (Get Other Licenses)**。

图 *1:* 获取其他许可证 *(Get Other Licenses)*



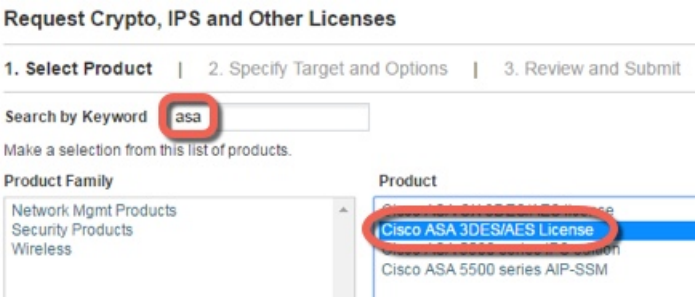
c) 选择 **IPS, Crypto, Other**。

图 *2: IPS*、加密、其他 *(IPS, Crypto, Other)*



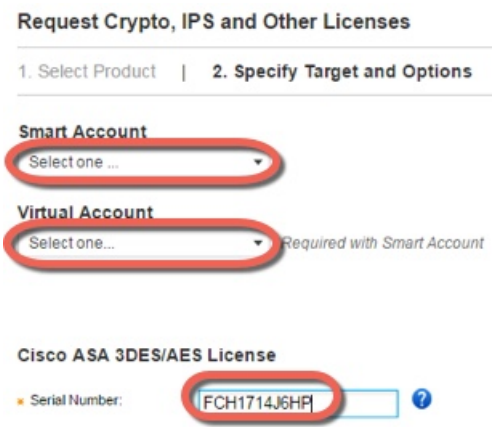
d) 在 **Search by Keyword** 字段，输入 **asa**，并选择 **Cisco ASA 3DES/AES License**。

图 *3:* 思科 *ASA 3DES/AES* 许可证 *(Cisco ASA 3DES/AES License)*



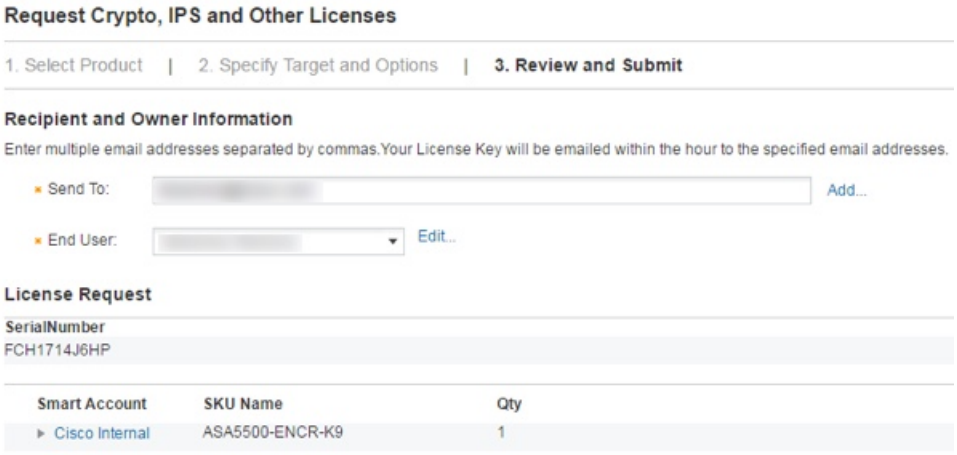
e) 选择您的**智能帐户 (Smart Account)**、**虚拟帐户 (Virtual Account)**，输入 ASA **序列号 (Serial Number)**，然后点击**下一步 (Next)**。

图 *4:* 智能帐户 *(Smart Account)*、虚拟帐户 *(Virtual Account)* 和序列号 *(Serial Number)*



f) 系统将自动填充您的 Send To 邮箱地址和 End User 名称；必要时输入其他邮箱地址。选中**我同意 (I Agree)** 复选框，然后点击**提交 (Submit)**。

图 *5:* 提交



g) 之后，您将会收到一封包含激活密钥的邮件，但您也可以立即从**管理 (Manage)** > **许可证 (Licenses)** 区域下载该密钥。

h) 如需从基础许可证升级到 Security Plus 许可证或者购买 AnyConnect 许可证，请访问：http://www.cisco.com/go/ccw.购买许可证后，您将收到一封邮件，其中包含您可以在 http://www.cisco.com/go/license 上输入的产品授权密钥 (PAK)。对于 AnyConnect 许可证，您将收到多用途 PAK，该 PAK 可应用于多个使用相同用户会话池的 ASA。此类激活密钥包含迄今为止为永久许可证（包括 3DES/AES 许可证）注册的所有功能。对于基于时间的许可证，每个许可证具有单独的激活密钥。

步骤 13 应用激活密钥。

activation-key 密钥

示例：

```
ciscoasa(config)# activation-key 7c1aff4f e4d7db95 d5e191a4 d5b43c08 0d29c996
Validating activation key. This may take a few minutes...
Failed to retrieve permanent activation key.
Both Running and Flash permanent activation key was updated with the requested key.
```

由于此 ASA 没有安装激活密钥，系统将显示“Failed to retrieve permanent activation key.”消息。您可以忽略此消息。

您只能安装一个永久密钥和多个基于时间的密钥。如果输入新的永久密钥，则它会覆盖已安装的永久密钥。如果您在安装 3DES/AES 许可证后订购了其他许可证，组合激活密钥将包含所有许可证以及该 3DES/AES 许可证，因此您可以将覆盖该独立 3DES/AES 密钥。

步骤 14 ASA FirePOWER 模块使用独立于 ASA 的许可机制。此模块没有预装任何许可证，但是根据您的订单，可能会在打印输出件上包含 PAK，从而使您可以获得以下许可证的许可证激活密钥：

- **控制和保护**。控制又称为“应用可视性与可控性(AVC)”或“应用”。保护又称为“IPS”。除了这些许可证的激活密钥外，您还需要“使用权”订用以自动更新这些功能。

  控制 (AVC) 更新随思科支持合同提供。

  保护 (IPS) 更新需要您从 http://www.cisco.com/go/ccw 购买 IPS 订用。此订用包括规则、引擎、漏洞和地理位置更新的授权。**注意**：此使用权订用不会生成也不需要 ASA FirePOWER 模块的 PAK/许可证激活密钥；它仅提供对更新的使用权。

如果您未购买具备 ASA FirePOWER 服务的 ASA 5500-X，则您可以通过购买升级捆绑包获取必要的许可证。有关详细信息，请参阅《具备 FirePOWER 服务的思科 ASA 订购指南》。

您可以购买的其他许可证包括：

- **高级恶意软件防护 (AMP)**
- **URL 过滤**

这些许可证确实会生成 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》。另请参阅《思科 FirePOWER 系统功能许可证》。

要安装控制和保护许可证以及其他可选许可证，请参阅《ASA 快速入门指南》查找您的型号。

重新映像 Firepower 2100 系列

Firepower 2100 系列支持 Firepower 威胁防御软件或 ASA 软件。

- 下载软件，第 20 页
- 从 ASA 重新映像到 Firepower 威胁防御，第 20 页
- 从 FirePOWER 威胁防御重新映像到 ASA，第 25 页

下载软件

获取 Firepower 威胁防御软件或 ASA 软件。本文档中的程序要求将软件放在 TFTP 服务器上，供初始下载使用。其他映像可以通过其他类型服务器（例如 HTTP 或 FTP）下载。有关确切的软件包和服务器类型，请参阅相关程序。

注释 需要 Cisco.com 登录信息和思科服务合同。

表 *3: Firepower* 威胁防御软件

Firepower 威胁防御型号	下载位置	软件包
Firepower 2100 系列	请参阅：https://www.cisco.com/go/ftd-software	
	Firepower 威胁防御软件包 选择您的型号 > **Firepower 威胁防御软件** > 版本。	软件包都有一个文件名，例如：cisco-ftd-fp2k.6.2.2.**SPA**。

表 *4: ASA* 软件

ASA 型号	下载位置	软件包
Firepower 2100 系列	请参阅：https://www.cisco.com/go/asa-firepower-sw	
	ASA 软件包 选择您的型号 > **Adaptive Security Appliance (ASA) Software** > 版本。	软件包都有一个文件名，例如：cisco-asa-fp2k.9.8.2.**SPA**。此软件包含有 ASA、ASDM、FXOS 和 Firepower 机箱管理器。
	ASDM 软件（升级） 要使用当前的 ASDM 或 ASA CLI 升级到更高版本的 ASDM，请选择您的型号 > **Adaptive Security Appliance (ASA) Device Manager** > 版本。	ASDM 软件文件都有一个文件名，例如：asdm-782**.bin**。

从 ASA 重新映像到 Firepower 威胁防御

要从 Firepower 2100 上的 ASA 重新映像到 Firepower 威胁防御软件，您必须调出 ROMMON 提示符。在 ROMMON 中，您必须移除磁盘，然后在管理接口 1/1 上使用 TFTP 加载 Firepower 威胁防御软件包中的 FXOS；仅支持 TFTP。在最初启动 FXOS 之后，您可以配置网络设置，从您选择的服务器下载 Firepower 威胁防御软件包，然后重新启动。

过程

步骤 1 无论是通过 ASA CLI/ASDM 还是通过智能软件许可服务器，都可以从智能软件许可服务器注销 ASA。

步骤 2 将 Firepower 威胁防御映像（请参阅下载软件，第 20 页）下载到 ASA 可通过管理接口 1/1 访问的 TFTP 服务器。

步骤 3 在控制台端口，以 **admin** 身份登录 FXOS，并重新格式化系统。

connect local-mgmt

format everything

```
firepower-2110# connect local-mgmt
firepower-2110(local-mgmt)# format everything
All configuration and bootable images will be lost.
Do you still want to format? (yes/no):yes
```

输入 **yes**，Firepower 2100 重新启动。

步骤 4 当系统提示进入 ROMMON 提示符时，需要在启动期间按 **Esc** 键。请密切注意显示器显示的内容。

示例：

```
********************************************************************************
Cisco System ROMMON, Version 1.0.03, RELEASE SOFTWARE
Copyright (c) 1994-2017  by Cisco Systems, Inc.
Compiled Thu 04/06/2017 12:16:16.21 by builder
********************************************************************************

Current image running: Boot ROM0
Last reset cause: ResetRequest
DIMM_1/1 : Present
DIMM_2/1 : Present

Platform FPR-2130 with 32768 MBytes of main memory
BIOS has been successfully locked !!
MAC Address: 0c:75:bd:08:c9:80

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

此时按 **Esc** 键。如果您错过了中断提示，Firepower 2100 会尝试重新启动 3 次；因为设备上没有映像，所以只有 ROMMON 可用。

步骤 5 设置管理 1/1 的网络设置，并使用以下 ROMMON 命令加载 FXOS（Firepower 威胁防御软件包的一部分）。

address *management_ip_address*

netmask *subnet_mask*

server *tftp_ip_address*

gateway *gateway_ip_address*

file*path/filename*

set

sync

tftp -b

FXOS 映像随即下载，并启动进入 CLI。

请参阅以下信息：

- **gateway**- 如果此网关地址与服务器 IP 地址在同一网络上，请将二者设置为同一地址。
- **set**- 显示网络设置。您还可以使用 **ping** 命令验证与服务器的连接。
- **sync**- 保存网络设置。
- **tftp -b**- 加载 FXOS。

示例：

```
rommon 1> address 10.86.118.4
rommon 2> netmask 255.255.252.0
rommon 3> server 10.86.118.21
rommon 4> gateway 10.86.118.21
rommon 5> file cisco-ftd-fp2k.6.2.2.SPA
rommon 6> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.4
  NETMASK=255.255.252.0
  GATEWAY=10.86.118.21
  SERVER=10.86.118.21
  IMAGE=cisco-ftd-fp2k.6.2.2.SPA
  CONFIG=
  PS1="rommon ! > "

rommon 7> sync
rommon 8> tftp -b
Enable boot bundle: tftp_reqsize = 268435456

             ADDRESS: 10.86.118.4
             NETMASK: 255.255.252.0
             GATEWAY: 10.86.118.21
              SERVER: 10.86.118.21
               IMAGE: cisco-asa-fp2k.9.8.2.SPA
             MACADDR: d4:2c:44:0c:26:00
           VERBOSITY: Progress
               RETRY: 40
          PKTTIMEOUT: 7200
             BLKSIZE: 1460
            CHECKSUM: Yes
                PORT: GbE/1
             PHYMODE: Auto Detect

link up
Receiving cisco-ftd-fp2k.6.2.2.SPA from 10.86.118.21!!!!!!!!
[…]
```

步骤 6 使用默认用户名 **admin** 和密码 **Admin123** 登录 FXOS。

在设备启动进入 FXOS 之后，您在 ROMMON 中设置的管理 IP 地址将被擦除并设置为默认值 192.168.45.45。您将需要先在 FXOS 中为您的网络设置正确的 IP 地址和其他相关设置，然后才能从服务器下载 Firepower 威胁防护软件包。

步骤 7 禁用 DHCP 服务器。

scope system

scope services

disable dhcp-server

commit-buffer

必须先禁用 DHCP 服务器，然后才能更改管理 IP 地址。

示例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # disable dhcp-server
firepower-2110 /system/services* # commit-buffer
```

步骤 8 配置 IPv4 管理 IP 地址，还可以配置网关（可选）。

scopefabric-interconnecta

setout-of-band staticip *ip_address***netmask** *network_mask***gw** *gateway_ip_address*

commit-buffer

要保留当前设置的网关（默认为 0.0.0.0，代表 Firepower 威胁防御数据接口），请省略 **gw** 关键字。如果您的下载服务器不在本地管理 1/1 网络上，则请更改网关 IP 地址；Firepower 威胁防御数据接口还不存在，因此您无法使用默认设置访问任何远程服务器。

示例：

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect #
firepower-2100 /fabric-interconnect # set out-of-band ip 10.86.118.4 netmask 255.255.255.0

Warning: When committed, this change may disconnect the current CLI session
firepower-2100 /fabric-interconnect* # commit-buffer
firepower-2100 /fabric-interconnect #
```

步骤 9 下载并启动 Firepower 威胁防御软件包。

a) 下载软件包。

scope firmware

download image *url*

show download-task

您可以从先前使用的同一 TFTP 服务器或管理 1/1 上可访问的其他服务器下载软件包。

示例：

```
firepower-2110# scope firmware
firepower-2110 /firmware # download image tftp://10.86.118.21/cisco-ftd-fp2k.6.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
firepower-2110 /firmware # show download-task
Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-ftd-fp2k.6.2.2.SPA
              Tftp     10.88.29.21             0                 Downloaded
```

b) 当软件包完成下载（**已下载**状态）时，启动软件包。

show package

scope auto-install

install security-pack version 版本

在 **show package** 输出中，复制与 **security-pack version** 号对应的 **Package-Vers** 值。机箱会安装 Firepower 威胁防御映像并重新启动。

示例：

```
firepower 2110 /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-ftd-fp2k.6.2.2.SPA                   6.2.2
firepower 2110 /firmware # scope auto-install
firepower 2110 /firmware/auto-install # install security-pack version 6.2.2
The system is currently installed with security software package not set, which has:
   - The platform version: not set
If you proceed with the upgrade 6.2.2, it will do the following:
   - upgrade to the new platform version 2.2.2.52
   - install with CSP ftd version 6.2.2
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Attention:
   If you proceed the system will be re-imaged. All existing configuration will be lost,

   and the default configuration applied.
Do you want to proceed? (yes/no):yes

Triggered the install of software package version 6.2.2
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
```

步骤 10 等待机箱完成重新启动（5-10 分钟），然后使用默认用户名 **admin** 和密码 **Admin123** 登录 FXOS。

虽然 FXOS 已经启动，但您仍然需要等待 Firepower 威胁防御启动（30 分钟）。请等待，直至显示以下消息：

```
[…]
User enable_1 logged in to firepower
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
firepower> Aug 26 01:31:48 firepower port-manager: Alert: Ethernet1/2 link changed to DOWN
Aug 26 01:31:48 firepower port-manager: Alert: Ethernet1/1 link changed to DOWN

firepower#
```

在显示其余的 Firepower 威胁防御启动消息之后，您即可返回到 FXOS 提示符。

步骤 11 连接到 Firepower 威胁防御 CLI。

connect ftd

步骤 12 系统会提示您接受 EULA；按 **Enter**，然后在 **More** 提示符处按**空格键**，直至屏幕上显示：

```
Please enter 'YES' or press <ENTER> to AGREE to the EULA:
```

输入 **yes**。

步骤 13 系统将提示您更改密码并执行初始设置。如需配置您的系统，请参阅Firepower 设备管理器或Firepower 管理中心快速入门指南。

从 FirePOWER 威胁防御重新映像到 ASA

要从Firepower 2100 上的Firepower 威胁防御重新映像到ASA 软件，您必须调出ROMMON 提示符。在ROMMON 中，您必须移除磁盘，然后在管理接口 1/1 上使用 TFTP 加载 ASA 软件包中的FXOS；仅支持 TFTP。在最初启动FXOS 之后，您可以配置网络设置，从您选择的服务器下载ASA 软件包，然后重新启动。

过程

步骤 1 如果从 Firepower 管理中心管理 Firepower 威胁防御设备，请从管理中心删除该设备。

步骤 2 如果您使用 Firepower 设备管理器管理 Firepower 威胁防御设备，无论是通过 Firepower 设备管理器还是通过智能软件许可服务器，请确保从智能软件许可服务器注销该设备。

步骤 3 将 ASA 映像（请参阅下载软件，第 20 页）下载到 Firepower 威胁防御设备可通过管理接口 1/1 访问的 TFTP 服务器。

步骤 4 在控制台端口，以 **admin** 身份登录 FXOS，并重新格式化系统。

connect local-mgmt

format everything

```
firepower-2110# connect local-mgmt
firepower-2110(local-mgmt)# format everything
All configuration and bootable images will be lost.
```

```
Do you still want to format? (yes/no):yes
```

输入 **yes**，Firepower 2100 重新启动。

步骤 5 当系统提示进入 ROMMON 提示符时，需要在启动期间按 **Esc** 键。请密切注意显示器显示的内容。

示例：

```
********************************************************************************
Cisco System ROMMON, Version 1.0.03, RELEASE SOFTWARE
Copyright (c) 1994-2017  by Cisco Systems, Inc.
Compiled Thu 04/06/2017 12:16:16.21 by builder
********************************************************************************

Current image running: Boot ROM0
Last reset cause: ResetRequest
DIMM_1/1 : Present
DIMM_2/1 : Present

Platform FPR-2130 with 32768 MBytes of main memory
BIOS has been successfully locked !!
MAC Address: 0c:75:bd:08:c9:80

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

此时按 **Esc** 键。如果您错过了中断提示，Firepower 2100 会尝试重新启动 3 次；因为设备上没有映像，所以只有 ROMMON 可用。

步骤 6 设置管理 1/1 的网络设置，并使用以下 ROMMON 命令加载 FXOS（ASA 软件包的一部分）。

address *management_ip_address*

netmask *subnet_mask*

server *tftp_ip_address*

gateway *gateway_ip_address*

file*path/filename*

set

sync

tftp -b

FXOS 映像随即下载，并启动进入 CLI。

请参阅以下信息：

- **gateway**- 如果此网关地址与服务器 IP 地址在同一网络上，请将二者设置为同一地址。
- **set**- 显示网络设置。您还可以使用 **ping** 命令验证与服务器的连接。
- **sync**- 保存网络设置。
- **tftp -b**- 加载 FXOS。

示例：

```
rommon 1> address 10.86.118.4
rommon 2> netmask 255.255.252.0
rommon 3> server 10.86.118.21
rommon 4> gateway 10.86.118.21
rommon 5> file cisco-asa-fp2k.9.8.2.SPA
rommon 6> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.4
  NETMASK=255.255.252.0
  GATEWAY=10.86.118.21
  SERVER=10.86.118.21
  IMAGE=cisco-asa-fp2k.9.8.2.SPA
  CONFIG=
  PS1="rommon ! > "

rommon 7> sync
rommon 8> tftp -b
Enable boot bundle: tftp_reqsize = 268435456

             ADDRESS: 10.86.118.4
             NETMASK: 255.255.252.0
             GATEWAY: 10.86.118.21
              SERVER: 10.86.118.21
               IMAGE: cisco-asa-fp2k.9.8.2.SPA
             MACADDR: d4:2c:44:0c:26:00
           VERBOSITY: Progress
               RETRY: 40
          PKTTIMEOUT: 7200
             BLKSIZE: 1460
            CHECKSUM: Yes
                PORT: GbE/1
             PHYMODE: Auto Detect

link up
Receiving cisco-asa-fp2k.9.8.2.SPA from 10.86.118.21!!!!!!!!
[…]
```

步骤 7 使用默认用户名 **admin** 和密码 **Admin123** 登录 FXOS。

在设备启动进入 FXOS 之后，您在 ROMMON 中设置的管理 IP 地址将被擦除并设置为默认值 192.168.45.45。您将需要在 FXOS 中为您的网络设置正确的 IP 地址和其他相关设置，然后才能从服务器下载 ASA 软件包。

步骤 8 禁用 DHCP 服务器。

scope system

scope services

disable dhcp-server

commit-buffer

必须先禁用 DHCP 服务器，然后才能更改管理 IP 地址。更改管理 IP 地址后，可以使用新客户端 IP 地址重新启用 DHCP。

示例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
```

```
firepower-2110 /system/services # disable dhcp-server
firepower-2110 /system/services* # commit-buffer
```

步骤 9 配置 IPv4 管理 IP 地址，还可以配置网关（可选）。

scopefabric-interconnecta

setout-of-band staticip *ip_address***netmask** *network_mask***gw** *gateway_ip_address*

要保留当前设置的网关（默认为 0.0.0.0，代表 ASA 数据接口），请省略 **gw** 关键字。如果您的下载服务器不在本地管理 1/1 网络上，则请更改网关 IP 地址；ASA 数据接口还不存在，因此您无法使用默认设置访问任何远程服务器。

示例：

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect #
firepower-2110 /fabric-interconnect # set out-of-band static ip 10.86.118.4 netmask
255.255.255.0
Warning: When committed, this change may disconnect the current CLI session
firepower-2110 /fabric-interconnect* #
```

步骤 10 删除 HTTPS、SSH 和 SNMP 的访问列表并添加新列表，以允许来自新网络的管理连接。

a) 为系统/服务设置范围。

scope system

scope services

示例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
```

b) 查看当前访问列表。

show ip-block

示例：

```
firepower-2110 /system/services # show ip-block

Permitted IP Block:
    IP Address      Prefix Length Protocol
    --------------- ------------- --------
    192.168.45.0               24 https
    192.168.45.0               24 ssh
firepower-2140 /system/services #
```

c) 添加新的访问列表。

IPv4：

enterip-block *ip_address* 前缀 [**http** | **snmp** | **ssh**]

IPv6：

enteripv6-block *ipv6_address* 前缀 [**https** | **snmp** | **ssh**]

对于 IPv4，请输入 **0.0.0.0** 和前缀 **0** 以允许所有网络。对于 IPv6，请输入 **::** 和前缀 **0** 以允许所有网络。还可以通过**平台设置 (Platform Settings)** > **访问列表 (Access List)** 在 Firepower 机箱管理器中添加访问列表。

示例：

```
firepower-2110 /system/services # enter ip-block 192.168.4.0 24 https
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 192.168.4.0 24 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* #
```

a) 删除旧的访问列表。

IPv4：

delete ip-block *ip_address* 前缀 [**http** | **snmp** | **ssh**]

IPv6：

delete ipv6-block *ipv6_address* 前缀 [**https** | **snmp** | **ssh**]

示例：

```
firepower-2110 /system/services # delete ip-block 192.168.45.0 24 https
firepower-2110 /system/services* # delete ip-block 192.168.45.0 24 ssh
firepower-2110 /system/services* #
```

步骤 11 （可选） 重新启用 IPv4 DHCP 服务器。

scope system

scope services

enable dhcp-server *start_ip_address end_ip_address*

示例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enable dhcp-server 10.86.118.10 10.86.118.20
```

步骤 12 保存配置。

commit-buffer

示例：

```
firepower-2110 /system/services* # commit-buffer
```

步骤 13 下载并启动 ASA 软件包。

a) 下载软件包。

scope firmware

download image *url*

show download-task

您可以从先前使用的同一 TFTP 服务器或管理 1/1 上可访问的其他服务器下载软件包。

示例：

```
firepower-2110# scope firmware
firepower-2110 /firmware # download image tftp://10.86.118.21/cisco-asa-fp2k.9.8.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
firepower-2110 /firmware # show download-task
Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.21             0                 Downloaded
```

b) 当软件包完成下载（已下载状态）时，启动软件包。

show package

scope auto-install

install security-pack version 版本

在 **show package** 输出中，复制与 **security-pack version** 号对应的 **Package-Vers** 值。机箱会安装 ASA 映像并重新启动。

示例：

```
firepower 2110 /firmware # show package
Name                                         Package-Vers
-------------------------------------------- ------------
cisco-asa-fp2k.9.8.2.SPA                     9.8.2
firepower 2110 /firmware # scope auto-install
firepower 2110 /firmware/auto-install # install security-pack version 9.8.2
The system is currently installed with security software package not set, which has:
   - The platform version: not set
If you proceed with the upgrade 9.8.2, it will do the following:
   - upgrade to the new platform version 2.2.2.52
   - install with CSP asa version 9.8.2
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Attention:
   If you proceed the system will be re-imaged. All existing configuration will be lost,

   and the default configuration applied.
Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.2
Install started. This will take several minutes.
```

```
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
```

步骤 14 等待机箱完成重新启动（5-10 分钟），然后使用默认用户名 **admin** 和密码 **Admin123** 登录 FXOS。

虽然 FXOS 已经启动，但您仍然需要等待 ASA 启动（5 分钟）。请等待，直至显示以下消息：

```
firepower-2110#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2 ...
Verifying signature for cisco-asa.9.8.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[…]
```

在显示其余的 ASA 启动消息之后，您可以返回到 FXOS 提示符。

步骤 15 如果在此过程中更改了 FXOS 管理 1/1 地址，则应更改 ASA 地址以使其保存在正确的网络中。默认 ASA 管理接口 1/1 IP 地址为 192.168.45.1。

a) 从控制台连接到 ASA CLI 并访问全局配置模式。

connect asa

enable

configure terminal

默认情况下，启用密码为空。

示例：

```
firepower-2110# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa> enable
Password: <blank>
ciscoasa# configure terminal
ciscoasa(config)#
```

b) 更改管理 1/1 IP 地址。

interface management1/1

ip address *ip_address mask*

示例：

```
ciscoasa(config)# interface management1/1
ciscoasa(config-ifc)# ip address 10.86.118.4 255.255.255.0
```

c) 更改可访问 ASDM 的网络。

no http 192.168.45.0 255.255.255.0 management

http *ip_address mask***management**

示例：

```
ciscoasa(config)# no http 192.168.45.0 255.255.255.0 management
ciscoasa(config)# http 10.86.118.0 255.255.255.0 management
```

d) 保存配置。

write memory

e) 要返回到 FXOS 控制台，请输入 **Ctrl+a**，**d**。

步骤 16 如需配置您的系统，请参阅适用于 Firepower 2100 系列的 ASA 入门指南。

下一步工作

Firepower 威胁防御

请参阅相关型号的快速入门指南和管理应用：

- ASA 5506-X 的 Firepower 设备管理器
- ASA 5506-X 的 Firepower 管理中心
- ASA 5508-X 和 5516-X 的 Firepower 设备管理器
- ASA 5506-X 和 5516-X 的 Firepower 管理中心
- ASA 5512-X 至 5555-X 的 Firepower 设备管理器
- ASA 5512-X 至 5555-X 的 Firepower 管理中心
- Firepower 2100 的 Firepower 设备管理器
- Firepower 2100 的 Firepower 管理中心

ASA

请参阅相关型号的快速入门指南

- 适用于 ASA 5506-X 的 ASA
- 适用于 ASA 5508-X 和 5516-X 的 ASA
- 适用于 ASA 5512-X 至 5555-X 的 ASA
- 用于 Firepower 2100 的 ASA