



适用于 Firepower 4100 的思科 ASA 快速入门指南

首次发布日期：2016 年 3 月 21 日

最后更新日期：2016 年 5 月 9 日

1. 关于适用于 Firepower 4100 的 ASA

Firepower 4100 安全设备包含一个可运行 ASA 应用的安全引擎。

ASA 如何与 Firepower 4100 配合使用

Firepower 4100 安全设备运行名为 Firepower 可扩展操作系统 (FXOS) 的独立操作系统。您可以使用 Firepower 机箱管理器 Web 界面或 CLI 配置硬件接口设置、智能许可和其他基本运行参数。

所有物理接口操作（包括建立外部 EtherChannel）均由 Firepower 4100 负责。您可以创建两种接口：数据接口和管理接口。您可以根据需要，在部署时或部署后将接口分配给 ASA。这些接口在 Firepower 4100 上使用的 ID 与 ASA 配置中的 ID 相同。Firepower 4100 通过内部背板 EtherChannel 将网络流量传送到 ASA。

部署 ASA 时，Firepower 4100 将下载您选择的 ASA 映像，并建立默认配置。ASA 既可作为独立逻辑设备部署，也可作为 ASA 集群部署（最多跨 6 个机箱）。

ASA 管理

部署 ASA 时，您可以预先配置管理接口和管理客户端信息，这样可使部署的 ASA 允许从该客户端访问 ASDM。

此外，您还可以使用内部 Telnet 连接从 Firepower 4100 CLI 访问 ASA CLI。在 ASA 内，您可以稍后通过其任意管理接口或数据接口配置 SSH 或 Telnet 访问。

注意：请参阅[适用于 Firepower 4100 的 ASA 的许可要求（第 1 页）](#)，了解访问 ASDM 的许可要求。

适用于 Firepower 4100 的 ASA 的许可要求

在适用于 Firepower 4100 的 ASA 上，智能软件许可配置分为两部分，分别在 Firepower 4100 和 ASA 中进行。

- Firepower 4100 - 在 Firepower 4100 上配置所有智能软件许可基础设施，包括用于与许可证颁发机构进行通信的参数。Firepower 4100 本身不需要任何许可证即可运行。
- ASA - 在 ASA 中配置所有许可证授权，包括所需的标准级许可证。在 ASA 中还可使用其他可选许可证。当您在 Firepower 4100 上应用注册令牌时，对于符合条件的用户，系统会自动启用强加密许可证，因此您无需进行其他操作。

注意：对于 Smart Software Manager satellite 部署，您必须先通过在 ASA 软件中请求授权来启用强加密 (3DES/AES) 许可证，才能使用 ASDM（以及 VPN 等功能）。您必须通过 ASA CLI 执行此任务，ASA CLI 可从 FXOS CLI 进行访问。若使用的是评估许可证，则无法收到强加密许可证。

2. 部署 ASA

您可以使用 Firepower 机箱管理器部署独立 ASA 或 ASA 集群。有关 CLI 操作步骤，请参阅《FXOS 配置指南》。

配置接口

在可以包括在 ASA 部署配置中的 Firepower 4100 上配置管理类型的接口。您还必须至少配置一个数据类型的接口。对于集群，您需要向用作机箱间的集群控制链路的端口通道 48 集群类型接口添加至少一个成员接口。

程序

1. 在 Firepower 机箱管理器中，选择**接口 (Interfaces)** 打开“接口” (Interfaces) 页面。
2. 添加一个 EtherChannel：
 - a. 点击**添加端口通道 (Add Port Channel)**。
 - b. 在“端口通道 ID” (Port Channel ID) 字段中，输入一个介于 1 和 47 之间的值。
 - c. 选中**启用 (Enable)**。
 - d. 对于“类型” (Type)，选择**管理 (Management)** 或**数据 (Data)**。您只能添加一个管理接口。请勿选择**集群 (Cluster)**。
 - e. 根据需要添加成员接口。
 - f. 点击 **确定 (OK)**。
3. 要添加单个接口，请执行以下操作：
 - a. 点击接口行中的**编辑 (Edit)** 图标，打开“编辑接口” (Edit Interface) 对话框。
 - b. 选中**启用 (Enable)**。
 - c. 对于“类型” (Type)，点击**管理 (Management)** 或**数据 (Data)**。您只能添加一个管理接口。
 - d. 点击**确定 (OK)**。
4. 要向用作集群控制链路的端口通道 48 添加一个成员端口，请执行以下操作：
 - a. 点击中的**编辑 (Edit)** 图标，打开“编辑接口” (Edit Interface) 对话框。
 - b. 从**可用接口 (Available Interface)** 窗口选择一个接口，然后点击**添加接口 (Add Interface)**。如有需要，请对其他接口重复上述操作；您至少需要添加一个接口。
 - c. 点击**确认 (OK)**。

部署独立 ASA

操作步骤

1. 选择**逻辑设备 (Logical Devices)** 打开“逻辑设备” (Logical Devices) 页面。
2. 点击**添加设备 (Add Device)** 打开“添加设备” (Add Device) 对话框。
3. 在**设备名称 (Device Name)** 字段中，为逻辑设备提供一个名称。此名称仅供 Firepower 4100 在配置管理设置以及分配接口时使用，而非在 ASA 配置中使用的设备名称。
4. 对于**模板 (Template)**，选择 **asa**。
5. 在**映像版本 (Image Version)** 部分，选择 ASA 软件版本。

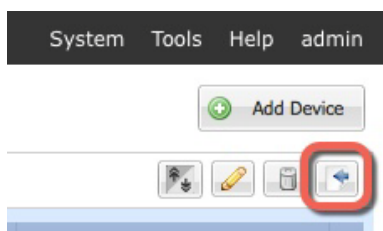
6. 在**设备模式 (Device Mode)** 中，点击**独立 (Standalone)** 单选按钮。
7. 点击**确定 (OK)**。屏幕将显示 *调配 - 设备名称 (Provisioning - device name)* 窗口。
8. 展开**数据端口 (Data Ports)** 区域，并确保所有接口均已分配到 ASA。
9. 点击屏幕中心的设备图标。系统将显示 **ASA 配置 (ASA Configuration)** 对话框。
10. 按照提示配置部署选项。
11. 点击**确定 (OK)** 关闭“ASA 配置” (ASA Configuration) 对话框。
12. 点击**保存 (Save)**。Firepower 4100 通过下载指定的软件版本，并将引导程序配置和管理接口设置推送到安全引擎来部署逻辑设备。

部署 ASA 集群

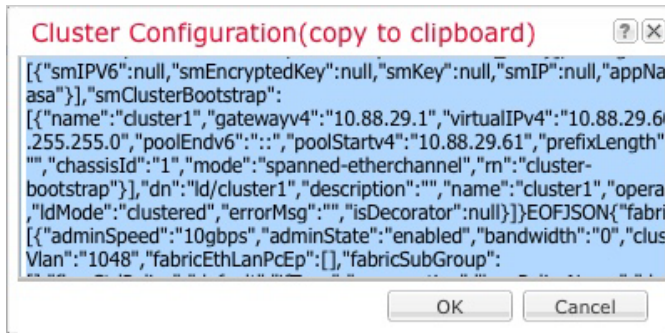
操作步骤

1. 选择**逻辑设备 (Logical Devices)** 打开“逻辑设备” (Logical Devices) 页面。
2. 点击**添加设备 (Add Device)** 打开“添加设备” (Add Device) 对话框。
3. 在**设备名称 (Device Name)** 字段中，为逻辑设备提供一个名称。此名称仅供 Firepower 4100 在配置集群/管理设置以及分配接口时使用，而非在 ASA 配置中使用的设备名称。
4. 对于**模板 (Template)**，选择 **asa**。
5. 在**映像版本 (Image Version)** 部分，选择 ASA 软件版本。
6. 在 **设备模式 (Device Mode)** 中，点击**集群 (Cluster)** 单选按钮。
7. 点击**创建新集群 (Create New Cluster)** 单选按钮。
8. 点击**确定 (OK)**。屏幕将显示 *调配 - 设备名称 (Provisioning - device name)* 窗口。
9. 展开**数据端口 (Data Ports)** 区域，并确保所有接口均已分配到 ASA。
10. 点击屏幕中心的设备图标。系统将显示 **ASA 配置 (ASA Configuration)** 对话框。
11. 按照提示配置部署选项。

注意：在**管理 IP 池 (Management IP Pool)** 字段中，配置本地 IP 地址池，其中一个地址将分配给接口的每个集群设备，方法是输入以连字符分隔的起始地址和结束地址。至少包含与集群中的设备数量相同的地址。如果计划扩展集群，则应包含更多地址。属于当前主设备的**虚拟 IP 地址 (Virtual IP address)**（称为主集群 IP 地址）不是此池的一部分；请务必在同一网络中为虚拟 IP 地址保留一个 IP 地址。您可以使用 IPv4 和/或 IPv6 地址。
12. 点击**确定 (OK)** 关闭“ASA 配置” (ASA Configuration) 对话框。
13. 点击**保存 (Save)**。Firepower 4100 通过下载指定的软件版本，并将引导程序配置和管理接口设置推送到安全引擎来部署逻辑设备。
14. 将下一个机箱添加到集群中：
 - a. 在第一个机箱的 Firepower 机箱管理器上，点击右上方的**显示集群详细信息 (Show Cluster Details)** 图标。



- b. 选择并复制显示的集群配置文本。



- c. 连接到下一机箱上的 Firepower 机箱管理器，并按照此程序添加逻辑设备。
- d. 选择**加入现有集群 (Join an Existing Cluster)**。
- e. 点击**复制配置 (Copy config)** 复选框，然后点击**确定 (OK)**。如果取消选中此复选框，必须手动输入设置，以匹配第一个机箱配置。
- f. 在**复制集群详细信息 (Copy Cluster Details)** 对话框中，粘贴第一个机箱的集群配置，然后点击**确定 (OK)**。
- g. 点击屏幕中心的设备图标。系统会预填充“机箱 ID” (Chassis ID) 外的所有集群信息；输入唯一的机箱 ID，然后点击**确定 (OK)**。
- h. 点击**保存 (Save)**。

3. 访问 ASA CLI

在进行初始配置或故障排除时，您可能需要从 Firepower 4100 CLI 访问 ASA CLI。

操作步骤

1. 连接到主 Firepower 4100 CLI；例如，连接到控制台端口或使用 SSH 连接到 Firepower 管理接口。
2. 连接到 ASA：

```
connect module 1 console
```

示例：

```
Firepower> connect module 1 console
Firepower-module1>
```

3. 首次连接到安全引擎时，您会进入 FXOS 安全引擎 CLI。您必须自行连接到 ASA 应用：

```
connect asa
```

示例：

```
Firepower-module1> connect asa
asa>
```

后续连接都会直接跳转到 ASA 应用。

4. 进入特权 EXEC（启用）模式，然后进入全局配置模式。默认情况下，启用密码为空。

```
enable  
configure terminal
```

示例：

```
asa> enable  
Password:  
asa# configure terminal  
asa(config)#
```

5. 对于 ASA 集群，如果需要，请确认此设备是主设备：

```
show cluster info
```

示例：

```
asa(config)# show cluster info  
Cluster cluster1: On  
  Interface mode: spanned  
  This is "unit-1-1" in state MASTER  
    ID      : 2  
    Version : 9.6(1)  
    Serial No.: FCH183770GD  
    CCL IP   : 127.2.1.1  
    CCL MAC  : 0015.c500.019f  
    Last join : 01:18:34 UTC Nov 4 2015  
    Last leave: N/A  
Other members in the cluster:  
  Unit "unit-2-1" in state SLAVE  
    ID      : 4  
    Version : 9.6(1)  
    Serial No.: FCH19057ML0  
    CCL IP   : 127.2.2.1  
    CCL MAC  : 0015.c500.018f  
    Last join : 20:29:57 UTC Nov 4 2015  
    Last leave: 20:24:55 UTC Nov 4 2015  
  Unit "unit-3-1" in state SLAVE  
    ID      : 1  
    Version : 9.6(1)  
    Serial No.: FCH19057ML0  
    CCL IP   : 127.2.3.1  
    CCL MAC  : 0015.c500.017f  
    Last join : 20:20:53 UTC Nov 4 2015  
    Last leave: 20:18:15 UTC Nov 4 2015  
  Unit "unit-4-1" in state SLAVE  
    ID      : 3  
    Version : 9.6(1)  
    Serial No.: FCH19057ML0  
    CCL IP   : 127.2.4.1  
    CCL MAC  : 0015.c500.020f  
    Last join : 20:19:57 UTC Nov 4 2015  
    Last leave: 20:24:55 UTC Nov 4 2015
```

如果其他机箱才是主设备，请退出当前连接，并连接到正确的机箱。有关如何退出连接，请参阅下文。

4.Smart Software Manager Satellite: 请求强加密 (3DES/AES) 许可证

要运行 ASDM 及其他功能（例如 VPN），您必须具有强加密 (3DES/AES) 许可证。当您使用 Smart Software Manager satellite 时，您必须使用 CLI 在 ASA 配置中请求此许可证。

准备工作

- 在 ASA 上配置许可证授权之前，必须在 Firepower 4100 上配置思科智能软件许可。
- 对于 ASA 集群，您需要访问主设备进行配置。查看 Firepower 机箱管理器，确定哪一台设备为主设备。您也可以从 ASA CLI 进行确认。

操作步骤

1. 访问 ASA CLI。请参阅 [3.访问 ASA CLI（第 4 页）](#)。

2. 进入许可证智能配置模式：

```
license smart
```

示例：

```
ciscoasa(config)# license smart  
ciscoasa(config-smart-lic)#
```

3. 设置功能层：

```
feature tier standard
```

仅标准层可用。层许可证是添加其他功能许可证的前提条件。

4. 请求强加密许可证，或者根据需要请求其他功能：

- 强加密 (3DES/AES)

```
feature strong-encryption
```

- 运营商 (Diameter、GTP/GPRS、SCTP)

```
feature carrier
```

- 安全情景

```
feature context <1-248>
```

5. 保存配置：

```
write memory
```

6. 键入 ~，退出控制台连接。您将退出至 Telnet 应用。输入**退出 (quit)**，退出到 Firepower 4100 CLI。

5.启动 ASDM

ASDM 包括许多易于使用的向导，以及一整套对应各项 ASA 功能的配置工具。

准备工作

- 请参阅 Cisco.com 上的 [ASDM 版本说明](#) 了解运行 ASDM 的要求。
- 您必须在 Firepower 4100 上配置思科智能软件许可，才能连接到 ASDM；要使用 ASDM，必须具有强加密 (3DES/AES)。当您在 Firepower 4100 上应用注册令牌时，对于符合条件的用户，系统会自动启用强加密许可证。有关 Smart Software Manager satellite 配置，请参阅 [4.Smart Software Manager Satellite: 请求强加密 \(3DES/AES\) 许可证（第 6 页）](#)。

操作步骤

1. 在连接到分配给 ASA 的管理接口的计算机上，启动 Web 浏览器。
2. 在地址栏中，输入以下 URL：https://ip_address/admin。ip_address 是您在部署 ASA 时为管理接口设置的地址。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)。

注意：如果您点击**安装 ASDM 启动程序 (Install ASDM Launcher)**，对于 Java 7 的某些版本，您需要按照[安装 ASDM 身份证书](#)中的说明为 ASA 安装身份证书。

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. 后续步骤

- 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。
- 查看所有 [FXOS 机箱相关文档](#)。

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)

本文档中使用的任何 Internet 协议 (IP) 地址都不是有意使用的真实地址。本文档中所含的任何示例、命令显示输出和图形仅供说明之用。说明内容中用到的任何真实 IP 地址都纯属巧合，并非有意使用。

© 2016 思科系统公司。版权所有。

