



使用入门

本章介绍如何开始使用 ASA。

- [访问命令行界面的控制台，第 1 页](#)
- [配置 ASDM 访问，第 5 页](#)
- [启动 ASDM，第 8 页](#)
- [自定义 ASDM 操作，第 9 页](#)
- [出厂默认配置，第 11 页](#)
- [开始配置，第 25 页](#)
- [在 ASDM 中使用命令行界面工具，第 26 页](#)
- [将配置更改应用于连接，第 27 页](#)

访问命令行界面的控制台

在某些情况下，可能需要使用 CLI 为 ASDM 访问配置基本设置。

对于初始配置，请从控制台端口直接访问 CLI。之后，您可以根据[管理访问](#)使用 Telnet 或 SSH 配置远程访问。如果系统已处于多情景模式，则访问控制台端口会将您引导至系统执行空间。



注释 有关 ASA virtual 控制台访问，请参阅《ASA virtual 快速入门指南》。

访问 ISA 3000 控制台

按照以下步骤访问设备控制台。

过程

- 步骤 1** 使用所提供的控制台电缆将计算机连接到控制台端口，并使用已设置为 9600 波特、8 个数据位、无奇偶校验、1 个停止位、无流量控制功能的终端仿真器连接到控制台。

请参阅 ASA 硬件指南，了解有关控制台电缆的详细信息。

步骤 2 按 **Enter** 键将看到以下提示符：

```
ciscoasa>
```

此提示符表明您正处于用户 EXEC 模式。用户 EXEC 模式仅能获取基本命令。

步骤 3 访问特权 EXEC 模式。

enable

第一次输入 **enable** 命令时，系统会提示您更改密码：

示例：

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: *****
Repeat Password: *****
ciscoasa#
```

在特权 EXEC 模式中，所有非配置命令均可用。还可从特权 EXEC 模式进入配置模式。

要退出特权模式，请输入 **disable**、**exit** 或 **quit** 命令。

步骤 4 访问全局配置模式。

configure terminal

示例：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

可从全局配置模式开始配置 ASA。要退出全局配置模式，请输入 **exit**、**quit** 或 **end** 命令。

访问 Firepower 1000和 Cisco Secure Firewall 3100/4200 控制台

Firepower 1000和 Cisco Secure Firewall 3100/4200 控制台端口可将您连接到 ASA CLI。然后，您可以在 ASA CLI 中使用 Telnet 连接到 FXOS CLI 进行故障排除。

过程

步骤 1 将管理计算机连接到控制台端口。确保为操作系统安装任何必要的串行驱动程序。使用以下串行设置：

- 9600 波特率

- 8 个数据位
- 无奇偶校验
- 1 个停止位

连接到 ASA CLI。默认情况下，访问控制台时不需要提供用户凭证。

步骤 2 访问特权 EXEC 模式。

enable

第一次输入 **enable** 命令时，系统会提示您更改密码。

示例：

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: *****
Repeat Password: *****
ciscoasa#
```

如果 ASA 无法启动，并且您进入 FXOS 故障保护模式，则您在 ASA 上设置的启用密码也是 FXOS 管理员用户密码。

在特权 EXEC 模式中，所有非配置命令均可用。还可从特权 EXEC 模式进入配置模式。

要退出特权 EXEC 模式，请输入 **disable**、**exit** 或 **quit** 命令。

步骤 3 访问全局配置模式。

configure terminal

示例：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

可从全局配置模式开始配置 ASA。要退出全局配置模式，请输入 **exit**、**quit** 或 **end** 命令。

步骤 4 （可选）连接到 FXOS CLI。

connect fxos [admin]

- **admin**- 提供管理员级的访问权限。如果不选择此选项，用户将拥有只读访问权限。请注意，即使在管理员模式下，也没有任何配置命令可用。

系统不会提示您提供用户凭证。当前的 ASA 用户名将传递给 FXOS，无需其他登录。要返回到 ASA CLI，请输入 **exit** 或键入 **Ctrl-Shift-6、x**。

在 FXOS 中，您可以使用 **scope security/show audit-logs** 命令查看用户活动。

示例：

```
ciscoasa# connect fxos admin
```

```
Connecting to fxos.  
Connected to fxos. Escape character sequence is 'CTRL-^X'.  
firepower#  
firepower# exit  
Connection with FXOS terminated.  
Type help or '?' for a list of available commands.  
ciscoasa#
```

访问 Firepower 4100/9300 机箱上的 ASA 控制台

对于初始配置，请通过依次连接到 Firepower 4100/9300 机箱管理引擎（连接控制台端口或使用 Telnet 或 SSH 进行远程连接）和 ASA 安全模块来访问命令行界面。

过程

步骤 1 连接到 Firepower 4100/9300 机箱管理引擎 CLI（控制台或 SSH），然后将会话连接到 ASA：

```
connect module slot {console | telnet}
```

使用 Telnet 连接的优点在于，您可以同时对模块开展多个会话，并且连接速度更快。

首次访问模块时，您将访问 FXOS 模块 CLI。然后必须连接到 ASA 应用。

```
connect asa
```

示例：

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

步骤 2 访问授权的 EXEC 模式，该模式具有最高权限级别。

```
enable
```

第一次输入 **enable** 命令时，系统会提示您更改密码。

示例：

```
asa> enable  
Password:  
The enable password is not set. Please set it now.  
Enter Password: *****  
Repeat Password: *****  
asa#
```

在特权 EXEC 模式中，所有非配置命令均可用。还可从特权 EXEC 模式进入配置模式。

要退出特权模式，请输入 **disable**、**exit** 或 **quit** 命令。

步骤 3 进入全局配置模式。

configure terminal

示例:

```
asa# configure terminal
asa(config)#
```

要退出全局配置模式，请输入 **disable**、**exit** 或 **quit** 命令。

步骤 4 输入 **Ctrl-a, d** 使应用程序控制台返回到 FXOS 模块 CLI

出于故障排除目的，您可能想使用 FXOS 模块 CLI。

步骤 5 返回 FXOS CLI 的管理引擎层。

退出控制台:

a) 输入 ~

您将退出至 Telnet 应用。

b) 要退出 Telnet 应用，请输入:

```
telnet>quit
```

退出 Telnet 会话:

a) 输入 **Ctrl-]**。

配置 ASDM 访问

本节介绍如何通过默认配置访问 ASDM，以及在没有默认配置的情况下如何配置访问。

使用出厂默认配置进行 ASDM 访问

通过出厂默认配置，已采用默认网络设置对 ASDM 连接进行了预配置。

过程

使用以下接口和网络设置连接到 ASDM:

- 管理接口取决于设备型号:
 - Firepower 1010 - Management 1/1 (192.168.45.1) 或内部以太网 1/2 至 1/8 (192.168.1.1)。管理主机限制为 192.168.45.0/24 网络，内部主机限制为 192.168.1.0/24 网络。
 - Firepower 1100、Cisco Secure Firewall 3100、4200 — 内部以太网 1/2 (192.168.1.1) 或 Management 1/1 (来自 DHCP)。内部主机限制为 192.168.1.0/24 网络。管理主机允许来自任何网络。

- Firepower 4100/9300 - 部署时定义的管理类型接口和您选择的 IP 地址。管理主机允许来自任何网络。
- ASA Virtual- Management 0/0（在部署期间设置）。管理主机仅限于管理网络。
- ISA 3000 - Management 1/1 (192.168.1.1)。管理主机受限于192.168.1.0/24 网络。

注释 如果更改为多情景模式，则可使用上述网络设置从管理情景访问 ASDM。

相关主题

[出厂默认配置](#)，第 11 页

[启用或禁用多情景模式](#)

[启动 ASDM](#)，第 8 页

自定义 ASDM 访问

如果满足一个或多个以下条件，可使用该程序：

- 没有出厂默认配置
- 想要更改为透明防火墙模式
- 想要更改为多情景模式

对于单一路由模式，为了实现快速轻松的 ASDM 访问，我们建议应用出厂默认配置，但可选择设置您自己的管理 IP 地址。只有您有特殊需求（如设置透明或多情景模式）或有需要保留的其他配置时，才应使用本节所述程序。



注释 对于 ASA v，可以在部署过程中配置透明模式，所以此程序主要用在类似于部署之后需要清除配置等情况。

过程

步骤 1 在控制台端口访问 CLI。

步骤 2（可选）启用透明防火墙模式：

该命令清除您的配置。

firewall transparent

步骤 3 配置管理接口：

```
interface interface_id
  nameif name
```

```
security-level level
no shutdown
ip address ip_address mask
```

示例:

```
ciscoasa(config)# interface management 0/0
ciscoasa(config-if)# nameif management
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
```

security-level 是介于 1 到 100 之间的数字，其中 100 为最安全级别。

步骤 4 （对于直连管理主机）为管理网络设置 DHCP 池:

```
dhcpd address ip_address-ip_address interface_name
dhcpd enable interface_name
```

示例:

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 management
ciscoasa(config)# dhcpd enable management
```

确保此范围内不包括接口地址。

步骤 5 （对于远程管理主机）配置管理主机路由:

```
route management_ifc management_host_ip mask gateway_ip 1
```

示例:

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50 1
```

步骤 6 为 ASDM 启用 HTTP 服务器:

```
http server enable
```

步骤 7 允许管理主机访问 ASDM:

```
http ip_address mask interface_name
```

示例:

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

步骤 8 保存配置:

```
write memory
```

步骤 9 （可选）将模式设置为多模式:

```
mode multiple
```

出现提示时，请确认要将现有配置转换为管理情景。然后系统将提示重新加载 ASA。

示例

以下配置将防火墙模式转换为透明模式，配置 Management 0/0 接口，并为管理主机启用 ASDM:

```
firewall transparent
interface management 0/0

ip address 192.168.1.1 255.255.255.0
nameif management
security-level 100
no shutdown

dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
http server enable
http 192.168.1.0 255.255.255.0 management
```

相关主题

[恢复出厂默认配置](#)，第 12 页

[设置防火墙模式（单模式）](#)

[访问 ISA 3000 控制台](#)，第 1 页

[启动 ASDM](#)，第 8 页

启动 ASDM

使用 ASDM-IDM 启动程序启动 ASDM。启动器是使用您可以连接用其连接到任意 ASA IP 地址的 Web 浏览器从 ASA 下载的一款应用。如果要连接至其他 ASA，无需重新下载该启动器。

在 ASDM 内，可以选择其他 ASA IP 地址进行管理。

本节介绍最初如何连接 ASDM，以及如何使用启动程序启动 ASDM。

ASDM 将文件存储在本地 \Users\\.asdm 目录（包括缓存、日志和首选项）和临时目录中（包括 Secure Client 配置文件）中。

过程

步骤 1 在指定为 ASDM 客户端的计算机上，输入以下 URL:

https://asa_ip_address/admin

注释 确保指定 **https://**，而非指定 **http://** 或只指定 IP 地址（默认为 HTTP）；ASA 不会自动将 HTTP 请求转发到 HTTPS。

系统将显示 ASDM 启动页面和以下按钮：

安装 ASDM 启动程序

步骤 2 要下载启动程序并开始 ASDM，请执行以下操作：

- a) 点击 **安装 ASDM 启动程序**。

图 1: 安装 ASDM 启动程序



- b) 将用户名和密码字段留空（适用于新安装），然后点击**确定 (OK)**。

如果未配置 HTTPS 身份验证，可以在没有用户名和 **enable** 密码（默认为空）的情况下获得对 ASDM 的访问权限。首次在 CLI 中输入 **enable** 命令时，系统会提示您更改密码；登录 ASDM 时不会强制执行此行为。建议您尽快更改启用密码，不要再保持空白状态；请参阅 [设置主机名、域名及启用密码和 Telnet 密码](#)。注意：如果您启用了 HTTPS 身份验证，则输入您的用户名及关联的密码。即使不使用身份验证，如果您在登录屏幕输入用户名和密码（而不是将用户名留空），ASDM 也会从本地数据库中检查是否有匹配项。

- c) 将安装程序保存到计算机，然后启动安装程序。安装完成后，将自动打开 ASDM-IDM 启动程序。
- d) 输入管理 IP 地址、同一个用户名和密码（新安装则留空），然后点击 **OK**。

自定义 ASDM 操作

可以安装身份证书来成功启动 ASDM 并增加 ASDM 堆内存，以便 ASDM 可以处理更大的配置。

为 ASDM 安装身份证书

使用 Java 7 update 51 及更高版本时，ASDM Launcher 需要可信任证书。满足证书要求的一个简单方法就是安装自签名身份证书。可使用 Java Web Start 启动 ASDM，直到安装证书。

请参阅以下文档，以便在 ASA 上安装用于 ASDM 的自签身份证书，并向 Java 注册证书。

<http://www.cisco.com/go/asdm-certificate>

增加 ASDM 配置内存

ASDM 最多支持 512 KB 的配置。如果超出此数量，可能会遇到性能问题。例如加载配置时，状态对话框显示已完成配置的百分比，但如果配置较大，它将停止递增并显示为暂停操作，即使 ASDM 仍可能在处理配置。如果发生此情况，我们建议考虑增加 ASDM 系统堆内存。要确认是否遇到内存耗尽问题，请监控 Java 控制台是否显示“java.lang.OutOfMemoryError”消息。

增加 Windows 中的 ASDM 配置内存

要增加 ASDM 堆内存大小，请通过执行以下程序编辑 **run.bat** 文件。

过程

步骤 1 转到 ASDM 安装目录，例如 C:\Program Files (x86)\Cisco Systems\ASDM。

步骤 2 使用任意文本编辑器编辑 **run.bat** 文件。

步骤 3 在以“start javaw.exe”开头的行中，更改前缀为“-Xmx”的参数以指定所需堆大小。例如，如需 768 MB 内存，请将参数更改为 -Xmx768M；如需 1 GB 内存，请将参数更改为 -Xmx1G。

步骤 4 保存 **run.bat** 文件。

增加 Mac 操作系统中的 ASDM 配置内存

要增加 ASDM 堆内存大小，请通过执行以下程序编辑 **Info.plist** 文件。

过程

步骤 1 右键单击 **Cisco ASDM-IDM** 图标，然后选择 **Show Package Contents**。

步骤 2 在 **Contents** 文件夹中，双击 **Info.plist** 文件。如果已安装开发人员工具，该文件会在 **Property List Editor** 中打开。否则，它将在 **TextEdit** 中打开。

步骤 3 在 **Java > VMOptions** 下面，更改前缀为“-Xmx”的字符串以指定所需堆大小。例如，如需 768 MB 内存，请将参数更改为 -Xmx768M；如需 1 GB 内存，请将参数更改为 -Xmx1G。

```

<key>CFBundleIconFile</key>
<string>asdm32.icns</string>

<key>VMOptions</key>
<string>-Xms64m -Xmx512m</string>

<key>CFBundleDocumentTypes</key>
<array>

```

步骤 4 如果该文件已锁定，则将看到如下错误：



步骤 5 点击 **Unlock** 并保存文件。

如果未看到 **Unlock** 对话框，请退出编辑器，右键点击 **Cisco ASDM-IDM** 图标，选择 **Copy Cisco ASDM-IDM**，并将其粘贴到您拥有写入权限的位置，例如桌面。然后从该副本更改堆大小。

出厂默认配置

出厂默认配置是思科对新的 ASA 应用的配置。

- Firepower 1010 - 出厂默认配置启用功能性内部/外部配置。您可以从管理接口或内部交换机端口使用 ASDM 管理 ASA。
- Firepower 1100 - 出厂默认配置启用功能性内部/外部配置。您可以从管理接口或内部接口使用 ASDM 管理 ASA。
- Secure Firewall 3100 - 出厂默认配置启用功能性内部/外部配置。您可以从管理 1/1 接口或内部接口使用 ASDM 管理 ASA。
- Secure Firewall 4200 - 出厂默认配置启用功能性内部/外部配置。您可以从管理 1/1 接口或内部接口使用 ASDM 管理 ASA。
- Firepower 4100/9300 机箱 - 在部署独立 ASA 或 ASA 集群时，出厂默认配置可配置管理接口，以便可以使用 ASDM 与其连接，然后通过它完成配置。

- **ASA Virtual**- 根据虚拟机监控程序，在部署过程中，部署配置（初始虚拟部署设置）可配置管理接口，以便可以使用 ASDM 与其连接，然后通过它完成配置。还可以配置故障转移 IP 地址。还可应用“出厂默认”配置（如果需要）。
- **ISA 3000**- 出厂默认配置是几乎完全透明的防火墙模式配置，所有内部和外部接口都位于同一网络中；您可以使用 ASDM 连接到管理接口来设置网络的 IP 地址。已为两个接口对。

对于设备，出厂默认配置仅可用于路由防火墙模式和单一情景模式，除了 ISA 3000，后者的出厂默认配置仅在透明模式中可用。对于 ASA virtual 和 Firepower 4100/9300 机箱，可以在部署时选择透明模式或路由模式。



注释 除映像文件和（隐藏的）默认配置外，以下文件夹和文件是闪存中的标准配置：`log/`、`crypto_archive/` 和 `coredumpinfo/coredump.cfg`。这些文件上的日期可能与闪存中映像文件的日期不匹配。这些文件有助于潜在的故障排除；它们不表示已发生故障。

恢复出厂默认配置

本节介绍如何恢复出厂默认配置。已提供 CLI 和 ASDM 程序。对于 ASA virtual，该程序可擦除部署配置并对各 ASA 5525-X 应用以下配置：

```
interface management 0/0
  ip address 192.168.1.1 255.255.255.0
  nameif management
  security-level 100
  no shutdown
!
asdm logging informational
asdm history enable
!
http server enable
http 192.168.1.0 255.255.255.0 management
!
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
```



注释 在 Firepower 4100/9300 上，恢复出厂默认配置会擦除配置；要恢复默认配置，必须从管理引擎重新部署 ASA。

开始之前

此功能仅在路由防火墙模式下可用，但 ISA 3000 除外，ISA 3000 仅在透明模式下支持此命令。此外，该功能仅可用于单一情景模式；已清除配置的 ASA 没有任何定义的情景可使用该功能自动进行配置。

过程

步骤 1 恢复出厂默认配置：

configure factory-default [*ip_address* [*mask*]]

示例：

```
ciscoasa(config)# configure factory-default 10.1.1.1 255.255.255.0
```

如果指定 *ip_address*，则根据设备型号设置内部或管理接口 IP 地址，而不是使用默认 IP 地址。有关由 *ip_address* 选项设置的接口，请参阅以下型号准则：

- Firepower 1010 - 设置管理界面 IP 地址。
- Firepower 1100-设置内部接口IP地址。
- 安全防火墙3100-设置内部接口IP地址。
- 安全防火墙4200-设置内部接口IP地址。
- Firepower 4100/9300-无影响。
- ASA Virtual—设置管理接口 IP 地址。
- ISA 3000 - 设置管理接口 IP 地址。

http 命令使用您指定的子网。同样，**dhcpd address** 命令范围包含比你指定的 IP 地址更高的所有可用地址。例如，如果指定10.5.6.78，子网掩码为255.255.255.0，则DHCP地址范围为10.5.6.79-10.5.6.254。

对于 Firepower 1000 和Cisco Secure Firewall 3100、4200：此命令会清除 **boot system** 命令（如有）以及配置的其余部分。此配置更改不会影响启动时的映像：继续使用当前加载的映像。

对于所有其他型号：此命令可清除 **boot system** 命令（如果存在）和其他配置。该命令允许您从特定映像启动。**boot system** 下次在恢复出厂配置后重新加载 ASA 时，它将从内部闪存中的第一个映像启动；如果内部闪存中无映像，ASA 将不启动。

示例：

```
docs-bxb-asa3(config)# configure factory-default 10.86.203.151 255.255.254.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256
```

```
WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.
```

```
Begin to apply factory-default configuration:
Clear all configuration
WARNING: The new maximum-session limit will take effect after the running-config is saved
and the system boots next time. Command accepted
WARNING: Local user database is empty and there are still 'aaa' commands for 'LOCAL'.
Executing command: interface management0/0
```

```

Executing command: nameif management
INFO: Security level for "management" set to 0 by default.
Executing command: ip address 10.86.203.151 255.255.254.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.86.202.0 255.255.254.0 management
Executing command: dhcpd address 10.86.203.152-10.86.203.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#

```

步骤 2 将默认配置保存到闪存:

write memory

该命令将运行配置保存到启动配置的默认位置，即使以前已将 **boot config** 命令配置为设置另一个位置也是如此；配置清除后，该路径也将清除。

步骤 3 (ASDM 程序。) 在 ASDM 主应用窗口中，执行以下操作:

a) 依次选择文件 > 将设备重置为出厂默认配置。

系统将显示 **Reset Device to the Default Configuration** 对话框。

b) (可选) 在 **Management IP address** 中输入管理或内部接口的管理 IP 地址，而不是使用默认地址。

有关每个型号设置的接口IP的详细信息，请参阅上一个CLI步骤。

c) (可选) 从下拉列表中选择 **Management Subnet Mask**。

d) 点击 **OK**。

系统将显示确认对话框。

注释 对于 Firepower 1000 和 Cisco Secure Firewall 3100、4200: : 此命令会清除引导映像 (如果有) 以及其余配置的位置。此配置更改不会影响启动时的映像: 继续使用当前加载的映像。

对于所有其他型号: 该操作还可清除启动映像 (如果存在) 以及其他配置。在 **Configuration > Device Management > System Image/Configuration > Boot Image/Configuration** 窗格中, 可从特定映像启动, 包括外部内存上的映像。下次在恢复出厂配置后重新加载 ASA 时, 它将从内部闪存的第一个映像启动; 如果内部闪存中无映像, ASA 将不启动。

e) 点击 **Yes**。

f) 恢复默认配置后, 将该配置保存到内部闪存。依次选择文件 > 将运行配置保存至闪存。

选择该选项可将运行配置保存到启动配置的默认位置, 即使之前已配置了另一个位置也是如此。配置清除后, 该路径也将清除。

恢复 ASA Virtual 部署配置

本节介绍如何恢复 ASA virtual 部署（第 0 天）配置。

过程

步骤 1 为了执行故障转移，请关闭备用设备。

为防止备用设备变成主用设备，必须将其关闭。如果让其处于打开状态，则当清除主用设备配置后，备用设备将变为主用设备。当原来的主用设备重新加载并且通过故障转移链路重新连接后，旧配置将从新主用设备同步，并且擦除所需要的部署配置。

步骤 2 重新加载后，恢复部署配置。为了执行故障转移，请在主用设备上输入以下命令：

write erase

注释 ASA virtual 会启动当前运行的映像，因此，不会恢复到原始启动映像。要使用原始启动映像，请参阅 **boot image** 命令。

请勿保存该配置。

步骤 3 重新加载 ASA virtual，并加载部署配置：

reload

步骤 4 为了执行故障转移，请开启备用设备。

主用设备重新加载后，开启备用设备。部署配置将同步备用设备。

Firepower 1010 默认配置

Firepower 1010 的出厂默认配置包含以下配置：

- 硬件交换机 - 以太网 1/2 至 1/8 属于 VLAN 1
- 内部→外部流量 - 以太网 1/1（外部），VLAN1（内部）
- 管理 - 管理端口 1/1（管理），IP 地址 192.168.45.1
- 从 DHCP 的外部 IP 地址，内部 IP 地址 - 192.168.1.1
- 内部接口、管理接口上的 **DHCP 服务器**
- 来自外部 DHCP 的默认路由
- **ASDM** 访问 - 允许管理和内部主机。管理主机限制为 192.168.45.0/24 网络，内部主机限制为 192.168.1.0/24 网络。
- **NAT** - 从内部到外部所有流量的接口 PAT。

- DNS 服务器 - OpenDNS 服务器已预配置。

配置由以下命令组成:

```
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface Management1/1
management-only
nameif management
no shutdown
security-level 100
ip address 192.168.45.1 255.255.255.0
!
interface Ethernet1/1
nameif outside
ip address dhcp setroute
no shutdown
!
interface Ethernet1/2
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/3
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/4
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/5
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/6
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/7
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/8
no shutdown
switchport
switchport mode access
switchport access vlan 1
```



```

!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd address 192.168.45.10-192.168.45.12 management
dhcpd enable inside
dhcpd enable management
!
http server enable
http 192.168.45.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 inside
!
dns domain-lookup outside
dns server-group DefaultDNS
  name-server 208.67.222.222 outside
  name-server 208.67.220.220 outside
!

```

Firepower 1100 默认配置

Firepower 1100 的出厂默认配置包含以下配置：

- 内部→外部流量 - 以太网 1/1（外部），以太网 1/2（内部）
- 外部 IP 地址来自 DHCP，内部 IP 地址—192.168.1.1
- 管理—管理 1/1（管理），IP 地址来自 DHCP
- DHCP 服务器在内部接口上
- 默认路由 来自外部 DHCP，管理 DHCP
- ASDM 访问 - 允许管理和内部主机。内部主机限制为 192.168.1.0/24 网络。
- NAT - 从内部到外部所有流量的接口 PAT。
- DNS 服务器 - OpenDNS 服务器已预配置。

配置由以下命令组成：

```

interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside

```

```

security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
object network obj_any
 subnet 0.0.0.0 0.0.0.0
 nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
 name-server 208.67.222.222 outside
 name-server 208.67.220.220 outside
!

```

Firepower 2100 设备模式默认配置

默认情况下，Firepower 2100 在设备模式下运行。



注释 对于9.13(1)之前的版本，平台模式是默认选项和唯一选项。如果从平台模式升级，则会保留平台模式。

设备模式下 Firepower 2100 的出厂默认配置包含以下配置：

- 内部→外部流量 - 以太网 1/1（外部），以太网 1/2（内部）
- 外部 IP 地址来自 DHCP，内部 IP 地址—192.168.1.1
- DHCP 中的管理 IP 地址 - 管理 1/1（管理）
- DHCP 服务器在内部接口上
- 默认路由 来自外部 DHCP，管理 DHCP
- ASDM 访问 - 允许管理和内部主机。内部主机限制为 192.168.1.0/24 网络。
- NAT - 从内部到外部所有流量的接口 PAT。
- DNS 服务器 - OpenDNS 服务器已预配置。

配置由以下命令组成：

```

interface Management1/1
 management-only
 nameif management
 security-level 100
 ip address dhcp setroute

```

```

no shutdown
!
interface Ethernet1/1
 nameif outside
 security-level 0
 ip address dhcp setroute
 no shutdown
!
interface Ethernet1/2
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 no shutdown
!
object network obj_any
 subnet 0.0.0.0 0.0.0.0
 nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 management
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
 name-server 208.67.222.222 outside
 name-server 208.67.220.220 outside
!

```

Secure Firewall 3100 默认配置

Secure Firewall 3100 的默认出厂配置用于配置以下内容:

- 内部→外部流量 - 以太网 1/1（外部），以太网 1/2（内部）
- 外部 IP 地址来自 DHCP，内部 IP 地址—192.168.1.1
- 管理—管理 1/1（管理），IP 地址来自 DHCP
- DHCP 服务器在内部接口上
- 默认路由 来自外部 DHCP，管理 DHCP
- ASDM 访问 - 允许管理和内部主机。内部主机限制为 192.168.1.0/24 网络。
- NAT - 从内部到外部所有流量的接口 PAT。
- DNS 服务器 - OpenDNS 服务器已预配置。

配置由以下命令组成:

```

interface Management1/1
 management-only
 nameif management
 security-level 100

```

```

    ip address dhcp setroute
    no shutdown
!
interface Ethernet1/1
    nameif outside
    security-level 0
    ip address dhcp setroute
    no shutdown
!
interface Ethernet1/2
    nameif inside
    security-level 100
    ip address 192.168.1.1 255.255.255.0
    no shutdown
!
object network obj_any
    subnet 0.0.0.0 0.0.0.0
    nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
    name-server 208.67.222.222 outside
    name-server 208.67.220.220 outside
!

```

安全防火墙4200默认配置

Cisco Secure Firewall 4200 的默认出厂配置用于配置以下内容：

- 内部→外部流量 - 以太网 1/1（外部），以太网 1/2（内部）
- 外部 IP 地址来自 DHCP，内部 IP 地址—192.168.1.1
- 管理—管理 1/1（管理），IP 地址来自 DHCP
- **DHCP 服务器**在内部接口上
- 默认路由 来自外部 DHCP，管理 DHCP
- **ASDM 访问** - 允许管理和内部主机。内部主机限制为 192.168.1.0/24 网络。
- **NAT** - 从内部到外部所有流量的接口 PAT。
- **DNS 服务器** - OpenDNS 服务器已预配置。

配置由以下命令组成：

```

interface Management1/1
    management-only
    nameif management

```

```
security-level 100
ip address dhcp setroute
no shutdown
!
interface Ethernet1/1
 nameif outside
 security-level 0
 ip address dhcp setroute
 no shutdown
!
interface Ethernet1/2
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 no shutdown
!
object network obj_any
 subnet 0.0.0.0 0.0.0.0
 nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
 name-server 208.67.222.222 outside
 name-server 208.67.220.220 outside
!
```

Firepower 4100/9300 机箱 默认配置

在 Firepower 4100/9300 机箱上部署 ASA 时，可预设置许多可供您使用 ASDM 连接到 Management 0/0 接口的参数。典型配置包括以下设置：

- 管理接口：
 - 您选择的管理类型接口已在 Firepower 4100/9300 机箱管理引擎上定义
 - 命名为 “management”
 - 您选择的 IP 地址
 - 安全级别为 0
 - 管理专用
- 通过管理接口的默认路由
- ASDM 访问 - 允许所有主机。

独立设备的配置包括以下命令。有关集群设备的其他配置，请参阅[创建 ASA 集群](#)。

```

interface <management_ifc>
  management-only
  ip address <ip_address> <mask>
  ipv6 address <ipv6_address>
  ipv6 enable
  nameif management
  security-level 0
  no shutdown
!
http server enable
http 0.0.0.0 0.0.0.0 management
http ::/0 management
!
route management 0.0.0.0 0.0.0.0 <gateway_ip> 1
ipv6 route management ::/0 <gateway_ipv6>

```

ISA 3000 的默认配置

ISA 3000 的默认出厂配置如下：

- **透明防火墙模式** - 透明防火墙是第 2 层防火墙，充当“嵌入式防火墙”或“隐藏防火墙”，并且不会被视作为所连接设备的路由器跃点。
- **1 个网桥虚拟接口** - 所有成员接口都位于同一网络中（**IP 地址未预先配置；必须进行设置以与您的网络相匹配**）：GigabitEthernet 1/1 (outside1)、GigabitEthernet 1/2 (inside1)、GigabitEthernet 1/3 (outside2)、GigabitEthernet 1/4 (inside2)
- 所有内部和外部接口均可互相通信。
- **管理 1/1 接口** - 192.168.1.1/24 用于 ASDM 访问。
- 用于管理上的客户端的 **DHCP**。
- **ASDM 访问** - 允许管理主机。
- 为以下接口对启用了**硬件旁路**：GigabitEthernet 1/1 和 1/2；GigabitEthernet 1/3 和 1/4



注释 当 ISA 3000 断电并进入硬件旁路模式时，只有上述接口对能够通信；inside1 和 inside2 以及 outside1 和 outside2 将不再能通信。这些接口之间的任何现有连接都将断开。在恢复供电后，将随着 ASA 接管流而发生短暂的连接中断。

配置由以下命令组成：

```

firewall transparent

interface GigabitEthernet1/1
  bridge-group 1
  nameif outside1
  security-level 0
  no shutdown

```

```
interface GigabitEthernet1/2
  bridge-group 1
  nameif inside1
  security-level 100
  no shutdown
interface GigabitEthernet1/3
  bridge-group 1
  nameif outside2
  security-level 0
  no shutdown
interface GigabitEthernet1/4
  bridge-group 1
  nameif inside2
  security-level 100
  no shutdown
interface Management1/1
  management-only
  no shutdown
  nameif management
  security-level 100
  ip address 192.168.1.1 255.255.255.0
interface BVI1
  no ip address

access-list allowAll extended permit ip any any
access-group allowAll in interface outside1
access-group allowAll in interface outside2

same-security-traffic permit inter-interface

hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4

http server enable
http 192.168.1.0 255.255.255.0 management

dhcpd address 192.168.1.5-192.168.1.254 management
dhcpd enable management
```

ASA Virtual 部署配置

部署 ASA virtual 时，可预设置许多可供您使用 ASDM 连接到 Management 0/0 接口的参数。典型配置包括以下设置：

- 路由或透明防火墙模式
- Management 0/0 接口：
 - 命名为 “management”
 - IP 地址或 DHCP
 - 安全级别为 0
- 管理主机 IP 地址的静态路由（如果其没有位于管理子网中）
- 启用或禁用 HTTP 服务器

- 管理主机 IP 地址的 HTTP 访问
- （可选）GigabitEthernet 0/8 的故障转移链路 IP 地址和 Management0/0 备用 IP 地址
- DNS 服务器
- 智能许可 ID 令牌
- 智能许可吞吐量水平和 基础 功能层
- （可选）Smart Call Home HTTP 代理 URL 和端口
- （可选）SSH 管理设置：
 - 客户端 IP 地址
 - 本地用户名和密码
 - 使用本地数据库进行 SSH 所需的身份验证
- （可选）启用或禁用 REST API



注释 要向思科许可颁发机构成功注册 ASA virtual，ASA virtual需要访问互联网。部署之后，可能需要执行其他配置，以实现互联网访问和成功注册许可证。

有关独立设备，请参阅以下配置示例：

```
interface Management0/0
  nameif management
  security-level 0
  ip address ip_address

  no shutdown
  http server enable
  http management_host_IP mask management
  route management management_host_IP mask gateway_ip 1
  dns server-group DefaultDNS
  name-server ip_address
  call-home
  http-proxy ip_address port port
  license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
  aaa authentication ssh console LOCAL
  username username password password
  ssh source_IP_address mask management
  rest-api image boot:/path
  rest-api agent
```



注释 基础许可证过去称为“标准”许可证。

有关故障转移对中的主要设备，请参阅以下配置示例：

```

nameif management
  security-level 0
  ip address ip_address standby standby_ip

  no shutdown
route management management_host_IP mask gateway_ip 1
http server enable
http management_host_IP mask management
dns server-group DefaultDNS
  name-server ip_address
call-home
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent
failover
failover lan unit primary
failover lan interface fover gigabitethernet0/8
failover link fover gigabitethernet0/8
failover interface ip fover primary_ip mask standby standby_ip

```

开始配置

要配置并监控 ASA，请执行以下步骤。



注释 ASDM 最多支持 512 KB 的配置。如果超出此量，可能会遇到性能问题。请参阅[增加 ASDM 配置内存，第 10 页](#)。

过程

- 步骤 1** 要使用启动向导进行初始配置，请依次选择 **Wizards > Startup Wizard**。
- 步骤 2** 要使用 IPsec VPN 向导配置 IPsec VPN 连接，请依次选择向导 > **IPsec VPN 向导**，然后完成系统显示每个屏幕。
- 步骤 3** 要使用 SSL VPN 向导配置 SSL VPN 连接，请依次选择向导 > **SSL VPN 向导**，然后完成系统显示的每个屏幕。
- 步骤 4** 要配置高可用性和可扩展性设置，请依次选择 **Wizards > High Availability and Scalability Wizard**。
- 步骤 5** 要使用数据包捕获向导配置数据包捕获，请依次选择 **Wizards > Packet Capture Wizard**。
- 步骤 6** 要显示 ASDM GUI 中可用的不同颜色和样式，请依次选择视图 > **办公室外观和体验**。

步骤 7 要配置功能，请点击工具栏上的 **Configuration** 按钮，然后点击其中一个功能按钮以显示相关联的配置窗格。

注释 如果 Configuration 屏幕为空，请点击工具栏上的 **Refresh** 以显示屏幕内容。

步骤 8 要监控 ASA，请点击工具栏上的 **Monitoring** 按钮，然后点击功能按钮来显示关联的监控窗格。

在 ASDM 中使用命令行界面工具

本节介绍如何使用 ASDM 输入命令以及如何处理 CLI。

使用命令行界面工具

该功能可提供基于文本的工具，用于向 ASA 发送命令并查看结果。

可通过 CLI 工具输入的命令取决于用户权限。在主 ASDM 应用窗口底部的状态栏中查看权限级别，以确保拥有执行特权级别 CLI 命令所需的权限。

开始之前

- 通过 ASDM CLI 工具输入的命令与通过 ASA 终端连接输入的命令可能以不同方式运行。
- 命令错误 - 如果由于输入错误命令而出现错误，则会跳过错误命令，并处理剩余命令。Response 区域将显示消息，提醒您是否出现错误，并且显示其他相关信息。
- 交互式命令 - CLI 工具不支持交互式命令。要在 ASDM 中使用这些命令，请使用 **noconfirm** 关键字（如果可用），如以下命令所示：

```
crypto key generate rsa modulus 1024 noconfirm
```

- 避免与其他管理员冲突 - 多个管理用户可更新 ASA 的运行配置。使用 ASDM CLI 工具对配置进行更改之前，检查是否存在其他活动管理会话。如果多个用户同时配置 ASA，则最近的更改生效。

要查看当前在同一 ASA 上的其他活动管理会话，请依次选择 **Monitoring > Properties > Device Access**。

过程

步骤 1 在主 ASDM 应用窗口中，依次选择 **工具 > 命令行界面**。

系统将显示 **Command Line Interface** 对话框。

步骤 2 选择需要的命令类型（单行或多行），然后从下拉列表中选择命令，或在提供的字段中键入命令。

- 步骤 3** 点击 **Send** 以执行命令。
- 步骤 4** 要输入新命令，请点击 **Clear Response**，然后选择（或键入）要执行的其他命令。
- 步骤 5** 选中 **Enable context-sensitive help (?)** 复选框，为该功能提供情景相关帮助。取消选中该复选框以禁用情景相关帮助。
- 步骤 6** 关闭 **Command Line Interface** 对话框后，如果已更改配置，请点击 **Refresh** 以查看 ASDM 中的更改。

在设备上显示 ASDM 忽略的命令

该功能可显示 ASDM 不支持的命令列表。通常，ASDM 忽略这些命令。ASDM 不从运行配置更改或删除这些命令。有关详细信息，请参阅[不受支持的命令](#)。

过程

-
- 步骤 1** 在主 ASDM 应用窗口中，依次选择工具 > 显示被设备上的 ASDM 忽略的命令。
- 步骤 2** 完成后点击 **OK**。

将配置更改应用于连接

更改配置的安全策略后，所有新连接将使用新安全策略。现有连接将继续使用在连接建立时配置的策略。原连接的 **show** 命令输出反映原配置，在某些情况下将不包括关于原连接的数据。

例如，如果要从接口删除 QoS **service-policy**，然后重新添加修改版本，则 **show service-policy** 命令仅显示与匹配新服务策略的新连接相关联的 QoS 计数器；旧策略的现有连接不再显示在命令输出中。

要确保所有连接使用新策略，需要断开当前连接，以便其使用新策略重新连接。

要断开连接，请输入以下命令：

```
• clear conn [all] [protocol {tcp | udp}] [address src_ip [-src_ip] [netmask mask]] [port src_port [-src_port]] [address dest_ip [-dest_ip] [netmask mask]] [port dest_port [-dest_port]]
```

该命令可在任何状态中终止连接。要查看所有当前连接，请参阅 **show conn** 命令。

如果不带参数，该命令将清除所有受影响的出站连接。要清除入站连接（包括当前的管理会话），请使用 **all** 关键字。要根据源 IP 地址、目标 IP 地址、端口和/或协议清除特定连接，可以指定所需选项。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。