管理访问

本章介绍如何通过 Telnet、SSH 和 HTTPS（使用 ASDM）访问 ASA 进行系统管理，如何对用户进行身份验证和授权以及如何创建登录横幅。

配置管理远程访问

本节介绍如何为 ASDM、Telnet 或 SSH 配置 ASA 访问，以及其他管理参数，例如登录横幅。

配置 HTTPS、Telnet 或 SSH 的 ASA 访问

本部分介绍如何配置 HTTPS，包括 ASDM 和 CSM、Telnet 或 SSH 的 ASA 访问。请参阅以下准则：

- 如要访问 ASA 接口进行管理访问，也不需要允许主机 IP 地址的访问规则，只需根据本章内各节配置管理访问。但是，如果您配置 HTTP 重定向以将 HTTP 连接自动重定向至 HTTPS，则必须启用允许 HTTP 的访问规则；否则，该接口无法侦听 HTTP 端口。
- 除了进入ASA时所经由的接口以外，不支持对其他接口进行管理访问。例如，如果管理主机位于外部接口上，则只能直接向外部接口发起管理连接。此规则的唯一例外是通过VPN连接。请参阅配置 VPN 隧道上的管理访问，第 10 页。
- ASA 允许：
  - 每个情景最多 5 个并发 Telnet 连接，在所有情景中最多分为 100 个连接（如果有）。
  - 每个情景最多 5 个并发 SSH 连接，在所有情景中最多分为 100 个连接（如果有）。
  - 在单情景模式下，最多30个ASDM并发会话。在多情景模式下，每个情景最多 5 个并发 ASDM 会话，在所有情景中最多分为 32 个 ASDM 实例。

ASDM 会话使用两个 HTTPS 连接：一个用于监控（始终存在），另一个用于进行配置更改（仅当进行更改时才存在）。例如，多情景模式系统限制为 32 个 ASDM 会话表示 HTTPS 会话数限制为 64。

- 在单情景模式或每个情景（如果可用）中，最多有6个并发非ASDM HTTPS会话，所有情景中最多有100个HTTPS会话。

配置用于 ASDM 的 HTTPS 访问、其他客户端

本部分介绍如何配置 HTTPS，包括 ASDM 和 CSM 的 ASA 访问。

如果在同一接口上同时启用 SSL (**webvpn** > **启用** 接口) 和 HTTPS 访问，则可以从 **https://***ip_address* 访问 Secure Client，从 **https://***ip_address*/**admin**访问端口 443。如果还启用了 HTTPS 身份验证 (配置用于 CLI、 ASDM 和 enable 命令访问的身份验证，第 16 页)，则必须为 ASDM 访问指定不同的端口。

开始之前

- 在多情景模式下，请在情景执行空间中完成本程序。要从系统更改为情景配置，请在 **Configuration > Device List** 窗格中双击主用设备 IP 地址下的情景名称。

过程

步骤 1 依次选择**配置** > **设备管理** > **管理访问** > **ASDM/HTTPS/Telnet/SSH**，然后点击**添加**。

系统将显示**添加设备访问配置**对话框。

步骤 2 选择 **ASDM/HTTPS**。

步骤 3 选择管理接口并设置允许的主机 IP 地址，然后点击**确定**。

指定任何已命名的接口。对于网桥组，请指定网桥组成员接口。对于仅 VPN 管理访问（请参阅 配置 VPN 隧道上的管理访问，第 10 页），请指定命名的 BVI 接口。

步骤 4 如需进行证书身份验证，在 **Specify the interface requires client certificate to access ASDM** 区域中，点击 **Add** 以指定成功身份验证必须匹配的接口和可选证书映射。请查看**配置** > **远程访问 VPN** > **网络（客户端）访问** > **高级** > **IPSec** > **证书到连接映射** > **规则**，以创建证书映射。有关详细信息，请参阅配置 ASDM 证书身份验证，第 17 页。

步骤 5 配置 **HTTP 设置**。

- **启用 HTTP 服务器** - 启用 HTTPS 服务器。
- **端口号** - 设置端口号。默认值为 443。
- **空闲超时** - 设置 ASDM 连接的空闲超时，范围为 1-1440 分钟。默认值为 20 分钟。ASA 会断开在设置的时间段内处于空闲状态的 ASDM 连接。
- **会话超时** - 为 ASDM 会话设置会话超时，范围为 1-1440 分钟。此超时默认处于禁用状态。ASA 会断开超过设置时间段的 ASDM 会话。

- **连接会话超时** - 设置所有 HTTPS 连接（包括 ASDM、WebVPN 和其他客户端）的空闲超时，范围为 10-86400 秒。此超时默认处于禁用状态。ASA 会断开在设置的时间段内处于空闲状态的连接。如果同时设置**空闲超时**和**连接会话超时**，则将优先以**连接会话超时**为准。

步骤 6 点击“**应用**”。

步骤 7 （可选）允许基于非浏览器的 HTTPS 客户端访问 ASA 上的 HTTPS 服务。默认情况下，允许 ASDM、CSM 和 REST API。

许多专业客户端（例如，python 库、curl 和 wget）不支持跨站请求伪造 (CSRF) 基于令牌的身份验证，因此，您需要特别允许这些客户端使用 ASA 基本身份验证方法。出于安全考虑，您应该只允许所需的客户端。

a) **配置** > **设备管理** > **管理访问** > **HTTP 非浏览器客户端支持**，然后点击**添加**。

b) 在 **HTTP 报头的用户代理字符串字段**中，在 HTTP 请求的 HTTP 报头中指定客户端的用户代理字符串。

您可以指定完整字符串或部分字符串；部分字符串必须与用户代理字符串的开头匹配。建议使用完整的字符串以提高安全性。请注意，文件夹名称区分大小写。

例如，**curl** 将匹配以下用户代理字符串：

```
curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic
ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

curl 将不匹配以下用户代理字符串：

```
abcd curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1
Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

curl 将不匹配以下用户代理字符串：

```
curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic
ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

配置 SSH 访问

本部分介绍如何配置 SSH 的 ASA 访问。请参阅以下准则：

- 要访问 ASA 接口以进行 SSH 访问，亦无需允许主机 IP 地址的访问规则。您只需按照本部分配置 SSH。
- 除了进入 ASA 时所经由的接口以外，不支持对其他接口进行 SSH 访问。例如，如果 SSH 主机位于外部接口上，则只能直接向外部接口发起管理连接。此规则的唯一例外是通过 VPN 连接（仅 ASA SSH 协议栈支持）。请参阅配置 VPN 隧道上的管理访问，第 10 页。
- ASA 允许每个情景/单模式最多有 5 个并发 SSH 连接，在所有情景中最多分为 100 个连接。但是，由于配置命令可能会锁定正在更改的资源，因此您应一次在一个SSH会话中进行更改，以确保正确应用所有更改。

- 默认情况下，ASA 使用 CiscoSSH 堆栈，它基于。您可以改为启用专有 ASA SSH 堆栈。CiscoSSH 支持：
  - FIPS 合规性
  - 定期更新，包括来自思科和开源社区的更新

  请注意，思科SSH堆栈不支持：
  - 通过VPN通过SSH连接到其他接口（管理访问）
  - EDDSA密钥对
  - FIPS模式下的RSA密钥对

  如果需要这些功能，应继续使用ASA SSH堆栈。

  CiscoSSH 堆栈的 SCP 功能略有变化：要使用 ASA **copy** 命令将文件复制到 SCP 服务器或从 SCP 服务器复制文件，您必须使用命令在 ASA 上为 SCP 服务器子网/主机启用 SSH 访问权限。
- 仅支持 SSH 版本 2。
- 不再支持 SSH 默认用户名。使用 SSH 以及 **pix** 或 **asa** 用户名和登录密码无法再连接至 ASA。要使用 SSH，必须通过依次选择 **Configuration** > **Device Management** > **Users/AAA** > **AAA Access** > **Authentication** 来配置 AAA 身份验证；然后通过依次选择 **Configuration** > **Device Management** > **Users/AAA** 来定义本地用户。如果要使用 AAA 服务器而不是本地数据库进行身份验证，建议也将本地身份验证配置为备用方法。

开始之前

在多情景模式下，请在情景执行空间中完成本程序。要从系统更改为情景配置，请在 **Configuration** > **Device List** 窗格中双击主用设备 IP 地址下的情景名称。

要设置 SSH 堆栈，请在**配置 (Configuration)** > **设备管理 (Device Management)** > **SSH 堆栈 (SSH Stack)** 上的系统空间中完成配置。

过程

步骤 1 依次选择**配置** > **设备管理** > **管理访问** > **ASDM/HTTPS/Telnet/SSH**，然后点击**添加**。

系统将显示**添加设备访问配置**对话框。

步骤 2 选择 **SSH**。

步骤 3 选择管理接口并设置允许的主机 IP 地址，然后点击**确定**。

指定任何已命名的接口。对于网桥组，请指定网桥组成员接口。对于仅 VPN 管理访问（请参阅 配置 VPN 隧道上的管理访问，第 10 页），请指定命名的 BVI 接口。

步骤 4 （可选） 配置 **SSH 设置**。

- **SSH 堆栈** - 选择 **ASA** 或**思科**。

注释　在多情景模式下，请参阅**配置 (Configuration)** > **设备管理 (Device Management)** > **SSH 堆栈 (SSH Stack)**。

- **SSH 超时** - 设置超时时间，范围为 1 到 60 分钟。默认值为 5 分钟。在大多数情况下，默认持续时间都太短，应增加为直到完成所有前期测试和故障排除所需的时间。
- **Key Exchange Hostkey** - 默认情况下，如果密钥存在，ASA 会尝试按以下顺序使用：EdDSA、ECDSA，然后是 RSA。如果明确选择 RSA 密钥，则必须生成 2048 位或更高的密钥。为了实现升级兼容性，仅当使用默认主机密钥设置时，ASA才会使用较小的RSA主机密钥。更高版本中将会删除对 RAS 密钥的支持，因此我们建议改为使用其他支持的密钥类型。
- **DH Key Exchange**（仅限管理员情景），请点击相应的单选按钮，以选择 Diffie-Hellman (DH) Key Exchange Group。如果未指定 DH 群密钥交换方法，则使用 DH 群 14 SHA256 密钥交换方法。有关使用 DH 密钥交换方法的详细信息，请参阅 RFC 4253。您只能在管理情景中设置密钥交换；此值供所有情景使用。

步骤 5 点击“**应用**”。

步骤 6 配置 SSH 用户身份验证。

a) （适用于密码访问）依次选择**配置** > **设备管理** > **用户/AAA** > **AAA 访问** > **身份验证**。

AAA 身份验证不影响使用 **Public Key Using PKF** 选项对用户名进行本地公共密钥身份验证。ASA 隐式使用本地数据库进行公共密钥身份验证。SSH 身份验证仅影响用户名与密码。如果要允许本地用户进行公共密钥身份验证或使用密码，您需要使用此程序显式配置本地身份验证，以允许进行密码访问。

b) 选中 **SSH** 复选框。

c) 从 **Server Group** 下拉列表中选择 **LOCAL** 数据库（或 AAA 服务器）。

d) 点击 **Apply**。

e) 添加本地用户。或者，您可以使用 AAA 服务器进行用户访问，但建议使用本地用户名。依次选择 **Configuration** > **Device Management** > **Users/AAA** > **User Accounts**，然后点击 **Add**。

系统将显示“**添加用户帐户-身份**”对话框。

f) 输入用户名和密码，然后确认密码。如果要强制用户使用公共密钥身份验证而不是密码身份验证，您可能需要不使用密码创建用户。如果您配置公共密钥身份验证以及密码，那么当您按照此程序显式配置 AAA 身份验证时，用户可以使用其中任意一种方法登录。

g) （可选） 要逐个用户启用公共密钥身份验证而不是/以及密码身份验证，请选择以下窗格之一：

- **公钥身份验证** - 粘贴 Base64 编码的公钥。您可以使用任何可生成 ssh-rsa、ecdsa-sha2-nistp 或 ssh-ed25519 原始密钥（不带证书）的 SSH 密钥生成软件（如 ssh keygen）生成密钥。您查看现有密钥时，该密钥会使用 SHA-256 散列算法进行加密。如果需要复制和粘贴散列密钥，请选中 **Key is hashed** 复选框。
- 要删除身份验证密钥，请点击 **Delete Key** 以显示确认对话框。点击 **Yes** 删除身份验证密钥，或者点击 **No** 保留该密钥。
- **Public Key Using PKF** - 选中 **Specify a new PKF key** 复选框，并粘贴或导入公共密钥文件 (PKF) 格式的密钥，密钥最大 4096 位。此格式用于由于过长而无法以 Base64 格式粘贴的密

钥。例如，可以使用 ssh keygen 生成 4096 位的密钥，然后将其转换为 PKF 格式，并在此窗格中导入。您查看现有密钥时，该密钥会使用 SHA-256 散列算法进行加密。如果需要复制和粘贴散列密钥，请将其从 **Public Key Authentication** 窗格复制并粘贴到已选中 **Key is hashed** 复选框的新 ASA 上的该窗格。

要删除身份验证密钥，请点击 **Delete Key** 以显示确认对话框。点击 **Yes** 删除身份验证密钥，或者点击 **No** 保留该密钥。

h) 点击 **OK**，然后点击 **Apply**。

步骤 7 生成密钥对（仅适用于物理 ASA）。

对于 ASAv，会在部署后自动创建密钥对。ASAv仅支持RSA密钥。

a) 依次选择**配置** > **设备管理** > **证书管理** > **身份证书**。
b) 点击 **Add**，然后点击 **Add a new identity certificate** 单选按钮。
c) 点击 **New**。
d) 在 **Add Key Pair** 对话框中，指定类型和大小，并点击 **Generate Now**。

使用的默认密钥对是 EdDSA，ECDSA，然后是 RSA。对于 RSA，请选择 2048 位或更大的大小。更高版本中将会删除对 RAS 密钥的支持，因此我们建议改为使用其他支持的密钥类型。

然后，您可以从证书对话框中“**取消**”，因为您只想生成密钥对。

注释 CisoSSH 堆栈不支持 EdDSA。

步骤 8 （可选） 配置 SSH 密码加密和集成算法：

a) 依次选择 **Configuration** > **Device Management** > **Advanced** > **SSH Ciphers**。
b) 选择“**加密**”，然后点击“**编辑**”。
c) 从 SSH cipher security level 下拉列表中，选择以下级别之一。

密码按其列出的顺序使用。对于预定义列表，从最高安全级别到最低安全级别列出。

- **全部 (All)** — 指定使用所有密码：3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr chacha20-poly1305@openssh.com aes192-ctr aes256-ctr
- **Custom** - 指定您在 **Cipher algorithms/custom string** 字段中输入的自定义密码加密配置字符串，以冒号隔开。
- **Fips** - 仅指定符合 FIPS 密码：aes128-cbc aes256-cbc
- **高 (High)** — 指定仅高强度密码：aes256-cbc chacha20-poly1305@openssh.com aes256-ctr
- **Low** - 指定低强度、中强度和高强度密码：3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr
- **Medium** - 指定中强度和高强度密码（默认）：3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr

d) 选择 **Integrity**，然后点击 **Edit**。
e) 从 SSH cipher security level 下拉列表中，选择以下级别之一：

- **All** - 指定使用所有密码：hmac-sha1 hmac-sha1-96 hmac-sha2-256 hmac-md5 hmac-md5-96
- **自定义** - 指定您在 **Cipher algorithms/custom string** 字段中输入的自定义密码加密配置字符串，以冒号隔开。
- **Fips** - 指定仅符合 FIPS 的密码：hmac-sha1 hmac-sha2-256
- **High** - 指定仅高 强度密码： hmac-sha2-256
- **低** - 指定低强度、中强度和高强度密码：hmac-sha1 hmac-sha1-96 hmac-md5 hmac-md5-96
- **Medium** - 指定中强度和高强度密码：hmac-sha1 hmac-sha1-96

步骤 9 启用安全复制服务器。

a) 视情景模式而定：

- 对于单模式，依次选择 **Configuration > Device Management > Management Access > File Access > Secure Copy (SCP)**。
- 对于系统中的多模式，依次选择 **Configuration > Device Management > Device Administration > Secure Copy**。

b) 选中 **Enable secure copy server** 复选框。

示例

以下示例将在 Linux 或 Macintosh 系统上为 SSH 生成一个共享密钥，并将其导入 ASA：

1. 在计算机上生成 的 EdDSA 公钥和私钥：

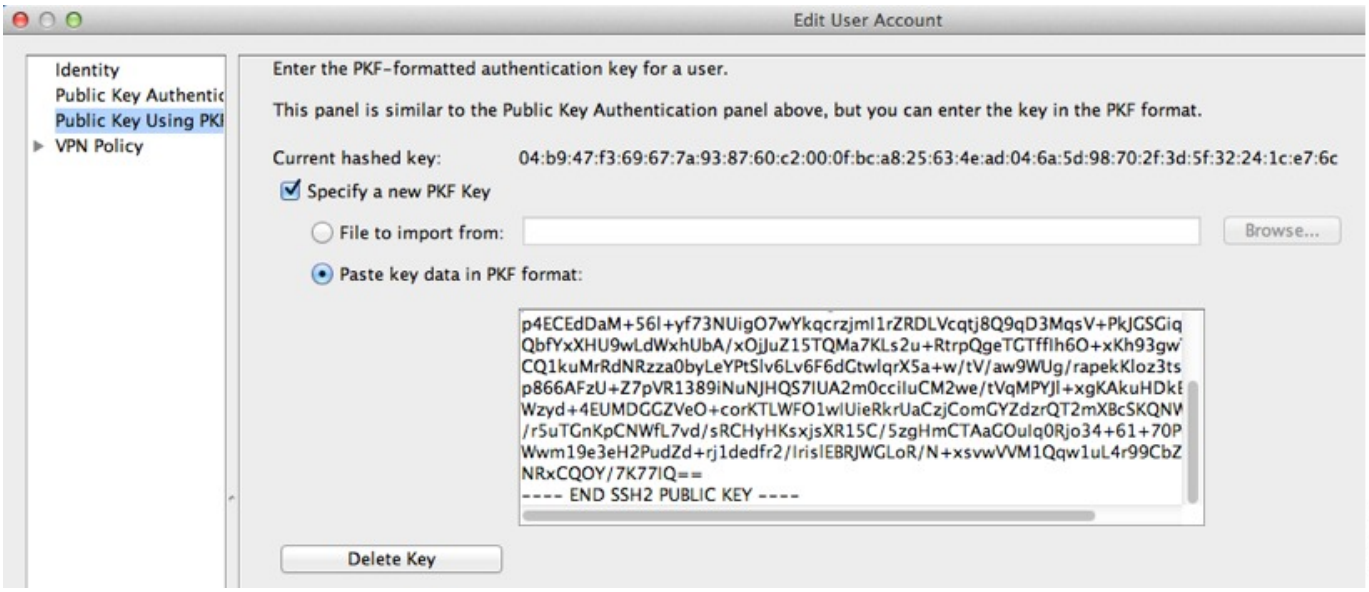
```
dwinchester-mac:~ dean$ ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/Users/dean/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase): key-pa$$phrase
Enter same passphrase again: key-pa$$phrase
Your identification has been saved in /Users/dean/.ssh/id_ed25519.
Your public key has been saved in /Users/dean/.ssh/id_ed25519.pub.
The key fingerprint is:
SHA256:ZHOjfJa3DpZG+qPAp9A5PyCEY0+Vzo2rkGHJpplpw8Q dean@dwinchester-mac

The key's randomart image is:
+--[ED25519 256]--+
|       .         |
|      o          |
|.  . + o+ o      |
|.E+ o ++.+ o     |
|B=.=   .S = .    |
|**  ooo. = o .   |
|.....o*.o = .    |
|  o .. *.+.o     |
|   .  . oo...    |
+----[SHA256]-----+
dwinchester-mac:~ dean$
```

2. 将密钥转换为 PKF 格式：

```
dwinchester-mac:~ dean$ cd .ssh
dwinchester-mac:.ssh dean$ ssh-keygen -e -f id_ed25519.pub
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "256-bit ED25519, converted by dean@dwinchester-mac from "
AAAAC3NzaC1lZDI1NTE5AAAAIDmIeTNfEOnuH0094p1MKX80fW2O216g4trnf7gwWe5Q
---- END SSH2 PUBLIC KEY ----
dwinchester-mac:.ssh dean$
```

3. 将密钥复制到剪贴板。

4. 在 ASDM 中，依次选择 **配置** > **设备管理** > **用户/AAA** > **用户帐户**，选择用户名，然后点击**编辑**。点击 **Public Key Using PKF** 并将密钥粘贴到窗口中：



5. 验证用户是否可以通过 SSH 连接到 ASA。对于密码，请输入您在创建密钥对时指定的 SSH 密钥密码。

```
dwinchester-mac:.ssh dean$ ssh dean@10.89.5.26
The authenticity of host '10.89.5.26 (10.89.5.26)' can't be established.
ED25519 key fingerprint is SHA256:6d1g2fe2Ovnh0GHJ5aag7GxZ68h6TD6txDy2vEwIeYE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.89.5.26' (ED25519) to the list of known hosts.
dean@10.89.5.26's password: key-pa$$phrase
User dean logged in to asa
Logins over the last 5 days: 2.  Last login: 18:18:13 UTC Jan 20 2021 from 10.19.41.227
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
asa>
```

以下示例显示与 ASA 的 SCP 会话。从外部主机上的客户端执行 SCP 文件传输。例如，在 Linux 中输入以下命令：

scp -v -pw *password* [*path*/]*source_filename*
username@asa_address:{**disk0**|**disk1**}:/[*path*/]*dest_filename*

-v 表示详细，如果您未指定 **-pw**，则会提示您输入密码。

配置 Telnet 访问

本部分介绍如何配置 Telnet 的 ASA 访问。除非使用 VPN 隧道中的 Telnet，否则无法使用 Telnet 访问最低安全级别的接口。

开始之前

- 在多情景模式下，请在情景执行空间中完成本程序。要从系统更改为情景配置，请在 **Configuration > Device List** 窗格中双击主用设备 IP 地址下的情景名称。
- 要使用 Telnet 访问 ASA CLI，请输入登录密码。使用 Telnet 前必须手动设置该密码。

过程

步骤 1 依次选择**配置** > **设备管理** > **管理访问** > **ASDM/HTTPS/Telnet/SSH**，然后点击**添加**。

系统将显示**添加设备访问配置**对话框。

步骤 2 选择 **Telnet**。

步骤 3 选择管理接口并设置允许的主机 IP 地址，然后点击**确定**。

指定任何已命名的接口。对于网桥组，请指定网桥组成员接口。对于仅 VPN 管理访问（请参阅 配置 VPN 隧道上的管理访问，第 10 页），请指定命名的 BVI 接口。

步骤 4 （可选） 设置 **Telnet 超时**。默认超时值为 5 分钟。

步骤 5 点击“**应用**”。

步骤 6 设置登录密码，然后才可以使用 Telnet 连接；没有默认密码。

a) 依次选择 **Configuration** > **Device Setup** > **Device Name/Password**。
b) 在 **Telnet Password** 区域选中 **Change the password to access the console of the security appliance** 复选框。
c) 输入旧密码（对于新 ASA 而言，将此字段留空）、新密码，然后确认新密码。
d) 点击**应用**。

为 ASDM 访问或无客户端 SSL VPN 配置 HTTP 重定向

您必须使用 HTTPS 连接至使用 ASDM 或无客户端 SSL VPN 的 ASA。为了方便起见，可以将 HTTP 管理连接重定向至 HTTPS。例如，通过重定向 HTTP，输入 **http://10.1.8.4/admin/** 或 **https://10.1.8.4/admin/** 均可访问位于该 HTTPS 地址的 ASDM 启动页面。

您可以重定向 IPv4 和 IPv6 流量。

开始之前

通常，您无需允许主机 IP 地址的访问规则。但是，对于 HTTP 重定向，您必须启用允许 HTTP 的访问规则；否则，该接口无法侦听 HTTP 端口。

过程

步骤 1 依次选择**配置** > **设备管理** > **HTTP 重定向**。

该表显示当前已配置的接口以及是否已在某个接口上启用重定向。

步骤 2 选择用于 ASDM 的接口，然后点击**编辑**。

步骤 3 在 **Edit HTTP/HTTPS Settings** 对话框中配置下列选项：

- **Redirect HTTP to HTTPS** - 重定向 HTTP 请求至 HTTPS。
- **HTTP Port** - 确定接口从其重定向 HTTP 连接的端口。默认值为 80。

步骤 4 点击**确定 (OK)**。

配置 VPN 隧道上的管理访问

如果 VPN 隧道在一个接口上终止，但是您需要通过访问不同的接口来管理 ASA，则必须将该接口标识为管理访问接口。例如，如果从外部接口进入 ASA，通过此功能可以使用 ASDM、SSH、 或 Telnet 连接到内部接口；或者，当从外部接口进入时，可以 Ping 内部接口。

注释 如果使用 CiscoSSH 堆栈（默认设置），则 SSH 不支持此功能。

注释 SNMP 不支持此功能。 对于基于 VPN 的 SNMP，我们建议在环回接口上启用 SNMP。您无需启用管理访问功能即可在环回接口上使用 SNMP。环回接口也适用于 SSH。

除了进入 ASA 时所经由的接口以外，不支持对其他接口进行 VPN 访问。例如，如果 VPN 访问位于外部接口上，则只能直接向外部接口发起连接。应在 ASA 的可直接访问的接口上启用 VPN，并使用域名解析，以便您不必记住多个地址。

通过以下类型的 VPN 隧道可以实现管理访问： IPsec 客户端、IPsec 站点间的简单 VPN 和 Secure Client SSL VPN 客户端。

开始之前

管理专用接口不支持此功能。

过程

步骤 1 依次选择**配置** > **设备管理** > **管理访问** > **管理接口**。

步骤 2 从“**管理访问接口**”下拉列表中选择具有最高安全级别的接口（内部接口）。

对于 Easy VPN 和站点间隧道，可以指定命名 BVI（在路由模式下）。

步骤 3 点击“**应用**”。

管理接口已指定，更改将保存到运行配置中。

更改控制台超时

控制台超时设置连接可保持处于特权 EXEC 模式下或配置模式下的时间；当达到超时时间后，会话将进入用户 EXEC 模式。默认情况下，会话不会超时。此设置不会影响可与控制台端口保持连接的时间，该连接永不超时。

过程

步骤 1 依次选择**配置** > **设备管理** > **管理访问** > **命令行 (CLI)** > **控制台超时**。

步骤 2 以分钟为单位定义一个新的超时值，要指定不受限制的时间，请输入 **0**。默认值为 0。

步骤 3 点击“**应用**”。

超时值更改将保存到运行配置中。

自定义 CLI 提示符

利用为提示符添加信息这项功能，可以大体了解在您有多个模块时登录哪一台 ASA。故障转移起价你，如果两台 ASA 具有相同的主机名，则此功能非常有用。

在多情景模式中，您可以在登录到系统执行空间或管理情景时查看扩展的提示符。在非管理情景中，您仅可看到默认提示符，即主机名和情景名称。

默认情况下，提示符显示 ASA 的主机名。在多情景模式下，提示符还显示情景名称。在 CLI 提示符中可以显示以下项目：

cluster-unit	显示集群设备名称。集群中的每台设备都有一个唯一的名称。
context	（仅多情景模式）显示当前情景的名称。
domain	显示域名。
hostname	显示主机名。

priority	显示故障转移优先级 pri（主要）或 sec（辅助）。
state	显示设备的流量传递状态或角色。 对于故障转移，会面向 state 关键字显示以下值： • **act** - 已启用故障转移，设备正在传递流量。 • **stby** - 已启用故障转移，设备未在传递流量，并且处于备用、故障或其他非活动状态。 • **actNoFailover** - 未启用故障转移，设备正在传递流量。 • **stbyNoFailover** - 未启用故障转移，设备未在传递流量。这可能会在待机设备上存在阈值以上的接口故障时发生。 对于集群，会显示控制和数据的值。

过程

步骤 1 依次选择**配置** > **设备管理** > **管理访问** > **命令行 (CLI)** > **CLI 提示符**。

步骤 2 执行以下任意操作以自定义提示符：

- 点击**可用提示 (Available Prompts)** 列表中的属性，然后点击**添加 (Add)**。可以将多个属性添加到提示符中。该属性将从 **Available Prompts** 列表移到 **Selected Prompts** 列表中。
- 点击**选定提示 (Selected Prompts)** 列表中的属性，然后点击**删除 (Delete)**。该属性将从 **Available Prompts** 列表移到 **Selected Prompts** 列表中。
- 点击**选定提示 (Selected Prompts)** 列表中的属性，然后点击**上移 (Move Up)** 或**下移 (Move Down)** 更改属性的显示顺序。

提示符将更改并显示在 **CLI Prompt Preview** 字段中。

步骤 3 点击 **Apply**。

新的提示符将保存到运行配置中。

配置登录横幅

您可以配置在用户连接至 ASA 时、在用户登录之前或在用户进入特权 EXEC 模式之前将显示的消息。

开始之前

- 从安全角度来看，重要的是横幅阻止未经授权的访问。请勿使用“欢迎”或“请”等措辞，因为它们像是在邀请入侵者。以下横幅为未经授权的访问设置正确的语调：

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk possible criminal consequences.
```

- 在添加横幅后，如果有以下情况，可能会关闭至 ASA 的 Telnet 或 SSH 会话：
  - 没有足够的系统内存可用来处理横幅消息。
  - 在尝试显示横幅消息时发生 TCP 写入错误。
- 有关横幅消息的准则，请参阅 RFC 2196。

过程

步骤 1 依次选择**配置** > **设备管理** > **管理访问** > **命令行 (CLI)** > **横幅**。

步骤 2 将横幅文本添加到为 CLI 创建的横幅类型所对应的字段中：

- 当用户在 CLI 中访问特权 EXEC 模式时，系统将显示会话 (exec) 横幅。
- 当用户登录 CLI 时，系统将显示 login 横幅。
- 当用户首次连接至 CLI 时，系统将显示 message-of-the-day (motd) 横幅。
- 当用户在通过用户身份验证后连接至 ASDM 时，系统将显示 ASDM 横幅。系统为用户提供两个选项解除横幅：
  - **Continue** - 解除横幅并完成登录。
  - **Disconnect** - 解除横幅并终止连接。
- 只允许使用 ASCII 字符，包括换行符（Enter 键按两个字符计算）。
- 请勿在横幅中使用制表符，因共并未保留在 CLI 版本中。
- 除了 RAM 和闪存对横幅长度的限制外，无其他长度限制。
- 通过包含字符串 **$(hostname)** 和 **$(domain)**，可以动态添加 ASA 的主机名或域名。
- 如果在系统配置中配置横幅，可以通过在情景配置中使用 **$(system)** 字符串来在情景中使用该横幅文本。

步骤 3 点击**应用 (Apply)**。

新的横幅保存到运行配置中。

设置管理会话配额

可以在 ASA 上建立允许的最大同时 ASDM、SSH 和 Telnet 会话数量。如果达到最大值，则不允许其他会话，并生成系统日志消息。如要防止系统锁定，则管理会话配额机制无法阻止控制台会话。

注释 在多情景模式下，如果最大 ASDM 会话数固定为 5，则无法配置会话数。

注释 如果您还为最大管理会话（SSH等）的每个情景设置资源限制，则将使用较低的值。

开始之前

在多情景模式下，请在情景执行空间中完成本程序。要从系统切换至情景配置，请在**配置** > **设备列表**窗格中，双击主用设备 IP 地址下方的情景名称。

过程

步骤 1 依次选择**配置** > **设备管理** > **管理访问** > **管理会话配额**。

步骤 2 输入最大并发会话数。

- 汇聚-设置介于1和15之间的汇聚会话数。默认值为 15。
- HTTP会话（HTTP Sessions）-设置最大HTTPS（ASDM）会话数，介于1和5之间。默认值为 5。
- SSH会话数-设置最大SSH会话数，介于1和5之间。默认值为 5。
- Telnet会话数-设置最大Telnet会话数，介于1和5之间。默认值为 5。
- User Sessions-设置每个用户的最大会话数，介于1和5之间。默认值为 5。

步骤 3 点击**应用**，保存配置更改。

为系统管理员配置 AAA

本部分介绍如何为系统管理员配置身份验证、管理授权和命令授权。

配置管理验证

配置用于 CLI 和 ASDM 访问的身份验证。

关于管理验证

如何登录 ASA 取决于是否启用身份验证。

关于 SSH 身份验证

请参阅以下行为了解在有身份验证和无身份验证的情况下进行 SSH 访问：

- 无身份验证时 - 在无身份验证的情况下，SSH 不可用。
- 身份验证 - 如果启用身份验证，请输入在 AAA 服务器或本地用户数据库中所定义的用户名和密码。对于公钥身份验证，ASA 仅支持本地数据库。 如果配置 SSH 公钥身份验证，则 ASA 隐式使用本地数据库。当您使用用户名和密码登录时，只需要明确配置 SSH 身份验证。您将进入用户 EXEC 模式。

关于 Telnet 身份验证

有关在使用身份验证和不使用身份验证的情况下的 Telnet 访问，请参阅以下行为：

- 无身份验证 - 如果不为 Telnet 启用任何身份验证，请勿输入用户名；您应该输入登录密码（。没有默认密码，因此您必须设置一个，才能通过 Telnet 连接到 ASA。您将进入用户 EXEC 模式。
- 有身份验证 - 如果启用 Telnet 身份验证，请输入在 AAA 服务器或本地用户数据库中所定义的用户名和密码。您将进入用户 EXEC 模式。

关于 ASDM 身份验证

有关在使用身份验证和不使用身份验证的情况下的 ASDM 访问，请参阅以下行为。您还可以配置证书身份验证，而不管是否使用 AAA 身份验证。

- 无身份验证 - 默认情况下，可以使用空的用户名以及通过设置的启用密码（默认为空）登录 ASDM。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。首次在CLI中输入命令时，系统会提示您更改密码；登录ASDM时不会强制执行此行为。 **enable** 请注意，如果在登录屏幕输入用户名和密码（而不是将用户名留空），则 ASDM 将检查本地数据库是否有匹配项。
- 证书身份验证 -（仅限单个、路由模式）您可以要求用户具备有效的证书。输入证书用户名和密码，ASA 会根据 PKI 信任点对证书进行验证。
- AAA 身份验证 - 启用 ASDM (HTTPS) 身份验证时，需要输入 AAA 服务器或本地用户数据库中定义的用户名和密码。不能再使用空用户名和启用密码登录 ASDM。
- AAA 身份验证加证书身份验证 -（仅限单个、路由模式）启用 ASDM (HTTPS) 身份验证时，需要输入 AAA 服务器或本地用户数据库中定义的用户名和密码。如果用户名和密码对于证书身份验证是不同的，系统将提示您输入它们。您可以选择预填充从证书派生的用户名。

关于串行身份验证

请参阅以下行为了解在有身份验证和无身份验证的情况下访问串行控制台端口：

- 无身份验证 - 如果不为串行访问启用任何身份验证，则不输入用户名或密码。您将进入用户 EXEC 模式。
- 身份验证 - 如果为串行访问启用身份验证，请输入在 AAA 服务器或本地用户数据库中所定义的用户名和密码。您将进入用户 EXEC 模式。

关于 Enable 身份验证

如要在登录后进入特权 EXEC 模式，请输入 **enable** 命令。此命令的工作方式取决于是否启用身份验证：

- No Authentication - 如果不配置 enable 身份验证，在输入 **enable** 命令，该密码默认留空。第一次输入 **enable** 命令时，系统会提示您更改密码。但是，如果不使用 enable 身份验证，在输入 **enable** 命令后，则不再以特定用户身份登录，这会影响基于用户的功能，如命令授权。为了保留用户名，请使用 enable 身份验证。
- Authentication - 如果配置 enable 身份验证，ASA 会提示您输入在 AAA 服务器或本地用户数据库上定义的用户名和密码。当执行命令授权时此功能特别有用，因为用户名在确定用户可以输入的命令时非常重要。

对于使用本地数据库的 enable 身份验证，可以使用 **login** 命令，来代替 **enable** 命令。**login** 命令会保留用户名，但不需要配置开启身份验证。

⚠

注意 如果您将可以访问 CLI 但您不希望其进入特权 EXEC 模式的用户添加到本地数据库中，则应该配置命令授权。在无命令授权的情况下，如果用户的权限级别为 2 或更高（2 是默认值），则用户可以在 CLI 使用自己的密码访问特权 EXEC 模式（以及所有命令）。或者，您可以使用 AAA 服务器而不是本地数据库进行身份验证，或将所有本地用户都设置为 1 级，以阻止使用 login 命令，这样就可以控制谁可以使用系统启用密码访问特权 EXEC 模式。

从主机操作系统到 ASA 的会话

有些平台支持将 ASA 作为单独的应用运行：例如，Catalyst 6500 上的 ASASM 或 Firepower 4100/9300 上的 ASA。对于从主机操作系统到 ASA 的会话，您可以配置串行和 Telnet 身份验证，具体取决于连接类型。

多情景模式下，无法在系统配置中配置任何 AAA 命令。但是，如果在管理员情景中配置 Telnet 或串行身份验证，则身份验证也适用于这些会话。在此情况下，使用管理员情景 AAA 服务器或本地用户数据库。

配置用于 CLI、 ASDM 和 enable 命令访问的身份验证

开始之前

- 配置 Telnet、SSH 或 HTTP 访问。
- 对于外部身份验证，请配置 AAA 服务器组。对于本地身份验证，请向本地数据库添加用户。
- HTTP 管理身份验证不支持 AAA 服务器组的 SDI 协议。

- 此功能不影响使用 **ssh authentication** 命令对本地用户名进行 SSH 公共密钥身份验证。ASA 隐式使用本地数据库进行公共密钥身份验证。此功能仅影响用户名与密码。如果要允许本地用户进行公共密钥身份验证或使用密码，您需要使用此程序显式配置本地身份验证，以允许进行密码访问。

过程

步骤 1 要对使用 **enable** 命令的用户进行身份验证，请依次选择**配置** > **设备管理** > **用户/AAA** > **AAA 访问** > **身份验证**，然后配置以下设置：

a) 选中 **Enable** 复选框。

b) 选择服务器组名称或 LOCAL 数据库。

c) （可选）如果选择 AAA 服务器，可以将 ASA 配置为在 AAA 服务器不可用时使用本地数据库作为回退方法。选中 **Use LOCAL when server group fails** 复选框。建议在本地数据库中使用与 AAA 服务器相同的用户名和密码，因为 ASA 提示符不会给出使用何种方法的任何指示。

步骤 2 要对访问 CLI 或 ASDM 的用户进行身份验证，请依次选择**配置** > **设备管理** > **用户/AAA** > **AAA 访问** > **身份验证**，然后配置以下设置：

a) 选中一个或多个以下复选框：

- **HTTP/ASDM** - 对使用 HTTPS 访问 ASA 的 ASDM 客户端进行身份验证。
- **Serial** - 对使用控制台端口访问 ASA 的用户进行身份验证。
- **SSH** - 对使用 SSH 访问 ASA 的用户进行身份验证（仅密码；公共密钥身份验证隐式使用本地数据库）。
- **Telnet** - 对使用 Telnet 访问 ASA 的用户进行身份验证。

b) 对于选中的每项服务选择服务器组名称或 LOCAL 数据库。

c) （可选）如果选择 AAA 服务器，可以将 ASA 配置为在 AAA 服务器不可用时使用本地数据库作为回退方法。选中 **Use LOCAL when server group fails** 复选框。建议在本地数据库中使用与 AAA 服务器相同的用户名和密码，因为 ASA 提示符不会给出使用何种方法的任何指示。

步骤 3 点击**应用**。

配置 ASDM 证书身份验证

无论是否有 AAA 身份验证，您都可以要求进行证书身份验证。ASA 将针对 PKI 信任点验证证书。

开始之前

仅在单个路由模式中支持此功能。

过程

步骤 1 依次选择**配置** > **设备管理** > **管理访问** > **ASDM/HTTPS/Telnet/SSH**。

步骤 2 在 **Specify the interface requires client certificate to access ASDM** 区域中，点击 **Add** 以指定成功身份验证必须匹配的接口和可选证书映射。

您应为每个接口配置证书身份验证，使得受信任/内部接口上的连接无需提供证书。请参阅**配置** > **站点间 VPN** > **高级** > **IPSec** > **连接映射证书** > **规则**创建证书映射。

步骤 3 （可选） 要设置 ASDM 用于从证书派生用户名的属性，依次选择 **Configuration** > **Device Management** > **Management Access** > **HTTP Certificate Rule**。

选择以下方法之一：

- **Specify the Certificate Fields to be used** - 从 **Primary Field** 和 **Secondary Field** 下拉列表中选择一个值。
- **Use the entire DN as the username**
- **Use script to select username** - 点击 **Add** 以添加脚本内容。

选中 **Prefill Username** 复选框可在提示身份验证时预填充用户名。如果用户名与您最初输入的不同，系统将显示一个新对话框，其中含有预填充的用户名。然后，您可以输入身份验证的密码。

默认情况下，ASDM 使用 CN OU 属性。

步骤 4 点击**应用**。

使用管理授权控制 CLI 和 ASDM 访问

ASA 使您可以在管理用户和远程访问用户进行身份验证时对他们加以区分。用户角色的区分可防止远程访问 VPN 和网络访问用户建立到 ASA 的管理连接。

开始之前

RADIUS 或 LDAP（映射的）用户

当用户通过 LDAP 进行身份验证时，可将本地 LDAP 属性及其值映射到 ASA 属性来提供特定授权功能。配置具有 0 和 15 之间的值的特权级别的 Cisco VSA CVPN3000-Privilege-Level。然后，将 LDAP 属性映射到 Cisco VAS CVPN3000-Privilege-Level。

当 RADIUS IETF **service-type** 属性作为 RADIUS 身份验证和授权请求的结果在访问接受消息中进行发送时，其用于表示授予通过身份验证的用户的服务类型

在访问接受消息中发送 RADIUS Cisco VSA **privilege-level** 属性 (Vendor ID 3076, sub-ID 220) 时，该属性用于表示用户的权限级别。

TACACS+ 用户

使用“service=shell”请求授权，服务器以 PASS 或 FAIL 作为响应。

本地用户

为给定用户名配置 **Access Restrictions** 选项。默认情况下，访问限制是 **Full Access**，允许对 **Authentication** 选项卡选项指定的任何服务进行完全访问。

管理授权属性

请参阅下表，了解管理授权的 AAA 服务器类型和有效值。ASA 使用这些值来确定管理访问的级别。

管理级别	**RADIUS/LDAP**（映射的）属性	**TACACS+** 属性	本地数据库属性
完全访问 - 允许完全访问**身份验证**选项卡选项所指定的任何服务	Service-Type 6（管理），Privilege-Level 1	PASS，特权级别 1	admin
部分访问 - 允许在您配置**身份验证**选项卡选项时访问 CLI 或 ASDM。但是，如果您使用 **Enable** 选项配置 **enable** 身份验证，则 CLI 用户无法使用 **enable** 命令访问 EXEC 特权模式。	Service-Type 7（NAS 提示），Privilege-Level 2 及更高级别 Framed (2) 和 Login (1) 服务类型按同一方式处理。	PASS，特权级别 2 及更高级别	nas-prompt
No Access - 拒绝管理访问。用户无法使用由 **Authentication** 选项卡选项指定的任何服务（不包括 **Serial** 选项；允许串行访问）。远程访问（IPsec 和 SSL）用户仍可对其远程访问会话进行身份验证并终止会话。所有其他服务类型（Voice、FAX 等）按同一方式处理。	Service-Type 5（出站）	FAIL	remote-access

其他准则

- 串行控制台访问不包含在管理授权中。
- 您还必须为管理访问配置 AAA 身份验证才能使用此功能。请参阅配置用于 CLI、 ASDM 和 enable 命令访问的身份验证，第 16 页。
- 如果您使用外部身份验证，则必须在启用此功能之前预配置 AAA 服务器组。
- HTTP 授权仅在单个路由模式下受支持。

过程

步骤 1 如要启用对 HTTP 会话的管理授权，请依次选择**配置** > **设备管理** > **用户/AAA** > **AAA 访问** > **授权**，然后选中**启用 ASA 命令访问授权**区域中的 **HTTP** 复选框。

注释 要配置 ASA 命令访问，请参阅配置本地命令授权，第 21 页。

步骤 2 要启用对 Telnet 和 SSH 会话的管理授权，请依次选择**配置** > **设备管理** > **用户/AAA** > **AAA 访问** > **授权**，然后选中**执行 exec 外壳访问授权**区域中的**启用**复选框。

步骤 3 选择 **Remote** 或 **Local** 单选按钮以指定用于 EXEC 外壳访问授权的服务器。

步骤 4 如要启用管理授权，请选中 **Allow privileged users to enter into EXEC mode on login** 复选框。

auto-enable 选项允许在特权 EXEC 模式下直接替换具有 Full Access 权限的用户。否则，用户将处于用户 EXEC 模式。

配置命令授权

如果要控制对命令的访问，可以通过ASA配置命令授权，在其中确定可供用户使用的命令。默认情况下，登录时可以访问用户 EXEC 模式，此模式仅提供最小数量的命令。输入 **enable** 命令时（或在使用本地数据库时输入 **login** 命令时），可以进入特权 EXEC 模式并访问高级命令（包括配置命令）。

可以使用两种命令授权方法之一：

- 本地权限级别
- TACACS+ 服务器权限级别

关于命令授权

您可以启用命令授权，以便只有授权用户可以输入命令。

支持的命令授权方法

可以使用两种命令授权方法之一：

- 本地权限级别 - 在 ASA 上配置命令权限级别。当本地、RADIUS 或 LDAP（如果将 LDAP 属性映射到 RADIUS 属性）用户面向 CLI 访问进行身份验证时，ASA 会为该用户指定由本地数据库、RADIUS 或 LDAP 服务器定义的权限级别。用户可以访问分配的权限级别及以下级别的命令。请注意，所有用户首次登录时都会进入用户 EXEC 模式（命令级别为 0 或 1）。用户需要使用 **enable** 命令再次进行身份验证才能进入特权 EXEC 模式（命令级别为 2 或更高），或使用 **login** 命令登录（仅限本地数据库）。

注释 您可以在本地数据库中没有任何用户，以及没有 CLI 也没有 **enable** 身份验证的情况下，使用本地命令授权。输入 **enable** 命令时，您需要输入系统启用密码，ASA 会为您指定级别 15。然后，您可以为每个级别创建启用密码，以便在输入 **enable** *n*（2 至 15）时，ASA 为您指定级别 *n*。除非启用本地命令授权，否则不使用这些级别。

- TACACS+ 服务器权限级别 - 在 TACACS+ 服务器上，配置用户或组在进行 CLI 访问的身份验证后可以使用的命令。用户在 CLI 输入的每个命令都使用 TACACS+ 服务器进行验证。

安全情景和命令授权

每个情景的 AAA 设置相互独立，不同情景之间不会共享这些设置。

配置命令授权时，必须分别配置每个安全情景。此配置能够实现对不同安全情境执行不同的命令授权。

当在安全情景之间切换时，管理员应知道登录时指定的用户名允许的命令在新情景会话中可能有所差异，或在新情景中可能根本无法配置该命令授权。如果管理员不知道安全情境之间的命令授权可能有所差异，就可能会对其造成困扰。

注释 系统执行空间不支持 AAA 命令；因此，命令授权在系统执行空间不可用。

命令权限级别

默认情况下，会为以下命令分配 0 级权限，为所有其他命令分配 15 级权限。

- **show checksum**
- **show curpriv**
- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

如果将任何配置模式命令移到低于 15 的级别，请确保也将“**configure**”命令移到同一级别，否则用户将无法进入配置模式。

配置本地命令授权

通过本地命令授权可以为 16 个权限级别（0 到 15）之一分配命令。默认情况下，会向每个命令分配 0 级或 15 级权限。您可以将每个用户定义在特定权限级别，每个用户可以输入分配的权限级别或以下级别的任何命令。ASA 支持在本地数据库、RADIUS 服务器或 LDAP 服务器（如果将 LDAP 属性映射到 RADIUS 属性）中定义的用户权限级别。

过程

步骤 1 依次选择**配置** > **设备管理** > **用户/AAA** > **AAA 访问** > **授权**。

步骤 2 选中 **Enable authorization for ASA command access** > **Enable** 复选框。

步骤 3 从 **Server Group** 下拉列表中选择 **LOCAL**。

步骤 4 当启用本地命令授权时，可以选择手动向单个命令或命令组分配权限级别，也可以启用预定义的用户帐户权限。

- 点击**设置 ASDM 定义的用户角色 (Set ASDM Defined User Roles)** 使用预定义的用户帐户权限。

  系统将显示 **ASDM Defined User Roles Setup** 对话框。点击**是 (Yes)** 使用预定义的用户帐户权限：**管理员 (Admin)**（15 级权限，可对所有 CLI 命令进行完全访问）；**只读 (Read Only)**（5 级权限，只读访问）；**仅监控 (Monitor Only)**（3 级权限，只能访问**监控**部分）。

- 点击**配置命令权限 (Configure Command Privileges)** 手动配置命令级别。

  系统将显示 **Command Privileges Setup** 对话框。您可以从 **Command Mode** 下拉列表中选择 **All Modes** 以查看所有命令，或者也可以选择配置模式以查看该模式中可用的命令。例如，如果选择情景，则可以查看该情景配置模式下的所有可用命令。如果某个命令可以在用户 EXEC 模式或特权 EXEC 模式下以及配置模式下输入，并且该命令在每个模式下执行不同的操作，则可以分别设置其在这些模式下的权限级别。

  Variant 列显示 show、clear 或 cmd。您可以仅为命令的显示、清除或配置形式设置权限。命令的配置形式通常是导致配置更改的形式，或者是以未修改的命令形式（无 show 或 clear 前缀），或者是以 no 形式。

  如要更改命令级别，请双击此命令或点击**编辑 (Edit)**。可将级别设置为 0 到 15。只能配置主命令的权限级别。例如，可以配置所有 **aaa** 命令的级别，但是不可以单独配置 **aaa authentication** 命令和 **aaa authorization** 命令的级别。

  要更改显示的所有命令的级别，请点击**全选 (Select All)**，然后点击**编辑 (Edit)**。

  点击**确定 (OK)** 接受更改。

步骤 5 （可选） 选中 **Perform authorization for exec shell access** > **Enable** 复选框，为命令授权启用 AAA 用户。如果没有此选项，则ASA仅支持本地数据库用户的权限级别，并将所有其他类型的用户默认设置为 15 级。

此命令还将启用管理授权。请参阅使用管理授权控制 CLI 和 ASDM 访问 ，第 18 页。

步骤 6 点击**应用 (Apply)**。

已分配授权设置，更改将保存到运行配置中。

在 Commands TACACS+ 服务器上配置命令

您可以在思科安全访问控制服务器 (ACS) TACACS+ 服务器上，为组或为单个用户将命令配置为共享配置文件组件。对于第三方 TACACS+ 服务器，请参阅服务器文档了解有关命令授权支持的详细信息。

请参阅以下在思科安全 ACS 3.1 版本中配置命令的准则；其中许多原则也适用于第三方服务器。

- ASA 将待授权的命令作为外壳命令发送，因此请在 TACACS+ 服务器上将命令配置为外壳命令。

注释 思科安全 ACS 可能包括名为“pix-shell”的命令类型。请勿将此类型用于 ASA 命令授权。

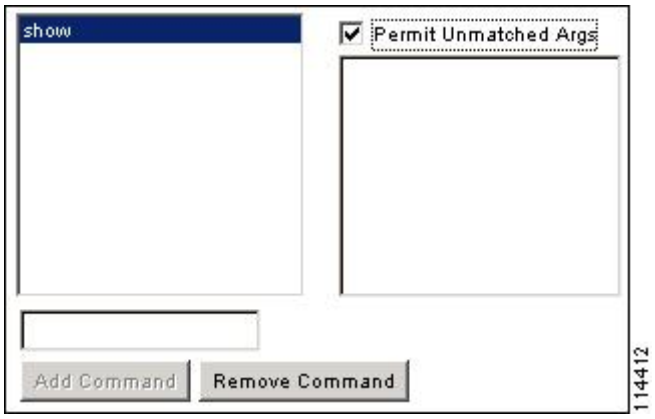
- 命令的第一个词被视为主命令。所有附加的单词都被视为参数，需要在其前面放置 **permit** 或 **deny**。

  例如，如要允许 **show running-configuration aaa-server** 命令，请向命令字段添加 **show running-configuration**，然后在参数字段键入 **permit aaa-server**。

- 通过选中 **Permit Unmatched Args** 复选框，可以允许未明确拒绝的所有命令参数。

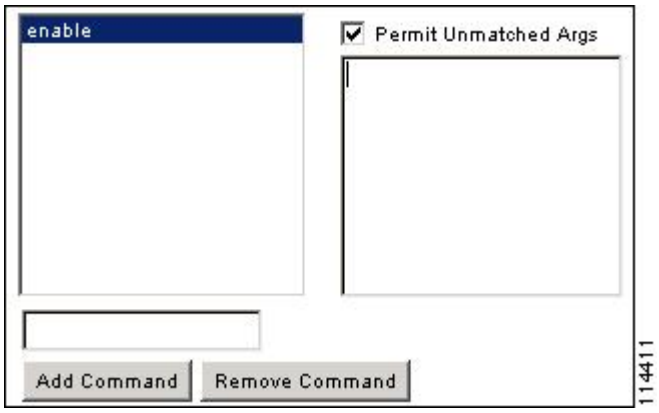
  例如，您可以仅配置 **show** 命令，那么将允许所有 **show** 命令。建议使用此方法，这样您就无需预测命令的每个变体（包括缩写和问号），其显示 CLI 的使用情况（请参阅下图）。

  图 *1:* 允许所有相关命令



- 对于单个单词的命令，即使命令没有参数，也必须允许不匹配的参数，例如 **enable** 或 **help**（请参见下图）。

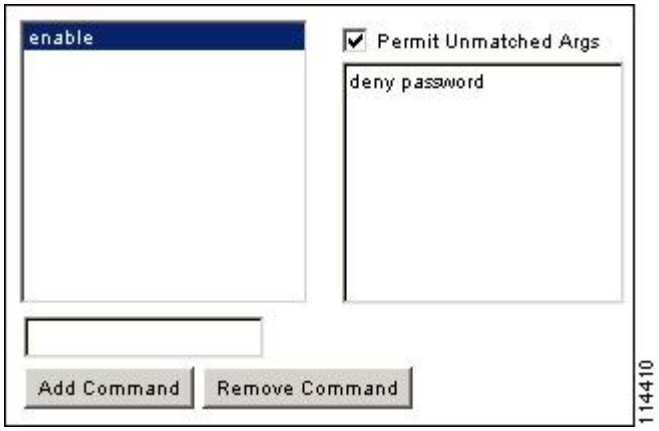
图 *2:* 允许单个单词的命令



- 如要禁止某些参数，请输入参数并在前面放置 **deny**。

  例如，如要允许 **enable**，但不允许 **enable password**，请在命令字段中输入 **enable**，在参数字段内输入 **deny password**。确保选中 **Permit Unmatched Args** 复选框，这样仍能允许单独使用的 **enable**（请参见下图）。

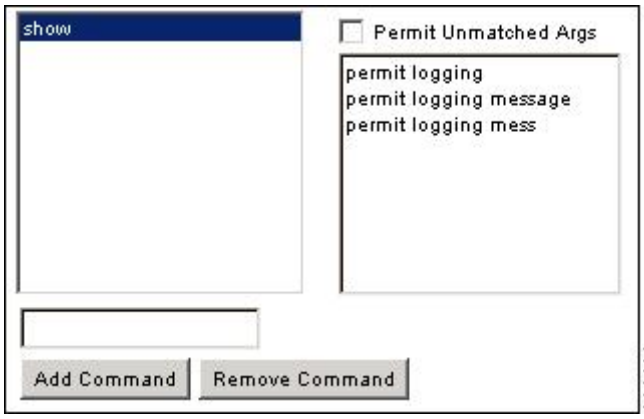
  图 *3:* 禁止参数



- 当您在命令行中缩写命令时，ASA 会将前缀和主命令扩展为全文，但对附加的参数却按照您输入的原样发送到 TACACS+ 服务器。

  例如，如果您输入 **sh log**，那么 ASA 将整个 **show logging** 命令发送到 TACACS+ 服务器。但是，如果您输入 **sh log mess**，那么 ASA 将 **show logging mess** 命令发送到 TACACS+ 服务器，而不是发送扩展的 **show logging message** 命令。您可以配置同一个参数的多种拼法以便预测其缩写（请参阅下图）。

图 *4:* 指定缩写



- 建议您允许所有用户使用以下基本命令：
  - **show checksum**
  - **show curpriv**
  - **enable**
  - **help**
  - **show history**
  - **login**
  - **logout**
  - **pager**
  - **show pager**
  - **clear pager**
  - **quit**
  - **show version**

配置 TACACS+ 命令授权

如果启用TACACS+命令授权，且用户在CLI上输入命令，ASA会将命令和用户名发送到TACACS+服务器以确定命令是否已授权。

在启用 TACACS+ 命令授权之前，请务必以 TACACS+ 服务器上定义的用户身份登录 ASA，并确保您具有必要的命令授权来继续配置 ASA。例如，您应该以获得所有命令授权的管理员用户身份登录。否则，可能会意外锁定。

在您确定配置会按预期方式运行之前，请勿保存配置。如果您因错误被锁定，通常可以通过重启 ASA 来恢复访问。

请确保您的TACACS+系统完全稳定且可靠。必要的可靠性级别通常需要您具有完全冗余的TACACS+服务器系统和完全冗余的与 ASA 的连接性。例如，在您的 TACACS+ 服务器池中包括一个与接口 1 连接的服务器和另一个与接口 2 连接的服务器。您还可以将本地命令授权配置为在 TACACS+ 服务器不可用时的回退方法。

如要使用 TACACS+ 服务器配置命令授权，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备管理** > **用户/AAA** > **AAA 访问** > **授权**。

步骤 2 选中**启用命令访问授权** > **启用**复选框。

步骤 3 从 **Server Group** 下拉列表中选择 AAA 服务器组名称。

步骤 4 （可选）您可以将 ASA 配置为在 AAA 服务器不可用时使用本地数据库作为回退方法。为此，请选中**在服务器组出现故障时使用本地数据库**复选框。建议在本地数据库中使用与AAA服务器相同的用户名和密码，因为ASA提示符不会给出使用何种方法的任何指示。请确保在本地数据库和命令权限级别中配置用户。

步骤 5 点击“**应用**”。

命令授权设置已指定，更改将保存到运行配置中。

为本地数据库用户配置密码策略

使用本地数据库配置用于CLI或ASDM访问的身份验证时，可以配置密码策略来要求用户在指定时间后更改密码并规定密码标准，例如最短长度和更改后的最小字符数。

密码策略仅适用于使用本地数据库的管理用户，而不适用于可以使用本地数据库的其他流量类型（例如用于网络访问的 VPN 或 AAA 流量），也不适用于通过 AAA 服务器进行身份验证的用户。

配置密码策略后，当您更改密码（自己本人的或其他用户的）时，密码策略将应用于新密码。所有现有密码都将成为祖父。新策略将应用于使用 **用户帐户**窗格以及**更改我的密码**窗格更改密码。

开始之前

- 使用本地数据库为 CLI 或 ASDM 访问配置 AAA 身份验证。
- 在本地数据库中制定用户名。

过程

步骤 1 依次选择**配置** > **设备管理** > **用户/AAA** > **密码策略**。

步骤 2 配置以下选项的任意组合：

- **Minimum Password Length** - 输入最小密码长度。有效值范围为 3 到 64 个字符。建议的最小密码长度为 8 个字符。
- **Lifetime** - 输入密码多久之后对远程用户到期（SSH、Telnet、HTTP）；控制台端口的用户永不会因密码到期而锁定。有效值为 0 到 65536 天。默认值为 0 天，表示密码不会到期。

  在密码到期前 7 天，系统会显示警告消息。在密码到期后，拒绝远程用户访问系统。如要在到期后访问，请执行以下操作之一：

  - 让另一位管理员更改您的密码。
  - 登录到物理控制台端口更改密码。

- **Minimum Number Of** - 从以下类型指定最小字符数：
  - **Numeric Characters** -输入密码必须具有的最小数字字符数。有效值为 0 和 64 个字符之间。默认值为 0。
  - **Lower Case Characters** - 输入密码必须具有的最小小写字符数。有效值范围为 0 到 64 个字符。默认值为 0。
  - **Upper Case Characters** - 输入密码必须具有的最小大写字符数。有效值范围为 0 到 64 个字符。默认值为 0。
  - **Special Characters** - 输入密码必须具有的最小特殊字符数。有效值范围为 0 到 64 个字符。特殊字符包括以下字符：!、@、#、$、%、^、&、*、“(”和“)”。默认值为 0。
  - **Different Characters from Previous Password** - 输入您必须在新密码和旧密码之间更改的最小字符数。有效值为 0 和 64 个字符之间。默认值为 0。字符匹配与位置无关，意味着只有新密码字符不在当前密码的任何地方出现时才视为被更改。

- **Enable Reuse Interval** - 您可以禁止重用与之前使用的密码（2 至 7 个之前的密码）相匹配的密码。之前的密码使用 **password-history** 命令以加密形式存储在每个用户名下的配置中；此命令用户不可配置。
- **Prevent Passwords from Matching Usernames** - 禁止使用与用户名匹配的密码。

步骤 3 （可选）选中 **Enable Password and Account Protection** 复选框，以要求用户在 **Change My Password** 窗格而非 **User Accounts** 窗格上更改其密码。默认设置为禁用：用户可以使用其中任一种方法更改密码。

如果启用此功能并尝试在 **User Accounts** 窗格中更改密码，系统会生成以下错误消息：

```
ERROR: Changing your own password is prohibited
```

步骤 4 点击 **Apply** 保存配置设置。

更改密码

如果在密码策略中配置了密码有效期，则需要在旧密码到期时将密码更改为新密码。如果启用密码策略身份验证，则要求用此密码更改方法。如果未启用密码策略身份验证，则既可以使用此方法也可以直接更改用户帐户。

如要更改用户名密码，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备管理** > **用户/AAA** > **更改密码**。

步骤 2 输入旧密码。

步骤 3 输入新密码。

步骤 4 确认新密码。

步骤 5 点击 **Make Change**。

步骤 6 点击 **Save** 图标将更改保存到运行配置中。

启用和查看登录历史

默认情况下，登录历史记录将保存 90 天。可以禁用此功能，也可更改持续时间，最多 365 天。

开始之前

- 登录历史仅按设备保存；在故障转移和集群环境中，每台设备都仅保留其自己的登录历史。
- 在重新加载后，不会保留登录历史数据。
- 当您为一种或多种 CLI 管理方法（SSH、ASDM、串行控制台）启用本地 AAA 身份验证时，此功能将适用于本地数据库中或来自 AAA 服务器的用户名。ASDM 登录不会保存在历史中。

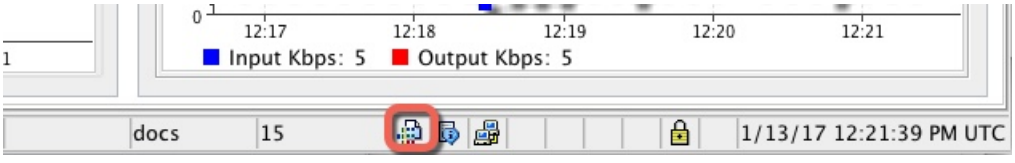
过程

步骤 1 依次选择 **Configuration** > **Device Management** > **Users/AAA** > **Login History**。

步骤 2 选中 **Configure login history reporting for administrators** 复选框。默认情况下启用此功能。

步骤 3 将 **Duration** 设置为 1 到 365 天之间。默认值为 90。

步骤 4 要查看登录历史，可在任何 ASDM 屏幕中点击底部 **Status** 栏中的 **Login History** 图标：



将在一个对话框中显示所有用户的登录历史。

配置管理访问记帐

在 CLI 中输入 **show** 命令之外的任何命令时，可以将记帐消息发送到 TACACS+ 记帐服务器。您可以配置在用户登录时、输入 **enable** 命令时或者发出命令时记帐。

对于命令记帐，只能使用 TACACS+ 服务器。

如要配置管理访问和 enable 命令记帐，请执行以下步骤：

过程

步骤 1 要在用户输入 **enable** 命令时启用记帐，请执行以下步骤：

a) 依次选择**配置** > **设备管理** > **用户/AAA** > **AAA 访问** > **记帐**，然后选中**要求记帐以允许对用户活动进行记帐** > **启用**复选框。

b) 选择 RADIUS 或 TACACS+ 服务器组名称。

步骤 2 要在用户使用 Telnet、SSH 或串行控制台访问 ASA 时启用记帐，请执行以下步骤：

a) 在 **Require accounting for the following types of connections** 区域中，选中 **Serial**、**SSH** 和/或 **Telnet** 复选框。

b) 为每个连接类型选择 RADIUS 或 TACACS+ 服务器组名称。

步骤 3 如要配置命令记帐，请执行以下步骤：

a) 在 **Require accounting for the following types of connections** 区域中，选中 **Enable** 复选框。

b) 选择 TACACS+ 服务器组名称。不支持 RADIUS。

在 CLI 中输入 **show** 之外的任何命令时，可将记帐消息发送到 TACACS+ 记帐服务器。

c) 如果使用 **Command Privilege Setup** 对话框自定义命令权限级别，可通过在 **Privilege level** 下拉列表中指定最低权限级别限制 ASA 使用的命令。ASA 不会使用低于该最低权限级别的命令。

步骤 4 点击“**应用**”。

记帐设置已指定，更改将保存到运行配置中。

从锁定中恢复

在某些情况下，当您打开命令授权或 CLI 身份验证时，可能会被锁定退出 ASA CLI。通常，重启 ASA 即可恢复访问。但是，如果您已经保存配置，则可能会被锁定。

下表列出了常见锁定条件以及如何从中恢复：

表 *1: CLI* 身份验证和命令授权锁定情景

功能	锁定条件	说明	解决方法： 单模	解决方法： 多模
本地 CLI 身份验证	未在本地数据库中配置用户。	如果本地数据库中没有用户，则您无法登录，并且无法添加任何用户。	登录并重置密码和 **aaa** 命令。	使用会话从交换机登录 ASA。您可以从系统执行空间更改为情景并添加用户。
TACACS+ 命令授权 TACACS+ CLI 身份验证 RADIUS CLI 身份验证	服务器关闭或无法访问，且没有配置回退方法。	如果服务器无法访问，则您无法登录或无法输入任何命令。	1. 登录并重置密码和 AAA 命令。 2. 将本地数据库配置为回退方法，这样您就不会在服务器关闭时被锁定。	1. 如果由于 ASA 上的网络配置不正确而无法访问服务器，请使用会话从交换机登录 ASA。您可以从系统执行空间更改为情景并重新配置网络设置。 2. 将本地数据库配置为回退方法，这样您就不会在服务器关闭时被锁定。
TACACS+ 命令授权	您以没有足够权限的用户身份或不存在的用户身份登录。	启用命令授权，但是随后发现用户无法再输入任何命令。	修复 TACACS+ 服务器用户帐户。 如果您没有访问 TACACS+ 服务器的权限并需要立即配置 ASA，可登录到维护分区并重置密码和 **aaa** 命令。	使用会话从交换机登录 ASA。您可以从系统执行空间更改为情景并完成配置更改。您也可以禁用命令授权，直到修复 TACACS+ 配置。
本地命令授权	您以没有足够权限的用户身份登录。	启用命令授权，但是随后发现用户无法再输入任何命令。	登录并重置密码和 **aaa** 命令。	使用会话从交换机登录 ASA。您可以从系统执行空间更改为情景并更改用户级别。

监控设备访问

- **Monitoring** > **Properties** > **Device Access** > **ASDM/HTTPS/Telnet/SSH Sessions**

  顶部窗格列出通过 ASDM、HTTPS 和 Telnet 会话连接的用户的连接类型、会话 ID 和 IP 地址。如要断开特定会话，请点击**断开连接 (Disconnect)**。

  下面的窗格列出客户端、用户名、连接状态、软件版本、传入加密类型、传出加密类型、传入 HMAC、传出 HMAC、SSH 会话 ID、剩余密钥更新数据、剩余密钥更新时间、基于数据的密钥更新以及最后一次密钥更新时间。如要断开特定会话，请点击**断开连接 (Disconnect)**。

- **Monitoring** > **Properties** > **Device Access** > **Authenticated Users**

此窗格列出通过 AAA 服务器进行身份验证的用户的用户名、IP 地址、动态 ACL、非活动超时（如果有）和绝对超时。

- **Monitoring** > **Properties** > **Device Access** > **AAA Locked Out Users**

  此窗格列出被锁定AAA本地用户的用户名、尝试身份验证的失败次数以及用户被锁定的次数。如要清除锁定的特定用户，请点击**清除选定的锁定 (Clear Selected Lockout)**。如要清除锁定的所有用户，请点击**清除所有锁定 (Clear All Lockouts)**。

- **工具 > 命令行界面**

  您可以在此窗格中发出各种非交互式命令并查看结果。

管理访问的历史记录

表 *2:* 管理访问的历史记录

功能名称	平台版本	说明
CiscoSSH 堆栈现在为默认设置	9.19(1)	现在默认使用思科 SSH 堆栈。 新建/修改的菜单项： • 单情景模式： **配置** > **设备管理** > **管 理访问** > **ASDM/HTTPS/Telnet/SSH** • 多情景模式： **配置** > **设备管理** > **SSH 堆栈**。
环回接口支持 SSH 和 Telnet	9.18(2)	您现在可以添加环回接口并用于以下功能： • SSH • Telnet 新增/修改的命令：**interface loopback**、**ssh**、**telnet** 新增/修改的屏幕： **配置** > **设备设置** > **接口设置** > **接口** > **添回环接口** 7.19 中添加了 ASDM 支持。

功能名称	平台版本	说明
思科 SSH 堆栈	9.17(1)	ASA 使用专有 SSH 堆栈进行 SSH 连接。现在，您可以选择使用基于 OpenSSH 的 CiscoSSH 堆栈。默认堆栈继续为ASA堆栈。思科SSH支持： • FIPS 合规性 • 定期更新，包括来自思科和开源社区的更新 请注意，CiscoSSH 堆栈不支持以下功能： • 通过VPN通过SSH连接到其他接口（管理访问） • EdDSA 密钥对 • FIPS模式下的RSA密钥对 如果需要这些功能，应继续使用ASA SSH堆栈。 CiscoSSH 堆栈的 SCP 功能略有变化：要使用 ASA **copy** 命令将文件复制到 SCP 服务器或从 SCP 服务器复制文件，您必须在 ASA 上为 SCP 服务器子网/主机启用 SSH 访问权限。 新建/修改的菜单项： • 单情景模式： **配置** > **设备管理** > **管 理访问** > **ASDM/HTTPS/Telnet/SSH** • 多情景模式： **配置** > **设备管理** > **SSH 堆栈**。
本地用户锁定更改	9.17(1)	ASA 可以在登录尝试失败达到可配置次数之后锁定账户。此功能不适用于权限级别为 15 的用户。此外，用户将被无限期锁定，直到管理员解锁其账户。现在，用户将在 10 分钟后解锁，除非管理员在此之前使用 **clear aaa local user lockout** 命令。权限级别为 15 的用户现在也受锁定设置的影响。 新增/修改的命令：**aaa local authentication attempts max-fail** 、**show aaa local user**
SSH 和 Telnet 密码更改提示	9.17(1)	本地用户首次使用 SSH 或 Telnet 登录 ASA 时，系统会提示他们更改密码。在管理员更改密码后，系统还会提示他们进行首次登录。但是，如果 ASA 重新加载，则系统不会提示用户，即使是首次登录也是如此。 请注意，任何使用本地用户数据库的服务（例如 VPN）也必须使用在 SSH 或 Telnet 登录期间更改的新密码。 新增/修改的命令：**show aaa local user**

功能名称	平台版本	说明
SSH 安全性改进	9.16（1）	SSH 现在支持以下安全性改进： • 主机密钥格式 - **crypto key generate** {**eddsa** | **ecdsa**}. 除了 RSA，我们还增加了对 EdDSA 和 ECDSA 主机密钥的支持。如果密钥存在，ASA 会尝试按以下顺序使用：EdDSA、ECDSA，然后是 RSA。如果使用 **ssh key-exchange hostkey rsa** 命令将 ASA 显式配置为使用 RSA 密钥，则必须生成 2048 位或更高位的密钥。为了实现升级兼容性，仅当使用默认主机密钥设置时，ASA才会使用较小的RSA主机密钥。RSA支持将在更高版本中删除。 • 密钥交换算法 - **ssh key-exchange group** {**ecdh-sha2-nistp256** | **curve25519-sha256**} • 加密算法 **-ssh cipher encryption chacha20-poly1305@openssh.com** • 不再支持 SSH 版本 1 - 已删除 **ssh version** 命令。 新建/修改的菜单项： • **配置** > **设备管理** > **管理访问** > **ASDM/HTTPS/Telnet/SSH** • **配置** > **设备管理** > **证书管理** > **身份证书** • **配置** > **设备管理** > **高级** > **SSH 密码**
SNMP 的管理访问	9.14(2)	在配置通过 VPN 隧道的管理访问时，在加密映射访问列表中包含外部接口的 IP 地址，作为通过站点间 VPN 进行安全 SNMP 轮询的 VPN 配置的一部分。
HTTPS 空闲超时设置	9.14(1)	现在，您可以为 ASA 的所有 HTTPS 连接设置空闲超时，包括 ASDM、WebVPN 和其他客户端。以前，使用 **http server idle-timeout** 命令只能设置 ASDM 空闲超时。如果同时设置两个超时，新命令优先执行。 新增/修改的菜单项：**配置** > **设备管理** > **管理访问** > **ASDM/HTTPS/Telnet/SSH** > **HTTP 设置** > **连接空闲超时**复选框。
SSH加密密码现在按预定义列表的安全性从最高到最低的顺序列出	9.13(1)	SSH加密密码现在按预定义列表（例如中等或高安全性）的安全性从最高到最低的顺序列出。在较早的版本中，它们是按从最低到最高的顺序列出的，这意味着低安全性密码的提议先于高安全性密码。 新建/修改的菜单项： **配置** > **设备管理** > **高级** > **SSH 密码**

功能名称	平台版本	说明
仅限在管理情景中设置SSH密钥交换模式	9.12(2)	您必须在 Admin 情景中设置 SSH 密钥交换；所有其他情景将继承此设置。 新增/修改的菜单项：**配置** > **设备管理** > **管理访问** > **ASDM/HTTPS/Telnet/SSH** > **SSH 设置** > **DH 密钥交换**
现在登录时需要更改 **enable** 密码	9.12(1)	**enable** 默认密码为空。现在，如果您尝试在ASA上进入特权EXEC模式，系统会要求您将密码改为一个至少包含3个字符的值，而不能将密码留空。**no enable password** 命令今后将不受支持。 在 CLI 中，您可以使用 **enable** 命令、**login** 命令（用户权限级别应在 2 级以上）或者 SSH 或 Telnet 会话（如果启用 **aaa authorization exec auto-enable**）来进入特权 EXEC 模式。无论使用哪种方法，您都必须设置密码。 但是在登录ASDM时，则没有这项更改密码的要求。默认情况下，在 ASDM 中，您无需使用用户名和 **enable** 密码即可登录。 未修改任何菜单项。
可配置管理会话限制	9.12(1)	现在，您可以配置汇聚管理会话数、每用户管理会话数和每协议管理会话数的最大值。以前，您只能配置汇聚会话数。此功能不会影响控制台会话。需要注意的是，在多情景模式下，如果最大HTTPS会话数固定为5，则无法配置会话数。此外，系统配置中也不再接受 **quota management-session** 命令，您只能在情景配置中进行此设置。现在，最大汇聚会话数为 15。如果您已将其配置为 0（无限制）或大于 16 的值，在升级设备时，此值会自动更改为 15。 新增/修改的菜单项：**配置** > **设备管理** > **管理访问** > **管理会话配额**
管理权限级别更改通知	9.12(1)	现在，在您授予访问权限 (**aaa authentication enable console**) 或允许直接进行特权 EXEC 访问 (**aaa authorization exec auto-enable**) 后，如果用户已分配的访问权限级别在上次登录后发生更改，ASA 会向用户显示通知。 新建/修改的菜单项： **状态**栏 > **登录历史记录**图标

功能名称	平台版本	说明
SSH 增强安全性	9.12(1)	请参阅以下 SSH 安全改进： • 支持 Diffie-Hellman 组 14 SHA256 密钥交换。此设置现在为默认值。先前默认值为组 1 SHA1。 • 支持 HMAC-SHA256 完整性加密。默认值现在是高安全性密码组（仅 hmac-sha2-256）。先前默认值为介质集。 新增/修改的屏幕： • **配置** > **设备管理** > **管理访问** > **ASDM/HTTPS/Telnet/SSH** • **配置** > **设备管理** > **高级** > **SSH 密码**
允许基于非浏览器的 HTTPS 客户端访问 ASA	9.12(1)	您可以允许基于非浏览器的 HTTPS 客户端访问 ASA 上的 HTTPS 服务。默认情况下，允许 ASDM、CSM 和 REST API。 新增/修改的屏幕。 **配置** > **设备管理** > **管理访问** > **HTTP 非浏览器客户端支持**
RSA 密钥对支持 3072 位密钥	9.9(2)	您现在可以将模数长度设为 3072。 新增或修改的菜单项：**配置** > **设备管理** > **证书管理** > **身份证书**
网桥虚拟机 (BVI) 上的 VPN 管理访问	9.9(2)	现在，如果在 BVI 上启用了 VPN **management-access**，可以在该 BVI 上启用管理服务（例如 **telnet**、**http** 和 **ssh**）。对于非 VPN 管理访问，应在网桥组成员接口上继续配置这些服务。 新增或修改的命令：**https**、**telnet**、**ssh**、**management-access**
已弃用 SSH 版本 1	9.9(1)	SSH 版本 1 已弃用，未来不再发行。默认设置已从 SSH v1 和 v2 更改为仅 SSH v2。 新建/修改的菜单项： • **配置** > **设备管理** > **管理访问** > **ASDM/HTTPS/Telnet/SSH**

功能名称	平台版本	说明
对使用SSH公钥身份验证的用户和具有密码的用户分别进行单独的身份验证	9.6(3)/9.8(1)	在 9.6(2) 以前的版本中，您在启用 SSH 公钥身份验证 (**ssh authentication**)时，可以不必明确启用基于本地用户数据库的AAA SSH 身份验证 (**aaa authentication ssh console LOCAL**)。在 9.6(2) 中，ASA 要求明确启用 AAA SSH 身份验证。在此版本中，您不再需要明确启用 AAA SSH 身份验证；当您为用户配置 **ssh authentication** 命令时，默认情况下会为使用此类型身份验证的用户启用本地身份验证。此外，在明确配置 AAA SSH 身份验证时，此配置将仅适用于具有密码的用户名，并且可以使用任何 AAA 服务器类型（例如 **aaa authentication ssh console radius_1**）。例如，某些用户可以使用公钥身份验证（使用本地数据库），而其他用户则可配合使用密码和 RADIUS。 未修改任何菜单项。
登录历史	9.8(1)	默认情况下，登录历史记录将保存 90 天。可以禁用此功能，也可更改持续时间，最多365天。仅当为一种或多种管理方法（SSH、ASDM、Telnet 等）启用本地 AAA 身份验证时，此功能才适用于本地数据库中的用户名。 引入了以下菜单项：**配置 > 设备管理 > 用户/AAA > 登录历史记录**
禁止重复使用密码以及禁止使用与某一用户名匹配的密码的密码策略实施	9.8(1)	现在，可以禁止重复使用过去的密码（最多7代），还可以禁止使用与某一用户名匹配的密码。 引入了以下菜单项：**配置 > 设备管理 > 用户/AAA > 密码策略**
ASDM 的 ASA SSL 服务器模式匹配	9.6(2)	对于通过证书进行身份验证的 ASDM 用户，您现在可以要求证书与证书映射匹配。 修改了以下菜单项：**配置 > 设备管理 > 管理访问 > ASDM/HTTPS/Telnet/SSH**
SSH 公钥身份验证改进	9.6(2)	在更早的版本中，您在启用 SSH 公钥身份验证 时，可以不必启用基于本地用户数据库的AAA SSH身份验证 。该配置现在已修复，您必须明确启用 AAA SSH 身份验证。要禁止用户使用密码而不是私钥，现在您可以创建未定义任何密码的用户名。 修改了以下菜单项： **配置 > 设备管理 > 管理访问 > ASDM/HTTPS/Telnet/SSH** **配置 > 设备管理 > 用户/AAA > 用户账户 > 添加/编辑用户账户**
ASDM 管理授权	9.4(1)	现在可以单独为 HTTP 访问与 Telnet 和 SSH 访问配置管理授权。 修改了以下菜单项：**配置 > 设备管理 > 用户/AAA > AAA 访问 > 授权**

功能名称	平台版本	说明
证书配置中的 ASDM 用户名	9.4(1)	当启用 ASDM 证书身份验证 时，可以配置 ASDM 从证书提取用户名的方式；还可以在出现登录提示时启用用户名预填充功能。 引入了以下菜单项：**配置 > 设备管理 > 管理访问 > HTTP 证书规则**。
改进的一次性密码身份验证	9.2(1)	有足够授权权限的管理员可以通过输入自己的身份验证凭证一次进入特权 EXEC 模式。**aaa authorization exec** 命令中添加了 **auto-enable** 选项。 修改了以下菜单项：配置 > 设备管理 > 用户/AAA > AAA 访问 > 授权。
对 IPV6 的 HTTP 重定向支持	9.1(7)/9.6(1)	现在，在为 ASDM 接入或无客户端 SSL VPN 启用 HTTP 重定向到 HTTPS 时，可将已发送的流量重定向到 IPv6 地址。 向以下菜单项添加了功能：**配置 > 设备管理 > HTTP 重定向**
可配置 SSH 加密和完整性密码	9.1(7.4)/9.3(3)/9.6(1)	用户可在执行 SSH 加密管理时选择密码模式，并可配置 HMAC 和加密来改变密钥交换算法。根据您的应用，您可能希望将密码变得更加严格或更不严格。请注意，安全复制的性能部分取决于所使用的加密密码。默认情况下，ASA 会按顺序协商以下其中一种算法：3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr。如果选择建议的第一种算法 (3des-cbc)，则性能会远远慢于 128-cbc 等更高效的算法。例如，要更改所需的密码，请使用 **ssh cipher encryption custom aes128-cbc**。 引入了以下屏幕：**Configuration > Device Management > Advanced > SSH Ciphers**
SSH 的 AES-CTR 加密	9.1(2)	ASA 中的 SSH 服务器实施现在支持 AES-CTR 模式加密。
改进的 SSH 重新生成密钥间隔	9.1(2)	在连接时间达到 60 分钟后或数据流量达到 1 GB 后，SSH 连接重新生成密钥。 。
对于在多情景模式下的 ASASM，支持从交换机进行 Telnet 和虚拟控制台身份验证。	8.5(1)	虽然从多情景模式下的交换机连接至 ASASM 将连接至系统执行空间，但是可以在管理员情景中配置身份验证来监管这些连接。
使用本地数据库时，支持管理员密码策略	8.4(4.1)、9.1(2)	使用本地数据库配置用于 CLI 或 ASDM 访问的身份验证时，可以配置密码策略来要求用户在指定时间后更改密码并规定密码标准，例如最短长度和更改后的最小字符数。 引入了以下屏幕：Configuration > Device Management > Users/AAA > Password Policy。

功能名称	平台版本	说明
支持 SSH 公钥身份验证	8.4(4.1)、9.1(2)	对于与 ASA 的 SSH 连接，您可以基于每个用户启用公钥身份验证。您可以指定公钥文件 (PKF) 格式的密钥或 Base64 密钥。PKF 密钥的长度可达 4096 位。对于由于过长而导致 ASA 不支持使用 Base64 格式（限长 2048 位）的密钥，请使用 PKF 格式。 引入了以下菜单项： Configuration > Device Management > Users/AAA > User Accounts > Edit User Account > Public Key Authentication Configuration > Device Management > Users/AAA > User Accounts > Edit User Account > Public Key Using PKF。 仅在 *9.1(2)* 及更高版本中支持 *PKF* 密钥格式。
支持用于 SSH 密钥交换的 Diffie-Hellman 组 14	8.4(4.1)、9.1(2)	已添加支持 Diffie-Hellman 组 14 进行 SSH 密钥交换。以前，只支持组 1。 修改了以下屏幕：配置 > 设备管理 > 管理访问 > ASDM/HTTPS/Telnet/SSH。
支持的管理会话最大数量	8.4(4.1)、9.1(2)	您可以设置并发 ASDM、SSH 和 Telnet 会话的最大数量。 引入了以下屏幕：Configuration > Device Management > Management Access > Management Session Quota。
提高了 SSH 安全性；不再支持 SSH 默认用户名。	8.4(2)	从 8.4(2) 开始，您无法再使用 pix 或 asa 用户名和登录密码通过 SSH 连接至 ASA。如要使用 SSH，必须使用 **aaa authentication ssh console LOCAL** 命令 (CLI) 或“配置 \> 设备管理 \> 用户/AAA \> AAA 访问 \> 身份验证 (ASDM)”来配置 AAA 身份验证；然后通过输入 **username** 命令 (CLI) 或依次选择“配置 \> 设备管理 \> 用户/AAA \> 用户帐户 (ASDM)”来定义本地用户。如果要使用 AAA 服务器而不是本地数据库进行身份验证，建议也将本地身份验证配置为备用方法。

功能名称	平台版本	说明
管理访问	7.0(1)	引入了此功能。 引入了以下屏幕： Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH Configuration > Device Management > Management Access > Command Line (CLI) > Banner Configuration > Device Management > Management Access > CLI Prompt Configuration > Device Management > Management Access > ICMP Configuration > Device Management > Management Access > File Access > FTP Client Configuration > Device Management > Management Access > File Access > Secure Copy (SCP) Server Configuration > Device Management > Management Access > File Access > Mount-Points Configuration > Device Management > Users/AAA > AAA Access > Authentication Configuration > Device Management > Users/AAA > AAA Access > Authorization Configuration > Device Management > Users/AAA > AAA Access > > Accounting。

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。