ASA版本9.x SSH和Telnet在内部和外部接口配置示例

目录

简介

本文描述如何配置在Cisco系列安全工具版本9.x和以上的内部和外部接口的安全壳SSH。当您必须用CLI远程配置和监控思科可适应安全工具(ASA)时，使用Telnet或SSH要求。由于Telnet通信在明文发送，能包括密码， SSH是高度推荐的。SSH流量在通道加密，并且从而帮助保护密码和其他敏感配置命令从拦截。

ASA允许对安全工具的SSH连接管理目的。安全设备对于每个安全上下文最多允许五个并发的 SSH 连接（如果有），而对于所有上下文合在一起全局最多支持 100 个连接。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据Cisco ASA防火墙软件版本9.1.5。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

> **注意**：ASA版本7.x和以上支持SSH版本2 (SSHv2)。

相关产品

此配置可能也与有软件版本的9.x Cisco ASA 5500系列安全工具一起使用和以后。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

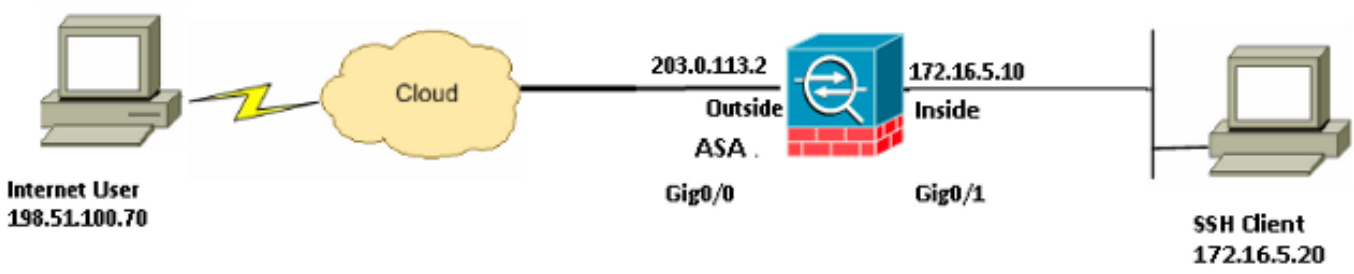
配置

请使用在此部分被提供为了配置功能在本文描述的信息。

> **注意**：描述的每配置步骤提供是必要为了使用CLI或可适应安全设备管理器的信息(ASDM)。

> **注意**：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图



在本例中配置示例， ASA认为SSH服务器。从SSH客户端的流量(198.51.100.70/32和172.16.5.20/24) SSH服务器的加密。安全工具支持在SSH版本1和2提供的SSH远程shell协议功能并且支持数据加密标准(DES)和3DES密码器。SSH 版本 1 和 2 存在差异，不可互操作。

SSH 配置

本文档使用以下配置：

- 通过 SSH 访问安全设备
- 如何使用 SSH 客户端
- ASA 配置

通过 SSH 访问安全设备

完成以下这些步骤，以便配置对安全设备的 SSH 访问：

1. SSH会话总是需要一个认证形式例如用户名和密码。有您能使用为了符合此要求的两个方法。

   您能使用为了符合此要求的**第一种方法**是配置与使用的一个用户名和密码验证、授权和统计(AAA)：
   ```
   ASA(config)#username username password password
   ASA(config)#aaa authentication {telnet | ssh | http | serial} console
   {LOCAL | server_group [LOCAL]}
   ```
   注意：如果使用一TACACS+或RADIUS服务器组验证，您能配置安全工具，以便使用本地数据库作为fallback方法，如果AAA服务器不可用。指定服务器组名称，然后指定 LOCAL（LOCAL 区分大小写）。思科建议您在本地数据库和AAA服务器使用相同用户名和密码，因为安全工具提示符不给予使用方法的任何征兆。为了指定**TACACS+的一个本地备份**，请使用此配置SSH验证：
   ```
   ASA(config)#aaa authentication ssh console TACACS+ LOCAL
   ```
   还可以使用本地数据库作为身份验证的主要方法，而不设置备用方法。为了执行此，单独回车**本地**：
   ```
   ASA(config)#aaa authentication ssh console LOCAL
   ```
   您能使用为了符合此要求的**第二种方法**是使用**ASA**默认用户名和**cisco**默认远程登录密码。可以用下面这个命令更改 Telnet 口令：
   ```
   ASA(config)#passwd password
   ```
   注意：在这种情况下**password命令**可能类似也使用，作为两个function命令。
2. 生成ASA防火墙的一个RSA密钥对，为SSH要求：
   ```
   ASA(config)#crypto key generate rsa modulus modulus_size
   ```
   注意：modulus_size（以位为单位）可以是 512、768、1024 或 2048。指定的密钥模数大小越大，生成 RSA 密钥对所需的时间就越长。推荐值为2048。使用为了生成一个RSA密钥对的命令为ASA软件版本早于版本7.x是不同的。在更早版本中，域名，在您能创建密钥前，必须设置。 在多个上下文模式，您必须生成每上下文的RSA密钥。
3. 指定允许连接到安全工具的主机。此命令指定允许连接SSH主机的源地址、网络屏蔽和接口。可以多次输入此命令，从而指定多个主机、网络或接口。在本例中，在内部的一台主机和在外部的一台主机允许：
   ```
   ASA(config)#ssh 172.16.5.20 255.255.255.255 inside
   ASA(config)#ssh 198.51.10.70 255.255.255.255 outside
   ```
4. 此步骤是可选的。默认情况下，安全工具允许SSH版本1和版本2.回车此命令为了限制对一个特定版本的连接：
   ```
   ASA(config)# ssh version <version_number>
   ```
   注意：version_number可以是**1**或**2**。
5. 此步骤是可选的。默认情况下， SSH会话在五分钟非活动之后关闭。此超时可以配置持续在1和60分钟之间：
   ```
   ASA(config)#ssh timeout minutes
   ```

ASA 配置

请使用此信息为了配置ASA ：

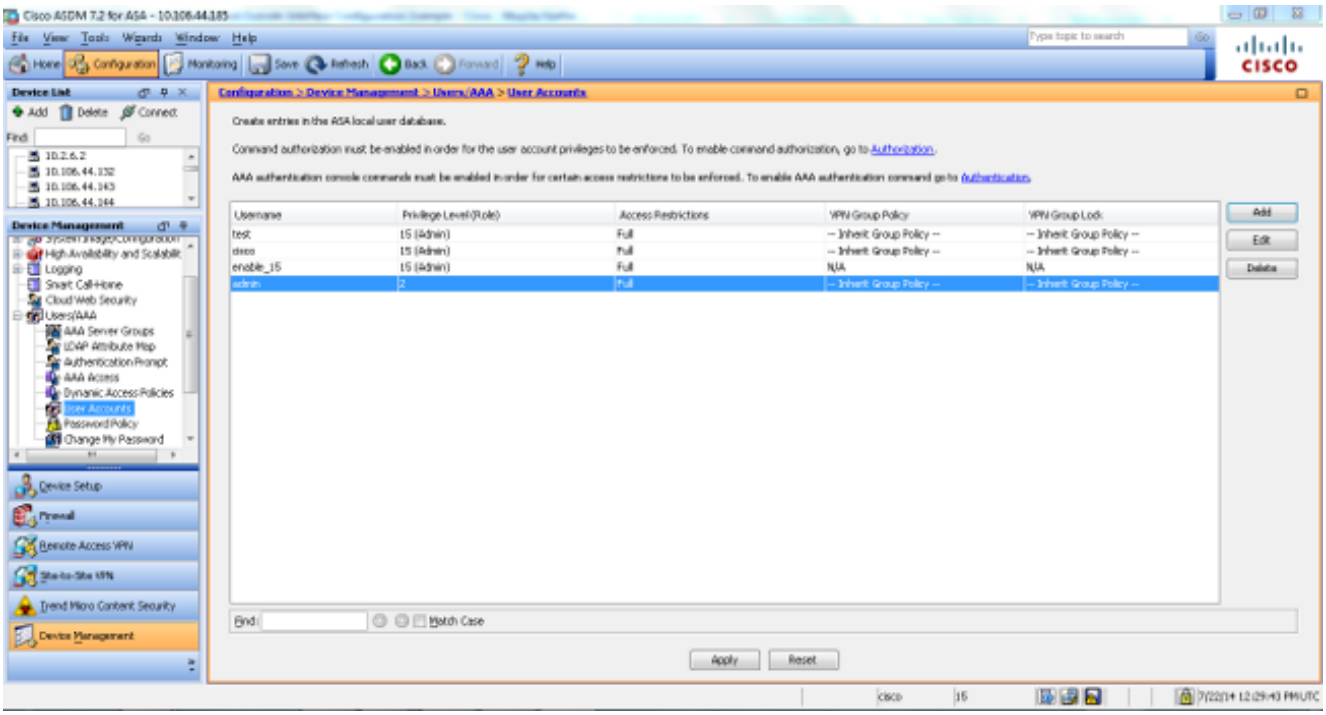
```
ASA Version 9.1(5)2
!
hostname ASA
domain-name cisco.com

interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 172.16.5.10 255.255.255.0
!
interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 203.0.113.2 255.255.255.0

!--- AAA for the SSH configuration

username ciscouser password 3USUcOPFUiMCO4Jk encrypted
aaa authentication ssh console LOCAL

http server enable
http 172.16.5.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstar
telnet timeout 5

!--- Enter this command for each address or subnet
!--- to identify the IP addresses from which
!--- the security appliance accepts connections.
!--- The security appliance accepts SSH connections from all interfaces.

ssh 172.16.5.20 255.255.255.255 inside
ssh 198.51.100.70 255.255.255.255 outside

!--- Allows the users on the host 172.16.5.20 on inside
!--- Allows SSH access to the user on internet 198.51.100.70 on outside
!--- to access the security appliance
!--- on the inside interface.

ssh 172.16.5.20 255.255.255.255 inside

!--- Sets the duration from 1 to 60 minutes
!--- (default 5 minutes) that the SSH session can be idle,
!--- before the security appliance disconnects the session.

ssh timeout 60

console timeout 0
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map global_policy
class inspection_default
inspect dns maximum-length 512
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
```

```
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
```

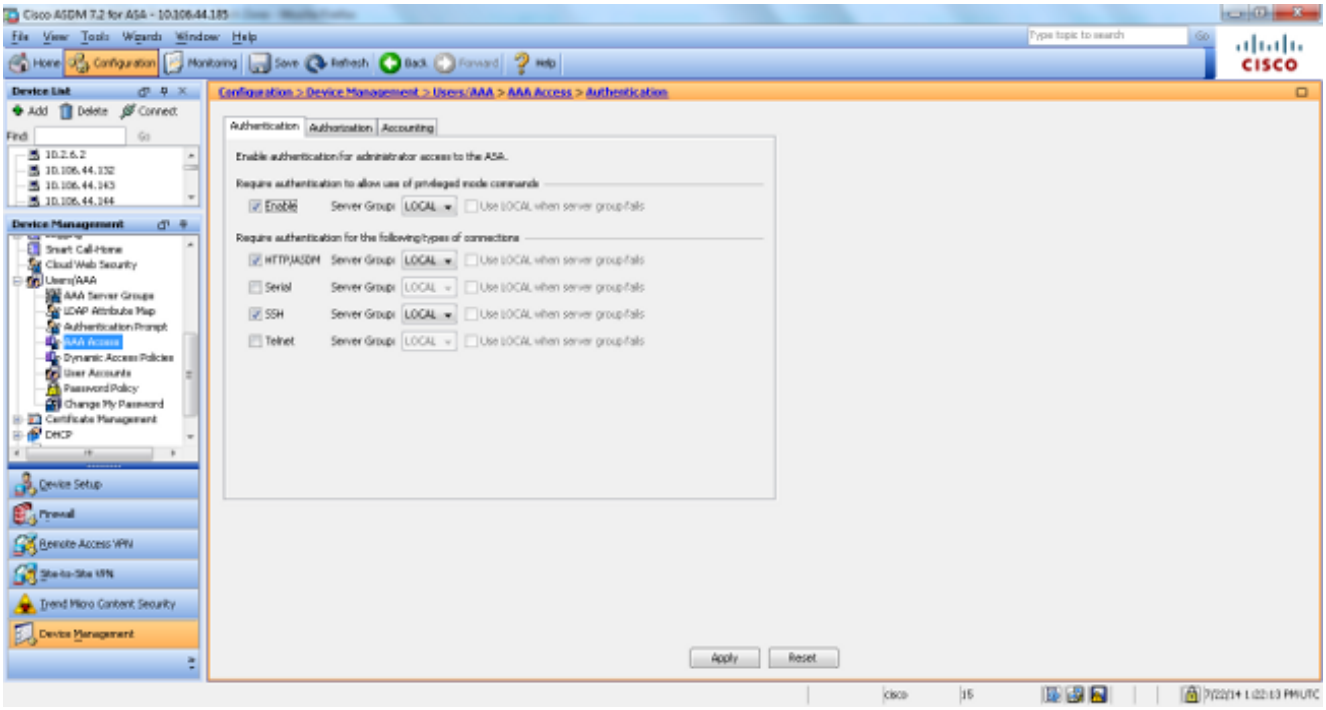
ASDM版本7.2.1配置

完成这些步骤为了配置ASDM版本7.2.1 ：

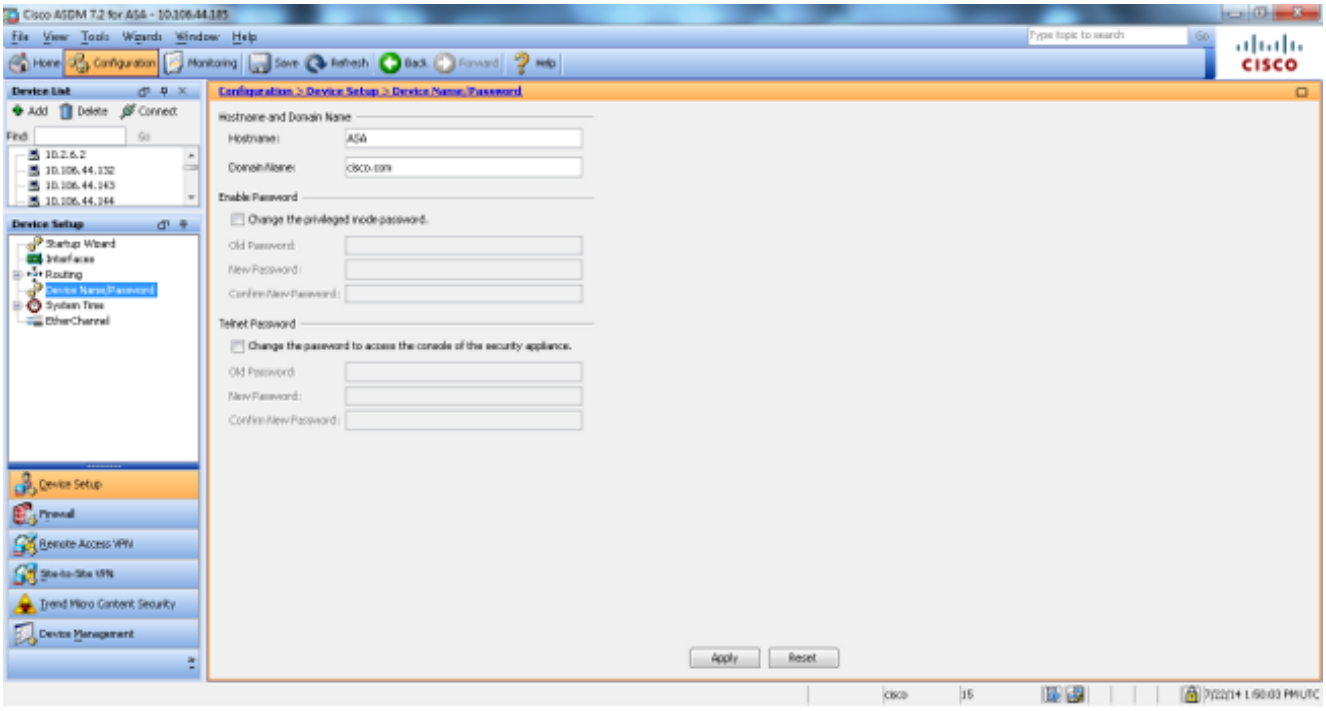
1. 导航对**Configuration>设备管理> Users/AAA >用户帐户**为了添加有ASDM的一个用户。



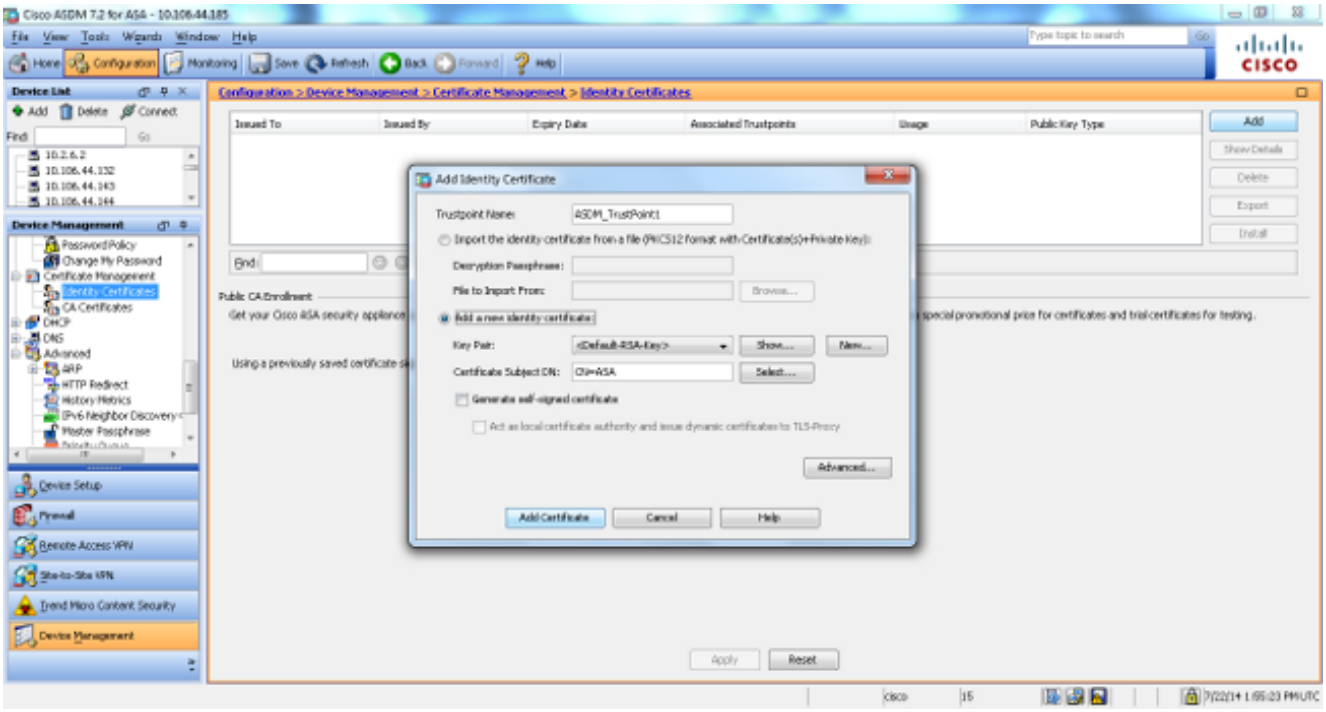
2. 导航对**Configuration>设备管理> Users/AAA >AAA访问>验证**为了设置SSH的AAA认证与ASDM。



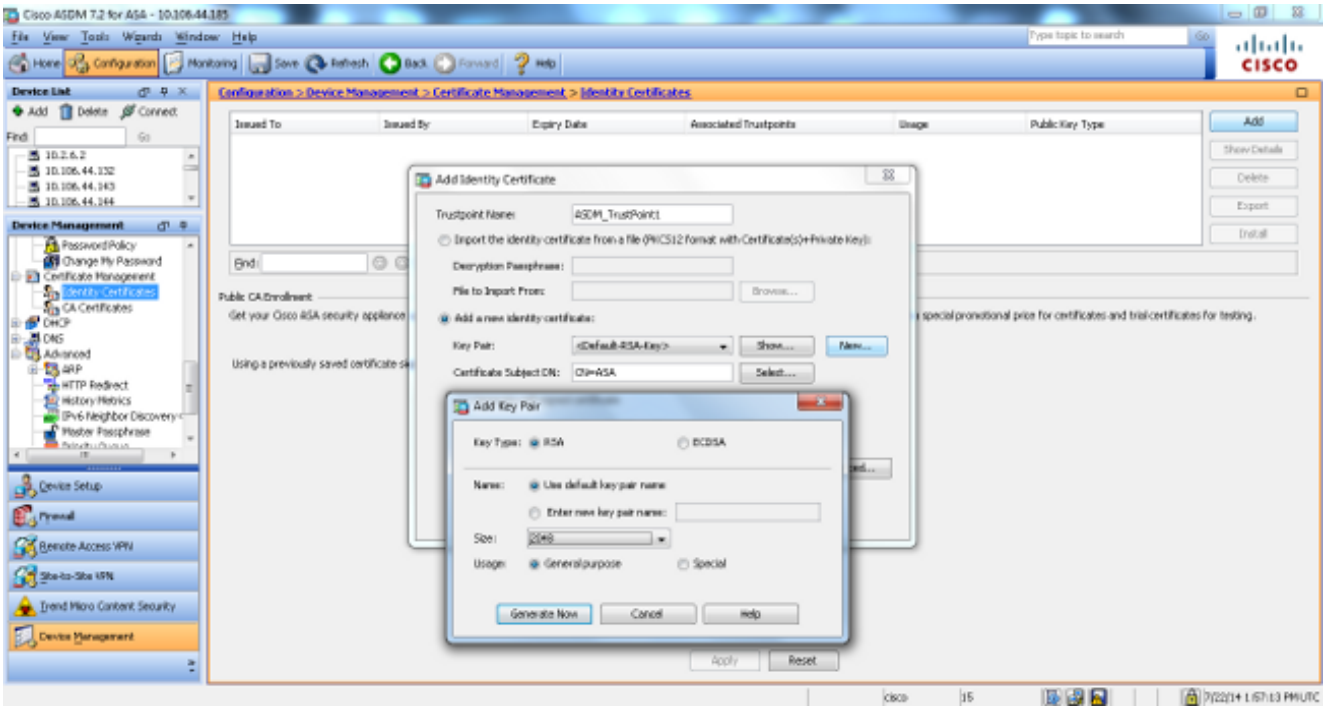
3. 导航对**Configuration>设备设置>设备名/密码**为了更改与ASDM的远程登录密码。



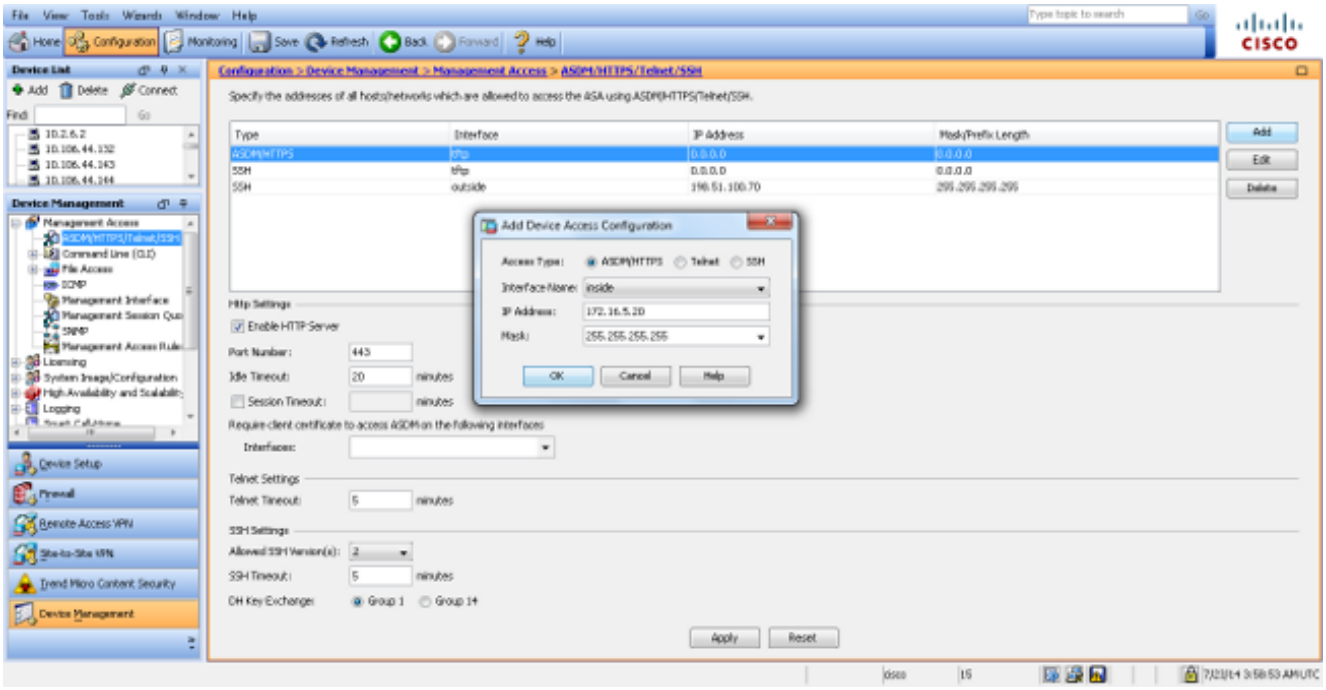
4. 导航对**Configuration>设备管理> Certificate Management >身份证书**，单击**添加**，并且使用是可用为了生成与ASDM的同样RSA密钥的默认选项。



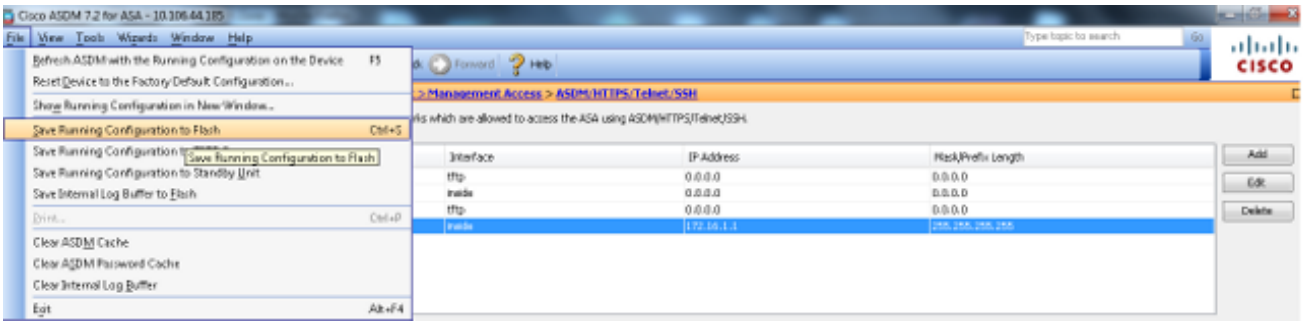
5. 如果一个不存在，点击**添加一个新的身份证书**单选按钮并且单击**新**为了添加一个DEFAULT键对。一旦完整，请单击**当前生成**。



6. 导航对**Configuration>设备管理>管理访问> Line命令(CLI) >安全壳SSH**为了使用ASDM，以便您能指定允许连接SSH的主机和为了指定版本和超时选项。



7. 点击从弹出窗口的**"Save"**为了保存配置。



8. 提示在闪存中保存配置时，选择 **Apply** 以保存配置。

Telnet 配置

为了添加对控制台的Telnet访问和设置空闲超时，请输入在全局配置模式的**Telnet命令**。默认情况下，Telnet 会话持续处于非活动状态五分钟，安全设备就会将其关闭。要从以前设置的 IP 地址中删除 Telnet 访问，请使用此命令的 *no* 形式。

```
telnet {{hostname | IP_address mask interface_name} | {IPv6_address
interface_name} | {timeout number}}
no telnet {{hostname | IP_address mask interface_name} | {IPv6_address
interface_name} | {timeout number}}
```

Telnet命令允许您指定能通过Telnet访问安全工具控制台的主机。

> **注意**：可以在所有接口上对安全设备启用 Telnet。然而，安全工具要求对外部接口的所有Telnet流量由IPsec保护。为了启用远程登录会话到外部接口，请配置在外部接口的IPsec，以便由在外部接口的安全工具和enable (event) Telnet生成的包括IP数据流。

> **注意**：一般来说，如果比其他接口有安全等级零或降低的任何接口， ASA不允许Telnet对该接口。

> **注意**：思科不通过远程登录会话推荐对安全工具的访问。验证证件信息，例如密码，发送作为明文。思科建议您使用SSH被巩固的数据通信。

输入**password命令**为了设置Telnet访问的一个密码对控制台。默认密码是**cisco**。输入**who命令**为了查看当前访问安全工具控制台的IP地址。输入**kill命令**为了终止一次活动远程控制台会话。

Telnet示例情形

为了启用远程登录会话到内部接口，请查看在此部分提供的示例。

示例 1

此示例允许仅主机**172.16.5.20**获得访问到安全工具控制台通过Telnet ：

```
ASA(config)#telnet 172.16.5.20 255.255.255.255 inside
```

示例 2

此示例允许仅网络**172.16.5.0/24**获得访问到安全工具控制台通过Telnet ：

```
ASA(config)#telnet 172.16.5.0 255.255.255.0 inside
```

示例 3

此示例允许所有网络获得访问到安全工具控制台通过Telnet ：

```
ASA(config)#telnet 0.0.0.0 0.0.0.0 inside
```

如果使用带有 console 关键字的 **aaa** 命令，则必须用身份验证服务器对 Telnet 控制台访问进行身份验证。

> **注意**：如果配置**aaa命令**为了要求安全工具和Telnet控制台访问的验证和控制台登录请求时代，您能获得访问到从串行控制台的安全工具。为此，请输入用 **enable password** 命令设置的安全设备用户名和口令。

发出 **telnet timeout** 命令，以便设置安全设备注销控制台 Telnet 会话之前该会话可处于空闲状态的最长时间。不能将 **no telnet** 命令与 telnet timeout 命令配合使用。

本示例显示如何更改会话空闲最长持续时间：

```
hostname(config)#telnet timeout 10

hostname(config)#show running-config telnet timeout

telnet timeout 10 minutes
```

验证

使用本部分可确认配置能否正常运行。

> **注意**：命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

调试 SSH

输入**debug ssh命令**为了启用SSH调试：

```
ASA(config)#debug ssh
SSH debugging on
```

此输出显示从一个内部的IP地址(172.16.5.20)的一SSH尝试对ASA的内部接口。这些调试表示一个成功的连接和验证：

```
Device ssh opened successfully.
SSH0: SSH client: IP = '172.16.5.20' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-2.0-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-2.0-Cisco-1.25
SSH0: receive SSH message: 83 (83)
SSH0: client version is - SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for Windows
client version string:SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for WindowsSSH0: begin ser ver key generation
SSH0: complete server key generation, elapsed time = 1760 ms
SSH2 0: SSH2_MSG_KEXINIT sent
SSH2 0: SSH2_MSG_KEXINIT received
SSH2: kex: client->server aes128-cbc hmac-md5 none
SSH2: kex: server->client aes128-cbc hmac-md5 none
SSH2 0: expecting SSH2_MSG_KEXDH_INIT
SSH2 0: SSH2_MSG_KEXDH_INIT received
SSH2 0: signature length 143
SSH2: kex_derive_keys complete
SSH2 0: newkeys: mode 1
SSH2 0: SSH2_MSG_NEWKEYS sent
SSH2 0: waiting for SSH2_MSG_NEWKEYS
SSH2 0: newkeys: mode 0
SSH2 0: SSH2_MSG_NEWKEYS received
SSH(cisco): user authen method is 'use AAA', aaa server group ID = 1
SSH2 0: authentication successful for cisco

!--- Authentication for the ASA was successful.

SSH2 0: channel open request
SSH2 0: pty-req request
SSH2 0: requested tty: vt100, height 25, width 80
SSH2 0: shell request
SSH2 0: shell message received
```

如果错误用户名输入，例如**cisco1**而不是**cisco**， ASA防火墙拒绝验证。下面的调试输出显示身份验证失败：

```
Device ssh opened successfully.
SSH0: SSH client: IP = '172.16.5.20' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-2.0-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-2.0-Cisco-1.25
SSH0: receive SSH message: 83 (83)
SSH0: client version is - SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for Windows
client version string:SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for WindowsSSH0: begin ser ver key generation
```

```
SSH0: complete server key generation, elapsed time = 1760 ms
SSH2 0: SSH2_MSG_KEXINIT sent
SSH2 0: SSH2_MSG_KEXINIT received
SSH2: kex: client->server aes128-cbc hmac-md5 none
SSH2: kex: server->client aes128-cbc hmac-md5 none
SSH2 0: expecting SSH2_MSG_KEXDH_INIT
SSH2 0: SSH2_MSG_KEXDH_INIT received
SSH2 0: signature length 143
SSH2: kex_derive_keys complete
SSH2 0: newkeys: mode 1
SSH2 0: SSH2_MSG_NEWKEYS sent
SSH2 0: waiting for SSH2_MSG_NEWKEYS
SSH2 0: newkeys: mode 0
SSH2 0: SSH2_MSG_NEWKEYS received
SSH(cisco): user authen method is 'use AAA', aaa server group ID = 1
SSH2 0: authentication failed for cisco1

!--- Authentication for ASA1 was not successful due to the wrong username.
```

同样地，如果提供不正确的密码，验证发生故障。下面的调试输出显示身份验证失败：

```
Device ssh opened successfully.
SSH0: SSH client: IP = '172.16.5.20' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-2.0-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-2.0-Cisco-1.25
SSH0: receive SSH message: 83 (83)
SSH0: client version is - SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for Windows
client version string:SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for WindowsSSH0: begin ser ver key generation
SSH0: complete server key generation, elapsed time = 1760 ms
SSH2 0: SSH2_MSG_KEXINIT sent
SSH2 0: SSH2_MSG_KEXINIT received
SSH2: kex: client->server aes128-cbc hmac-md5 none
SSH2: kex: server->client aes128-cbc hmac-md5 none
SSH2 0: expecting SSH2_MSG_KEXDH_INIT
SSH2 0: SSH2_MSG_KEXDH_INIT received
SSH2 0: signature length 143
SSH2: kex_derive_keys complete
SSH2 0: newkeys: mode 1
SSH2 0: SSH2_MSG_NEWKEYS sent
SSH2 0: waiting for SSH2_MSG_NEWKEYS
SSH2 0: newkeys: mode 0
SSH2 0: SSH2_MSG_NEWKEYS received
SSH(cisco): user authen method is 'use AAA', aaa server group ID = 1
SSH2 0: authentication failed for cisco1

!--- Authentication for ASA was not successful due to the wrong password.
```

查看活动的 SSH 会话

输入此命令为了验证的SSH会话数量连接(和连接状态)对ASA ：

```
ASA(config)# show ssh sessions

SID Client IP    Version Mode Encryption Hmac State           Username
0   172.16.5.20 2.0     IN   aes256-cbc sha1 SessionStarted  cisco
                        OUT  aes256-cbc sha1 SessionStarted  cisco
```

导航到**Monitoring>属性>设备访问> Secure Shell塞申斯**为了查看有ASDM的会话。

输入**socket命令显示asp的表**为了验证TCP会话建立：

```
ASA(config)# show asp table socket

Protocol Socket State Local Address Foreign Address

SSL 02444758 LISTEN 203.0.113.2:443 0.0.0.0:*
TCP 02448708 LISTEN 203.0.113.2:22 0.0.0.0:*
SSL 02c75298 LISTEN 172.16.5.10:443 0.0.0.0:*
TCP 02c77c88 LISTEN 172.16.5.10:22 0.0.0.0:*
TCP 02d032d8 ESTAB 172.16.5.10:22 172.16.5.20:52234
```

查看公共RSA密钥

输入此命令为了查看RSA密钥的公共部分在安全工具的：

```
ASA(config)#show crypto key mypubkey rsa
Key pair was generated at: 23:23:59 UTC Jul 22 2014
Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 2048
 Key:

 30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
 00aa82d1 f61df1a4 7cd1ae05 c92322c1 1ce490e3 c9db00fd d75afe77 1ea0b2c2
 3325576f a7dc5ffe a6166bf5 7f0f2551 25b8cb23 a8908b49 81c42618 c98e3aea
 ce6f9e42 367974d1 5c2ea6b1 e7aac40b 44a6c0a5 23c4d845 a57d4c04 6de49dbb
 2c6f074e 25e3b19e 7c5da809 ac7d775c 0c01bb9d 211b7078 741094b4 94056e75
 72d5e938 c59baaec 12285005 ee6abf81 90822610 cf7ee4c1 ae8093d9 6943bde3
 16d8748c d86b5f66 1a6ccf33 9cde0432 b3cabab5 938b1874 c3d7c13e 43a95a8f
 ed36db2e f9ca5d2c 0c65858e 3e513723 2d362b47 7984d845 faf22579 654113d1
 24d59f27 55d2ddf3 20af3b65 62f039cb a3aafc31 d92a3d9b 14966eb3 cb6ca249
 55020301 0001
```

导航对**Configuration>属性>证书>密钥对**并且单击**显示详细信息**为了查看与ASDM的RSA密钥。

故障排除

此部分提供您能使用为了排除故障您的配置的信息。

从ASA去除RSA密钥

在某些情况下，例如，当您升级ASA软件或更改在ASA时的SSH版本，您也许要求去除和再创RSA密钥。输入此命令为了从ASA删除RSA密钥对：

```
ASA(config)#crypto key zeroize rsa
```

导航对**Configuration>属性>证书>密钥对**并且点击**删除**为了去除与ASDM的RSA密钥。

SSH 连接失败

您收到在ASA的此错误消息：

```
%ASA-3-315004: Fail to establish SSH session because RSA host key retrieval failed.
```

这是出现在SSH客户端计算机的错误消息：

```
Selected cipher type <unknown> not supported by server.
```

为了解决此问题，请去除并且再创RSA密钥。输入此命令为了从ASA删除RSA密钥对：

```
ASA(config)#crypto key zeroize rsa
```

输入此命令为了生成新密钥：

```
ASA(config)# crypto key generate rsa modulus 2048
```