內部和外部介面上的ASA 9.x SSH和Telnet配置示例

目錄

簡介

本檔案介紹如何在思科系列安全裝置9.x版及更新版本的內部和外部介面上設定安全殼層(SSH)。如果必須使用CLI遠端配置和監控思科自適應安全裝置(ASA)，則需要使用Telnet或SSH。由於Telnet通訊以明文形式傳送，可能包括密碼，因此強烈建議使用SSH。SSH流量在通道中加密，因此有助於保護密碼和其他敏感配置命令免遭攔截。

ASA允許出於管理目的與安全裝置建立SSH連線。如果可用，安全裝置允許每個安全情景最多同時建立5個SSH連線，並且所有合併的情景最多允許100個連線。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊基於Cisco ASA防火牆軟體版本9.1.5。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

> **附註**：ASA 7.x及更高版本支援SSH第2版(SSHv2)。

相關產品

此配置還可以與軟體版本9.x及更高版本的Cisco ASA 5500系列安全裝置配合使用。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

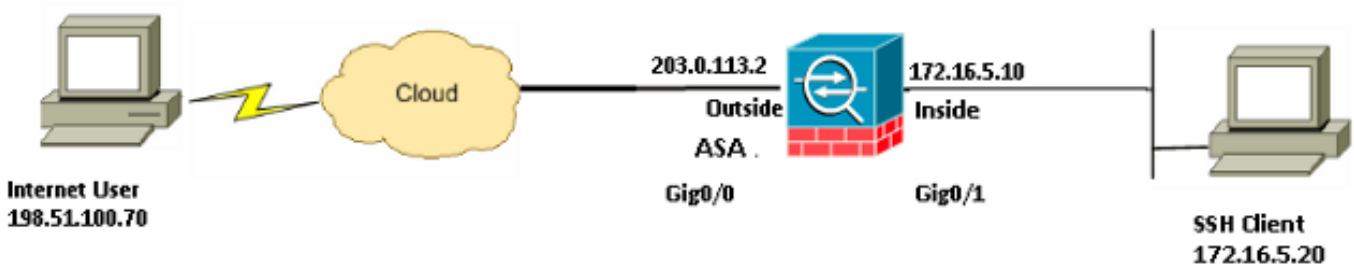
設定

使用本節提供的資訊以設定本檔案中所述的功能。

> **附註**：所述的每個配置步驟都提供了使用CLI或自適應安全裝置管理器(ASDM)所需的資訊。

> **附註**：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

網路圖表



在此配置示例中，ASA被視為SSH伺服器。從SSH客戶端(198.51.100.70/32和172.16.5.20/24)到SSH伺服器的流量會加密。安全裝置支援SSH版本1和2中提供的SSH遠端外殼功能，並支援資料加密標準(DES)和3DES密碼。SSH版本1和2不同，無法互操作。

SSH配置

本檔案會使用以下設定：

- 對安全裝置的SSH訪問
- 如何使用SSH客戶端
- ASA配置

對安全裝置的SSH訪問

完成以下步驟，配置對安全裝置的SSH訪問：

1. SSH會話始終需要使用者名稱和密碼等身份驗證形式。有兩種方法可用於滿足此要求。

   為了滿足此要求，您可以使用的第一種方法是使用驗證、授權和記帳(AAA)來設定使用者名稱和密碼：

   ```
   ASA(config)#username username password password
   ASA(config)#aaa authentication {telnet | ssh | http | serial} console
   {LOCAL | server_group [LOCAL]}
   ```

   附註：如果使用TACACS+或RADIUS伺服器組進行身份驗證，則可以配置安全裝置，使其在AAA伺服器不可用時使用本地資料庫作為回退方法。指定伺服器組名稱，然後指定LOCAL(LOCAL區分大小寫)。 思科建議在本地資料庫和AAA伺服器中使用相同的使用者名稱和密碼，因為安全裝置提示符不會顯示使用的方法的任何指示。若要指定TACACS+的LOCAL**備份，請對SSH身份驗證使用以下配置：**

   ```
   ASA(config)#aaa authentication ssh console TACACS+ LOCAL
   ```

   也可以使用本地資料庫作為無回退的主要身份驗證方法。若要執行此操作，請單獨輸入LOCAL:

   ```
   ASA(config)#aaa authentication ssh console LOCAL
   ```

   滿足此要求的第二種方法是使用ASA的預設使用者名稱**和**cisco的預設Telnet**密碼**。您可以使用以下命令更改Telnet密碼：

   ```
   ASA(config)#passwd password
   ```

   附註：在這種情況下，也可以使用password命令，因為兩個命令的作用類似。
2. 為ASA防火牆生成RSA金鑰對，這是SSH所必需的：

   ```
   ASA(config)#crypto key generate rsa modulusmodulus_size
   ```

   附註：modulus_size（以位為單位）可以是512、768、1024或2048。指定的金鑰係數大小越大，生成RSA金鑰對所需的時間就越長。建議值為2048。用於生成RSA金鑰對的命令對於低於版本7.x的ASA軟體版本不同。在早期版本中，必須先設定域名，然後才能建立金鑰。在多情景模式下，必須為每個情景生成RSA金鑰。
3. 指定允許連線到安全裝置的主機。此命令指定允許使用SSH連線的主機的源地址、網路掩碼和介面。可以多次輸入多個主機、網路或介面。在本範例中，允許內部有一台主機和外部有一台主機：

   ```
   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. 此步驟是可選的。預設情況下，安全裝置允許SSH版本1和版本2。輸入以下命令可將連線限製為特定版本：

   ```
   ASA(config)# ssh version
   ```

   附註：version_number可以是1或2。
5. 此步驟是可選的。預設情況下，SSH會話在五分鐘不活動後關閉。此超時可配置為持續時間為1到60分鐘：

   ```
   ASA(config)#ssh timeout minutes
   ```

ASA配置

使用以下資訊配置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.
```

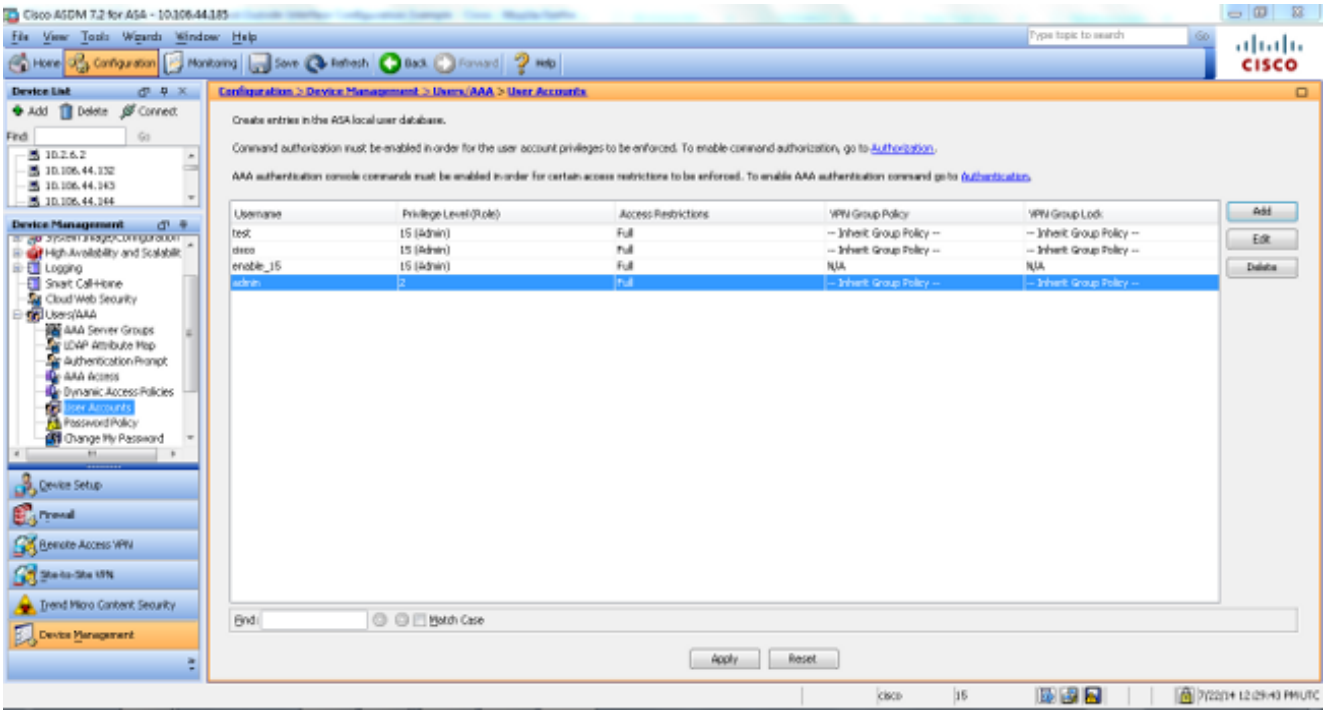
```
ssh timeout 60

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
```

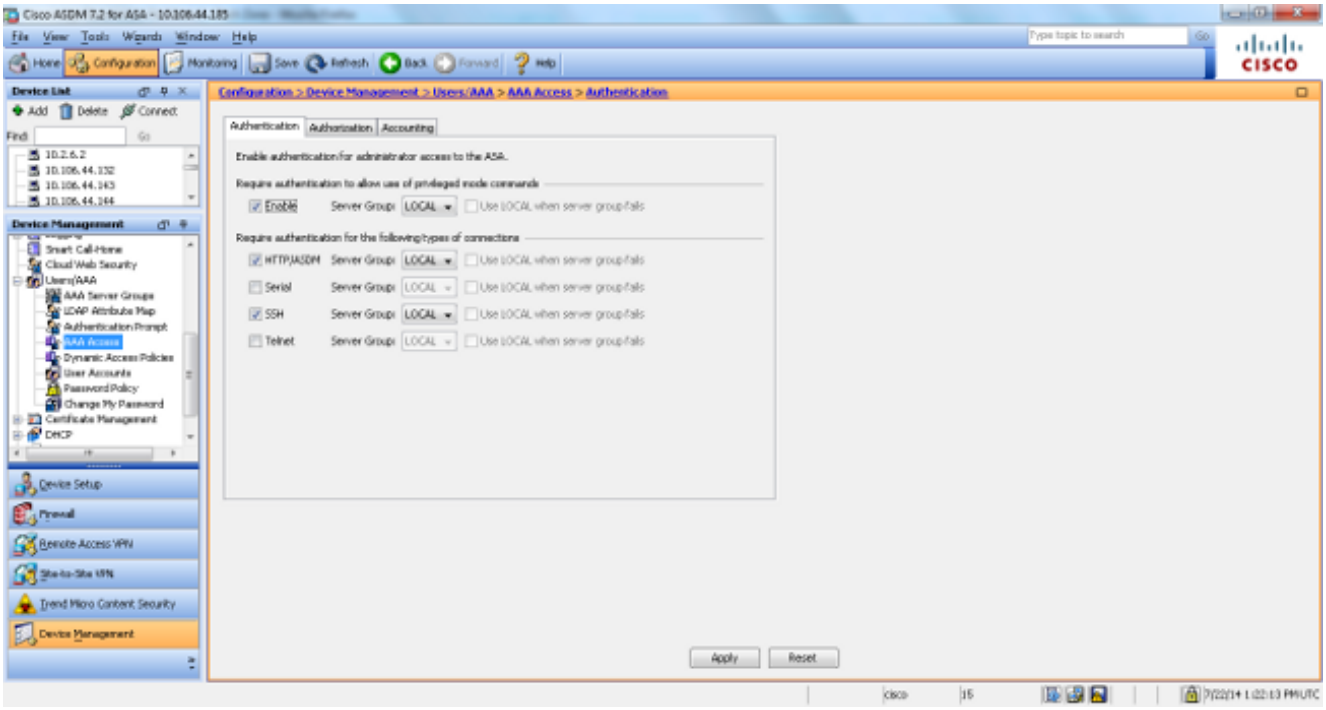
ASDM 7.2.1版配置

完成以下步驟以配置ASDM 7.2.1版：

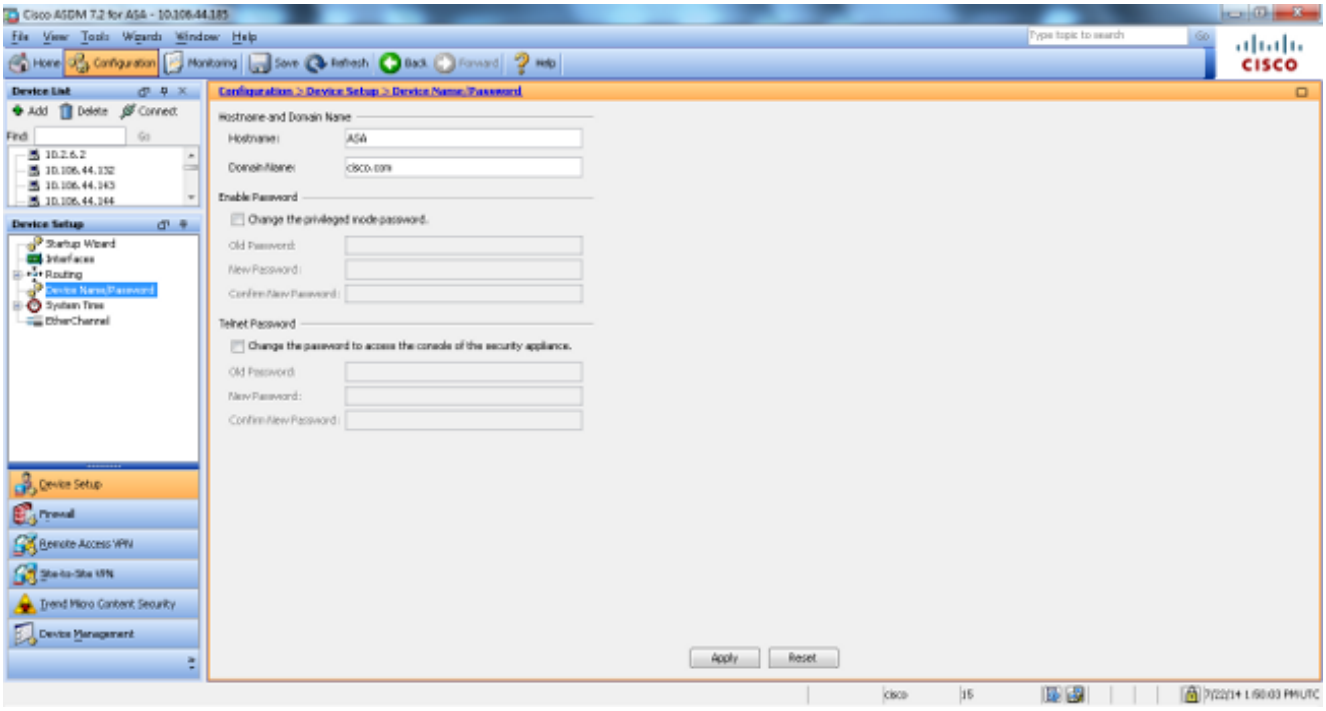
1. 導航到**Configuration > Device Management > Users/AAA > User Accounts**，以便使用ASDM新增使用者。



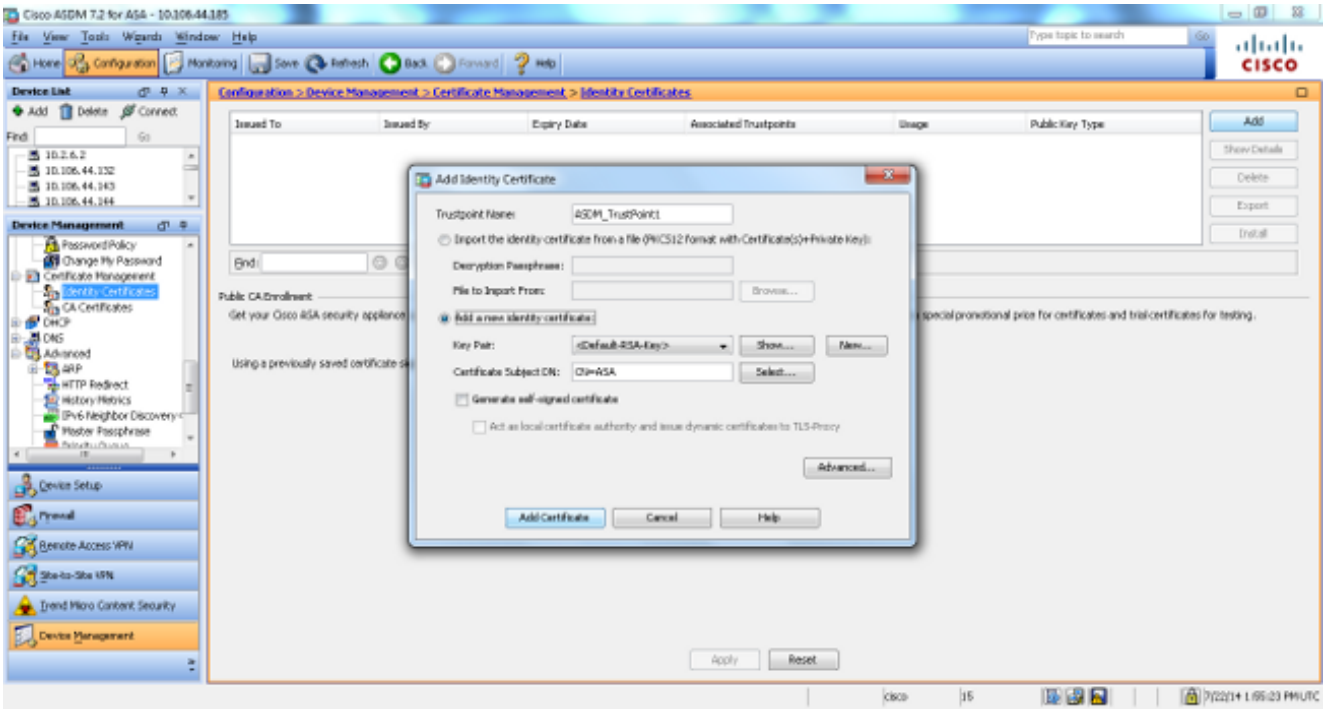
2. 導覽至**Configuration > Device Management > Users/AAA > AAA Access > Authentication**，以便使用ASDM為SSH設定AAA身份驗證。



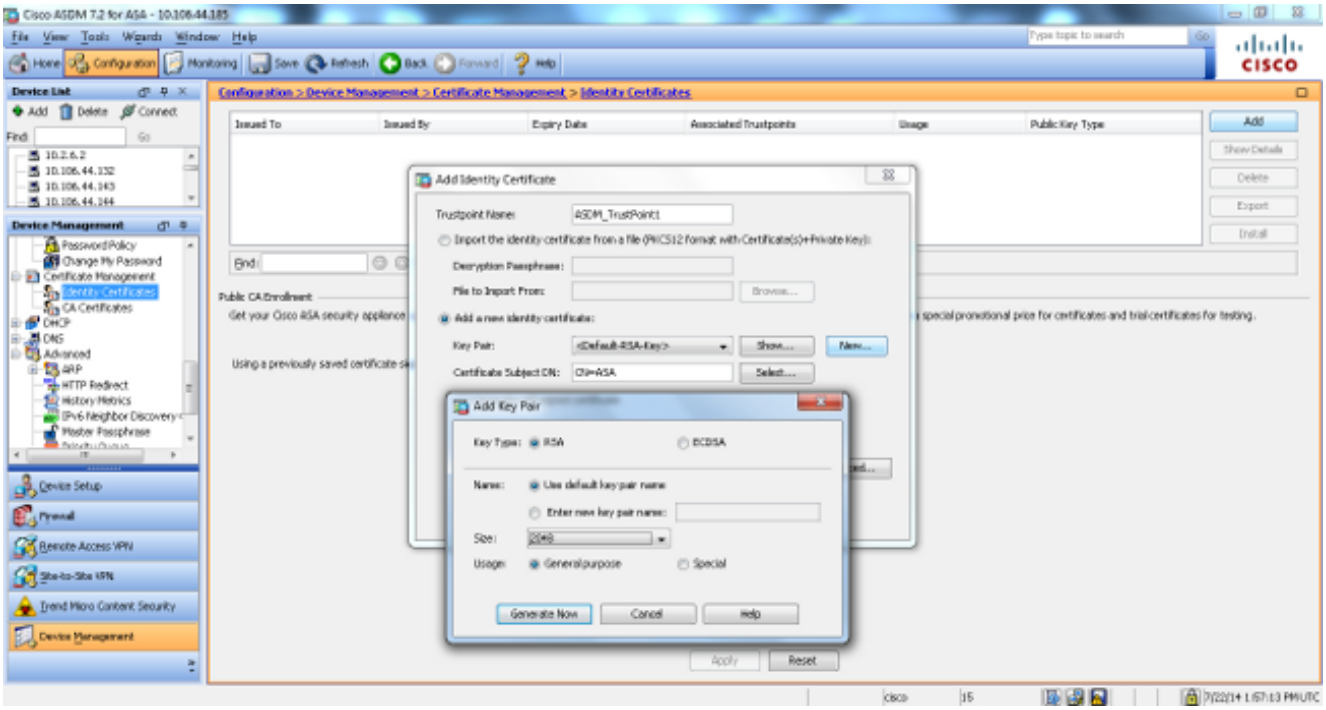
3. 導覽至**Configuration > Device Setup > Device Name/Password**，以便使用ASDM更改Telnet密碼。



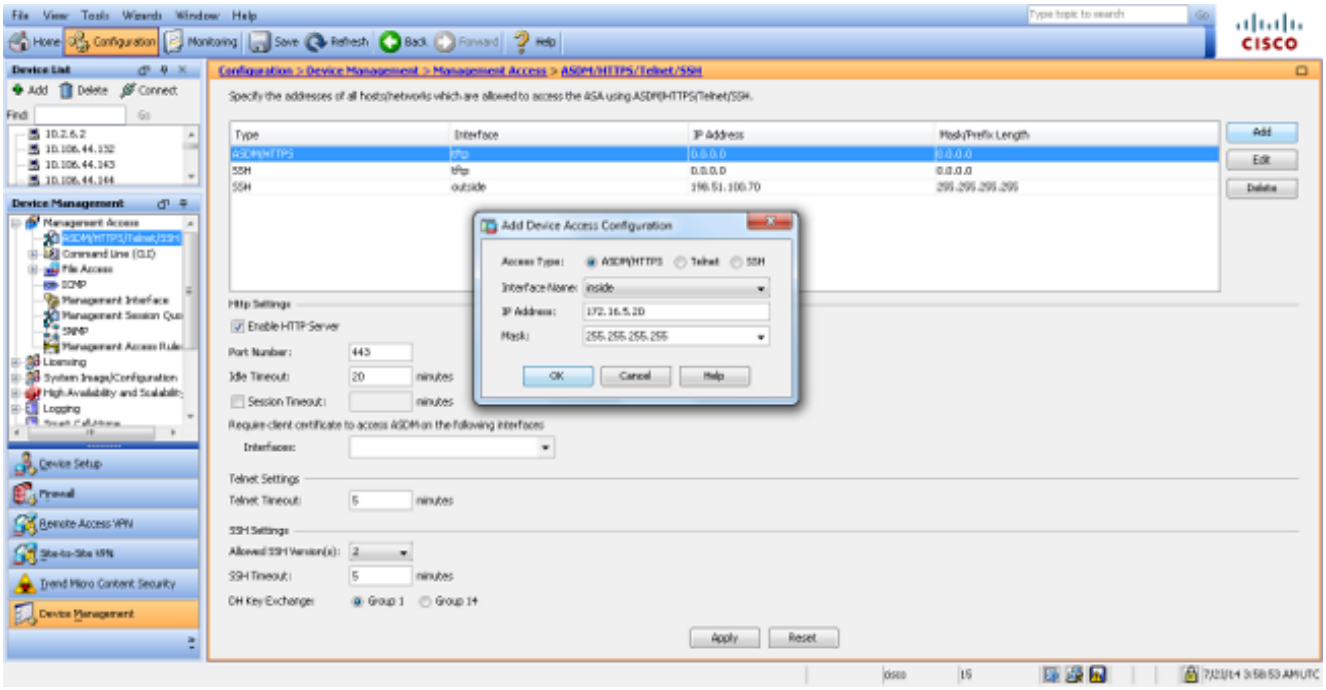
4. 導航到**Configuration > Device Management > Certificate Management > Identity Certificates**，按一下**Add**，然後使用可用的預設選項生成與ASDM相同的RSA金鑰。



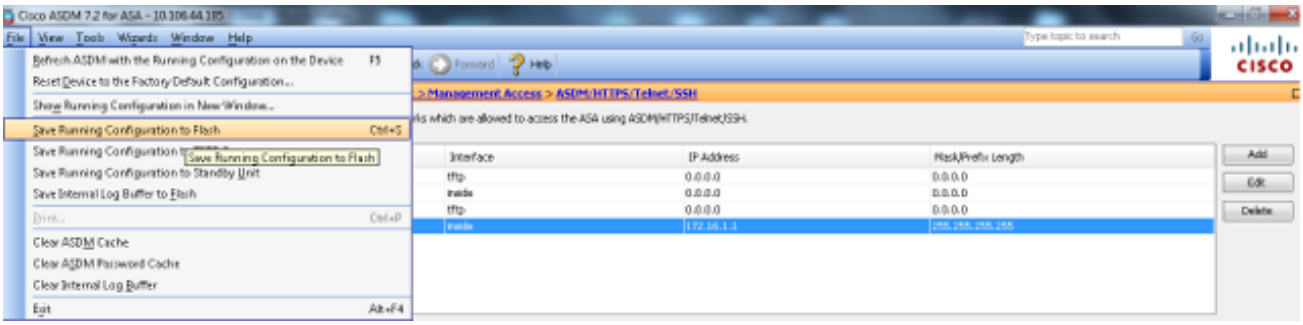
5. 按一下**Add a new Identity certificate**單選按鈕，然後按一下**New**以新增預設金鑰對（如果不存在）。完成後，按一下**Generate Now**。



6. 導覽至**Configuration > Device Management > Management Access > Command Line(CLI)> Secure Shell(SSH)**，以便使用ASDM，以便您可以指定允許使用SSH連線的主機，以及指定版本和超時選項。



7. 在快顯視窗中按一下**Save**，以便儲存組態。



8. 當系統提示將組態儲存到快閃記憶體時，選擇**Apply**以儲存組態。

Telnet配置

若要向控制檯新增Telnet訪問並設定空閒超時，請在全域性配置模式下輸入**telnet**命令。預設情況下，安全裝置會關閉閒置5分鐘的Telnet會話。若要從先前設定的IP位址中移除Telnet存取許可權，請使用此命令的**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命令允許您指定可通過Telnet訪問安全裝置控制檯的主機。

> **附註**：您可以在所有介面上啟用Telnet至安全裝置。但是，安全裝置要求所有到外部介面的Telnet流量都受IPsec保護。要啟用到外部介面的Telnet會話，請在外部介面上配置IPsec，使其包括安全裝置生成的IP流量，並在外部介面上啟用Telnet。

> **附註**：一般來說，如果任何介面的安全級別為零或低於任何其他介面，則ASA不允許Telnet到該介面。

附註：思科不建議通過Telnet會話訪問安全裝置。身份驗證憑證資訊（例如密碼）以明文形式傳送。Cisco建議您使用SSH實現更安全的資料通訊。

輸入**password**命令以設定對主控台的Telnet存取密碼。預設密碼為**cisco**。輸入**who**命令以檢視當前訪問安全裝置控制檯的IP地址。輸入**kill**命令以終止活動的Telnet控制檯會話。

Telnet範例案例

要啟用到內部介面的Telnet會話，請檢視本節中提供的示例。

範例 1

此範例僅允許主機**172.16.5.20**透過Telnet存取安全裝置主控台：

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

範例 2

此示例僅允許網路**172.16.5.0/24**通過Telnet訪問安全裝置控制檯：

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

範例 3

此範例允許所有網路透過Telnet存取安全裝置主控台：

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

如果使用帶有console關鍵字的**aaa**命令，則必須使用身份驗證伺服器對Telnet控制檯訪問進行身份驗證。

附註：如果配置**aaa**命令以要求安全裝置的身份驗證和Telnet控制檯訪問，並且控制檯登入請求超時，則可以從串列控制檯訪問安全裝置。為此，請輸入安全裝置使用者名稱和使用**enable password**命令設定的密碼。

發出**telnet timeout**命令，以設定控制檯Telnet會話在被安全裝置註銷之前可以空閒的最長時間。不能將**no telnet** 命令與**telnet timeout** 命令一起使用。

此示例說明如何更改最大會話空閒持續時間：

```
hostname(config)#telnet timeout 10

hostname(config)#show running-config telnet timeout

telnet timeout 10 minutes
```

驗證

使用本節內容，確認您的組態是否正常運作。

> **附註**：輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**指令輸出的分析。

調試SSH

輸入**debug ssh**命令以啟用SSH調試：

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

此輸出顯示了從內部IP地址(172.16.5.20)到ASA內部介面的SSH嘗試。以下調試描述了成功的連線和身份驗證：

```
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
```

如果輸入的使用者名稱錯誤，例如**cisco1**而不是**cisco**，則ASA防火牆將拒絕身份驗證。此調試輸出顯示失敗的身份驗證：

```
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.
```

同樣，如果提供的密碼不正確，則身份驗證失敗。此調試輸出顯示失敗的身份驗證：

```
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.
```

檢視活動SSH會話

輸入以下命令可驗證連線到ASA的SSH會話數量（以及連線狀態）：

```
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
```

導航到**Monitoring > Properties > Device Access > Secure Shell Sessions**，以檢視具有ASDM的會話。

輸入**show asp table socket**命令以驗證TCP會話是否已建立：

```
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
```

檢視公共RSA金鑰

輸入以下命令可檢視安全裝置上RSA金鑰的公共部分：

```
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
```

導航到**Configuration > Properties > Certificate > Key Pair**，然後按一下**Show Details**以檢視ASDM的RSA金鑰。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

從ASA中刪除RSA金鑰

在某些情況下，例如當您升級ASA軟體或更改ASA中的SSH版本時，可能需要刪除並重新建立RSA金鑰。輸入以下命令以從ASA中刪除RSA金鑰對：

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

導航到**Configuration > Properties > Certificate > Key Pair**，然後點選**Delete**以刪除RSA金鑰和ASDM。

SSH連線失敗

您在ASA上收到以下錯誤消息：

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

以下是SSH客戶端電腦上顯示的錯誤消息：

```
Selected cipher type
```

為了解決此問題，請刪除並重新建立RSA金鑰。輸入以下命令以從ASA中刪除RSA金鑰對：

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

輸入以下命令可產生新金鑰：

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