Esempio di configurazione di ASA versione 9.x SSH e Telnet sulle interfacce interna ed esterna

Sommario

Introduzione

In questo documento viene descritto come configurare Secure Shell (SSH) sulle interfacce interna ed esterna di Cisco Series Security Appliance versione 9.x e successive. Quando è necessario configurare e monitorare Cisco Adaptive Security Appliance (ASA) in remoto con la CLI, è necessario usare Telnet o SSH. Poiché le comunicazioni Telnet vengono inviate in formato testo non crittografato, che può includere password, si consiglia di utilizzare il protocollo SSH. Il traffico SSH è crittografato in un tunnel e contribuisce a proteggere le password e altri comandi di configurazione sensibili dall'intercettazione.

L'ASA consente le connessioni SSH all'appliance di sicurezza per scopi di gestione. L'appliance di sicurezza consente un massimo di cinque connessioni SSH simultanee per ciascun contesto di sicurezza, se disponibili, e un massimo globale di 100 connessioni per tutti i contesti combinati.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per la stesura del documento, è stato usato il software Cisco ASA Firewall versione 9.1.5.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

> **Nota:** SSH versione 2 (SSHv2) è supportato nelle versioni ASA 7.x e successive.

Prodotti correlati

Questa configurazione può essere utilizzata anche con l'appliance di sicurezza Cisco ASA serie 5500 con software versione 9.x e successive.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

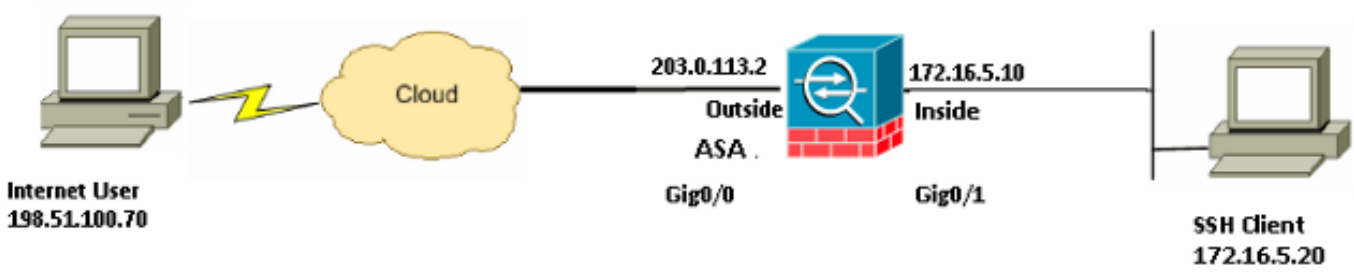
Configurazione

Utilizzare le informazioni fornite in questa sezione per configurare le funzionalità descritte più avanti nel documento.

> **Nota:** Ogni passaggio di configurazione descritto fornisce le informazioni necessarie per utilizzare la CLI o Adaptive Security Device Manager (ASDM).

> **Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete



Nell'esempio di configurazione, l'ASA è considerata il server SSH. Il traffico tra i client SSH (198.51.100.70/32 e 172.16.5.20/24) e il server SSH è crittografato. L'appliance di sicurezza supporta la funzionalità SSH della shell remota fornita nelle versioni 1 e 2 del protocollo SSH e le cifrature Data Encryption Standard (DES) e 3DES. SSH versioni 1 e 2 sono diverse e non sono interoperabili.

Configurazioni SSH

Nel documento vengono usate queste configurazioni:

- Accesso SSH alle appliance di sicurezza
- Come utilizzare un client SSH
- Configurazione ASA

Accesso SSH alle appliance di sicurezza

Per configurare l'accesso SSH all'appliance di sicurezza, attenersi alla seguente procedura:

1. Le sessioni SSH richiedono sempre una forma di autenticazione, come un nome utente e una password. Per soddisfare questo requisito è possibile utilizzare due metodi.

   Il primo metodo che è possibile utilizzare per soddisfare questo requisito è configurare un nome utente e una password con l'utilizzo di Authentication, Authorization, and Accounting (AAA):

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

   Nota: Se si utilizza un gruppo di server TACACS+ o RADIUS per l'autenticazione, è possibile configurare l'appliance di sicurezza in modo che utilizzi il database locale come metodo di fallback se il server AAA non è disponibile. Specificare il nome del gruppo di server, quindi **LOCAL** (**LOCAL** fa distinzione tra maiuscole e minuscole). Cisco consiglia di utilizzare lo stesso nome utente e la stessa password nel database locale e nel server AAA, in quanto il prompt dell'appliance di sicurezza non fornisce alcuna indicazione sul metodo utilizzato.Per specificare un backup **LOCALE** per **TACACS+**, utilizzare questa configurazione per l'autenticazione SSH:

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

   In alternativa, è possibile utilizzare il database locale come metodo di autenticazione principale senza fallback. A tale scopo, immettere solo **LOCAL**:

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

Il secondo metodo che è possibile utilizzare per soddisfare questo requisito è usare il nome utente predefinito dell'**ASA** e la password Telnet predefinita di **cisco**. È possibile modificare la password Telnet con questo comando:

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

Nota: In questa situazione è possibile usare anche il comando **password**, poiché entrambi i comandi funzionano in modo simile.

2. Generare una coppia di chiavi RSA per il firewall ASA, necessario per SSH:

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

Nota: Il valore di **modulus_size** (in bit) può essere 512, 768, 1024 o 2048. Maggiore è la dimensione del modulo chiave specificata, maggiore sarà il tempo necessario per generare la coppia di chiavi RSA. Si consiglia un valore di 2048. Il comando usato per generare una coppia di chiavi RSA è diverso nelle versioni software dell'ASA precedenti alla versione 7.x. Nelle versioni precedenti, è necessario impostare un nome di dominio prima di poter creare le chiavi. In modalità contesto multiplo, è necessario generare le chiavi RSA per ogni contesto.

3. Specificare gli host autorizzati alla connessione all'appliance di sicurezza. Questo comando specifica l'indirizzo di origine, la netmask e l'interfaccia degli host a cui è consentita la connessione con SSH. Può essere immesso più volte per più host, reti o interfacce. Nell'esempio, sono consentiti un host all'interno e un host all'esterno:

```
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. Questo passaggio è facoltativo. Per impostazione predefinita, l'appliance di sicurezza supporta sia SSH versione 1 che SSH versione 2. Immettere questo comando per limitare le connessioni a una versione specifica:

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

Nota: Il valore di **version_number** può essere **1** o **2**.

5. Questo passaggio è facoltativo. Per impostazione predefinita, le sessioni SSH vengono chiuse dopo cinque minuti di inattività. È possibile configurare questo timeout in modo che duri da 1 a 60 minuti:

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

Configurazione ASA

Per configurare l'ASA, usare queste informazioni:

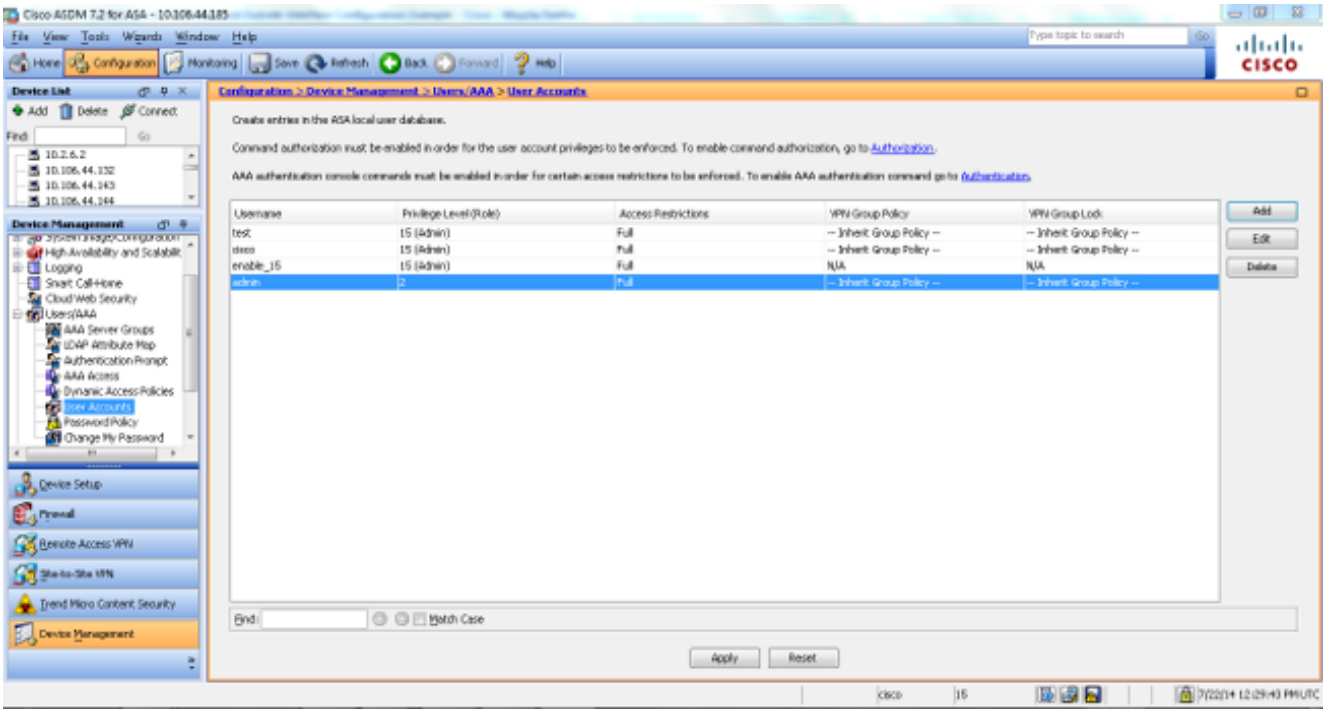
```
ASA Version 9.1(5)2
!
hostname ASA
domain-name cisco.com

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
```

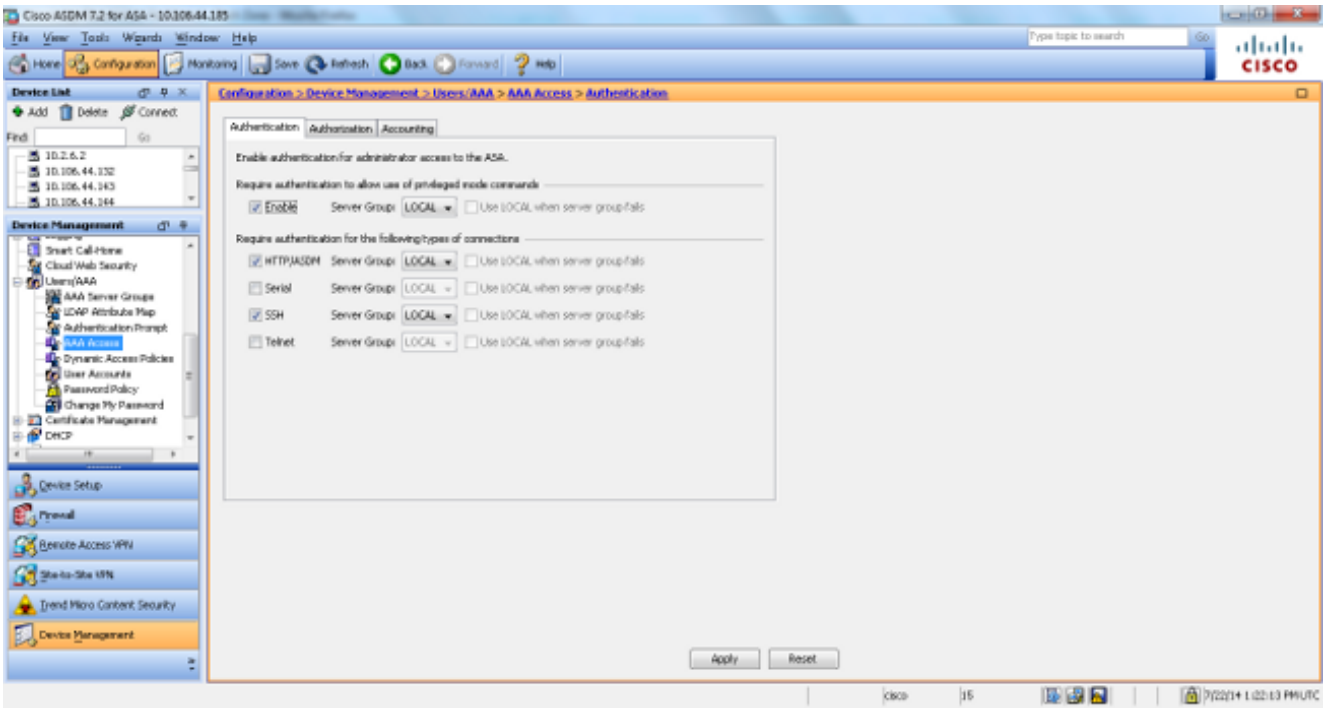
Configurazione di ASDM versione 7.2.1

Per configurare ASDM versione 7.2.1, completare i seguenti passaggi:

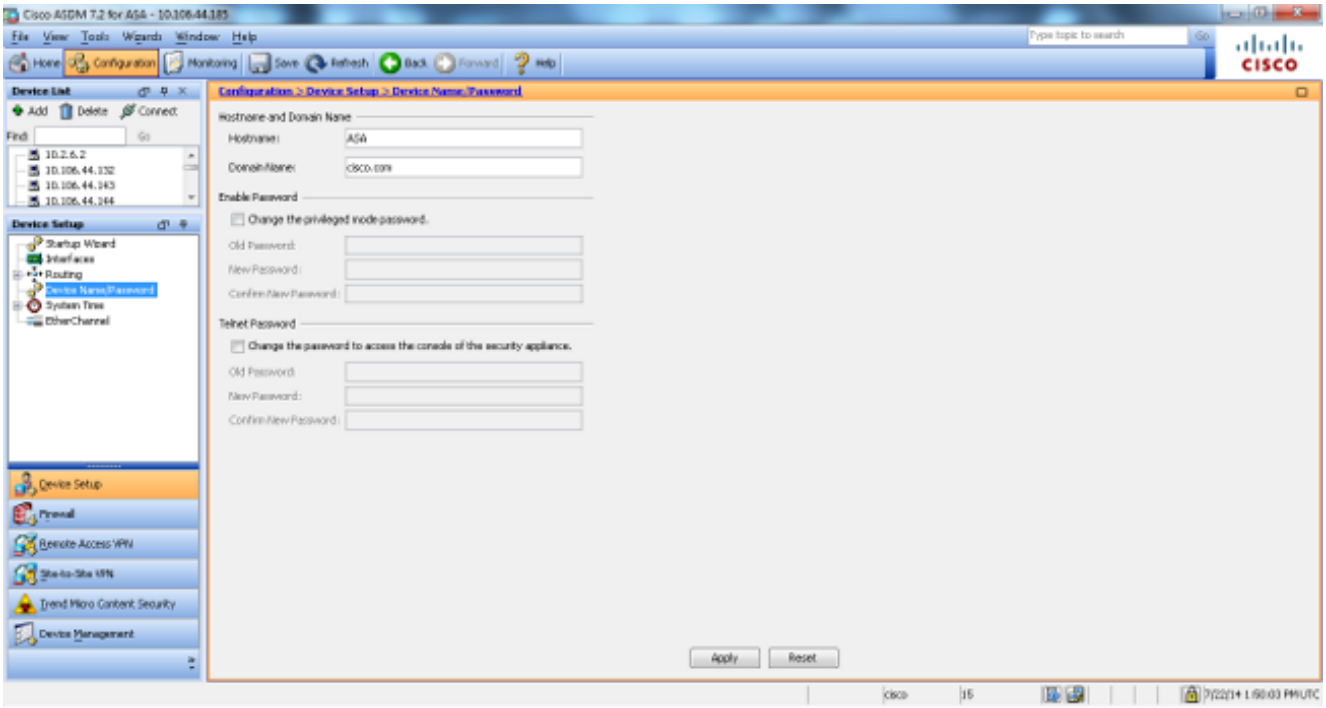
1. Per aggiungere un utente con ASDM, selezionare **Configurazione > Gestione dispositivi > Utenti/AAA > Account utente**.



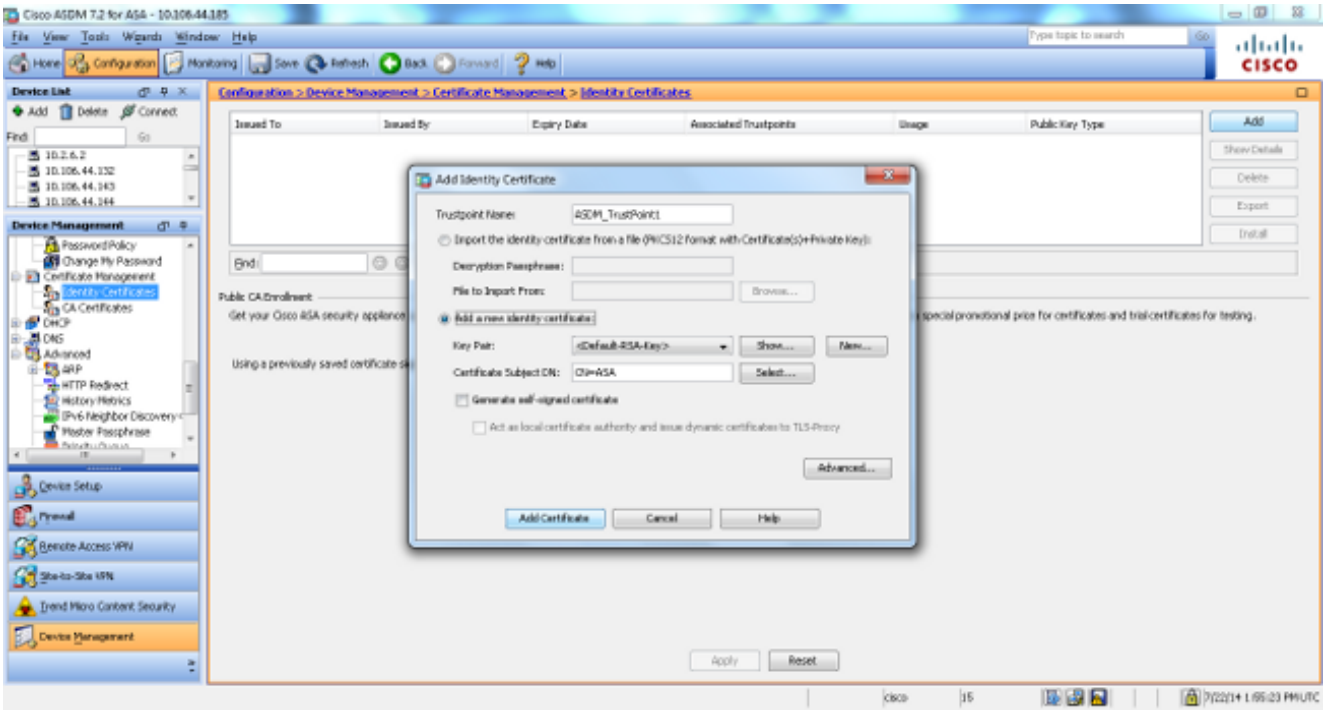
2. Per configurare l'autenticazione AAA per SSH con ASDM, selezionare **Configurazione > Gestione dispositivi > Utenti/AAA > Accesso AAA > Autenticazione**.



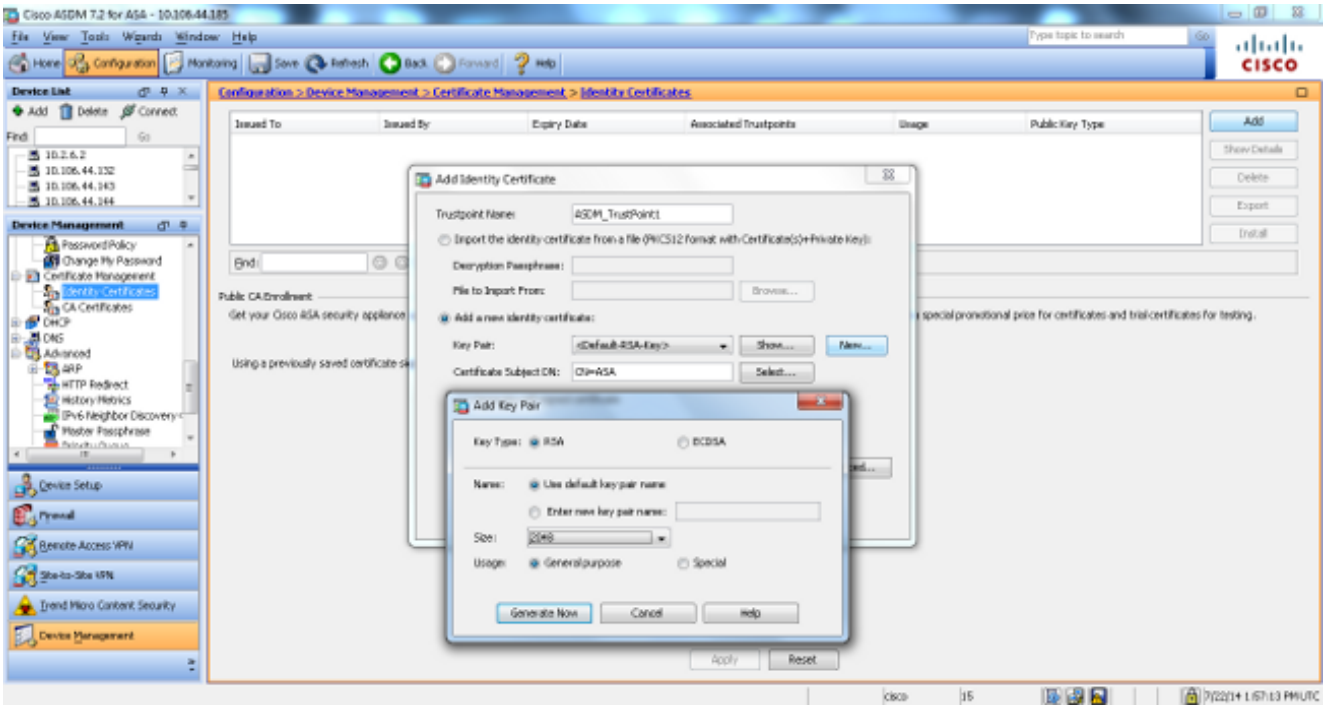
3. Per modificare la password Telnet con ASDM, selezionare **Configurazione > Configurazione dispositivo > Nome/password**.



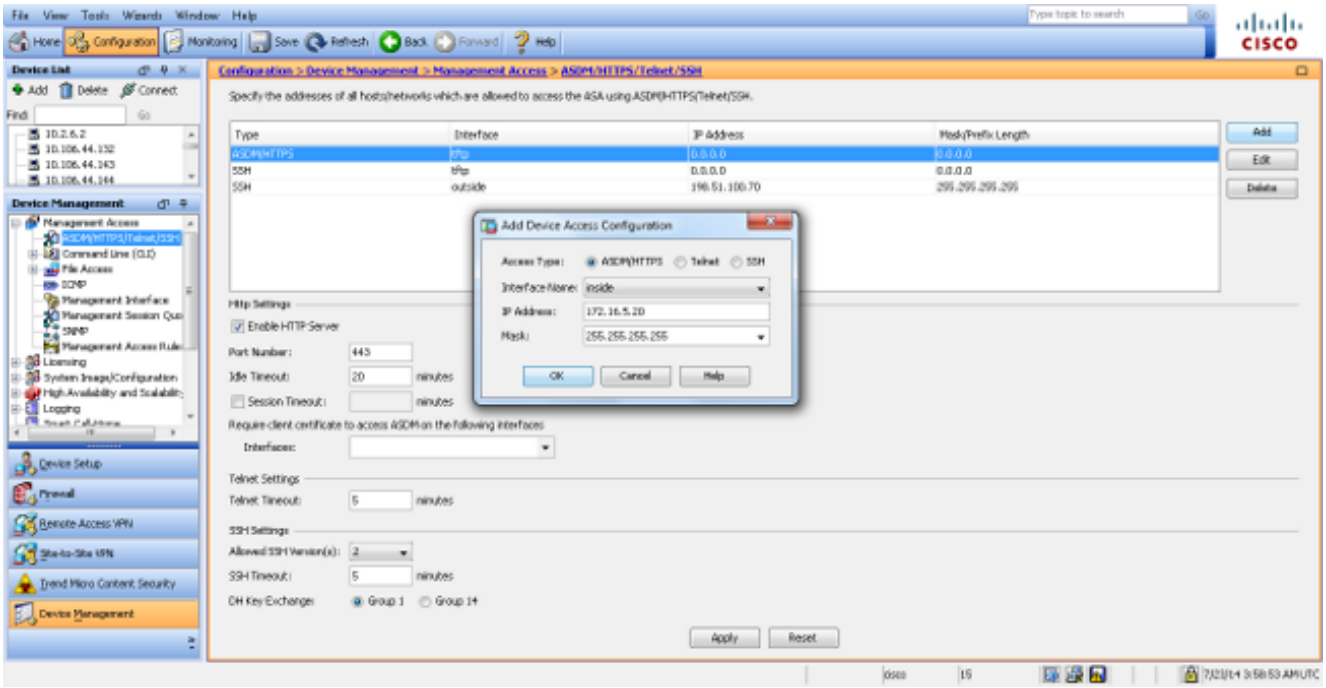
4. Selezionare **Configurazione > Gestione dispositivi > Gestione certificati > Certificati di identità**, fare clic su **Aggiungi** e usare le opzioni predefinite disponibili per generare le stesse chiavi RSA con ASDM.



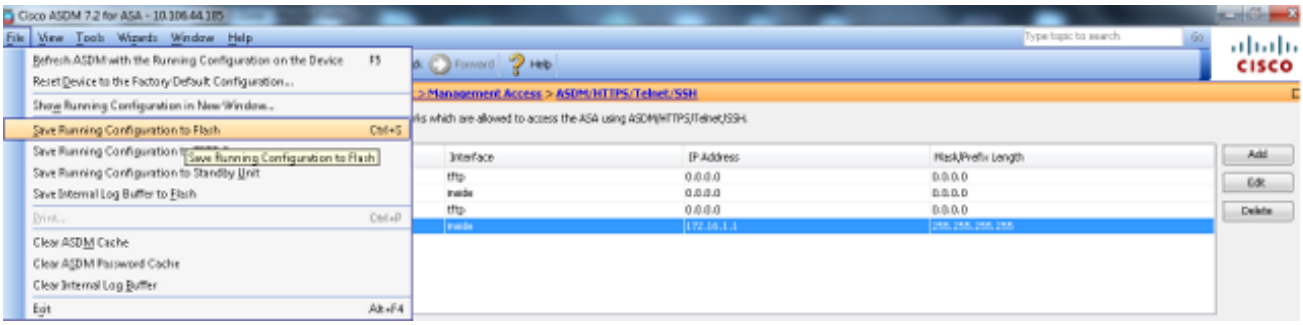
5. Fare clic sul pulsante di scelta **Aggiungi nuovo certificato di identità** e scegliere **Nuovo** per aggiungere una coppia di chiavi predefinita, se non ne esiste una. Al termine, fare clic su **Genera adesso**.



6. Per utilizzare ASDM in modo da poter specificare gli host a cui è consentito connettersi con SSH e specificare le opzioni di versione e timeout, selezionare **Configuration > Device Management > Management Access > Command Line (CLI) > Secure Shell (SSH)**.



7. Per salvare la configurazione, fare clic su **Save** (Salva) dalla finestra popup.



8. Quando viene chiesto di salvare la configurazione sulla memoria flash, scegliere **Apply** (Applica) per salvarla.

Configurazione Telnet

Per aggiungere l'accesso Telnet alla console e impostare il timeout di inattività, immettere il comando **telnet** in modalità di configurazione globale. Per impostazione predefinita, le sessioni Telnet rimaste inattive per cinque minuti vengono chiuse dall'appliance di sicurezza. Per rimuovere l'accesso Telnet da un indirizzo IP impostato in precedenza, utilizzare la forma **no** di questo comando.

```
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}}
```

Il comando **telnet** consente di specificare gli host che possono accedere alla console dell'appliance di sicurezza tramite Telnet.

> **Nota:** È possibile abilitare Telnet per l'appliance di sicurezza su tutte le interfacce. Tuttavia, l'appliance di sicurezza richiede che tutto il traffico Telnet diretto all'interfaccia esterna sia protetto da IPsec. Per abilitare una sessione Telnet con l'interfaccia esterna, configurare IPsec sull'interfaccia esterna in modo che includa il traffico IP generato dall'appliance di sicurezza e abilitare Telnet sull'interfaccia esterna.

> **Nota:** In generale, se un'interfaccia ha un livello di sicurezza pari a zero o inferiore a quello di un'altra interfaccia, l'ASA non consente il collegamento Telnet all'interfaccia.

> **Nota:** Cisco sconsiglia di accedere all'appliance di sicurezza tramite una sessione Telnet. Le informazioni sulle credenziali di autenticazione, ad esempio la password, vengono inviate come testo non crittografato. Cisco consiglia di utilizzare il protocollo SSH per una comunicazione dei dati più protetta.

Immettere il comando **password** per impostare una password per l'accesso Telnet alla console. La password predefinita è **cisco**. Immettere il comando **who** per visualizzare gli indirizzi IP che accedono attualmente alla console dell'appliance di sicurezza. Immettere il comando **kill** per terminare una sessione console Telnet attiva.

Scenari di esempio in Telnet

Per abilitare una sessione Telnet per l'interfaccia interna, rivedere gli esempi forniti in questa sezione.

Esempio 1

Nell'esempio seguente viene consentito solo all'host **172.16.5.20** di accedere alla console dell'appliance di sicurezza tramite Telnet:

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

Esempio 2

Nell'esempio seguente viene consentito solo l'accesso alla console dell'accessorio di sicurezza tramite Telnet alla rete **172.16.5.0/24**:

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

Esempio 3

Nell'esempio seguente viene consentito a tutte le reti di accedere alla console dell'accessorio di protezione tramite Telnet:

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

Se si utilizza il comando **aaa** con la parola chiave console, l'accesso alla console Telnet deve essere autenticato con un server di autenticazione.

> **Nota:** Se si configura il comando **aaa** per richiedere l'autenticazione dell'accessorio di sicurezza e l'accesso alla console Telnet e la richiesta di accesso alla console scade, è possibile accedere all'accessorio di sicurezza dalla console seriale. A tale scopo, immettere il nome utente e la password dell'accessorio di protezione impostati con il comando **enable password**.

Utilizzare il comando **telnet timeout** per impostare il tempo massimo di inattività di una sessione Telnet della console prima che l'accessorio di sicurezza la disconnetta. non è possibile usare il comando **no telnet** con il comando **telnet timeout**.

Nell'esempio viene mostrato come modificare la durata massima di inattività della sessione:

```
hostname(config)#telnet timeout 10

hostname(config)#show running-config telnet timeout

telnet timeout 10 minutes
```

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

> **Nota:** Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Debug SSH

Immettere il comando **debug ssh** per abilitare il debug SSH:

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

Questo output mostra un tentativo SSH da un indirizzo IP interno (172.16.5.20) all'interfaccia interna dell'ASA. I debug riportati di seguito mostrano la riuscita della connessione e dell'autenticazione.

```
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
```

Se si immette un nome utente errato, ad esempio **cisco1** anziché **cisco**, il firewall ASA rifiuta l'autenticazione. Questo output di debug visualizza l'autenticazione non riuscita:

```
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.
```

Analogamente, se viene specificata una password errata, l'autenticazione non riesce. Questo output di debug visualizza l'autenticazione non riuscita:

```
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.
```

Visualizzazione delle sessioni SSH attive

Immettere questo comando per verificare il numero di sessioni SSH connesse (e lo stato della connessione) all'appliance 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
```

Per visualizzare le sessioni con ASDM, selezionare **Monitoraggio > Proprietà > Accesso dispositivo > Sessioni Secure Shell**.

Immettere il comando **show asp table socket** per verificare che la sessione TCP sia stata stabilita:

```
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
```

Visualizza chiavi RSA pubbliche

Immettere questo comando per visualizzare la parte pubblica delle chiavi RSA sull'appliance di sicurezza:

```
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
```

Passare a **Configurazione > Proprietà > Certificato > Coppia di chiavi** e fare clic su **Mostra dettagli** per visualizzare le chiavi RSA con ASDM.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Rimozione delle chiavi RSA dall'appliance ASA

In alcune situazioni, ad esempio quando si aggiorna il software ASA o si modifica la versione SSH nell'appliance ASA, potrebbe essere necessario rimuovere e ricreare le chiavi RSA. Immettere questo comando per rimuovere la coppia di chiavi RSA dall'appliance ASA:

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

Selezionare **Configurazione > Proprietà > Certificato > Coppia di chiavi**, quindi fare clic su **Elimina** per rimuovere le chiavi RSA da ASDM.

Connessione SSH non riuscita

Sull'appliance ASA viene visualizzato questo messaggio:

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

Questo è il messaggio di errore che viene visualizzato sul computer client SSH:

```
Selected cipher type
```

Per risolvere il problema, rimuovere e ricreare le chiavi RSA. Immettere questo comando per rimuovere la coppia di chiavi RSA dall'appliance ASA:

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

Immettere questo comando per generare la nuova chiave:

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