Come configurare l'autenticazione con chiave pubblica SSH per il login all'ESA senza password

Introduzione

In questo documento viene descritto come generare una chiave SSH (Secure Shell) privata e come usarla per il nome utente e l'autenticazione quando si accede all'interfaccia della riga di comando (CLI) su Cisco Email Security Appliance (ESA).

Come configurare l'autenticazione con chiave pubblica SSH per il login all'ESA senza password

L'autenticazione a chiave pubblica (PKI) è un metodo di autenticazione basato su una coppia di chiavi pubblica/privata generata. Con PKI, viene generata una "chiave" speciale che ha una proprietà molto utile: Chiunque sia in grado di leggere la metà pubblica della chiave è in grado di crittografare i dati che possono essere letti solo da una persona che ha accesso alla metà privata della chiave. In questo modo, l'accesso alla metà pubblica di una chiave consente di inviare informazioni segrete a chiunque abbia la metà privata, e di verificare che una persona abbia effettivamente accesso alla metà privata. È facile capire come questa tecnica possa essere utilizzata per l'autenticazione.

Gli utenti possono generare una coppia di chiavi e posizionare la metà pubblica della chiave su un sistema remoto, ad esempio sull'ESA. Il sistema remoto è quindi in grado di autenticare l'ID utente e di consentirvi di accedere semplicemente dimostrando di avere accesso alla metà privata della coppia di chiavi. Questa operazione viene effettuata a livello di protocollo all'interno del protocollo SSH e viene eseguita automaticamente.

Ciò significa tuttavia che è necessario proteggere la privacy della chiave privata. In un sistema condiviso in cui non si dispone di root, è possibile eseguire questa operazione crittografando la chiave privata con una passphrase, che funziona in modo simile a una password. Prima che SSH possa leggere la chiave privata per eseguire l'autenticazione della chiave pubblica, vi verrà chiesto di fornire la passphrase in modo che la chiave privata possa essere decrittografata. Su sistemi più sicuri (come un computer in cui l'utente è l'unico utente o un computer di casa in cui nessun estraneo avrà accesso fisico) è possibile semplificare questo processo creando una chiave privata non crittografata (senza passphrase) o immettendo la passphrase una volta e quindi memorizzando la chiave nella cache per la durata del tempo trascorso al computer. OpenSSH contiene uno strumento chiamato ssh-agent che semplifica questo processo.

Esempio di ssh-keygen per Linux/Unix

Completare la procedura seguente per configurare una workstation (o un server) Linux/Unix per la connessione all'ESA senza password. In questo esempio non verrà specificata come passphrase.

1) Sulla workstation (o sul server), generare una chiave privata utilizzando il comando Unix **ssh-**

keygen:

```
$ ssh-keygen -b 2048 -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/[USERID]/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/[USERID]/.ssh/id_rsa.
Your public key has been saved in /home/[USERID]/.ssh/id_rsa.pub.
The key fingerprint is:
00:11:22:77:f6:a9:1e:19:f0:ca:28:9c:ff:00:11:22 [USERID]@hostname.com
The key's randomart image is:
+--[ RSA 2048]----+
| +... +|
| o= o+|
| o o ..|
| . ..o . + |
| . ES. o + |
| o + . . |
| o . . |
| o o |
| . . |
+-----------------+
```

(*quanto sopra è stato generato da un Ubuntu 14.04.1)

2) Aprire il file della chiave pubblica (id_rsa.pub) creato in #1 e copiare l'output:

```
$ cat .ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDJg9W3DeGf83m+E/PLGzUFPalSoJz5F
t54Wl2wUS36NLxm4IO4Xfrrb5bA97I+ZA4YcB1l/HsFLZcoljAK4uBbmpY5kXg96A6Wf
mIYMnl+nV2vrhrODgbcicEAdMcQN3wWHXiEWacV+6u+FlHlonkSAIDEug6vfnd+bsbcP
Zz2uYnx1llxbVtGftbWVssBK3LkFp9f0GwDiYs7LsXvQbTkixrECXqeSrr+NLzhU5hf6
eb9Kn8xjytf+eFbYAslam/NEfl9i4rjide1ebWN+LnkdcE5eQ0ZsecBidXv0KNf45RJa
KgzF7joke9niLfpf2sgCTiFxg+qZ0rQludntknw [USERID]@hostname.com
```

3) Effettuare il login all'appliance e configurare l'ESA in modo che riconosca la workstation (o il server) usando la chiave SSH pubblica creata al numero 1, quindi **eseguire** il **commit** delle modifiche. Notare la richiesta della password durante l'accesso:

```
$ ssh admin@192.168.0.199
******************************
CONNECTING to myesa.local
Please stand by...
******************************

Password:[PASSWORD]
Last login: Mon Aug 18 14:11:40 2014 from 192.168.0.200
Copyright (c) 2001-2013, Cisco Systems, Inc.


AsyncOS 8.5.6 for Cisco C100V build 074

Welcome to the Cisco C100V Email Security Virtual Appliance

myesa.local> sshconfig

Currently installed keys for admin:
```

```
Choose the operation you want to perform:
- NEW - Add a new key.
- USER - Switch to a different user to edit.
[]> new

Please enter the public SSH key for authorization.
Press enter on a blank line to finish.
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDJg9W3DeGf83m+E/PLGzUFPalSoJz5F
t54Wl2wUS36NLxm4IO4Xfrrb5bA97I+ZA4YcB1l/HsFLZcoljAK4uBbmpY5kXg96A6Wf
mIYMnl+nV2vrhrODgbcicEAdMcQN3wWHXiEWacV+6u+FlHlonkSAIDEug6vfnd+bsbcP
Zz2uYnx1llxbVtGftbWVssBK3LkFp9f0GwDiYs7LsXvQbTkixrECXqeSrr+NLzhU5hf6
eb9Kn8xjytf+eFbYAslam/NEfl9i4rjide1ebWN+LnkdcE5eQ0ZsecBidXv0KNf45RJa
KgzF7joke9niLfpf2sgCTiFxg+qZ0rQludntknw [USERID]@hostname.com

Currently installed keys for admin:
1. ssh-rsa AAAAB3NzaC1yc2EAA...rQludntknw ([USERID]@hostname.com)

Choose the operation you want to perform:
- NEW - Add a new key.
- DELETE - Remove a key.
- PRINT - Display a key.
- USER - Switch to a different user to edit.
[]>

myesa.local> commit
```

4) Uscire dall'accessorio e accedere nuovamente. Si noti che la richiesta della password viene rimossa e l'accesso viene concesso direttamente:

```
myesa.local> exit

Connection to 192.168.0.199 closed.
robert@ubuntu:~$ ssh admin@192.168.0.199
******************************
CONNECTING to myesa.local
Please stand by...
******************************

Last login: Mon Aug 18 14:14:50 2014 from 192.168.0.200
Copyright (c) 2001-2013, Cisco Systems, Inc.


AsyncOS 8.5.6 for Cisco C100V build 074

Welcome to the Cisco C100V Email Security Virtual Appliance
myesa.local>
```

esempio ssh-keygen per Windows

Completare i seguenti passaggi per configurare una workstation Windows (o un server) per la connessione all'ESA senza password. In questo esempio non verrà specificata come passphrase.

> **Nota**: sono presenti differenze nell'applicazione console utilizzata da Windows. Sarà necessario ricercare e trovare la soluzione più adatta per la propria applicazione console. In questo esempio verranno utilizzati PuTTy e PuTTyGen.

1) Aprire PuttyGen.

2) Per Tipo di chiave da generare, selezionare SSH-2 RSA.

3) Fare clic sul pulsante **Genera**.

4) Spostare il mouse nell'area sotto la barra di avanzamento. Quando la barra di avanzamento è piena, PuTTYgen genera la coppia di chiavi.

5) Digitare una passphrase nel campo Passphrase chiave. Digitare la stessa passphrase nel campo Conferma passphrase. È possibile utilizzare una chiave senza una passphrase, ma questa operazione non è consigliata.

6) Fare clic sul pulsante **Save private key** (Salva chiave privata) per salvare la chiave privata.

> **Nota**: è necessario salvare la chiave privata. Sarà necessario per la connessione al computer.

7) Fare clic con il pulsante destro del mouse nel campo di testo Chiave pubblica per incollare nel file OpenSSH authorized_keys e scegliere **Seleziona tutto**.

8) Fare nuovamente clic con il pulsante destro del mouse nello stesso campo di testo e scegliere **Copia**.

9) Usando PuTTY, accedere all'appliance e configurare l'ESA in modo che riconosca la workstation Windows (o il server) usando la chiave SSH pubblica salvata e copiata dal numero 6 al numero 8, quindi eseguire il commit delle modifiche. Notare la richiesta della password durante l'accesso:

```
login as: admin
Using keyboard-interactive authentication.
Password: [PASSWORD]
Last login: Mon Aug 18 11:46:17 2014 from 192.168.0.201
Copyright (c) 2001-2013, Cisco Systems, Inc.


AsyncOS 8.5.6 for Cisco C100V build 074

Welcome to the Cisco C100V Email Security Virtual Appliance
myesa.local> sshconfig

Currently installed keys for admin:

Choose the operation you want to perform:
- NEW - Add a new key.
- USER - Switch to a different user to edit.
[]> new

Please enter the public SSH key for authorization.
Press enter on a blank line to finish.
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAj6ReI+gqLU3W1uQAMUG0620B+tpdkjkgBn
5NfYc+qrtyB93stG38O1T4s0zHnhuKJLTdwBg/JHdFuNO77BY+21GYGS27dMp3UT9/VuQ
TjP8DmWKOa+8Mpc9ePdCBZp1C4ct9oroidUT3V3Fbl5M9rL8q4/gonSi+7iFc9uOaqgDM
/h+RxhYeFdJLechMY5nN0adViFloKGmV1tz3K9t0p+jEW5l9TJf+fl5X6yxpBBDoNcaB9
jNwQ5v7vcIZBv+fl98OcXD9SNt08G0XaefyD2VuphtNA5EHwx+f6eeA8ftlmO+PgtqnAs
c2T+i3BAdC73xwML+1IG82zY51pudntknw rsa-key-20140818

Currently installed keys for admin:
1. ssh-rsa AAAAB3NzaC1yc2EAA...51pudntknw (rsa-key-20140818)
```

```
Choose the operation you want to perform:
- NEW - Add a new key.
- DELETE - Remove a key.
- PRINT - Display a key.
- USER - Switch to a different user to edit.
[]>

myesa.local> commit
```

10) Dalla finestra di configurazione di PuTTy e la sessione salvata preesistente per l'ESA, scegliere **Connessione > SSH > Auth** e nel campo *File della chiave privata per l'autenticazione*, fare clic su **Sfoglia** e individuare la chiave privata salvata dal passo 6.

11) Salvare la sessione (profilo) in PuTTY e fare clic su **Apri**. Eseguire l'accesso con il nome utente, se non è già stato salvato o specificato dalla sessione preconfigurata. Si noti l'inclusione di "Autenticazione con chiave pubblica "[NOME FILE DELLA CHIAVE PRIVATA SALVATA]" durante l'accesso:

```
login as: admin
Authenticating with public key "rsa-key-20140818"
Last login: Mon Aug 18 11:56:49 2014 from 192.168.0.201
Copyright (c) 2001-2013, Cisco Systems, Inc.


AsyncOS 8.5.6 for Cisco C100V build 074

Welcome to the Cisco C100V Email Security Virtual Appliance
myesa.local>
```

Informazioni correlate

- Cisco Email Security Appliance - Guide per l'utente
- Documentazione e supporto tecnico – Cisco Systems