Introducción

Este documento describe cómo generar una clave privada del Secure Shell (SSH) y utilizar eso para el nombre de usuario y la autenticación al registrar en el comando line interface(cli) en el dispositivo de seguridad del correo electrónico de Cisco (ESA).

Cómo configurar la autenticación de la clave pública de SSH para el login al ESA sin una contraseña

La autenticación de la clave pública (PKI) es un método de autentificación que confía en un keypair público/privado generado. Con el PKI, se genera una “clave especial” que tiene una propiedad muy útil: Cualquier persona que puede leer la mitad pública de la clave puede cifra los datos que se pueden entonces leer solamente por una persona que tenga acceso a la mitad privada de la clave. De esta manera, tener acceso a la mitad pública de una clave permite que usted envíe la información secreta a cualquier persona con la mitad privada, y también que la verifique que una persona de hecho tiene acceso a la mitad privada. Es fácil ver cómo esta técnica se podría utilizar para autenticar.

Como usuario, usted puede generar un keypair y después poner la mitad pública de la clave en un sistema remoto, tal como su ESA. Ese sistema remoto puede entonces autenticar su identificación del usuario, y permite que usted inicie sesión apenas teniéndole demuestra que usted tiene acceso a la mitad privada del keypair. Esto se hace en el nivel del protocolo dentro de SSH y sucede automáticamente.

, Sin embargo, significa que usted necesita proteger la aislamiento de la clave privada. En un sistema compartido donde usted no tiene raíz esto puede ser lograda cifrando la clave privada con un passphrase, que funciona semejantemente a una contraseña. Antes de que SSH pueda leer su clave privada para realizar la autenticación de la clave pública le pedirán suministrar el passphrase para poder desencriptar la clave privada. En más sistemas seguros (como una máquina donde usted está el único usuario, o una máquina en su hogar en donde ningunos extranjeros tendrán acceso físico) usted puede simplificar este proceso creando una clave privada unencrypted (sin el passphrase) o ingresando su passphrase una vez y después ocultando la clave en la memoria para la duración de su tiempo en el ordenador. OpenSSH contiene una herramienta llamada el SSH-agente que simplifica este proceso.

ejemplo de SSH-keygen para Linux/Unix

Complete los pasos siguientes para configurar su un linux/un puesto de trabajo de unix (o un servidor) a conectar con el ESA sin una contraseña. En este ejemplo, no especificaremos como passphrase.

1) En su puesto de trabajo (o el servidor), genere una clave privada usando el 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 |
| . . |
+-----------------+
```

(el *the antedicho fue generado de Ubuntu 14.04.1)

2) abre el archivo de clave pública (id_rsa.pub) creó en #1 y copia la salida:

```
$ 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) Inicie sesión a su dispositivo y configure su ESA para reconocer su puesto de trabajo (o el servidor) usando la clave pública de SSH que usted creó en #1, y **confíe los** cambios. Note el prompt de contraseña durante el login:

```
$ 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) Salga el dispositivo de los, y el re-login. Note que el prompt de contraseña está quitado, y el acceso está concedido directamente:

```
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>
```

ejemplo de SSH-keygen para Windows

Complete los pasos siguientes para configurar su una estación de trabajo con Windows (o el servidor) a conectar con el ESA sin una contraseña. En este ejemplo, no especificaremos como passphrase.

> Nota: Hay una variación en la aplicación de consola usada de Windows. Usted necesitará investigar y encontrar la solución que trabaja mejor para su aplicación de consola. Este

ejemplo utilizará el putty y PuTTyGen.

1) Abra PuttyGen.

2) Para el tipo de clave a generar, seleccione SSH-2 RSA.

3) Haga clic el botón de la **generación**.

4) Mueva su ratón en el área debajo de la barra de progreso. Cuando la barra de progreso es llena, el PuTTYgen genera su par clave.

5) Teclee un passphrase en el campo dominante del passphrase. Teclee el mismo passphrase en el campo del passphrase del confirmar. Usted puede utilizar una clave sin un passphrase, pero esto no se recomienda.

6) Haga clic el botón de la **clave privada de la salvaguardia** para salvar la clave privada.

Nota: Usted debe salvar la clave privada. Usted la necesitará conectar con su máquina.

7) Haga clic con el botón derecho del ratón en el campo de texto etiquetado clave pública para pegar en los authorized_keys de OpenSSH el archivo y elija **selecto todos**.

8) Haga clic con el botón derecho del ratón otra vez en el mismo campo de texto y elija la **copia**.

9) Usando el putty, inicie sesión a su dispositivo y configure su ESA para reconocer su estación de trabajo con Windows (o el servidor) usando la clave pública de SSH que usted guardó y copió de #6 - #8, y confía los cambios.

```
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) De la ventana de configuración del putty, y de su sesión guardada preexistente para su ESA, elija la **conexión > SSH > el auth** y en el *archivo de clave privado para el* campo de la *autenticación*, el tecleo **hojea** y encuentra su clave privada guardada del paso #6.

11) Salve la sesión (perfil) en el putty, y haga clic **abierto**. Inicie sesión con el nombre de usuario, si no guardado ya o especificado de la sesión preconfigurada. Note la inclusión de la "autenticidad con la clave pública "[FILE-NAME OF SAVED PRIVATE KEY]" al abrir una sesión:

```
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
```

Información Relacionada

- Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final
- Soporte Técnico y Documentación - Cisco Systems