如何配置SSH公鑰身份驗證，以便在不使用密碼的情況下登入ESA

簡介

本文說明如何產生私人安全殼層(SSH)金鑰，並在登入思科電子郵件安全裝置(ESA)上的指令行介面(CLI)時使用該金鑰進行使用者名稱和驗證。

如何配置SSH公鑰身份驗證，以便在不使用密碼的情況下登入ESA

公開金鑰驗證(PKI)是一種依賴產生的公開/私人金鑰對的驗證方法。使用PKI生成了一個特殊的「金鑰」，它具有非常有用的特性：任何能夠讀取金鑰的公用部分的人都能夠加密資料，然後只有有權訪問金鑰的專用部分的人才能讀取資料。通過這種方式，您可以訪問金鑰的公用部分，從而向擁有該公用部分的任何人傳送秘密資訊，並且還可以驗證個人是否實際擁有該公用部分的訪問許可權。我們很容易明白如何利用這種技術來進行身份驗證。

作為使用者，您可以生成金鑰對，然後將金鑰的公用部分放在遠端系統（例如ESA）上。然後，該遠端系統可以驗證您的使用者ID，並讓您通過證明您有權訪問金鑰對的私有部分來登入。此操作在SSH內的協定級別完成，並自動執行。

但是，這意味著您需要保護私鑰的隱私。在沒有root許可權的共用系統上，可以通過使用密碼短語加密私鑰來完成此操作，該密碼的作用與密碼類似。在SSH能夠讀取您的私鑰以執行公鑰驗證之前，系統會要求您提供密碼以便可以解密私鑰。在更安全的系統上（例如您是唯一的使用者的電腦，或您家裡沒有陌生人可以實際訪問的電腦），您可以簡化此過程，方法是：建立一個未加密的私鑰（沒有密碼短語），或者輸入一次您的密碼短語，然後在電腦中儲存該金鑰一段時間。OpenSSH包含一個稱為ssh-agent的工具，可簡化此過程。

ssh-keygen Linux/Unix示例

完成以下步驟，設定linux/unix工作站（或伺服器），使其無需密碼即可連線到ESA。 在此範例中，我們不會指定為密碼短語。

1)在工作站（或伺服器）上，使用Unix命令**ssh-keygen**生成私鑰：

```
$ 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 |
| . . |
+-----------------+
```

（*上述資料來自Ubuntu 14.04.1）

2)開啟在中建立的公鑰檔案(id_rsa.pub#1並複製輸出：

```
$ 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)登入您的裝置並配置ESA以使用您在#1中建立的公共SSH金鑰識別您的工作站（或伺服器），然後提交更改內容。 請注意登入期間的密碼提示：

```
$ 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)退出裝置，然後重新登入。 請注意，密碼提示已刪除，且直接授予訪問許可權：

```
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>
```

windows的ssh-keygen示例

完成以下步驟，設定您的Windows工作站（或伺服器），使其無需密碼即可連線到ESA。 在此範例中，我們不會指定為密碼短語。

> **注意**：在Windows中使用的控制檯應用程式上存在變體。 您需要研究和尋找最適合您的控制檯應用程式的解決方案。 本示例將使用PuTTy和PuTTyGen。

1)開啟PuttyGen。

2)對於要生成的金鑰型別，請選擇SSH-2 RSA。

3)按一下**Generate**按鈕。

4)在進度條下方的區域移動滑鼠。當進度條已滿時，PuTTYgen會生成金鑰對。

5)在Key passphrase欄位中鍵入密碼。在「確認密碼短語」欄位中鍵入相同的密碼短語。您可以使用沒有密碼短語的金鑰，但不建議這樣做。

6)按一下**Save private key**按鈕儲存私鑰。

> **註**：必須儲存私鑰。您需要它才能連線到您的電腦。

7)在標有Public key（公鑰）的文本欄位中按一下右鍵，以貼上到OpenSSH authorized_keys檔案中，然後選擇**Select All**。

8)在同一文本欄位中再次按一下右鍵，然後選擇**Copy**。

9)使用PuTTY登入您的設備，使用您從#6 - #8儲存和複製的公共SSH金鑰配置ESA以識別您的Windows工作站（或伺服器），然後提交更改。 請注意登入期間的密碼提示：

```
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)在PuTy配置視窗和預先存在的ESA已儲存會話中，選擇**Connection > SSH > Auth**，然後在*Private key file for authentication*欄位中，按一下**Browse**，從步驟#6中查詢已儲存的私鑰。

11)在PuTTY中儲存會話（配置檔案），然後按一下**Open**。 使用使用者名稱（如果尚未儲存或從預配置的會話指定）登入。 請注意登入時包含「使用公鑰進行身份驗證」[已儲存私鑰的檔名]:

```
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>
```

相關資訊

- Cisco Email Security Appliance — 最終使用手冊
- 技術支援與文件 - Cisco Systems