如何配置SSH登录的公共密钥验证到ESA，不用密码

简介

本文描述如何生成一私有安全壳SSH密钥和使用那用户名和验证，当登录在Cisco电子邮件安全工具时(ESA)的命令行界面(CLI)。

如何配置SSH登录的公共密钥验证到ESA，不用密码

公共密钥验证(PKI)是依靠一生成的公共/私有密钥对的认证方法。使用PKI，有一非常有用的属性的一特殊"密钥"生成：能读密钥的公共半的人能加密可能由人只然后读访问密钥的私有半的数据。这样，访问密钥的公共半允许您发送秘密信息到任何人与私有半和也验证人实际上访问私有半。发现是容易的此技术如何可能用于验证。

作为用户，您在一个远程系统能生成密钥对然后放置密钥的公共半，例如您的ESA。该远程系统然后能验证您的用户ID，并且允许您由有登陆您显示出，您访问密钥对的私有半。这执行在协议级在SSH里面并且自动地发生。

它，然而，请意味着您需要保护专用密钥的保密性。在您没有根的一个共享系统上这可以通过加密与密码短语的专用密钥完成，类似作用于密码。在SSH能读您的专用密钥为了执行公共密钥验证前您将询问供应密码短语，以便专用密钥可以解密。在更多安全系统上(类似您是唯一的用户的计算机或者一计算机在陌生人不会访问物理访问)的您的家您能简化此进程通过创建一未加密专用密钥(没有密码短语)或通过一次输入您的密码短语然后缓存密钥在内存处于您的时间的在计算机。OpenSSH包含呼叫简化此进程的SSH代理程序的工具。

Linux/Unix的SSHkeygen示例

完成以下步骤设置您)连接的Linux/UNIX工作站(或服务器对ESA，不用密码。 在本例中，我们不会指定作为密码短语。

1) 在您的工作站(或服务器上)使用unix命令**SSHkeygen**，请生成专用密钥：

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

(以上的*the从Ubuntu 14.04.1)生成

2)打开在#1 (id_rsa.pub)创建的公共密钥关键文件并且复制输出：

```
$ 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) 登陆到您的设备并且配置您的ESA认可您的工作站(或服务器)使用您在#1创建的公共SSH密钥，并且**确认**更改。 在登录期间，注意密码提示：

```
$ 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) 退出在设备和重新登录外面。 注意密码提示删除，并且访问直接地授权：

```
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SSHkeygen示例

完成以下步骤设置您)连接的Windows工作站(或服务器对ESA，不用密码。 在本例中，我们不会指定作为密码短语。

> **Note**: 有在从Windows使用的控制台应用程序的变化。 您将需要研究和查找工作最佳您的控制台应用程序的解决方案。 此示例将使用PuTTY和PuTTyGen。

1) 打开PuttyGen。

2) 对于生成的密钥的类型，请选择SSH-2 RSA。

3) 点击**生成**按钮。

4) 在进度条之下移动您的鼠标在区域。当进度条全双工时， PuTTYgen生成您的密钥对。

5) 在关键密码短语字段键入一密码短语。在确认密码短语字段键入同样密码短语。您能使用密钥，不用密码短语，但是没有推荐这。

6) 点击**保存专用密钥**按钮保存专用密钥。

> **Note**: 您必须保存专用密钥。您将需要它连接到您的计算机。

7) 在文本字段用鼠标右键单击被标记粘贴的到OpenSSH authorized_keys文件公共密钥并且选择**选择所有**。

8) 在同一个文本字段再用鼠标右键单击并且选择**复制**。

9) 使用PuTTY，请登陆到您的设备并且配置您的ESA认可您的Windows工作站(或服务器)使用从#6已保存和复制的您- #8，和确认更改的公共SSH密钥。 在登录期间，注意密码提示：

```
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) 从PuTTY配置窗口和您已存在的已保存会话您的ESA的，请选择**连接> SSH >验证**和在*专用密钥文件验证*字段的，单击**浏览**并且查找您的已保存专用密钥从步骤#6。

11) 救会话(配置文件) PuTTY的，并且点击**开放**。 登陆与用户名，如果不已经已保存或指定从预先配置的会话。 请注意“正在验证包括用公共密钥“[FILE-NAME OF SAVED PRIVATE KEY]”，当登陆时：

```
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
```

相关信息

- **思科电子邮件安全工具-最终用户指南**

- 技术支持和文档 - Cisco Systems