So konfigurieren Sie die SSH Public Key Authentication für die Anmeldung bei der ESA ohne Kennwort

Einführung

In diesem Dokument wird beschrieben, wie Sie einen SSH-Schlüssel (Private Secure Shell) generieren und diesen für Benutzernamen und Authentifizierung verwenden, wenn Sie sich bei der Befehlszeilenschnittstelle (CLI) der Cisco E-Mail Security Appliance (ESA) anmelden.

So konfigurieren Sie die SSH Public Key Authentication für die Anmeldung bei der ESA ohne Kennwort

Die Public-Key-Authentifizierung (PKI) ist eine Authentifizierungsmethode, die auf einem generierten öffentlichen/privaten Tastenfeld basiert. Mit PKI wird ein spezieller "Schlüssel" generiert, der eine sehr nützliche Eigenschaft besitzt: Jeder, der die öffentliche Hälfte des Schlüssels lesen kann, kann Daten verschlüsseln, die dann nur von einer Person gelesen werden können, die Zugriff auf die private Hälfte des Schlüssels hat. Auf diese Weise, den Zugang zur öffentlichen Hälfte eines Schlüssels ermöglicht es Ihnen, geheime Informationen an jeden mit der privaten Hälfte zu senden und auch zu überprüfen, dass eine Person tatsächlich Zugriff auf die private Hälfte. Es ist leicht zu erkennen, wie diese Technik verwendet werden könnte, um sich zu authentifizieren.

Als Benutzer können Sie ein Tastenfeld generieren und dann die öffentliche Hälfte des Schlüssels auf einem Remote-System wie der ESA ablegen. Dieses Remote-System kann dann Ihre Benutzer-ID authentifizieren und Sie können sich anmelden, indem Sie zeigen, dass Sie Zugriff auf die private Hälfte der Tastatur haben. Dies erfolgt auf Protokollebene innerhalb von SSH und erfolgt automatisch.

Dies bedeutet jedoch, dass Sie die Privatsphäre des privaten Schlüssels schützen müssen. Auf einem freigegebenen System ohne root kann dies durch die Verschlüsselung des privaten Schlüssels mit einer Passphrase erreicht werden, die ähnlich wie ein Kennwort funktioniert. Bevor SSH Ihren privaten Schlüssel lesen kann, um die Authentifizierung des öffentlichen Schlüssels durchzuführen, werden Sie aufgefordert, die Passphrase anzugeben, damit der private Schlüssel entschlüsselt werden kann. Auf sichereren Systemen (wie einem Computer, auf dem Sie der einzige Benutzer sind, oder einem Computer zu Hause, auf dem keine Fremden physischen Zugriff haben) können Sie diesen Prozess entweder durch Erstellen eines unverschlüsselten privaten Schlüssels (ohne Passphrase) oder durch einmalige Eingabe Ihrer Passphrase und anschließendes Zwischenspeichern des Schlüssels im Speicher für die Dauer Ihrer Zeit am Computer vereinfachen. OpenSSH enthält ein Tool namens ssh-agent, das diesen Prozess vereinfacht.

ssh-keygen-Beispiel für Linux/Unix

Führen Sie die folgenden Schritte aus, um eine Linux/Unix-Workstation (oder einen Server) für die

Verbindung zur ESA ohne Kennwort einzurichten. In diesem Beispiel geben wir keine Passphrase an.

1) Erstellen Sie auf Ihrer Workstation (oder Ihrem Server) mithilfe des Unix-Befehls **ssh-keygen** einen privaten Schlüssel:

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

(*die obigen Informationen wurden aus Ubuntu 14.04.1 generiert)

2) Öffnen Sie die in Nr. 1 erstellte öffentliche Schlüsseldatei (id_rsa.pub), und kopieren Sie die Ausgabe:

```
$ 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) Melden Sie sich bei Ihrer Appliance an, konfigurieren Sie die ESA so, dass Ihre Workstation (oder Ihr Server) mithilfe des öffentlichen SSH-Schlüssels, den Sie in Schritt 1 erstellt haben, erkannt wird, und **bestätigen Sie** die Änderungen. Beachten Sie bei der Anmeldung die Kennwortaufforderung:

```
$ 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) Beenden Sie die Anwendung, und melden Sie sich erneut an. Beachten Sie, dass die Kennwortaufforderung entfernt wird und der Zugriff direkt gewährt wird:

```
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>
```

ssh-keygen-Beispiel für Windows

Führen Sie die folgenden Schritte aus, um eine Windows-Workstation (oder einen Server) für die Verbindung zur ESA ohne Kennwort einzurichten. In diesem Beispiel geben wir keine Passphrase an.

Hinweis: Es gibt eine Variante der von Windows verwendeten Konsolenanwendung. Sie müssen die für Ihre Konsolenanwendung am besten geeignete Lösung recherchieren und finden. In diesem Beispiel werden PuTy und PuTyGen verwendet.

1) Öffnen Sie PuttyGen.

2) Wählen Sie als Typ des zu generierenden Schlüssels SSH-2 RSA aus.

3) Klicken Sie auf die Schaltfläche **Generieren**.

4) Bewegen Sie die Maus in den Bereich unterhalb der Fortschrittsleiste. Wenn die Fortschrittsleiste voll ist, generiert PuTTYgen Ihr Schlüsselpaar.

5) Geben Sie eine Passphrase in das Feld Schlüssel-Passphrase ein. Geben Sie dieselbe Passphrase in das Feld Passphrase bestätigen ein. Sie können einen Schlüssel ohne Passphrase verwenden, dies wird jedoch nicht empfohlen.

6) Klicken Sie auf die Schaltfläche **Privaten Schlüssel speichern**, um den privaten Schlüssel zu speichern.

Hinweis: Sie müssen den privaten Schlüssel speichern. Sie benötigen es, um eine Verbindung zu Ihrem Computer herzustellen.

7) Klicken Sie mit der rechten Maustaste in das Textfeld Öffentlicher Schlüssel zum Einfügen in die Datei OpenSSH authorized_keys, und wählen Sie **Alles auswählen aus**.

8) Klicken Sie erneut mit der rechten Maustaste in das gleiche Textfeld, und wählen Sie **Kopieren aus**.

9) Melden Sie sich mit PuTTY bei Ihrer Appliance an, und konfigurieren Sie die ESA zur Erkennung Ihrer Windows-Workstation (oder Ihres Servers) mithilfe des öffentlichen SSH-Schlüssels, den Sie unter Schritt 6 - Nr. 8 gespeichert und kopiert haben, und bestätigen Sie die Änderungen. Beachten Sie bei der Anmeldung die Kennwortaufforderung:

```
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) Wählen Sie im Puy-Konfigurationsfenster und in der bereits vorhandenen Saved Session für Ihre ESA **Connection > SSH > Auth** aus, und klicken Sie im Feld *Private Key File for authentication (Privater Schlüssel für Authentifizierung)* auf **Browse (Durchsuchen),** und suchen Sie Ihren gespeicherten privaten Schlüssel in Schritt 6.

11) Speichern Sie die Sitzung (Profil) in PuTTY, und klicken Sie auf **Open (Öffnen)**. Melden Sie sich mit dem Benutzernamen an, falls dieser noch nicht in der vorkonfigurierten Sitzung gespeichert oder angegeben wurde. Beachten Sie bei der Anmeldung die Option "Authenticating with public key "[FILE NAME OF SAVED PRIVATE KEY]" (Authentifizierung mit öffentlichem Schlüssel):

```
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>
```

Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Technischer Support und Dokumentation - Cisco Systems