Comment configurer l'authentification de clé publique de SSH pour la procédure de connexion à l'ESA sans mot de passe

Introduction

Ce document décrit comment générer une clé privée de Protocole Secure Shell (SSH) et utiliser cela pour le nom d'utilisateur et l'authentification en se connectant dans l'interface de ligne de commande (CLI) sur l'appliance de sécurité du courrier électronique de Cisco (ESA).

Comment configurer l'authentification de clé publique de SSH pour la procédure de connexion à l'ESA sans mot de passe

L'authentification de clé publique (PKI) est une méthode d'authentification qui se fonde sur keypair public/privé généré. Avec le PKI, on génère une « clé » spéciale qui a une propriété très utile : N'importe qui qui peut lire la moitié publique de la clé peut chiffrent les données qui peuvent alors seulement être lues par une personne qui a accès à la moitié privée de la clé. De cette façon, avoir accès à la moitié publique d'une clé te permet pour envoyer les informations secrètes à n'importe qui avec la moitié privée, et pour les vérifier également qu'une personne a en fait accès à la moitié privée. Il est facile de voir comment cette technique pourrait être utilisée pour authentifier.

En tant qu'utilisateur, vous pouvez générer un keypair et puis placer la moitié publique de la clé sur un système distant, tel que votre ESA. Ce système distant peut alors authentifier votre user-id, et te permet pour ouvrir une session juste en vous ayant expliquent que vous avez accès à la moitié privée du keypair. Ceci est fait au niveau de protocole à l'intérieur du SSH et se produit automatiquement.

Il, cependant, signifie que vous devez protéger l'intimité de la clé privée. Sur un système partagé où vous n'avez pas la racine ceci peut être accompli en chiffrant la clé privée avec un mot de passe, qui fonctionne pareillement à un mot de passe. Avant que le SSH puisse lire votre clé privée afin d'exécuter l'authentification de clé publique vous serez invité à fournir le mot de passe de sorte que la clé privée puisse être déchiffrée. Sur plus les systèmes sécurisés (comme un ordinateur où vous êtes le seul utilisateur, ou un ordinateur à votre maison où aucun étranger n'aura accès physique) vous pouvez simplifier ce processus en créant une clé privée décryptée (sans le mot de passe) ou en entrant dans votre mot de passe une fois et en cachant alors la clé dans la mémoire pour la durée de votre temps à l'ordinateur. OpenSSH contient un outil appelé le ssh-agent qui simplifie ce processus.

exemple de ssh-keygen pour le Linux/Unix

Terminez-vous les étapes suivantes pour installer votre un Linux/poste de travail d'unix (ou un serveur) à connecter à l'ESA sans mot de passe. Dans cet exemple, nous ne spécifierons pas comme mot de passe.

1) Sur votre poste de travail (ou serveur), générez une clé privée utilisant le **ssh-keygen de** commande d'Unix :

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

(le *the ci-dessus a été généré d'Ubuntu 14.04.1)

2) ouvrent le fichier principal public (id_rsa.pub) créé dans #1 et copient la sortie :

```
$ 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) Ouvrez une session à votre appliance et configurez votre ESA pour identifier votre poste de travail (ou serveur) utilisant le ssh key public que vous avez créé dans #1, et **commettez les** modifications. Notez l'invite du mot de passe pendant la procédure de connexion :

```
$ 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) Quittez hors de l'appliance, et de la re-procédure de connexion. Notez que l'invite du mot de passe est retirée, et l'accès est directement accordé :

```
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>
```

exemple de ssh-keygen pour Windows

Terminez-vous les étapes suivantes pour installer votre un poste Windows (ou le serveur) à connecter à l'ESA sans mot de passe. Dans cet exemple, nous ne spécifierons pas comme mot de passe.

> **Note**: Il y a une variation sur l'application de console utilisée de Windows. Vous devrez rechercher et trouver la solution qui fonctionne le meilleur pour votre application de console. Cet exemple utilisera le mastic et le PuTTyGen.

1) Ouvrez PuttyGen.

2) Pour le type de clé à se produire, SSH-2 choisi RSA.

3) Cliquez sur le bouton de **générer**.

4) Déplacez votre souris dans la zone au-dessous de la barre de progression. Quand la barre de progression est pleine, PuTTYgen génère votre paire de clés.

5) Tapez un mot de passe dans le domaine principal de mot de passe. Tapez le même mot de passe dans le domaine de mot de passe de confirmer. Vous pouvez utiliser une clé sans mot de passe, mais ceci n'est pas recommandé.

6) Cliquez sur le bouton de **clé privée de sauvegarde** pour sauvegarder la clé privée.

> **Note**: Vous devez sauvegarder la clé privée. Vous aurez besoin de lui pour se connecter à votre ordinateur.

7) Cliquez avec le bouton droit dans le champ texte étiqueté clé publique pour coller dans des authorized_keys d'OpenSSH le fichier et choisissez **choisi tous**.

8) Cliquez avec le bouton droit de nouveau dans le même champ texte et choisissez la **copie**.

9) Utilisant le mastic, la procédure de connexion à votre appliance et configurent votre ESA pour identifier votre poste Windows (ou serveur) utilisant le ssh key public que vous avez enregistré et avez copié de #6 - #8, et commettez les modifications. Notez l'invite du mot de passe pendant la procédure de connexion :

```
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 fenêtre de configuration de mastic, et de votre session enregistrée préexistante pour votre ESA, choisissez la **connexion > le SSH > authentique** et dans le *fichier principal privé pour le* champ d'*authentification*, le clic **parcourent** et trouvent votre clé privée enregistrée de l'étape #6.

11) Sauvegardez la session (profil) en mastic, et cliquez sur **ouvert**. Ouvrez une session avec le nom d'utilisateur, sinon déjà enregistré ou spécifié de la session préconfigurée. Notez l'intégration de « authentifier avec la clé publique « [NOM DU FICHIER DE CLÉ PRIVÉE SAVED] » en ouvrant une session :

```
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
```

Informations connexes

- Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur
- Support et documentation techniques - Cisco Systems