Hoe kunt u SSH-verificatie configureren voor inloggen op de ESA zonder wachtwoord

Inleiding

Dit document beschrijft hoe u een SSH-toets (Private Secure Shell) kunt genereren en gebruiken die voor gebruikersnaam en verificatie bij vastlegging in de opdrachtregel interface (CLI) op Cisco Email Security Appliance (ESA).

Hoe kunt u SSH-verificatie configureren voor inloggen op de ESA zonder wachtwoord

PKI-verificatie (Public-key Authenticatie) is een authenticatiemethode die afhankelijk is van een gegenereerd publiek/privaat toetsenbord. Met PKI wordt een speciale "key" gegenereerd die een zeer bruikbare eigenschap heeft: Iedereen die de helft van de sleutel kan lezen, kan gegevens versleutelen die dan alleen gelezen kunnen worden door iemand die toegang heeft tot de privé-helft van de sleutel. Op die manier kan je, als je toegang hebt tot de publieke helft van een sleutel, geheime informatie sturen naar iedereen met de particuliere helft, en ook controleren of iemand toegang heeft tot de particuliere helft. Het is gemakkelijk om te zien hoe deze techniek gebruikt kan worden om echt te zijn.

Als gebruiker kunt u een toetsenbord genereren en vervolgens de openbare helft van de toets op een extern systeem plaatsen, zoals het ESA. Dat externe systeem kan uw gebruiker-ID dan echt maken en u kunt alleen inloggen door aan te tonen dat u toegang hebt tot de privéhelft van het toetsenbord. Dit gebeurt op protocolniveau binnen SSH en wordt automatisch uitgevoerd.

Het betekent echter dat je de privacy van de privé-sleutel moet beschermen. Op een gedeeld systeem waar u geen wortel hebt, kan dit worden bereikt door de privé-toets te versleutelen met een wachtwoord, dat gelijk is aan een wachtwoord. Voordat SSH uw privésleutel kan lezen om de openbare basisauthenticatie uit te voeren, zal u worden gevraagd om het wachtwoord te leveren zodat de privésleutel kan worden gedecrypteerd. Op veiligere systemen (zoals een machine waar u de enige gebruiker bent, of een machine in uw huis waar geen vreemden fysieke toegang hebben) kunt u dit proces vereenvoudigen ofwel door een niet-versleutelde privé-sleutel te maken (zonder wachtwoord) of door uw wachtwoord eenmaal in te voeren en vervolgens de sleutel in het geheugen te plaatsen voor de duur van uw tijd op de computer. OpenSSH bevat een tool dat ssh-agent wordt genoemd en dit proces vereenvoudigt.

SH-keygenvoorbeeld voor Linux/Unix

Volg de volgende stappen om uw linux/Unix-werkstation (of server) in te stellen om zonder een wachtwoord verbinding te maken met de ESA. In dit voorbeeld, zullen we niet als wachtwoord specificeren.

1) Voer op uw werkstation (of server) een privésleutel in met behulp van de Unix-opdracht **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 |
| . . |
+-----------------+
```

(*het bovenstaande is gegenereerd door een Ubuntu 14.04.1)

2) Open het openbare sleutelbestand (id_rsa.pub) dat met #1 is gemaakt en kopieer de uitvoer:

```
$ 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) Meld u aan bij uw apparaat en stel de ESA's aan om uw werkstation (of server) te herkennen met behulp van de openbare SSH-toets die u in #1 hebt aangemaakt, en **zet** de wijzigingen **aan**. Let op de wachtwoordmelding bij de inlognaam:

```
$ 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) Sluit het apparaat af en loger opnieuw in. Merk op dat de wachtwoordprompt wordt verwijderd en dat de toegang rechtstreeks is verleend:

```
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>
```

SH-keygenvoorbeeld voor Windows

Volg de volgende stappen om uw Windows-werkstation (of server) in te stellen voor aansluiting op de ESA zonder wachtwoord. In dit voorbeeld, zullen we niet als wachtwoord specificeren.

> **Opmerking**: er is een variatie in de console-toepassing die vanuit Windows gebruikt wordt. U moet de oplossing zoeken en vinden die het beste werkt voor uw console-toepassing. Dit voorbeeld gebruikt PuTy en PuTyGen.

1) Open PuttyGen.

2) Selecteer SSH-2 RSA voor type sleutel die moet worden gegenereerd.

3) Klik op de knop **Generate**.

4) Verplaats de muis in het gebied onder de voortgangsbalk. Als de voortgangsbalk vol is, genereert PuTTYgen uw sleutelpaar.

5) Typ een wachtwoord in het veld Key wachtwoord. Typ hetzelfde wachtwoord in het veld Wachtwoord bevestigen. U kunt een toets gebruiken zonder wachtwoord, maar dit wordt niet aanbevolen.

6) Klik op de knop **Private** Save om de privétoets op te slaan.

> **Opmerking**: U moet de privé-toets opslaan. U hebt deze nodig om verbinding te maken met uw machine.

7) Klik met de rechtermuisknop op het tekstveld met het label Openen voor het plakken in het bestand OpenSSH geautoriseerde_keys en kies **Alles selecteren**.

8) Klik met de rechtermuisknop weer in hetzelfde tekstveld en kies **Kopie**.

9) Gebruik PuTTY om aan uw apparaat in te loggen en pas uw ESA aan om uw Windows-werkstation (of server) te herkennen met behulp van de openbare SSH-toets die u hebt opgeslagen en gekopieerd van #6 - #8 en om deze wijzigingen vast te leggen. Let op de wachtwoordmelding bij de inlognaam:

```
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) Kies in het configuratievenster van PuTy en uw reeds bestaande Opgeslagen sessie voor uw ESA, **Connection > SSH > Auth** en in het *Private key file voor verificatie*, klik op **Bladeren** en vind uw opgeslagen privé-sleutel uit stap #6.

11) Sla de sessie (profiel) op in PuTTY en klik op **Openen**. Aanmelden met de gebruikersnaam, indien niet al opgeslagen of gespecificeerd in de vooraf ingestelde sessie. Merk op dat "Authenticating with public key" [FILE NAME OF SAVED PRIVATE KEY]" is opgenomen bij het inloggen van:

```
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>
```

Gerelateerde informatie

- Cisco e-mail security applicatie - eindgebruikershandleidingen
- Technische ondersteuning en documentatie – Cisco Systems