비밀번호 없이 ESA에 로그인할 수 있도록 SSH 공개 키 인증을 구성하는 방법

소개

이 문서에서는 SSH(Private Secure Shell) 키를 생성하고 Cisco ESA(Email Security Appliance)의 CLI(Command Line Interface)에 로그인할 때 사용자 이름 및 인증에 사용하는 방법에 대해 설명합니다.

비밀번호 없이 ESA에 로그인할 수 있도록 SSH 공개 키 인증을 구성하는 방법

PKI(Public-Key Authentication)는 생성된 공용/개인 키 쌍을 사용하는 인증 방법입니다.PKI에서는 매우 유용한 속성을 가진 특수 "키"가 생성됩니다.키의 절반을 읽을 수 있는 사람은 데이터를 암호화할 수 있습니다. 그러면 키의 절반만 액세스할 수 있는 사용자만 읽을 수 있습니다.이렇게 하면 키의 절반과 공개에 액세스할 수 있으므로, 비밀 정보를 사적인 반쪽에게 보내고, 실제로 개인이 비공개 반쪽에 액세스할 수 있는지 확인할 수 있습니다.이 기술을 사용하여 인증하는 방법을 쉽게 확인할 수 있습니다.

사용자는 키 쌍을 생성한 다음 키의 일부를 ESA와 같은 원격 시스템에 배치할 수 있습니다.그런 다음 원격 시스템에서 사용자 ID를 인증할 수 있으며, 키 쌍의 비공개 부분에 액세스할 수 있음을 보여줌으로써 로그인할 수 있습니다.이는 SSH 내의 프로토콜 레벨에서 수행되며 자동으로 수행됩니다.

그러나 이는 개인 키의 개인 정보를 보호해야 함을 의미합니다.루트가 없는 공유 시스템에서는 암호와 유사한 기능을 하는 패스프레이즈로 개인 키를 암호화하여 이 작업을 수행할 수 있습니다 .SSH가 공개 키 인증을 수행하기 위해 개인 키를 읽을 수 있으려면 먼저 개인 키의 암호를 제공하여 암호를 해독할 수 있도록 하라는 메시지가 표시됩니다.더 안전한 시스템(예: 사용자가 유일한 사용자이거나, 모르는 사람이 물리적 액세스를 가지지 않는 가정 내 시스템)에서 암호화되지 않은 개인 키를 만들거나(암호 없이) 암호를 한 번 입력한 다음 컴퓨터에서 시간 동안 메모리에 키를 캐싱하여 이 프로세스를 단순화할 수 있습니다.OpenSSH에는 이 프로세스를 간소화하는 ssh-agent라는 도구가 포함되어 있습니다.

Linux/Unix용 ssh-keygen 예

비밀번호 없이 ESA에 연결하기 위해 linux/unix 워크스테이션(또는 서버)을 설정하려면 다음 단계를 완료합니다. 이 예에서는 패스프레이즈로 지정하지 않습니다.

1) 워크스테이션(또는 서버)에서 Unix 명령 ssh-keygen을 사용하여 개인 키를 생성합니다.

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

(*위 항목은 Ubuntu 14.04.1에서 생성됨)

2) #1에서 만든 공개 키 파일(id_rsa.pub)을 열고 출력을 복사합니다.

```
$ 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) 어플라이언스에 로그인하고 #1에서 생성한 공개 SSH 키를 사용하여 워크스테이션(또는 서버)을 인식하도록 ESA를 구성하고 변경 사항을 **커밋합니다**. 로그인 시 비밀번호 프롬프트를 확인합니다.

```
$ 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) 어플라이언스를 종료하고 다시 로그인합니다. 비밀번호 프롬프트가 제거되고 액세스 권한이 직접 부여됩니다.

```
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>
```

Windows용 ssh-keygen 예

비밀번호 없이 ESA에 연결하기 위해 Windows 워크스테이션(또는 서버)을 설정하려면 다음 단계를 완료합니다. 이 예에서는 패스프레이즈로 지정하지 않습니다.

> **참고**: Windows에서 사용하는 콘솔 응용 프로그램에는 변형이 있습니다. 콘솔 응용 프로그램에 가장 적합한 솔루션을 조사하고 찾아야 합니다. 이 예에서는 PuTty 및 PuTyGen을 사용합니다.

1) PuttyGen 열기

2) 생성할 키 유형에서 SSH-2 RSA를 선택합니다.

3) Generate(생성) 버튼**을** 클릭합니다.

4) 진행 표시줄 아래의 영역에서 마우스를 이동합니다.진행률 표시줄이 꽉 차면 PuTTYgen에서 키 쌍을 생성합니다.

5) Key passphrase 필드에 암호를 입력합니다.Confirm passphrase 필드에 동일한 패스프레이즈를 입력합니다.암호 없이 키를 사용할 수 있지만 권장하지 않습니다.

6) 개인 **키 저장** 단추를 클릭하여 개인 키를 저장합니다.

참고: 개인 키를 저장해야 합니다.컴퓨터에 연결하려면 해당 정보가 필요합니다.

7) OpenSSH authorized_keys 파일에 붙여넣으려면 Public key라는 텍스트 필드를 마우스 오른쪽 버튼으로 클릭하고 Select **All을** 선택합니다.

8) 동일한 텍스트 필드에서 다시 마우스 오른쪽 버튼을 클릭하고 **복사**를 선택합니다.

9) PuTTY를 사용하여 어플라이언스에 로그인하고, #6 - #8에서 저장 및 복사한 공개 SSH 키를 사용하여 Windows 워크스테이션(또는 서버)을 인식하도록 ESA를 구성하고 변경 사항을 커밋합니다. 로그인 시 비밀번호 프롬프트를 확인합니다.

```
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) PuTTy 컨피그레이션 창 및 ESA에 대한 기존 저장된 세션에서 **Connection > SSH > Auth를** 선택하고 *Private key file for authentication(인증을 위한 개인 키 파일)* 필드에서 Browse(찾아보기)**를** 클릭하고 #6 단계에서 저장된 개인 키를 찾습니다.

11) PuTTY에 세션(프로필)을 저장하고 **열기**를 클릭합니다. 미리 구성된 세션에서 저장 또는 지정되지 않은 경우 사용자 이름으로 로그인합니다. 로그인할 때 "공개 키 "[저장된 개인 키의 파일 이름]"을 사용하여 인증하는 것을 확인합니다.

```
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>
```

관련 정보

- Cisco Email Security Appliance – 엔드 유저 가이드
- 기술 지원 및 문서 – Cisco Systems