Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Túnel SSH invertit - [Tunel SSH inverso] (29402 lectures)

Per **Joan**, *Joan* ()

Creado el 07/01/2004 13:59 modificado el 07/01/2004 23:47

Tinc un ordinador amb linux a casa (Venus) que està firewalled i al que hi vull accedir-hi amb ssh des del linux que tinc al despatx (Mart). No puc redirigir cap port del gateway que dóna sortida a Internet a Venus. Per solucionar-ho establiré un túnel ssh invertit des de Venus a Mart ;-)

[En casa tengo un ordenador con linux (Venus) que esta firewalled y al que quiero acceder con ssh desde el linux que tengo en la oficina (Mart). No puedo redirigir ningun puerto del gateway que da salida a Internet a Venus. Para solucionarlo establecere un tunel ssh inverso desde Venus a Mart.]

Actualizado: Ahora tambien en castellano.

Túnel SSH invertit - [Tunel SSH inverso]

Tinc un ordinador amb linux a casa (Venus) que està firewalled i al que hi vull accedir-hi amb ssh des del linux que tinc al despatx (Mart). No puc redirigir cap port del gateway que dóna sortida a Internet a Venus. Per solucionar-ho establiré un túnel ssh invertit des de Venus a Mart.

[En casa tengo un ordenador con linux (Venus) que esta firewalled y al que quiero acceder con ssh desde el linux que tengo en la oficina (Mart). No puedo redirigir ningun puerto del gateway que da salida a Internet a Venus. Para solucionarlo establecere un tunel ssh inverso desde Venus a Mart.]

No he trobat cap tutorial que expliqui com fer-ho en la seva totalitat, sobretot el punt d'automatitzar l'autenticació per establir el túnel ssh invertit. Per això m'he decidit a escriure-ho. Suposo que hi haurà altres maneres de fer-ho, potser més fàcils, no sóc un expert així que demano disculpes pels errors que el document pugui tenir.

[No he encontrado ningun tutorial que explique como hacerlo en su totalidad, en especial la automatizacion de la autenticacion para establecer el tunel ssh inverso. Por eso me he decidido a escribirlo. Supongo que habra otros modos de hacerlo, a lo mejor mas faciles, no soy un experto asi que pido disculpas por los errores que el documento pueda tener.]

El problema

Tenim dos ordinadors amb linux en dues xarxes diferents, estan físicament separades i només poden comunicar-se a través d'Internet:

[Tenemos dos ordenadores con linux en dos redes diferentes, estan fisicamente separadas y solo pueden intercomunicarse a traves de Internet:]

- **Mart**: Te el port 22 (ssh) accessible des de Internet, te la direcció *el_meu_domini.com*. Per tant, des de qualsevol lloc d'Internet podem fer "*ssh root@el_meu_domini.com*" per obrir un shell.

  [Tiene el puerto 22 (ssh) accesible desde Internet, tiene la direccion *el_meu_domini.com*. Por lo tanto, desde qualquier lugar de Internet puedo hacer "*ssh root@el_meu_domini.com*" para abrir un shell.]

- **Venus**: Es troba dins d'una WAN, no hi ha cap redirecció de ports (*port forwarding*) des del gateway que li dóna sortida a Internet. Per tant no hi podem accedir des de fora, col·loquialment en diem que "*està firewalled*". Aquest és l'ordinador al que hi volem poder accedir-hi amb un ssh des de Mart.

  [Se encuentra dentro de una WAN, no hay ninguna redireccion de puertos (*port forwarding*) desde el gateway que le da salida a Internet. Por lo tanto, no podemos acceder desde fuera, coloquialmente decimos que "*esta firewalled*". Este es el ordenador al que queremos poder acceder con ssh desde Mart.]

Des de Venus podem accedir a qualsevol lloc d'Internet, per exemple podem obrir un ssh a Mart. Des de Mart també podem accedir a qualsevol lloc d'Internet però no a Venus, ni molt menys obrir un ssh a Venus, que és el que volem.

[Desde Venus podemos acceder a cualquier lugar de Internet, por ejemplo podemos abrir un ssh a Mart. Desde Mart tambien podemos acceder a qualquier lugar de Internet pero no a Venus, ni mucho menos abrir un ssh a Venus, que es lo que queremos.]

La manera més fàcil de solucionar-ho seria redireccionar un port del gateway (que fa servir Venus per sortir a Internet) cap a Venus. Això no és de moment possible per raons que no venen al cas. Així que buscarem una solució alternativa aprofitant que tenim Mart. Aquest sistema només és factible si tenim un altre ordinador com Mart, que estigui a Internet amb al menys un port accessible.

[El modo mas facil de solucionarlo seria redireccionar un puerto del gateway (que usa Venus para salir a Internet) hacia Venus. Esto de momento no es posible por varias razones. Buscaremos una solucion alternativa aprovechando que tenemos Mart. Este sistema solo es factible si tenemos otro ordenador como MArt, que este en Internet con al menos un puerto accesible.]

La Solució

[La Solucion]

El primer serà el de crear un túnel ssh invertit (*reverse ssh*) entre Venus i Mart. El que fem es deixar un túnel ssh obert entre els dos ordinadors, aquest túnel s'ha d'executar des de Venus. Recordeu que des de Mart no ho podem fer, Venus no és accessible des de Internet.

[Lo primero sera crear un tunel ssh inverso entre Venus y Mart. Lo que hacemos es dejar un tunel ssh abierto entre los dos ordenadores, este tunel se tiene que ejecutar desde Venus. Recordad que desde Mart no lo podemos hacer, Venus no es accesible desde Internet.]

Per establir un túnel ssh invertit, hem d'especificar l'usuari sota el que correrà el túnel a Mart. En el meu cas he creat un nou usuari a Mart, aquest nou usuari *tunelssh* només el tindré per això. Es una mania meva, el túnel el podeu establir amb qualsevol usuari ja existent de Mart.

[Para establecer un tunel ssh inverso, tenemos que especificar el usuario bajo el que correra el tunel en Mart. En mi caso he creado un nuevo usuario en Mart, este nuevo usuario *tunelssh* solo lo voy a tener para esto. Es una mania mia, el tunel lo podeis establecer con qualquier usuario ya existente en Mart.]

```
joan@venus ~ $ ssh -l tunelssh -R 22000:localhost:22 -f -N el_meu_domini.com
```

Ens demanarà el password de l'usuari tunelssh, una vegada l'hem entrat ja tenim el túnel ssh invertit preparat per a fer servir. Al establir una connexió amb el port 22000 de Mart, la conexió s'inverteix i redirigeix cap a Venus. En comptes de fer servir el port 22000 pots fer-ho amb el que vulguis. Ara des de Mart ja podem accedir a Venus amb:

[Nos pedira el password del usuario tunelssh, una vez se lo hayamos dado ya tendremos el tunel ssh inverso listo para usar. Al establecer una conexion con el puerto 22000 de Mart, la conexion se invierte y redirige hacia Venus. En vez de usar el puerto 22000 lo podeis hacer con el que querais. Ahora desde Mart ya podemos acceder a Venus con:]

```
root@mart ~ $ ssh -p 22000 joan@localhost
```

En aquest punt poden passar dues coses. Una és que ens pregunti el password de root de Venus i l'invent funcioni correctament, i l'altre és que ens doni un error: "*WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!*". Això és degut a que el fingerprint de les claus RSA que estan guardades a *~/.ssh/known_hosts*, estan associades a un host. Quan l'error surt vol dir que teniu guardat un fingerprint associat a root@localhost, i que no és el mateix al que ara rep. No és el mateix perquè ara estem fent trampa, hem rebut el fingerprint de root@venus i es pensa que és el de root@localhost (recordem que estem a Mart). Això ho podem solucionar de varies maneres, la que crec que és més fàcil és editar */etc/hosts* i en la línea on tinguem:

[Aqui pueden pasar dos cosas. Una es que nos pregunte por el password de root en Venus i el invento funcione correctamente, la otra es que tengamos el error: "*WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!*". Esto es debido a que el fingerprint de las llaves RSA que estan guardadas en *~/.ssh/known_hosts*, estan asociadas a un host. Cuando tebemos este error quiere decir que tenemos guardado un fingerprint associado a root@localhost, i que no el mismo que acaba de recibir. No es el mismo porque estamos haciendo trampa, hemos recibido un fingerprint de root@venus i el cree que es el de root@localhost (recrodemos que estamos en Mart). Esto lo podemos solucionar de varios modos, el que creo mas facil es editar */etc/hosts* y en la linea donde tengamos:]

```
127.0.0.1       localhost
```

Modificar-la per:

[La modificamos por:]

```
127.0.0.1       localhost venus
```

Ara ja podem fer:

[Ahora ya podemos hacer:]

```
root@mart ~ $ ssh -p 22000 joan@venus
```

Amb això ens guardarà el fingerprint de venus amb el nom de venus, i si mai hem de fer un ssh a localhost per la raó que sigui, no ens donarà cap problema. El ssh es pot executar des de qualsevol usuari de Mart cap a qualsevol usuari de Venus.

[Con esto nos guardara el fingerprint de venus con el nombre de venus, i si alguna vez tenemos que hacer ssh a localhost, no tendremos ningun problema. El ssh se puede ejecutar desde cualquier usuario de Mart hacia cualquier usuario de Venus.]

Automatitzant-ho

[Automatizandolo]

Ja sabem com iniciar el túnel ssh invertit manualment. Això de fet no ens serveix de gran cosa ja que pot marxar la corrent, tallar-se la connexió uns minuts, etc. Llavors ens quedem sense túnel i no podem accedir des de Mart a Venus. Hauríem de desplaçar-nos físicament a Venus i executar el túnel de nou. Hem de fer un script que contínuament comprovi l'estat del túnel i el reinicialitzi en cas de que es perdi.

[Ya sabemos como iniciar el tunel manualmente. Esto no nos sirve de mucho ya que si se corta la conexion nos quedaremos sin tunel y no podremos acceder desde Mart a Venus. Nos tendriamos que desplazar fisicamente a Venus i ejecutar un nuevo tunel. Tenemos que hacer un script que continuamente compruebe el estado del tunel y lo reinicialize en caso que se desconecte.]

Aquí ens trobem amb un petit problema, que és com ens autentiquem per establir el túnel. Ssh ja esta preparat per això, generarem un parell de claus RSA pública/privada. La creació de claus es pot fer a l'ordinador que vulguem, seguint el meu cas:

[Aqui tenemos un pequeño problema, que es como autenticarnos para establecer el tunel. Ssh ya esta preparado para esto, generaremos un par de llaves RSA publica/privada. La creacion de llaves la podemos hacer en el ordenador que queramos, siguiendo mi caso:]

```
tunnelssh@mart ~ $  ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): clau1
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in clau1.
Your public key has been saved in clau1.pub.
The key fingerprint is:
a6:63:a7:3e:7d:17:42:83:b2:85:79:ef:44:e8:89:67 tunnelssh@mart
tunnelssh @mart ~ $ ll clau1*
-rw-------    1 tunnelssh     tunnelssh          887 dec 31 12:00 clau1
-rw-r--r--    1 tunnelssh     tunnelssh          234 dec 31 12:00 clau1.pub
tunnelssh @mart ~ $
```

Ara ja tenim el parell de claus. La clau pública (*clau1.pub*) s'ha d'afegir als fitxer *~/.ssh/known_hosts* del usuari sota el que s'executarà el túnel a l'ordinador que te el port 22 obert a Internet. En el nostre cas es l'usuari *tunelssh* de Mart:

[Ahora ya tenemos las llaves. La llave publica (*clau1.pub*) se tiene que añadir al fichero *~/.ssh/known_hosts* del usuario bajo el que se ejecute el tunel en el ordenador que tenga el puerto 22 abierto a Internet. En nuestro caso es el usuario *tunelssh* de Mart:]

```
tunnelssh@mart ~ $ cat clau1.pub >> ~/.ssh/known_hosts
```

La clau privada (*clau1*) s'ha de guardar en algun lloc de l'ordinador que està firewalled on l'usuari que executi el script hi tingui accés. Es important que el fitxer de clau privada sigui només accessible per el usuari propietari del fitxer, si no li fem el chmod el ssh ens ho demanarà així quan intentem establir el túnel. Seguint el nostre cas:

[La llave privada (*clau1*) se tiene que guardar en algun lugar del ordenador que esta firewalled donde el usuario que ejecute el script pueda acceder. Es importante que el fichero de llave privada solo sea accesible para el usuario propietario del fichero, si no ssh nos lo exigira por razones de seguridad cuando intentemos establecer el tunel. Siguiendo nuestro caso:]

```
joan@venus ~ $ scp tunelssh@el_meu_domini.com:clau1 .
tunelssh@mart's password:
clau1                100% |*****************************|    887       00:00
joan@venus ~ $ ll clau1
-rw-r--r--    1 joan     joan           887 dec 31 12:10 clau1
joan@venus ~ $ chmod 600 clau1
joan@venus ~ $ ll clau1
-rw-------    1 joan     joan           887 dec 31 12:10 clau1
joan@venus ~ $
```

Ara ja ho podem provar-ho, abans hem de pensar en eliminar el túnel que haguem obert prèviament si és que ho hem fet, trobarem el túnel executant:

[Ya lo podemos probar, tenemos que acordarnos de eliminar el tunel abierto anteriormente si es que lo hemos hecho, encontraremos el tunel con:]

```
joan@venus ~ $ ps x | grep 22000:localhost:22
```

Eliminem (*kill*) el túnel i provem d'establir-ne un de nou sense tenir que autenticar-nos:

[Eliminamos (*kill*) el tunel y probamos de establecer uno nuevo sin tener que autenticarnos:]

```
joan@venus ~ $ ssh -i ~/clau1 -l tunelssh -R 22000:localhost:22 -f -N el_meu_domini.com
```

Si ho hem fet tot bé, hem obert el túnel sense tenir que escriure el password. Ara només ens cal fer un script i posar-lo al *crontab* per comprovar el túnel amb la freqüència que vulguem:

[Si lo hemos hecho todo bien, hemos abierto el tunel sin tener que escribir el password. Ahora solo tenemos que hacer un script i ponerlo en el crontab para comprobar el tunel con la frequencia que queramos:]

```
#!/usr/bin/perl -w
if ( `ps x | grep 22000:localhost:22 | grep -v grep` ) {
        print "Tunel SSH en funcionament! \n";
        } else {
        print "Establint tunel SSH ... \n";
        system("ssh -i ~/clau1 -l tunelssh -R 22000:localhost:22 -f -N el_meu_domini.com ");
};
```

Aquest script està tret d'aqui [1], només hi he afegit l'autenticació.

[Este script lo he sacado de aqui [1], solo le he añadido la autenticacion.]

Ja estem. Podem accedir a Venus des de Mart, i com que a Mart hi podem accedir des de qualsevol punt de Internet, Venus és accessible des de qualsevol lloc d'Internet. L'únic inconvenient d'aquest sistema és que necessitem d'un altre ordinador com Mart que estigui accessible per Internet sempre per a poder establir el túnel ssh invertit. Espero que no us hagueu marejat en tot aquest viatje interplanetari ;-)

[Hemos acabado. Podemos acceder a Venus desde Mart, y como que podemos acceder a Mart desde cualquier punto de Internet, Venus tambien es accesible desde cualquier lugar. El unico inconveniente de este sistema es que necesitamos otro ordenador como Mart que este accesible siempre por Internet para poder establecer el tunel ssh inverso. Espero que no os esteis mareados con este viaje interplanetario ;-)]

Com ja he dit abans, la totalitat del aquí exposat s'ha extret de:

[Como ya he dicho antes, la totalidad de lo aqui expuesto lo he sacado de:]

http://www.colug.net/pipermail/colug/2003-October/009006.html[2]
http://www.cs.umd.edu/~arun/misc/ssh.html[3]
http://www.afp548.com/Articles/security/ssh-tunnels.html[1]

Lista de enlaces de este artículo:

1. http://www.afp548.com/Articles/security/ssh-tunnels.html
2. http://www.colug.net/pipermail/colug/2003-October/009006.html
3. http://www.cs.umd.edu/~arun/misc/ssh.html

E-mail del autor: joan _ARROBA_ calmaginet.com