M0374 - Administració de SO

RA4 - ACCÉS REMOT

SSH TUNNELING

Redreçament de ports TCP i túnels amb SSH

La major part dels protocols que utilitzem en les nostres comunicacions estan basats en **dissenys de fa gairebé 30 anys**, quan la seguretat en xarxes telemàtiques no era un problema.

Telnet, FTP, POP3, protocols d'ús quotidià, **descuiden la seguretat i confidencialitat de les dades que envien.**

Redreçament de ports TCP i túnels amb SSH

No serveix de res protegir els servidors, implantar una bona política de contrasenyes i actualitzar les versions dels nostres dimonis si després, quan un usuari de POP3, per exemple, vol veure el seu correu electrònic des de la nostra xarxa, envia el seu usuari i contrasenya en text pla per la xarxa.

Túnel SSH

Fent servir **SSH** es poden establir **túnels encriptats** pels quals es pot transmetre qualsevol protocol que faci servir TCP. Així és possible, per exemple, emprar un túnel SSH per:

- descarregar el correu mitjançant POP3 i enviar-lo fent servir SMTP.
- accedir a un servidor web mitjançant HTTP.
- accedir a un sistema d'arxius remot mitjançant NFS.

Túnel SSH

La idea en què es basa aquest procediment, és la de **fer un túnel pel qual viatjaran les dades de manera segura** (tunneling).

A cada un dels extrems del túnel hi ha les aplicacions estàndard (un dimoni POP3 estàndard, el nostre client de correu preferit, FTP, un navegador web, etc.), i **la comunicació s'assegura gràcies a la potència criptogràfica d'SSH.**

Túnel SSH

SSH recull les dades que el client vol enviar i les reenvia pel **túnel o canal segur**. A l'altre costat del túnel es recullen les dades i es tornen a enviar al servidor corresponent.

El redreçament estàtic de ports ens permet crear un **canal de comunicació segur i transparent a l'usuari entre un port de la màquina local i un altre port de la màquina remota**, que pot ser un dels ports estàndards que fan servir qualsevol dels serveis de xarxa.

Classes de Túnels

OpenSSH ens permet crear dues classes de túnels : **locals i remots.**

• **LOCAL**: es **redirecciona** un **port de la màquina local (client) cap a un port en una màquina remota** a la qual el servidor tingui accés .

https://www.zonasystem.com/2019/01/tunel-ssh-port-forwarding-local-remote-dynamic.html

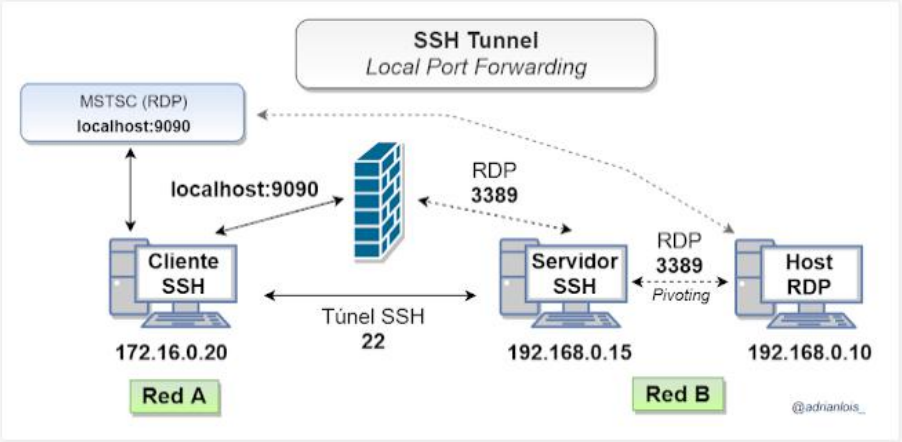

Figura 2: SSH port forwarding - Túnel SSH local.

Classes de Túnels

• **REMOT**: el que es fa és **redireccionar** un **port des d'una màquina remota a la que el servidor tingui accés cap a un port de la màquina local .**

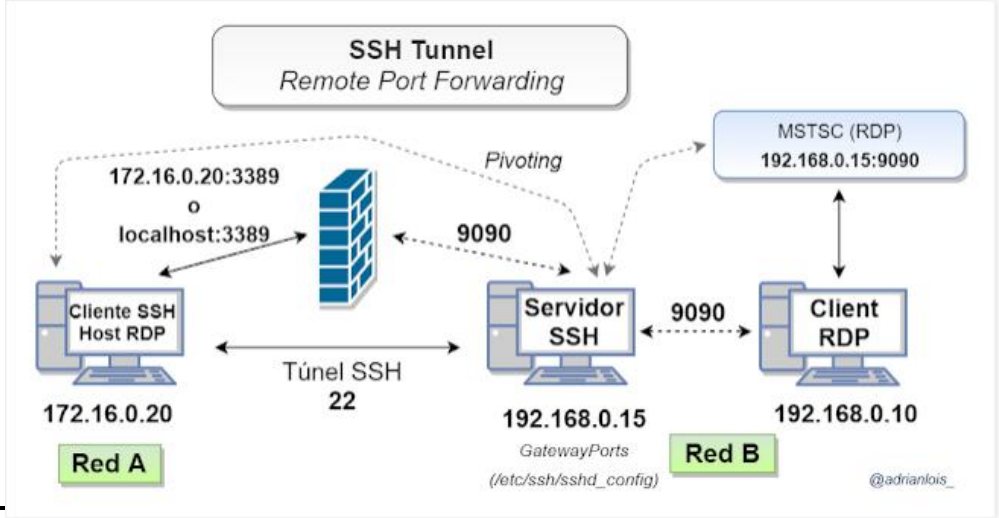

Figura 4: SSH port forwarding - Túnel SSH remoto.

Túnel Local

La forma de crear túnels locals amb OpenSSH és mitjançant l'opció **- L**, la sintaxi és :

```
-L [ dirección_escolta : ] port_escolta : màquina_remota : port_màquina_remota
```

En cas d'emprar adreces IPv6 , es pot utilitzar la següent sintaxi :

```
-L [ direcció_escolta / ] port_escolta / màquina_remota / port_màquina_remota
```

Túnel Local

Els túnels locals s'estableixen de la següent manera: primer **es crea un connector** (**socket**) **d'escolta en la màquina local**, **associat al port *port_escolta*** i, opcionalment, a l'adreça direcció_escolta.

Quan es realitzi una connexió al port en què està escoltant el connector, **OpenSSH canalitzarà la connexió a través del canal segur** cap a la màquina remota a la qual el servidor tingui accés, indicada per la IP ***màquina_remota*** i el port ***port_màquina_remota*** .

Túnel Remot

La forma de crear túnels remots amb OpenSSH és mitjançant l'opció **- R,** la sintaxi és :

```
-R [ dirección_escolta : ] port_escolta : màquina_remota : port_màquina_remota
```

En cas d'emprar adreces IPv6 , es pot utilitzar la següent sintaxi :

```
-R [ direcció_escolta / ] port_escolta / màquina_remota / port_màquina_remota
```

Túnel Remot

El mecanisme emprat per a establir els túnels remots és: **es crea un connector (socket) al servidor associat al port indicat per *port_escolta*** i, opcionalment, a l'adreça IP dirección_escolta.

Posteriorment, quan es realitzi una connexió a aquest connector, l**a connexió serà canalitzada a través del canal segur** cap a una màquina a la qual l'equip local tingui accés, indicada per la IP ***màquina_remota*** i el port ***port_màquina_remota***.

Exemple

Per establir un túnel SSH entre el port local *10025* i el port *25* (corresponent al servei SMTP) de l'estació *192.168.10.100* establint la connexió amb l'usuari *usuari* faríem:

```
ssh usuari@192.168.10.100 -L 10025:192.168.10.100:25
```

Un cop establerta la sessió SSH, i mentre es mantingui, existirà un túnel encriptat entre el port TCP local 10025 i el 25 de l'estació 192.168.10.100.

Exemple Túnel Local

En un servidor web necessitem visualitzar alguna pàgina protegida pel servidor (pels fitxers . Htaccess) .

El problema a les pàgines protegides mitjançant aquest mètode és que cada vegada que ingressem un usuari i contrasenya, aquestes **viatgen per la xarxa com a text pla** i pot ser interceptada per algun tercer.

Usant túnels SSH podem controlar aquest problema , ja que totes les dades viatgen encriptades i assegurades .

Exemple Túnel Local

Per redireccionar el port que escolta el servidor web remot al nostre ordinador , executem :

```
ssh -L 10080:localhost:80 usuari@servidor-web-remot.com
```

El paràmetre **-L** ens permet realitzar el túnel a través d'un port local . Amb això , ja tenim creat un Túnel entre el port 10080 del nostre ordinador i el port 80 que atén el servidor web remot .

Si teclegem al navegador web **http://localhost:10080** podrem accedir sense problemes al servidor web remot amb la seguretat que totes les dades viatgen encriptades.

Exemple Túnel Remot

Seguint amb l'exemple abans esmentat, imaginem un servidor web escoltant el port 80 i desitgem que un ordinador remot pugui tenir accés al port del servidor web i en aquest cas, ens trobem del costat del servidor. Per realitzar el túnel remot executem:

```
ssh -R 10080:localhost:80 usuari@pc-client-remot
```

Usant el paràmetre **-R** podrem crear túnels remots des del port del servidor.