5. Túnels i redirecció de ports

Què és un túnel SSH?

Una connexió SSH pot transportar connexions TCP d'altres aplicacions. El client i el servidor SSH actuen com a extrems d'un canal xifrat.

Per exemple, es pot accedir des del navegador local a un servei web que només escolta en la interfície de bucle local del servidor. El túnel requerix accés SSH i els permisos corresponents; no elimina les polítiques del tallafocs.

Redirecció local: -L

S'executa en el client:

```
ssh -N -L 127.0.0.1:8080:127.0.0.1:80 alumne@192.168.0.1
```

Part	Significat
Primer `127.0.0.1:8080`	Escolta en el client local
Segon `127.0.0.1:80`	Destinació vista des del servidor SSH
`-N`	Manté el túnel sense obrir una shell
`alumne@192.168.0.1`	Compte i servidor SSH

Amb la connexió oberta, el navegador del client visita `http://127.0.0.1:8080`. El servidor SSH inicia la connexió al seu propi port 80. El navegador no interpreta `localhost` de la mateixa manera que l'extrem remot: cada equip té el seu propi bucle local.

La destinació també pot ser un altre equip accessible des del servidor SSH:

```
ssh -N -L 127.0.0.1:8080:192.168.99.10:80 alumne@192.168.0.1
```

En este cas, el tram entre el servidor SSH i `192.168.99.10` no queda protegit pel túnel SSH; dependrà del protocol de l'aplicació.

Exemple a classe: Webmin en una instància d'AWS

Un cas típic de redirecció local és administrar un servei web que **no** volem publicar a Internet. A classe ho hem fet amb Webmin, una interfície web d'administració que escolta al port 10000 de la instància d'AWS.

Al grup de seguretat només hi ha obert el port 22. Des del client Linux Mint obrim el túnel:

```
ssh -i ~/Baixades/labsuser.pem -N -L 10000:localhost:10000 ubuntu@<IP_PUBLICA>
```

I al navegador del client visitem `https://localhost:10000`. La connexió arriba al port 10000 del client, viatja xifrada dins de la sessió SSH i el servidor SSH la lliura a `localhost:10000` de la instància, on escolta Webmin. El port 10000 no s'ha obert mai al grup de seguretat.

El procediment complet, incloent-hi la revisió de la seguretat d'SSH amb Webmin, està a l'activitat AF.3.1.12 — Administració d'SSH amb Webmin a través d'un túnel SSH.

Redirecció remota: -R

```
ssh -N -R 127.0.0.1:8080:127.0.0.1:80 alumne@192.168.0.1
```

Ara el port 8080 escolta en el bucle local del **servidor SSH**. Les connexions es transporten fins al port 80 del **client SSH**. El servei web ha d'existir en eixe client.

Per a exposar una redirecció remota en altres interfícies intervenen també `GatewayPorts`, l'adreça d'escolta i el tallafocs.

Permisos i diferència respecte de NAT

`AllowTcpForwarding` controla si el servidor admet estes redireccions; `PermitOpen` i `PermitListen` poden restringir-les. No s'ha de confondre este mecanisme amb `net.ipv4.ip_forward` del kernel.

Mecanisme	Funcionament
DNAT en un encaminador	Modifica la destinació dels paquets
Túnel SSH	Transporta connexions a través d'una sessió SSH autenticada i xifrada

El túnel es manté mentre continua activa la connexió SSH. Es pot afegir `-o ExitOnForwardFailure=yes` per a detectar errors en crear la redirecció, però això no garantix que el servei final responga.

Referències

- ssh: opcions -L, -R i -N.
- sshd_config: permisos de redirecció.
- Webmin: descàrrega i instal·lació.
- Amazon EC2: grups de seguretat.