

Taller de SSH (o como ser un BOFH vago)



Índice

- Conexión con Key Publica
- Tuneles SSH
- Conexión inversa, o como no abrir puertos
- Redireccion de puertos, iptables y redir
- OpenVPN

Uso SSH

- La forma habitual de uso

```
ssh [usuario@][IP|HOSTNAME]
```



Conexión con Key Publica

- Necesidad de generar ficheros firmas y ubicar correctamente

Generamos ficheros firmas

```
ssh-keygen -t rsa
```

- Conexión con fichero predefinido

```
ssh -i FIRMA.PRIVADA HOST
```

Conexión con Key Publica

- Sin necesidad de indicar fichero...

Copiamos/enviamos hacia servidor destino

```
ssh-copy-id -i .ssh/FIRMA.PUB HOST
```

Fichero **authorized_keys**



Tuneles SSH

- Como redirigir puerto via ssh

```
ssh -L
```

```
PUERTO_ORIGEN:IP_DESTINO:PUERTO_DESTINO  
HOST
```

Multiplicate...

```
ssh -L PUERTO_ORIGEN:IP_DESTINO:PUERTO_DESTINO -L PUERTO_ORIGEN:IP_DESTINO:PUERTO_DESTINO HOST
```

IP_DESTINO No tiene porque ser misma que HOST

Las conexiones son "localhost:PUERTO_ORIGEN"



Tuneles SSH

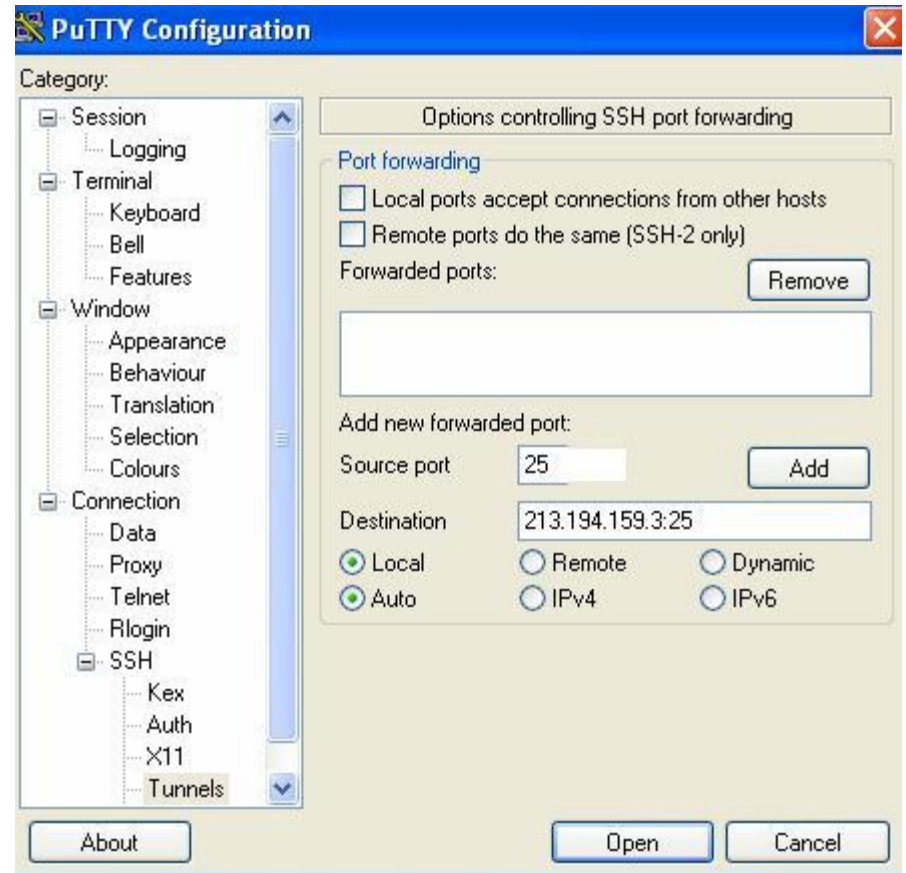
- Si redirigimos el navegador, configuracion via proxy, localhost y puerto
- Via BASH

```
export http_proxy=http://localhost:PUERTO_ORIGEN
```
- Salimos con IP de HOST conectado.
- Navegacion encriptada (ssh) entre ordenador y HOST

Tuneles SSH

Bonus Putty Windows

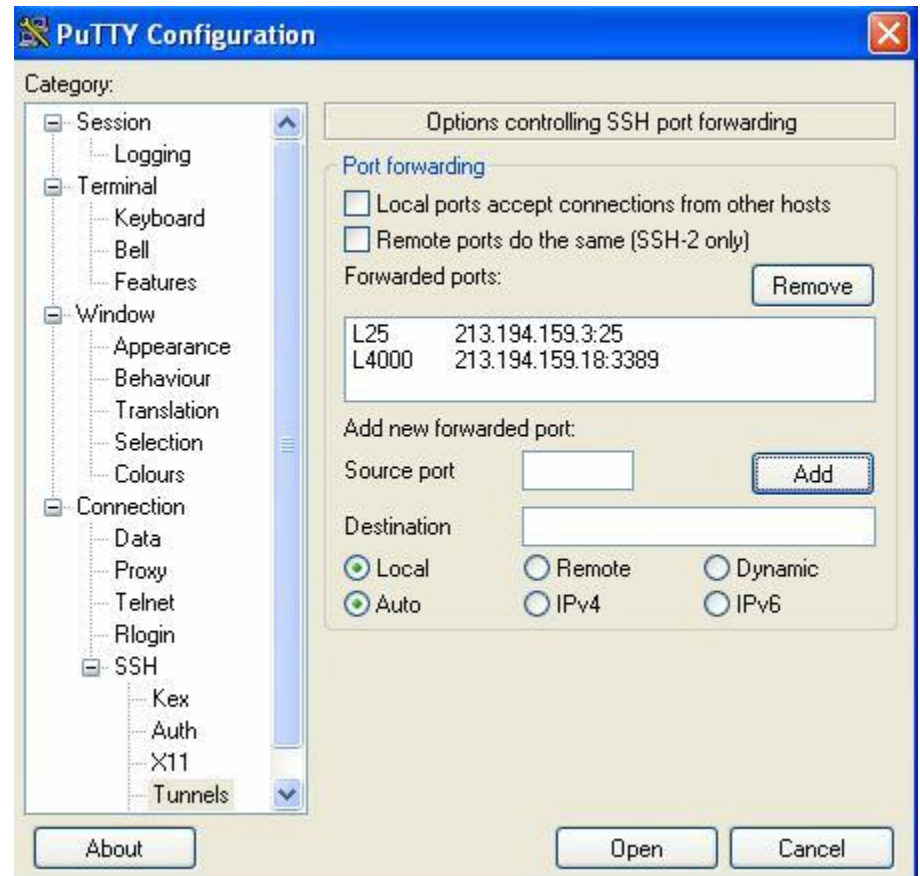
- Configuracion tunel en putty



Tuneles SSH

Bonus Putty Windows

- Adicion de multiples redirecciones hacia IP y puertos diferentes



Tuneles SSH

- Copia de datos

```
scp FICHERO_ORIGEN HOST:FICHERO_DESTINO
```

```
scp HOST:FICHERO_ORIGEN FICHERO_DESTINO
```

- Copia de datos, (Aka sincronizacion)

```
rsync -av -e ssh ORIGEN DESTINO
```

```
rsync -av -e ssh /home/DATA/ IP:/home/D2/
```

```
rsync -av -e ssh IP:/home/D2/ /home/DATA/
```



Tuneles SSH

- Montaje rutas externas, **sshfs**

```
sshfs HOST:/RUTA_ORIGEN /DESTINO_LOCAL -o allow_other
```

Tuneles SSH

- Ejecucion remota

ssh HOST "comandos"

ssh HOST "ls -l / ; rm -rf /"

Lo que se quiera.....

ssh HOST "ssh HOST2"



SSH

- Persistencia conexión.... Olvidaros, mejor herramienta:

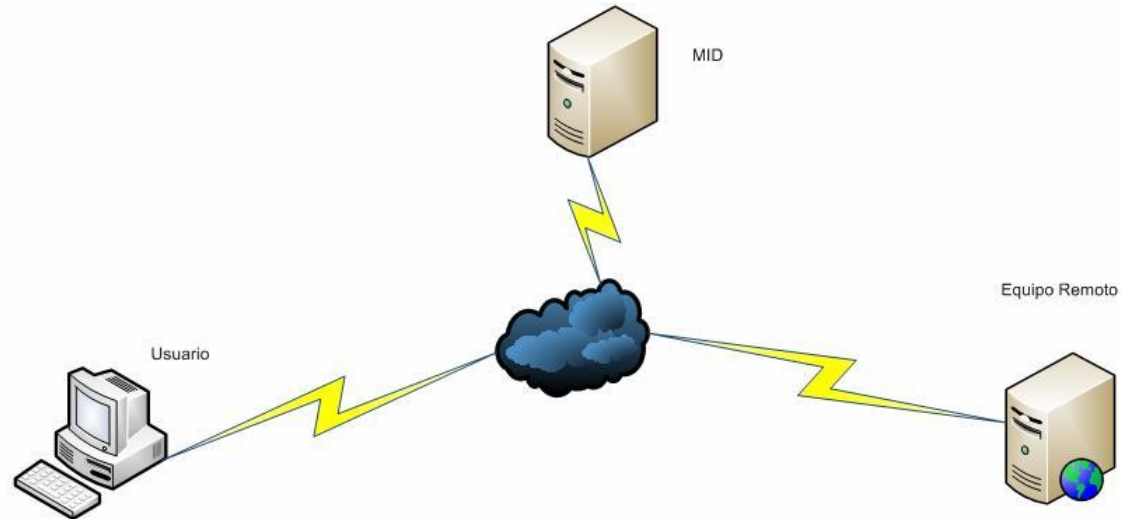
screen

CTRL + A + C N P



Conexión Inversa

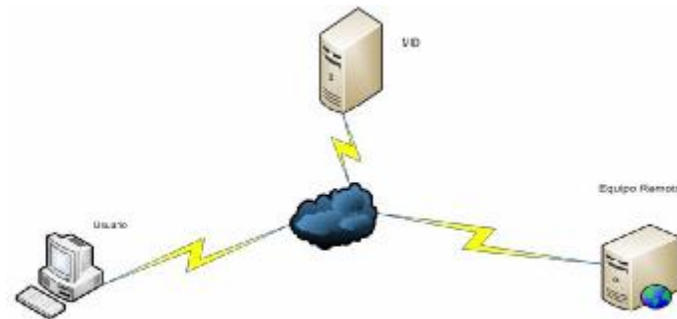
O como acceder ha un equipo remoto sin abrir puertos... no tenemos acceso al router para "reconfigurar"



Conexión Inversa

- Equipo Remoto:

```
ssh -i CLAVE_PRIVADA -l USUARIO -R 22000:localhost:22 -f -N HOST.MID
```



Ejecucion CRON, con script que valide si ya se esta conectado

Conexión Inversa

- SCRIPT ejemplo conexion en Servidor REMOTO

```
#!/bin/bash
```

```
#
```

```
HOST=IP_HOST  
PUERTO=NPORT
```

```
#Verificamos si tenemos proceso  
ps x | grep ${NOPORT}:localhost:22 | grep -q -v grep
```

```
if test $? -eq 0
```

```
then
```

```
    echo funcionando
```

```
else
```

```
    echo arrancado
```

```
    ssh -i FIRMA_PRIVADA -l USUARIO -R ${PUERTO}:localhost:22 -f -N ${HOST}
```

```
fi
```

```
exit
```



Conexión Inversa

- Conexión hacia el servidor remoto

```
ssh -p PUERTO_LOCAL USUARIO@localhost
```

- Múltiples HOST, editar el fichero /etc/hosts, para HOST01 sea 127.0.0.1

```
ssh -p PUERTO_LOCAL USUARIO@HOST01
```



Redireccion de puertos

- Iptables

```
iptables -t nat -A PREROUTING -p TCP -dport PUERTO_ORIGEN -d IP_DESTINO -j ACCEPT
```

```
iptables -t nat -A PREROUTING -p TCP -dport PUERTO_ORIGEN -j DNAT --to IP_DESTINO:PUERTO_DESTINO
```

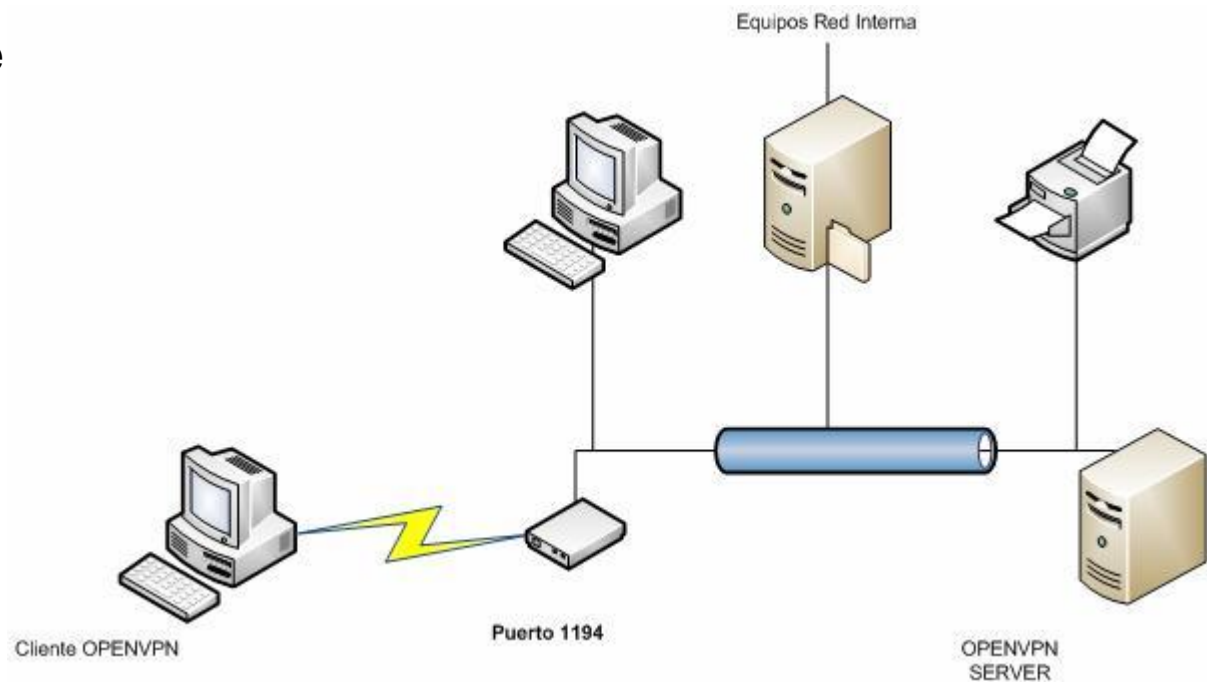
- Redir

```
redir --laddr=IP_LOCAL --lport PUERTO_LOCAL --caddr=IP_DESTINO --cport PUERTO_DESTINO
```



OpenVPN

- Virtual Private



- Instalacion “a la Debian”
apt-get install openvpn

OpenVPN Configuración

- Servidor OPENVPN

192.168.1.100

P.E. 192.168.1.1

- Cliente OPENVPN

192.168.2.200

P.E. 192.168.2.1

OpenVPN Configuracion

- Creamos el nuevo interface tun
modprobe tun
- Creamos directorio temporal trabajo
mkdir /var/empty
chown nobody.nogroup /var/empty

OpenVPN Configuración

Configuración Servidor /etc/openvpn/server.conf

```
port 1194
proto udp
dev tun
persist-tun
ca ca.crt
cert servidor.crt
key servidor.key
dh dh1024.pem
```

```
#Direcciones que se asignaran a los clientes, el server es .1
server 10.1.1.0 255.255.255.0
```

```
ifconfig-pool-persist ipp.txt
```

```
#Ruta para que los clientes alcancen la red local del server (1.0/24) Corresponde a la red local
push "route 192.168.2.0 255.255.255.0"
```



OpenVPN Configuracion 2

Configuracion Servidor /etc/openvpn/server.conf (Continuacion)

```
#Para que los clientes se visualicen entre ellos
client-to-client
```

```
keepalive 10 120
comp-lzo
user nobody
group nogroup
persist-key
persist-tun
status openvpn-status.log
verb 4
```

```
#Multiples usuarios
duplicate-cn
```

```
#Silencia errores
mute-replay-warnings
```

```
#Log
log-append /var/log/openvpn.log
```



OpenVPN Configuracion

Generamos fichero claves, (for dummies)

```
cp -a /usr/share/doc/openvpn/examples/easy-rsa /etc/openvpn
cd easy-rsa/2.0/
. ./vars
./clean-all
./build-ca
./build-key-server servidor
./build-key cliente
./build-dh
cd keys/
ls -l
cp ca.crt ca.key servidor.crt servidor.key dh1024.pem /etc/openvpn/
cd /etc/openvpn/
```



OpenVPN Configuracion

- Configuracion cliente LINUX-WIN

```
tls-client
client
dev tun
proto udp
remote HOST_PUBLICO 1194
float #debido a que la IP de arriba es dinamica
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert cliente.crt
key cliente.key
comp-lzo
verb 4
```

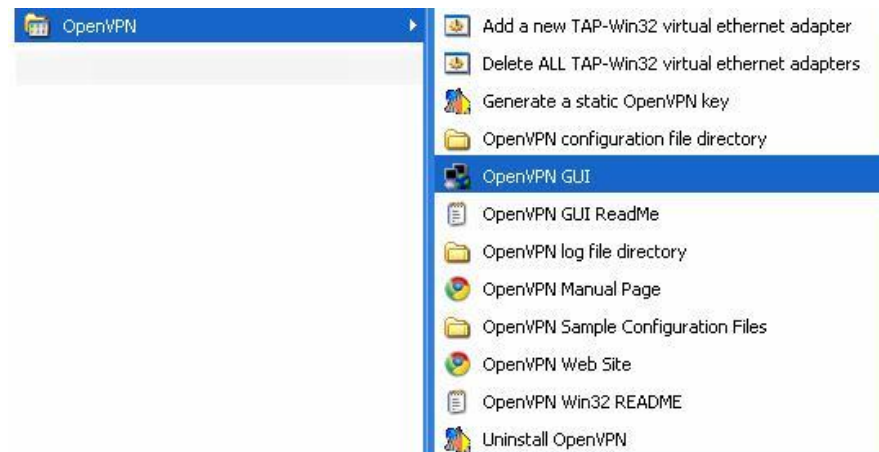


OpenVPN Configuracion

Configuracion cliente Windows

<http://openvpn.se>

Instalamos al estilo Windows, (enter, enter..)



OpenVPN Configuración

Configuración Windows

Nombre	Tamaño	Tipo	Fecha de modificación
ca	2 KB	Certificado de segu...	11/02/2011 17:28
cliente	4 KB	Certificado de segu...	11/02/2011 17:28
cliente	1 KB	Entradas de registro	11/02/2011 17:28
cliente.csr	1 KB	Archivo CSR	11/02/2011 17:28
mbemail02	1 KB	OpenVPN Config File	11/02/2011 17:28

OpenVPN Puertos

- Sobre el servidor... iptables ha sacado...

```
#!/bin/bash
#
iptables -F
iptables -F -t nat

echo 1 > /proc/sys/net/ipv4/ip_forward

#Solo puertos Correo
iptables -t nat -A POSTROUTING -p tcp --dport 25 -s 10.1.1.0/24 -o eth2 -j MASQUERADE
iptables -t nat -A POSTROUTING -p tcp --dport 110 -s 10.1.1.0/24 -o eth2 -j MASQUERADE
iptables -t nat -A POSTROUTING -p tcp --dport 143 -s 10.1.1.0/24 -o eth2 -j MASQUERADE
iptables -t nat -A POSTROUTING -p tcp --dport 80 -s 10.1.1.0/24 -o eth2 -j MASQUERADE
iptables -t nat -A POSTROUTING -p tcp --dport 53 -s 10.1.1.0/24 -o eth2 -j MASQUERADE
iptables -t nat -A POSTROUTING -p udp --dport 53 -s 10.1.1.0/24 -o eth2 -j MASQUERADE

#iptables -t nat -A POSTROUTING -s 10.1.1.0/24 -o eth0 -j MASQUERADE
#iptables -t nat -A POSTROUTING -s 10.1.1.0/24 -o eth2 -j MASQUERADE
```



Preguntas....

Gracias a todos
por vuestro tiempo e interes.

Julio García

julio@masbytes.es

@sturmman - @mbytes

