Si nuestra oficina o centro de trabajo tiene implementado un cortafuegos que no nos deja hacer prácticamente nada, debemos saber que es probable que el tráfico mediante el puerto 22 no lo tengan capado. Esto nos permitirá crear un túnel hasta un servidor SSH modificado que tengamos instalado en casa y sacar todo, o parte del tráfico, mediante él. Digo modificado porque es necesario hacer dos cambios al servidor SSH por defecto, para que esto se pueda realizar.

REQUISITOS

El servidor SSH de casa tiene que permitir:

IP4 O IP6 FORWARDING

Para permitirlo, modificamos el archivo **/etc/sysctl.conf** de la siguiente forma:

PARA IPV4:

```
sed -i -e 's|#net.ipv4.ip_forward=1|net.ipv4.ip_forward=1|g' /etc/sysctl.conf
```

PARA IPV6 (SÓLO SI ES NECESARIO):

```
sed -i -e 's|##net.ipv6.conf.all.forwarding=1|#net.ipv6.conf.all.forwarding=1|g' /etc/sysctl.conf
```

TCP FORWARDING

Para permitirlo, en el servidor SSH de casa modificamos el archivo **/etc/ssh/sshd_config** de la siguiente forma:

```
sed -i -e 's|#AllowTcpForwarding yes|AllowTcpForwarding yes|g' /etc/ssh/sshd_config
```

O bien creamos el archivo **/etc/ssh/sshd_config.d/AllowTCPForwarding.conf** con el texto «AllowTcpForwarding yes» (sin las comillas), ejecutando como root:

```
echo "AllowTcpForwarding yes" > /etc/ssh/sshd_config.d/AllowTCPForwarding.conf
```

Luego, reiniciamos el servidor SSH, ejecutando como root:

```
systemctl restart ssh
```

Después de reiniciar el servidor SSH, ya tendremos los requisitos satisfechos.

¿PARA QUÉ PODEMOS UTILIZARLO?

Esto son sólo algunos ejemplos de las cosas que podemos hacer:

PARA CONECTARNOS AL ESCRITORIO DEL ORDENADOR CASA

Podemos conectarnos al escritorio remoto de nuestro ordenador Windows (o Debian con xrdp, por ejemplo) de esta forma:

```
ssh -L 63389:192.168.0.100:3389 nico@81.82.83.84
```

Esto estaría creando en el puerto 63389 del ordenador desde el cual estemos ejecutando el comando, un túnel hacia el puerto 3389 (RDP) del ordenador de casa que tiene la IP 192.168.0.100 y que está en el servidor SSH que responde en la IP 81.82.83.84 (que sería la IP de nuestra casa). Esa IP puede ser numérica o puede ser un nombre de dominio, como por ejemplo:

```
ssh -L 63389:192.168.0.100:3389 nico@casadenico.ddns.net
```

Entonces, si desde el ordenador desde el que hemos creado el túnel, abrimos la aplicación de escritorio remoto y nos conectamos a la IP **127.0.0.1:63389** nos estaríamos conectando mediante escritorio remoto a nuestro ordenador de casa.

Esto también es posible hacerlo si tenemos el servidor SSH en un puerto diferente al 22, de esta forma:

```
ssh -L 63389:192.168.0.100:3389 nico@casadenico.ddns.net -p 11122
```

PARA NAVEGAR CON LA IP PÚBLICA DE CASA

Si no nos interesa que en la oficina o en el centro de trabajo vean los dominios que estamos visitando o si queremos acceder a dominios que el cortafuegos del curro tiene capados, nos interesará enviar todo nuestro tráfico web a través del túnel. Para ello, primero creamos el túnel, con:

```
ssh -D 3128 nico@casadenico.ddns.net
```

Puede ser cualquier puerto local que esté libre. He puesto el 3128 por costumbre.

De la misma forma que antes, si el servidor está en otro puerto diferente al 22, lo indicaríamos con:

```
ssh -D 3128 nico@casadenico.ddns.net -p 11122
```

Además, si no queremos que se nos quede abierta la ventana SSH, es decir, que nos logueemos efectivamente en el servidor de destino, podemos indicar el comando -fN, de forma que la conexión quede abierta, pero en background. Esto sería así:

```
ssh -fN -D 3128 nico@casadenico.ddns.net -p 11122
```

Esto es útil para que la conexión no se rompa si cerramos sin querer la ventana de terminal. Aunque, bien es cierto, que el proceso nos quedará abierto en segundo plano y, para terminarlo, deberemos ejecutar lo siguiente:

En Windows:

```
taskkill /F /IM ssh.exe /T
```

En Linux:

```
x
```

En MacOS:

```
x
```

Para finalizar, configuramos nuestro navegador Firefox para que utilice ese puerto local como puerto proxy socks5 de la siguiente forma:

- Ajustes >> General >> Configuración de red (abajo del todo).
- Marcamos «Configuración manual del proxy».
- En el campo «Host SOCKS», ponemos: 127.0.0.1 y en el campo «Puerto» ponemos 3128.
- Le damos al botón «Aceptar».

A partir de entonces, nuestro navegador utilizará el túnel para navegar por Internet. Pero cuidado, sólo el navegador web. El resto del software del ordenador del centro desde el que hemos creado el sock, así como el propio ordenador del centro, continuarán realizándo las conexiones con la IP que nos haya asignado el DHCP del curro.