openvpn

- PKI
- private internet access (PIA)

instalación

```
aptitude install openvpn
```

```
aptitude install easy-rsa
```

configuración servidor

copiar ficheros para facilitar la generación de claves y certificados:

```
cp -rd /usr/share/doc/openvpn/examples/easy-rsa/ /etc/openvpn/
```

creación keys

modificamos el fichero **vars** del directorio **easy-rsa**

/etc/openvpn/easy-rsa/vars

```
export KEY_DIR=“/etc/openvpn/keys”
```

empezamos la generación de la CA (Autoridad de Certificación):

```
# root o sudo
mkdir /etc/openvpn/keys
source vars
./clean-all
build-ca
```

se pueden dejar todos los valores por defecto

creamos el fichero de intercambio de claves (Diffie-Hellmann):

```
./build-dh
```

creamos la pareja de claves para el servidor:

```
./build-key-server <servidor>
```

esta instrucción genera los ficheros **.key**, **.crt**, **.csr**
hay que estar atentos cuando nos solicite los datos, a la pregunta de si deseamos firmar el certificado hay que responder **si**

personalizar fichero configuración

copiamos un fichero de configuración *base* para la parte servidor:

```
zcat /usr/share/doc/examples/sample-config-files/server.conf.gz > /etc/openvpn/server.conf
```

y modificamos las claves **ca**, **cert**, **key** y **dh** para las generadas (en `/etc/openvpn/keys`)

arrancar el servicio

```
service openvpn start
```

esto debería montar un nuevo dispositivo de red que podemos consultar a través de `ifconfig`

y si no es así, podemos depurar mirando en `tail -f /var/log/daemon.log`

configuración cliente

generación llaves

(suponemos que el fichero **vars** ya está correctamente configurado:

/etc/openvpn/easy-rsa

```
export vars
./build-key <cliente>
```

personalizar configuración

copiamos un fichero *base* para la configuración del cliente:

```
cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf /etc/openvpn/
```

y editamos este fichero para modificar las claves **remote**, **ca**, **crt** y **csr** para los valores del serividor y de las claves generadas para el cliente respectivamente

iniciar servicio

```
service openvpn start
```

esto debería crear un nuevo dispositivo de red visible con `ifconfig`

enlaces

- https://linuxboss.wordpress.com/?s=openvpn

- cliente mac: https://nordvpn.com/tutorials/x-mac-os-x/openvpn/