# OpenVPN Community VPN daemon

## CONCEPTS

> An option on the command line is the same as in a config file, just with the leading -- dropped: --verb 4 becomes verb 4.

**Client** tun0 device
↓ TLS handshake
**Control channel** certs, tls-crypt
↓ keys
**Data channel** data-ciphers
↓ UDP 1194
**Server** tun0, routes

## RUN

**openvpn --config** *<file>*
Start with a config file

**openvpn --config** *<file>* **--daemon**
Detach and run in background

**openvpn --config** *<file>* **--verb 4**
Set log verbosity (0-11, default 1)

**openvpn --config** *<file>* **--status** *<file>* *<sec>*
Write a status file every N seconds

## CLIENT OPTIONS

**client**
Pull options from the server, act as TLS client

**remote** *<host>* *<port>* *<proto>*
Server to connect to

**dev tun**
Routed IP tunnel device

**proto udp**
Transport: udp, tcp-client, tcp-server

**auth-user-pass** *<file>*
Username and password from a file

## KEYS AND TLS

**ca** *<file>*
CA certificate to trust

## KEYS AND TLS (cont.)

**cert** *<file>*
Your certificate

**key** *<file>*
Your private key

**tls-crypt** *<file>*
Encrypt and authenticate control channel

**remote-cert-tls server**
Require a server-purpose certificate

**data-ciphers** *<list>*
Colon-separated data channel ciphers

**openvpn --genkey tls-crypt** *<file>*
Create a tls-crypt key

## SERVER OPTIONS

**server** *<network>* *<netmask>*
Server mode with a client address pool

**push "***<option>***"**
Send an option to every client

**client-config-dir** *<dir>*
Per-client files named by common name

**keepalive** *<interval>* *<timeout>*
Ping and restart on silence

## ROUTING AND DNS

**push "redirect-gateway def1"**
Send all client traffic via the VPN

**redirect-gateway def1**
Same, set on the client

**push "route** *<network>* *<netmask>***"**
Give clients a route to a subnet

## OPERATE

**systemctl start openvpn-client@***<name>*
Start /etc/openvpn/client/<name>.conf

## TROUBLESHOOT

**ip addr show tun0**
Check the tunnel got an address