OpenVPN

openvpn_install

```
wget -O - https://swupdate.openvpn.net/repos/repo-public.gpg|apt-key add -
echo "deb http://build.openvpn.net/debian/openvpn/stable stretch main" > /etc/apt/sources.list.d/openvpn-aptrepo.list
apt update && apt install openvpn

adduser --system --shell /usr/sbin/nologin --no-create-home ovpn
groupadd ovpn
usermod -g ovpn ovpn

openvpn --genkey --secret /etc/openvpn/server/ta.key
openssl genpkey -genparam -algorithm DH -out /etc/openvpn/server/dhp4096.pem -pkeyopt dh_paramgen_prime_len:4096
```

easy_rsa

```
make-cadir ./ca
cd ca
ln -s openssl-1.0.0.cnf openssl.cnf
nano vars #-> edit key default values
source ./vars
./clean-all

./build-ca
./build-key-server <common-name>

scp ./keys/{ca.crt,<common-name>.crt,<common-name>.key} root@ip:/etc/openvpn/server
scp root@ip:/etc/openvpn/server/ta.key ./keys

cd ca && source ./vars && ./build-key client1
./build-key client1
```

ufw

```
ufw allow 1194/udp

nano /etc/default/ufw
-> DEFAULT_FORWARD_POLICY="ACCEPT"

nano /etc/ufw/before.rules
# START OPENVPN RULES
# NAT table rules
```

```
*nat
:POSTROUTING ACCEPT [0:0]
# Allow traffic from OpenVPN client to eth0
-A POSTROUTING -s 10.8.0.0/8 -o eth0 -j MASQUERADE
COMMIT
# END OPENVPN RULES
```

server.conf

```
dev tun
persist-key
persist-tun
topology subnet
port 1194
proto udp
keepalive 10 120

# Location of certificate authority's cert.
ca /etc/openvpn/server/ca.crt

# Location of VPN server's TLS cert.
cert /etc/openvpn/server/server.crt

# Location of server's TLS key
key /etc/openvpn/server/server.key

# Location of DH parameter file.
dh /etc/openvpn/server/dhp4096.pem

# The VPN's address block starts here.
server 10.8.0.0 255.255.255.0

explicit-exit-notify 1

# Drop root privileges and switch to the `ovpn` user after startup.
user ovpn

# OpenVPN process is exclusive member of ovpn group.
group ovpn

# Cryptography options. We force these onto clients by
# setting them here and not in client.ovpn. See
# `openvpn --show-tls`, `openvpn --show-ciphers` and
#`openvpn --show-digests` for all supported options.
tls-crypt /etc/openvpn/server/ta.key
auth SHA512    # This needs to be in client.ovpn too though.
tls-version-min 1.2
tls-cipher TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-AES-256-CBC-SHA256
ncp-ciphers AES-256-GCM:AES-256-CBC
```

```
# Logging options.
ifconfig-pool-persist ipp.txt
status openvpn-status.log
log /var/log/openvpn.log
verb 3
```

client.ovpn

```
# No cryptography options are specified here because we want
# the VPN server to push those settings to clients rather than
# allow clients to dictate their crypto.

client
dev tun
persist-key
persist-tun
proto udp
nobind
#user ovpn
#group ovpn
remote-cert-tls server
auth SHA512
verb 3

# Remote server's IP address and port. IP is
# preferable over hostname so as not to rely
# on DNS lookups.
remote <your_linode's IP address> 1194

# To successfully import this profile, you
# want the client device's CA certificate copy,
# client certificate and key, and HMAC signature
# all in the same location as this .ovpn file.
ca ca.crt
cert client1.crt
key client1.key
tls-crypt ta.key
```

```
journalctl -f | grep vpn
journalctl -xe | grep vpn
```