Initial setup

* apt-get update
* apt-get install openvpn iptables openssl ca-certificates -y
* wget -O ~/easyrsa.tgz "https://github.com/OpenVPN/easy-rsa/releases/download/v3.0.5/EasyRSA-nix-3.0.5.tgz" 2>/dev/null
* tar xzf ~/easyrsa.tgz -C ~/
* mv ~/EasyRSA-3.0.5/ /etc/openvpn/
* mv /etc/openvpn/EasyRSA-3.0.5/ /etc/openvpn/easy-rsa/
* chown -R root:root /etc/openvpn/easy-rsa/
* rm -f ~/easyrsa.tgz
* cd /etc/openvpn/easy-rsa/
* ./easyrsa init-pki
* ./easyrsa --batch build-ca nopass
* EASYRSA\_CERT\_EXPIRE=3650 ./easyrsa build-server-full server nopass
* EASYRSA\_CRL\_DAYS=3650 ./easyrsa gen-crl
* cp pki/ca.crt pki/private/ca.key pki/issued/server.crt pki/private/server.key pki/crl.pem /etc/openvpn
* chown nobody:nogroup /etc/openvpn/crl.pem
* openvpn --genkey --secret /etc/openvpn/ta.key

echo ' -----BEGIN DH PARAMETERS-----

MIIBCAKCAQEA//////////+t+FRYortKmq/cViAnPTzx2LnFg84tNpWp4TZBFGQz

+8yTnc4kmz75fS/jY2MMddj2gbICrsRhetPfHtXV/WVhJDP1H18GbtCFY2VVPe0a

87VXE15/V8k1mE8McODmi3fipona8+/och3xWKE2rec1MKzKT0g6eXq8CrGCsyT7

YdEIqUuyyOP7uWrat2DX9GgdT0Kj3jlN9K5W7edjcrsZCwenyO4KbXCeAvzhzffi

7MA0BM0oNC9hkXL+nOmFg/+OTxIy7vKBg8P+OxtMb61zO7X8vC7CIAXFjvGDfRaD

ssbzSibBsu/6iGtCOGEoXJf//////////wIBAg==

-----END DH PARAMETERS-----' > /etc/openvpn/dh.pem

* // PROBABLY NOT iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE
* iptables -t nat -A POSTROUTING -s 10.8.0.0/24 ! -d 10.8.0.0/24 -j SNAT --to $IP
* iptables -t nat -A POSTROUTING -s 10.8.1.0/24 ! -d 10.8.1.0/24 -j SNAT --to $IP
* sysctl -w net.ipv4.ip\_forward=1

**Server conf (/etc/openvpn/tcp.conf)**

port 443

proto tcp

dev tun

sndbuf 0

rcvbuf 0

ca ca.crt

cert server.crt

key server.key

dh dh.pem

auth SHA512

tls-auth ta.key 0

topology subnet

server 10.8.0.0 255.255.255.0

ifconfig-pool-persist ipp.txt

push "redirect-gateway def1 bypass-dhcp”

push "dhcp-option DNS 1.1.1.1"

push "dhcp-option DNS 1.0.0.1"

keepalive 10 120

cipher AES-256-CBC

user nobody

group nogroup

persist-key

persist-tun

status openvpn-status.log

verb 3

crl-verify crl.pem

**Server conf (/etc/openvpn/udp.conf)**

port 1194

proto udp

dev tun

sndbuf 0

rcvbuf 0

ca ca.crt

cert server.crt

key server.key

dh dh.pem

auth SHA512

tls-auth ta.key 0

topology subnet

server 10.8.1.0 255.255.255.0

ifconfig-pool-persist ipp.txt

push "redirect-gateway def1 bypass-dhcp”

push "dhcp-option DNS 1.1.1.1"

push "dhcp-option DNS 1.0.0.1"

keepalive 10 120

cipher AES-256-CBC

user nobody

group nogroup

persist-key

persist-tun

status openvpn-status.log

verb 3

crl-verify crl.pem

* systemctl restart [openvpn@tcp/udp.service](mailto:openvpn@tcp/udp.service)
* **server**.server is the name of the conf file

Cert generation

* EASYRSA\_CERT\_EXPIRE=3650 ./easyrsa build-client-full ${reqId} nopass

**Client conf (one tcp\_template and on udp\_template)**

client

dev tun

proto $PROTOCOL

sndbuf 0

rcvbuf 0

remote $IP $PORT

resolv-retry infinite

nobind

persist-key

persist-tun

remote-cert-tls server

auth SHA512

cipher AES-256-CBC

setenv opt block-outside-dns

key-direction 1

verb 3

auth-nocache

<ca>

cat /etc/openvpn/easy-rsa/pki/ca.crt

</ca>

<cert>

CERT PLACEHOLDER

</cert>

<key>

KEY PLACEHOLDER

</key>

<tls-auth>

cat /etc/openvpn/ta.key

</tls-auth>