

# VPS als Gateway zum Hosting / übergehen DynDNS

## VPN-Server aufsetzen

Server auf den neusten Stand bringen

```
sudo apt update && sudo apt upgrade -y
```

Open-VPN und easy-rsa installieren

```
sudo apt install openvpn easy-rsa -y
```

Easy-RSA Umgebung einrichten

```
make-cadir ~/openvpn-ca  
cd ~/openvpn-ca  
./easyrsa clean-all  
./easyrsa build-ca
```

Server-Zerti erstellen

```
./easyrsa gen-req server nopass  
./easyrsa sign-req server server
```

DH und TLS-Auth

```
./easyrsa gen-dh  
openvpn --genkey --secret ta.key
```

Client-Zerti

```
./easyrsa gen-req client nopass
```

```
./easyrsa sign-req client client
```

Alles kopieren und OpenVPN Config erstellen in /etc/OpenVPN

```
port 1194
proto udp
dev tun

ca ca.crt
cert server.crt
key server.key
dh dh.pem

tls-auth ta.key 0

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 8.8.8.8"

keepalive 10 120
cipher AES-256-CBC
user nobody
group nogroup
persist-key
persist-tun
status openvpn-status.log
log-append /var/log/openvpn.log
verb 3
explicit-exit-notify 1
```

Starten und in systemctl aktivieren

```
sudo systemctl enable openvpn@server
sudo systemctl start openvpn@server
sudo systemctl status openvpn@server
```

# Firewall und IP-Forwarding

Firewall auf Hostenseite nicht vergessen!

```
# IP-Forwarding aktivieren
echo 1 > /proc/sys/net/ipv4/ip_forward
sudo sed -i 's/#net.ipv4.ip_forward=1/net.ipv4.ip_forward=1/' /etc/sysctl.conf
sudo sysctl -p
```

```
# NAT über iptables
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE
sudo apt install iptables-persistent -y
sudo netfilter-persistent save
```

## Client-Konfiguration

OpenVPN-Config für den Client:

```
client
dev tun
proto udp
remote YOUR.SERVER.IP 1194
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
cipher AES-256-CBC
verb 3
key-direction 1

ca ca.crt
cert client1.crt
key client1.key
tls-auth ta.key 1
```

Befehl zum Kopieren über SSH

```
pscp user@vps-ip:/root/openvpn-ca/ta.key C:\Users\DeinBenutzer\Downloads\  
pscp user@vps-ip:/root/openvpn-ca/pki/ca.crt C:\Users\DeinBenutzer\Downloads\  
pscp user@vps-ip:/root/openvpn-ca/pki/issued/client.crt C:\Users\DeinBenutzer\Downloads\  
pscp user@vps-ip:/root/openvpn-ca/pki/private/client.key C:\Users\DeinBenutzer\Downloads\
```

# IP-Tables-Regeln setzen

```
# Weiterleitung von Port 80 an 10.8.0.5:80  
sudo iptables -t nat -A PREROUTING -p tcp -d 85.215.196.99 --dport 80 -j DNAT --to-destination 10.8.0.5:80  
  
# Erlauben, dass die Pakete auch rausgehen dürfen  
sudo iptables -t nat -A POSTROUTING -j MASQUERADE  
sudo netfilter-persistent save
```

---

Revision #2

Created 25 June 2025 08:06:07 by Admin

Updated 25 June 2025 08:31:02 by Admin