

Server-Konfiguration

```
#####  
##  
# sources for configuration:  
# http://sarwiki.informatik.hu-berlin.de/OpenVPN_(deutsch)  
# http://www.online--tutorials.net/security/openvpn-tutorial/  
  
### BASICS  
mode server  
# bridged vpn with client IP range  
server-bridge 192.168.72.1 255.255.255.0 192.168.72.61 192.168.72.100  
  
# Protocol/port  
proto udp  
port 1194  
  
### Type of operation  
# operation with PKI  
tls-server  
# instead for using a symmetric key  
# secret /etc/openvpn/server_static.key  
# for vpn with shared key  
# tls-auth xxx 1  
  
# Device type  
dev tap0  
  
# receive connection request on this local adress only  
# if not defined, use all interfaces  
local 192.168.172.1  
  
# topology and network  
topology subnet  
# make IPs persistant  
ifconfig-pool-persist ipp.txt  
# clients can see each other  
client-to-client  
  
# see  
http://winaero.com/blog/speed-up-openvpn-and-get-faster-speed-over-its-channel/  
sndbuf 393216  
rcvbuf 393216  
  
## PKI - certificates and keys, directory of cert/key  
cd /etc/openvpn  
## Root CA which signed openvpn server and client certs  
ca /etc/easyrsa-pki/ca.crt
```

```
## cert of openvpn server
cert /etc/openvpn/locutus.netzwissen.local.crt
## key of server
key /etc/openvpn/locutus.netzwissen.local.key
# diffie hellman parameter
# create with: openssl genpkey -genparam -algorithm DH -out
/etc/openvpn/dh2014.pem
dh /etc/easyrsa-pki/dh.pem
# certificate revocation list, should be copied from CA
crl-verify /etc/openvpn/crl.pem

# Verification of certs
# Details: https://community.openvpn.net/openvpn/wiki/Openvpn23ManPage
# old method (Name/name-prefix from CN field)
# verify-x509-name locutus.netzwissen.local name
# new method from RFC3280: type of certificate must be client
remote-cert-eku "TLS Web Client Authentication"

# Cipher algorithm
cipher AES-256-CBC
# HMAC Authentication
auth SHA256

# tunnel compression
comp-lzo

# hardening. Beware: can exclude pre-2.3.3 clients
# tls-version-min 1.2

## pushed configs for clients for routing & dns
## redirect all traffic to VPN
## push "redirect-gateway def1"
push "route 192.168.72.0 255.255.255.0 172.168.72.1"
push "dhcp-option DOMAIN netzwissen.local"
push "dhcp-option DNS 192.168.72.1"
push "dhcp-option WINS 192.168.72.1"
#
http://winaero.com/blog/speed-up-openvpn-and-get-faster-speed-over-its-channel/
push "sndbuf 393216"
push "rcvbuf 393216"

# will not work with --ifconfig-pool-persist
# duplicate-cn
# permissions after connect
user nobody
group nogroup
# dont re-read keys after --ping-restart
persist-key
# dont restart tun after --ping-restart
persist-tun
```

```
### LOGGING
log /var/log/openvpn.log
# Status info
status /var/log/openvpn-status.log 20
# dont repeat messages so often
mute 20
# Log-Levels: 0 no logging, 4 standard, 5 + 6 debugging, 9 max
verb 6

# Daemon-Mode: write to syslog - activate after the configuration finished
daemon

# Management console
management localhost 7505
```

Management Console

Die Management Konsole läuft auf localhost und ist über P. 7505 erreichbar.

```
root@server6:/etc/openvpn/staticclients# telnet localhost 7505
```

Beenden mit quit.

```
INFO:OpenVPN Management Interface Version 1 -- type 'help' for more info
help
Management Interface for OpenVPN 2.3.10 x86_64-pc-linux-gnu [SSL (OpenSSL)]
[LZO] [EPOLL] [PKCS11] [MH] [IPv6] built on Feb  2 2016
Commands:
auth-retry t           : Auth failure retry mode (none,interact,nointeract).
bytecount n           : Show bytes in/out, update every n secs (0=off).
echo [on|off] [N|all] : Like log, but only show messages in echo buffer.
exit|quit             : Close management session.
forget-passwords      : Forget passwords entered so far.
help                  : Print this message.
hold [on|off|release] : Set/show hold flag to on/off state, or
                       release current hold and start tunnel.
kill cn               : Kill the client instance(s) having common name cn.
kill IP:port          : Kill the client instance connecting from IP:port.
load-stats            : Show global server load stats.
log [on|off] [N|all]  : Turn on/off realtime log display
                       + show last N lines or 'all' for entire history.
mute [n]              : Set log mute level to n, or show level if n is
absent.
needok type action    : Enter confirmation for NEED-OK request of 'type',
                       where action = 'ok' or 'cancel'.
needstr type action   : Enter confirmation for NEED-STR request of 'type',
                       where action is reply string.
net                   : (Windows only) Show network info and routing table.
```

```

password type p      : Enter password p for a queried OpenVPN password.
remote type [host port] : Override remote directive, type=ACCEPT|MOD|SKIP.
proxy type [host port flags] : Enter dynamic proxy server info.
pid                  : Show process ID of the current OpenVPN process.
pkcs11-id-count     : Get number of available PKCS#11 identities.
pkcs11-id-get index : Get PKCS#11 identity at index.
client-auth CID KID : Authenticate client-id/key-id CID/KID (MULTILINE)
client-auth-nt CID KID : Authenticate client-id/key-id CID/KID
client-deny CID KID R [CR] : Deny auth client-id/key-id CID/KID with log
reason
                        text R and optional client reason text CR
client-kill CID [M]  : Kill client instance CID with message M
(def=RESTART)
env-filter [level]  : Set env-var filter level
client-pf CID       : Define packet filter for client CID (MULTILINE)
rsa-sig             : Enter an RSA signature in response to>RSA_SIGN
challenge
                    Enter signature base64 on subsequent lines followed
by END
signal s            : Send signal s to daemon,
                    s = SIGHUP|SIGTERM|SIGUSR1|SIGUSR2.
state [on|off] [N|all] : Like log, but show state history.
status [n]          : Show current daemon status info using format #n.
test n              : Produce n lines of output for testing/debugging.
username type u     : Enter username u for a queried OpenVPN username.
verb [n]            : Set log verbosity level to n, or show if n is
absent.
version             : Show current version number.

```

Debugging auf OpenVPN Client Seite (Linux)

```
journalctl -fu NetworkManager
```

Client IPs fest zuweisen

In die *.conf kommt eine neue Direktive:

```
client-config-dir /etc/openvpn/staticclients
```

In diesem Verzeichnis für jeden Client einen Datei openvpn_dvsdnet_[name] legen. Diese enthält die IP Adresse und die Netzmaske des Clients:

```
ifconfig-push 192.168.50.16 255.255.255.0
```

OpenVPN liest diese Datei beim Connect zusätzlich ein, aber DNS und Gateway kommen weiterhin

über die zentralen push Kommandos. Ggf kann man auch ein Client-spezifisches Push anhängen, siehe dazu <http://michlstechblog.info/blog/openvpn-set-a-static-ip-address-for-a-client/>

Quelle: <https://github.com/OpenVPN/easy-rsa>

EASYRSA: CA einrichten

```
./easyrsa init-pki  
./easyrsa build-ca
```

DH erzeugen

```
./easyrsa gen-dh
```

EASYRSA: Zertifikate erzeugen

Signing Request (CSR) erzeugen, mit **nopass** = Key **ohne** Passwort

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

danach signieren mit

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

server und *client* bestimmt, ob es ein Server oder Client Zertifikat ist.

Achtung bei OpenVPN: der Client sollte den im OpenVPN Zertifikat angegebenen Common Name prüfen. Server prüft seinerseits den Zertifikatstyp des Clients (RFC3280):

```
# Verification of certs  
# Details: https://community.openvpn.net/openvpn/wiki/Openvpn23ManPage  
# old method (Name/name-prefix from CN field)  
# verify-x509-name locutus.netzwissen.local name  
# new method from RFC3280: type of certificate must be client  
remote-cert-eku "TLS Web Client Authentication"
```

Zertifikate zurückziehen

```
./easysrsa revoke server EntityName
```

Danach mit easysrsa gen-crl die zurückgezogenen zertifikate in die crl aufnehmen.

pki/index.txt zeigt, welche Zertifikate zurückgezogen wurden.

Inhalte kontrollieren

CSR

```
openssl req -in www2.netzwissen.de.csr -text -noout
```

Zertifikat

```
openssl x509 -in certificate.crt -text -noout
```

From:
<https://wiki.netzwissen.de/> - **netzwissen.de Wiki**

Permanent link:
<https://wiki.netzwissen.de/doku.php?id=openvpn&rev=1503566646>

Last update: **17/08/2024 - 07:06**

