WireGuard - VPN-Server

Quelle: https://www.howtoforge.de/anleitung/wireguard-vpn-unter-debian-11-installieren/

Wireguard: Private-Key mit GPG verschlüsselt speichern

Server einrichten

```
sudo apt update
```

```
sudo apt install wireguard
```

Am einfachsten alles als root
Server-Schlüssel - privat (key) und öffentlich (pub) generieren

```
wg genkey | sudo tee /etc/wireguard/server.key
```

```
chmod 0400 /etc/wireguard/server.key
```

```
cat /etc/wireguard/server.key | wg pubkey | sudo tee
/etc/wireguard/server.pub
```

Client-Schlüssel - privat (key) und öffentlich (pub) generieren (auf dem Server durchführen)

```
mkdir -p /etc/wireguard/clients
```

```
wg genkey | tee /etc/wireguard/clients/client1.key
```

```
cat /etc/wireguard/clients/client1.key | wg pubkey | tee
/etc/wireguard/clients/client1.pub
```

Client1 kann auch anders benannt werden - z.B. mit dem Namen eines Users oder einer Workstation

Server-Konfiguration erstellen

```
nano /etc/wireguard/wg0.conf
```

```
[Interface]
# Wireguard Server private key - server.key
PrivateKey = <PRIVATKEY-SERVER>
# Wireguard interface will be run at 10.8.0.1
Address = 10.8.0.1/24
# Clients will connect to UDP port 51820
ListenPort = 51820
# Ensure any changes will be saved to the Wireguard config file
```

```
SaveConfig = true

[Peer]
# Wireguard client public key - client1.pub
PublicKey = <PUBLIC-KEY-CLIENT_n>
# clients' VPN IP addresses you allow to connect
# possible to specify subnet ? [10.8.0.0/24]
AllowedIPs = 10.8.0.2/32

[Peer]
# weitere Clients sind möglich > client public key - kmueller.pup
PublicKey = <PUBLIC-KEY-CLIENT_n>
AllowedIPs = 10.8.0.3/32
```

ÄNDERN:

- <PRIVATKEY-SERVER>
- <PUBLIC-KEY-CLIENT_n>

zu AllowedIPs: mit 1 Peer hat die Grundeinstellung /24 geklappt, bei mehreren musste das umgestellt werden auf /32.

Port-Forwarding

```
nano /etc/sysctl.conf
```

Einfügen in die Datei

```
# Port Forwarding for IPv4
net.ipv4.ip_forward=1
# Port forwarding for IPv6
net.ipv6.conf.all.forwarding=1
```

Änderungen übernehmen

```
sysctl -p
```

Firewall

siehe Firewall

```
ufw allow OpenSSH
```

Internetschnittstelle des Servers ermitteln

```
ip route list default
```

Ergebnis z.B. default via 162.37.1.1 dev eth0

Hier ist eth0 die Schnittstelle

WireGuard-Serverkonfiguration

```
nano /etc/wireguard/wg0.conf
```

Einfügen in Abschnitt Interface

```
PostUp = ufw route allow in on wg0 out on eth0
PostUp = iptables -t nat -I POSTROUTING -o eth0 -j MASQUERADE
PostUp = ip6tables -t nat -I POSTROUTING -o eth0 -j MASQUERADE
PreDown = ufw route delete allow in on wg0 out on eth0
PreDown = iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE
PreDown = ip6tables -t nat -D POSTROUTING -o eth0 -j MASQUERADE
```

Port in Firewall öffnen

```
ufw allow 51820/udp
```

```
ufw reload
```

WG-Server starten

```
systemctl start wg-quick@wg0.service
```

enable = mit System starten

```
systemctl enable wg-quick@wg0.service
```

```
systemctl status wg-quick@wg0.service
```

Schnittstelle wg0 überprüfen

```
ip a show wg0
```

WG-Server starten und stoppen

```
wg-quick up /etc/wireguard/wg0.conf
```

```
wg-quick down /etc/wireguard/wg0.conf
```

Linux Client einrichten

```
sudo apt install wireguard-tools
```

Konfigurationsdatei erstellen. Diese Datei kann, z.B. als clint1.conf, inhaltsgleich für den Import eines Windowsclients genutzt werden. Die u.a. Kommentare stören den Import nicht.

```
sudo nano /etc/wireguard/wg-client1.conf
```

```
[Interface]
# Define the IP address for the client - must be matched with wg0 on
Wireguard Server
Address = 10.8.0.2/24
# specific DNS Server
DNS = 192.168.178.1
# Private key for the client - client1.key
PrivateKey = <PRIVATKEY-CLIENT1>

[Peer]
# Public key of the Wireguard server - server.pub
PublicKey = <PUBLICKEY-SERVER>
# Allow all traffic to be routed via Wireguard VPN
AllowedIPs = 0.0.0.0/0
# Public IP address of the Wireguard Server
Endpoint = <IP_SERVER>:51820
# Sending Keepalive every 25 sec
PersistentKeepalive = 25
```

ÄNDERN:

- <PRIVATKEY-CLIENT1>
- <PUBLICKEY-SERVER>
- <IP_SERVER>

Wireguard starten

```
wg-quick up wg-client1
```

Evtl. installieren bei Fehlermeldung beim Start VPN

```
sudo apt install openresolv
```

Schnittstelle prüfen

```
ip a show wg-client1
```

Verbindung anzeigen » einmal auf dem Client und einmal auf dem Server

```
sudo wg show
```

Server-Zugriff vom Client testen

```
ping -c5 10.8.0.1
```

```
ping -c5 1.1.1.1
```

```
ping -c5 duckduckgo.com
```

Wireguard beenden (Server und Client)

```
wg-quick down wg-client1
```

Windows-Client einrichten

1. Installationsdatei herunterladen
2. Installieren
3. Konfigurationsdatei importieren, siehe Linux Client einrichten einrichten