# Wireguard

Wichtig: Wireguard ist ein peer-to-peer VPN!

Quelle: https://www.linux-community.de/ausgaben/linuxuser/2018/11/tunnelbauer/

## Schlüsselpaar erzeugen

```
cd /etc/wireguard
umask 077
sudo wg genkey > private.key
sudo wg pubkey > public.key < private.key
# alternativ auf einem Client
sudo wg genpsk > psk.key
```

wg zeigt die Konfiguration

```
locutus:/etc/wireguard # wg
interface: wg0
  public key: LgHjmEbTBoIyG5jSvZ0ArG2pB9XPax0NqfZGu+JiXS8=
  private key: (hidden)
  listening port: 33060
```

## Schnittstelle und Netzwerk erzeugen

listen port frei wählbar, hier 33060. Netzwerk:

```
# Client1
sudo ip link add wg0 type wireguard
sudo ip addr add 10.0.01/24 dev wg0
sudo wg set wg0 private-key ./private.key
# Bei Bedarf zusätzlich
sudo wg set wg0 listen-port 33060
# Client2
sudo ip link add wg0 type wireguard
sudo ip addr add 10.0.02/24 dev wg0
sudo wg set wg0 private-key ./private.key
```

Beide Clients gegenseitig bekanntmachen

```
sudo wg set wg0 peer //Public Key von Client2// persistent-keepalive 25
preshared-key //Preshared Key von Client1 und Client2// allowed-ips
10.0.0.2/24 endpoint 192.168.178.25:44234
```

Notebook: als `allowed-ips` darf der String `0.0.0.0/0` stehen. Das bedeutet, Sie vertrauen dem

Server, das gesamte Internet zu tunneln. Bei `endpoint` hinterlegen Sie die reale interne IP-Adresse von `Client2` und dem von Ihnen oder dem System dafür vergebenen Port. Bei `Client1` mussten wir anstatt der IP-Adresse die Domain angeben. Sollten Sie also mit der IP-Adresse eine Meldung bekommen, sie sei unbekannt, so klappt es mit dem Domain-Namen.

## Masquerading zwischen den beiden Clients

```
/sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE echo 1 >
/proc/sys/net/ipv4/ip_forward
```