

Wireguard

Kryptografie

Privaten Schlüssel erzeugen

```
wg genkey > wg-c2s-private.key
```

Öffentlichen Schlüssel erzeugen

```
cat wg-c2s-private.key | wg pubkey > wg-c2s-public.key
```

Konfiguration

Wireguard wird über Konfigurationsdateien verwaltet. Diese liegen unter `/etc/wireguard/<interface name>.conf`.

Eine solche Datei sieht ungefähr so aus.

[/etc/wireguard/wg0.conf](#)

```
# Lokales Interface
[Interface]
Address = 192.168.123.1/24
PrivateKey = <private key of local interface>
ListenPort = 51820 # Netzwerport
PostUp = <bash command>
PostDown = <bash command>

# Client 1
[Peer]
PublicKey = <public key of client 1>
AllowedIPs = 192.168.123.11/32

# Client 2
[Peer]
PublicKey = <public key of client 2>
AllowedIPs = 192.168.123.12/32
```

- **AllowedIPs** dient WireGuard zum routen von Paketen

Wireguard verwenden

Interface starten

```
wg-quick up <interface name>
```

Interface stoppen

```
wg-quick down <interface name>
```

Interface starten systemd

```
systemctl start wg-quick@<interface name>
```

Interface stoppen systemd

```
systemctl stop wg-quick@<interface name>
```

Interface persistent starten systemd

```
systemctl enable wg-quick@<interface name>
```

Beispiele

Gute Beispiele hier: <https://github.com/pirate/wireguard-docs>

Client-Server-Client

Server

[/etc/wireguard/wg-csc.conf](#)

```
[Interface]
Address = 192.168.123.1/24 # IP Adresse des Servers
PrivateKey = <private key of server>
ListenPort = 51820 # Port, auf dem der Server läuft
# Forwardingregeln, damit Clients untereinander reden können
PostUp = iptables -A FORWARD -i %i -j ACCEPT; iptables -A FORWARD -o %i
-j ACCEPT; ip6tables -A FORWARD -i %i -j ACCEPT; ip6tables -A FORWARD -
o %i -j ACCEPT;
```

```
PostDown = iptables -D FORWARD -i %i -j ACCEPT; iptables -D FORWARD -o
%i -j ACCEPT; ip6tables -D FORWARD -i %i -j ACCEPT; iptables -D FORWARD
-o %i -j ACCEPT;

# Client 1
[Peer]
PublicKey = <public key of client 1>
AllowedIPs = 192.168.123.11/32 # IP des Client 1

# Client 2
[Peer]
PublicKey = <public key of client 2>
AllowedIPs = 192.168.123.12/32 # IP des Client 2
```

Wichtig ist an dieser Stelle, dass auf dem Server folgende Systemvariablen gesetzt sind:

```
net.ipv4.ip_forward=1
net.ipv6.conf.all.forwarding=1
```

Herausfinden kann man das folgendermaßen:

```
sysctl net.ipv4.ip_forward
sysctl net.ipv6.conf.all.forwarding
```

Dauerhaft aktivieren lässt sich das in der `/etc/sysctl.conf`

[/etc/sysctl.conf](#)

```
net.ipv4.ip_forward=1
net.ipv6.conf.all.forwarding=1
```

Achtung! `net.ipv6.conf.all.forwarding=1` verhindert IPv6 Autokonfig auf allen Interfaces. Aus diesem Grund sollte dies **vorher** statisch eingerichtet werden.

Client 1

[/etc/wireguard/wg-csc.conf](#)

```
[Interface]
PrivateKey = <private key of client 1>
Address = 192.168.123.11/24 # IP Adresse des Client 1

[Peer]
Endpoint = wireguard-1.clerie.de:51820 # Hostname und Port auf dem der
Server lauscht
PublicKey = <public key of server>
AllowedIPs = 192.168.123.0/24 # IPs die über WireGuard getunnelt werden
```

sollen

Client 2

[/etc/wireguard/wg-csc.conf](#)

```
[Interface]
PrivateKey = <private key of client 2>
Address = 192.168.123.12/24 # IP Adresse des Client 2

[Peer]
Endpoint = wireguard-1.clerie.de:51820 # Hostname und Port auf dem der
Server lauscht
PublicKey = <public key of server>
AllowedIPS = 192.168.123.0/24 # IPs die über WireGuard getunnelt werden
sollen
```

From:
<https://wiki.clerie.de/> - **clerie's Wiki**

Permanent link:
<https://wiki.clerie.de/notiz/wireguard>

Last update: **2020/03/31 00:31**

