

Wireguard

- Heimnetz <-> Server (lonos)

Heimnetz <-> Server (Ionos)

Situation

Es gibt mehrere Services, die ich betreiben möchte, für die ich den VPS nutzen möchte

- RustDesk als Alternative zu Teamviewer
- Checkmk Server für das Monitoring
- externer VPN Server

Ich nutze seit vielen Jahren Teamviewer und bin damit auch sehr zufrieden, allerdings stört mich die Preispolitik für Private Use. Permanent erhalte ich die Nachricht meine Benutzer wären verbraucht.

Würde Teamviewer eine Private Fee von 50€ im Jahr aufrufen und dann hätte man für Privat eine normalen uneingeschränkten Teamviewer, meinetwegen ohne Support wäre ich dabei. Aber die kleinste Lizenz zu mehreren 100€ - da bin ich raus.

Die ganze Zeit, gab es keine wirkliche Alternative, jetzt gibt es RustDesk. Mal sehen ob das was wird.

Checkmk mache ich ja auch beruflich, darum bin ich hier etwas ausufernder als wahrscheinlich viele andere. Für Checkmk benötige ich allerdings zwingend einen Intel basierten Server, den ich nicht mehr betreibe. Aktuell nur MACs und Raspberry's im Haus.

Der externe VPN Server für GEO Location D aus dem Ausland heraus :-)

Vserver bei ionos

Ich habe den Server bei Ionos gehostet, da ich hier die Firewall Richtlinien konfigurieren kann. Ich hatte es vorher mit einem vps bei Start versucht, da ging das nicht. Hierzu gibt es auch weitere Berichte im Netz.



Konfiguration:

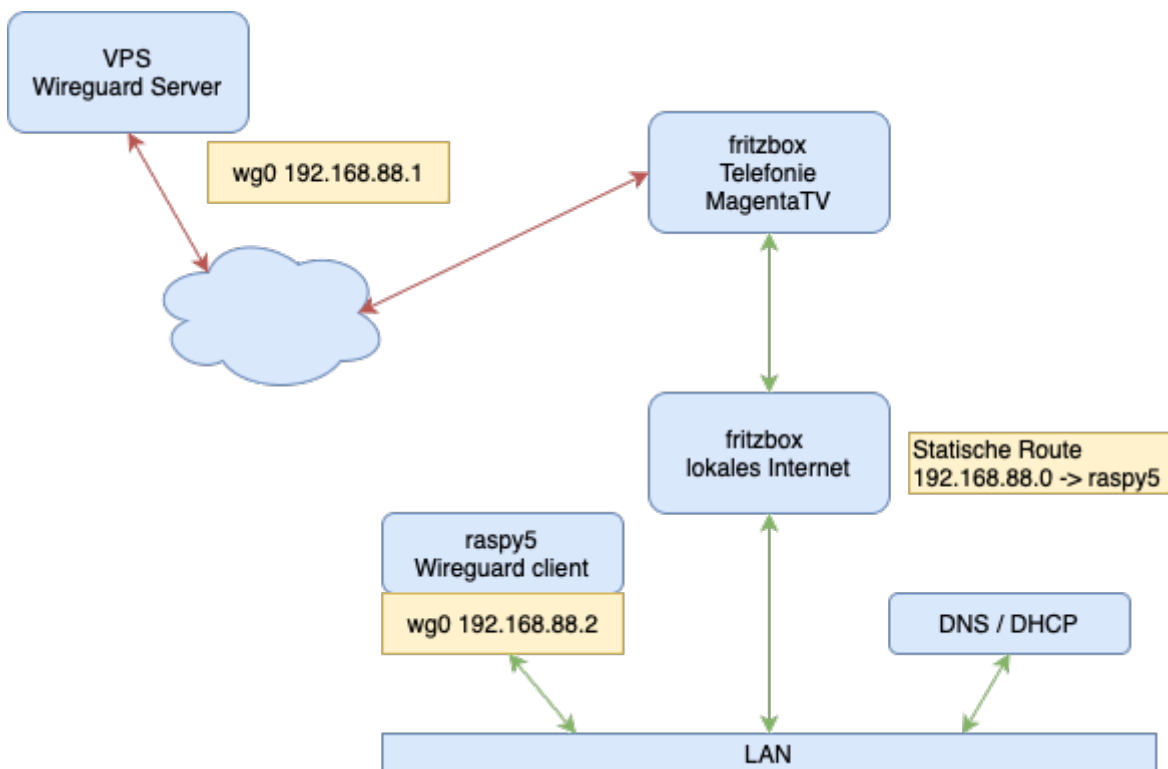
Typ:	Cloud Server XL
CPU:	4 vCore
RAM:	8 GB
SSD:	160 GB



Bandbreite bis zu: 400 Mbps

Ich glaube der kostet so 10€ / Monat - das ist es mir wert.

Konfiguration



Fritz!Box (Intranet)



Die Routen Konfiguration geschieht unter

Heimnetz -> Netzwerk -> Netzwerkeinstellungen -> IPv4 Routen

Wenn Ihr Netzwerk aus mehreren Subnetzen besteht, die nicht direkt mit der FRITZ!Box verbunden sind, können Sie für diese statische IPv4-Routen in der FRITZ!Box einrichten.

Achtung!

Änderungen auf dieser Seite können dazu führen, dass die FRITZ!Box nicht mehr erreichbar ist. Beachten Sie unbedingt die Hilfe, bevor Sie Änderungen vornehmen.

Aktiv	Netzwerk ↕	Subnetzmaske ↕	Gateway ↕	
<input checked="" type="checkbox"/>	192.168.88.0	255.255.255.0	IP des WireguardClients	 

VPS Firewall

Im Ionos Control Panel unter:

Netzwerk -> Firewall Richtlinien

Zulassen Alle UDP 51820 Wireguard Deamon



Wireguard Installation

Howto: check UDP open port

```
nc -vz -u <ip> <port>
```

Beide Rechner

```
# werde ROOT
sudo -i

# update system
apt-get update
apt-get upgrade

# install wireguard
apt-get install wireguard

### enable ip routing
vi /etc/sysctl.conf
'uncomment' net.ipv4.ip_forward=1

## apply changes
```

```
sysctl -p
```

```
# create private and public keys
```

```
cd /etc/wireguard
```

```
umask 077
```

```
wg genkey > privatekey
```

```
wg pubkey < privatekey > publickey
```

Auf dem VPS

```
vi /etc/wireguard/wg0.conf
```

```
[Interface]
```

```
Address = 192.168.88.1/24
```

```
SaveConfig = true
```

```
PostUp = iptables -A FORWARD -i %i -j ACCEPT; iptables -A FORWARD -o %i -j ACCEPT; iptables -t nat -A
```

```
POSTROUTING -o ens192 -j MASQUERADE
```

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

```
POSTROUTING -o ens192 -j MASQUERADE
```

```
ListenPort = 51820
```

```
PrivateKey = <privatekey vps>
```

```
[Peer]
```

```
PublicKey = <publickey client>
```

```
AllowedIPs = 192.168.88.0/24, 192.168.178.0/24
```

```
Endpoint = <dyn-adresse-des-heimnetzes>:37503
```

Auf dem Client

```
vi /etc/wireguard/wg0.conf
```

```
[Interface]
```

```
SaveConfig = true
```

```
ListenPort = 51820
```

```
PrivateKey = <privatekey client>
```

```
PostUp = iptables -A FORWARD -i wg0 -j ACCEPT; iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

```
PostDown = iptables -D FORWARD -i wg0 -j ACCEPT; iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE
```

```
[Peer]
```

```
PublicKey = <public key vps>
```

```
AllowedIPs = 192.168.88.0/24
```

Endpoint = <ip-adresse-vps>:51820

Auf beiden Rechnern

```
## Starte Wireguard
wg-quick up wg0

## Zeige Status
wg show

## enable on system boot

sudo systemctl enable wg-quick@wg0.service
sudo systemctl daemon-reload
sudo systemctl start wg-quick@wg0
```

Ich habe mir für das Management der Wireguard Konfiguration ein paar Alices besetzt

~/bash_aliases oder ~/.bashrc

```
19 alias wg-down="wg-quick down wg0"
20 alias wg-up="wg-quick up wg0"
21 alias wg-restart="wg-quick down wg0 && wg-quick up wg0"
22 alias vwg="wg-down ; vi /etc/wireguard/wg0.conf ; wg-up"
23 alias cdwg="cd /etc/wireguard"
```

der Alias "vwg" nimmt wg0 down bevor es wg0.conf bearbeitet. Das ist notwendig, da nur im Down Zustand die wg0.conf bearbeitet werden kann.