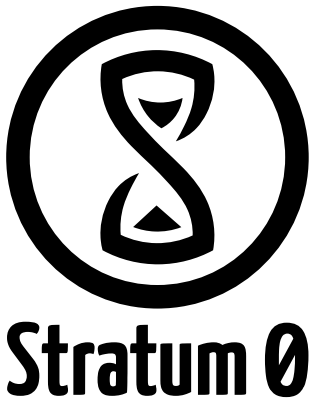
Wireguard

Secure in kernel VPN



<Emantor>

14. November 2017

Was ist Wireguard?

- Ein Kernel Modul
- Management interface: `wg`
- VPN über Endpoint und AllowedIPs
- Schnellstart Skript: `wg-quick` (systemd-service file: wg-quick@.service)

Aber es gibt doch schon OpenVPN?

- OpenVPN ist langsam:
  - Userspace copies
- OpenVPN ist kompliziert zu konfigurieren
  - Zertifikate und Keys für mehrere Endpoints
  - Peer To Peer mit PSK
- OpenVPN ist auf eingebetteten Geräten zu langsam
  - WDR4300 12MBit/s
  - WRT1200AC 90MBit/s

Darum Wireguard

- Wireguard ist schnell:
  - im kernel (keine Userspace copies)
- wireguard ist einfach zu konfigurieren
  - Privatekey und Publickey
  - AllowedIPs
  - Endpoint
- Wireguard ist auf eingebetteten Geräten schnell
  - WRT1200AC 280MBit/s

Aber Emantor, wie konfiguriere ich das denn?

1. Publickey & Privatekey generieren

```
wg genkey | tee privatekey | wg pubkey > publickey
```

2. Interface erstellen

```
ip link add wg_stratum type wireguard
ip address add dev wg_stratum 192.168.176.10/32
```

3. Wireguard eingeben

```
wg set wg_stratum private-key ./privatekey allowed-ips
    192.168.76.0/22 endpoint roadwarrior.stratum0.net:51820
```

4. Route hinzufügen

```
ip r add 192.168.176/22 dev wg_stratum scope link
```

Aber das war voll lang, geht das nicht einfacher?

1. Config exportieren

```
wg showconf wg_stratum > /etc/wireguard/wg_stratum.conf
```

2. Config starten

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

Okay und von Anfang an mit Konfig?

```
[Interface]
Address = 192.168.176.10/32
PrivateKey = (hidden)

[Peer]
PublicKey = Ebbp993K4NP0m+JVdApBxJ66gRiV2ZznzaJgs1y84VI=
AllowedIPs = 192.168.176.0/22
Endpoint = roadwarrior.stratum0.net:51820
```

Okay und wo kann ich meinen PubKey abgeben?

Mail: phoenix@emantor.de
Antwort enthält deine Adresse und eine Konfiguration

Was steckt den eigentlich dahinter?

- ED25519 für Key Exchange (ECDH)
- ChaCha20 und Poly1305 für authenticated encryption
- BLAKE2s for hashing

Und wo kann ich jetzt mehr erfahren?

https://www.wireguard.com/papers/wireguard.pdf

Noch Fragen?

Fragen sie jetzt!