Surfen mit WireGuard

Über das eigene VPN ins Internet

. . .

Linux am Dienstag

geplantes Szenario

Wir wollen einen Rechner (z.B. ein Notebook), per WireGuard-VPN, mit einem Gateway-Rechner (z.B. ein vServer) verbinden.
Über das VPN sollen dann alle Verbindungen ins Internet laufen inkl. DNS-Auflösung.

Voraussetzungen

- Notebook
  - NetworkManager
  - systemd-resolved
  - iptables / iptables-nft
- Gateway
  - statische IP (z.B.: 123.132.36.63)
  - unbound
  - firewalld

WG Installation

Auf beiden Knoten ausführen

```
sudo -i

dnf install -y wireguard-tools

mkdir -p /root/wireguard/vpn0

cd /root/wireguard/vpn0

(umask 77 && wg genkey > private.key)
wg pubkey < private.key > public.key
```

GW: Wireguard einrichten

```
ip link add dev vpn0 type wireguard
ip address add dev vpn0 192.168.88.1/24

wg set vpn0 listen-port 51820 private-key ./private.key

wg set vpn0 peer PUBLICKEYNOTEBOOK  \
  allowed-ips 192.168.88.2/32

ip link set up dev vpn0
ip route add 192.168.88.2 dev vpn0 scope link

touch /etc/wireguard/vpn0.conf
wg-quick save vpn0
```

GW: /etc/wireguard/vpn0.conf

```
[Interface]
Address = 192.168.88.1/24
ListenPort = 51820
PrivateKey =

[Peer]
PublicKey =
AllowedIPs = 192.168.88.2/32
```

GW: firewall-config

```
1 firewall-cmd --zone=public --add-port=51820/udp
2
3 firewall-cmd --runtime-to-permanent
```

Soweit vorhanden
Port auch in der Firewall des Providers freischalten.

NB: Wireguard einrichten

```
ip link add dev vpn0 type wireguard
ip address add dev vpn0 192.168.88.2/32

wg set vpn0 listen-port 0 private-key ./private.key

wg set vpn0 peer PUBLICKEYGATEWAY  \
  endpoint 123.132.36.63:51820  \
  persistent-keepalive 25 allowed-ips 192.168.88.1/32

touch /etc/wireguard/vpn0.conf
wg-quick save vpn0

ip link set up dev vpn0
ip route add 192.168.88.2 dev vpn0 scope link
```

/etc/wireguard/vpn0.conf

```
[Interface]
Address = 192.168.88.2/24
PrivateKey =

[Peer]
PublicKey =
AllowedIPs = 192.168.88.2/32
Endpoint = 123.132.36.63:51820
PersistentKeepalive = 25
```

VPN automatisch starten

(Auf allen Knoten)

```
ip link delete vpn0

systemctl enable --now wg-quick@vpn0.service
```

Teil 2

VPN als Default-Route einrichten um den kompletten Datenverkehr über das VPN zu leiten.

GW: Firewall-Zone einrichten

```
firewall-cmd --permanent --new-zone=vpn0
firewall-cmd --reload

firewall-cmd --zone=vpn0 --add-interface=vpn0
firewall-cmd --zone=vpn0 --add-service=dns

firewall-cmd --runtime-to-permanent
```

Notebook: /etc/wireguard/vpn0.conf

```
[Interface]
Address = 192.168.88.2/32
PrivateKey =
DNS = 192.168.88.1

[Peer]
PublicKey =
AllowedIPs = 192.168.88.1/32, 0.0.0.0/0
Endpoint = 123.132.36.63:51820
PersistentKeepalive = 25
```

GW: NAT einrichten

```
firewall-cmd --new-policy public-vpn0 --permanent
firewall-cmd --reload

firewall-cmd --policy public-vpn0  \
    --add-ingress-zone=vpn0

firewall-cmd --policy public-vpn0  \
    --add-egress-zone=public

firewall-cmd --policy public-vpn0  \
    --set-target=ACCEPT

firewall-cmd --zone=public --add-masquerade
firewall-cmd --runtime-to-permanent
```