

WireGuard

L2 tunnel

Wireguard je L3 tunnel. Pokud se pres wireguard potrebuju dostat do vzdaleny site na L2 vrstve, musim pouzit dalsi tunnel ktery pobezi pres wireguardove ip adresy. Tento druhý L2 tunel ma proti klasické centralizovane L2 VPN nevyhodu, ze jde jen o p2p spojeni. Samozrejme je mozne na centralnim serveru dat vsechny tunely do bridge. Zalezi na use case.

WireGuard+SSH

Nasledujici prikaz lze pouzit pro L2 tunnel na ssh server za wireguardem. Na vzdalenem serveru alokuje první volny tap interface a prida ho do bridge vmbr0, která musí na serveru již existovat. Lokalne vytvori tap7, na kterem si mohu pak lokalne pustit treba dhcp klienta. Funguje jen pokud na obou stranach ssh spojeni je uzivatel root a v sshd_config je PermitTunnel yes.

```
ssh -o Tunnel=ethernet -w 7:any root@wg_ip_adresa 'ip link set $SSH_TUNNEL master vmbr0 up'
```

Pripadne je mozne nazev tap zarizeni dynamicky alokovat na obou stranach a rovnou iniciovat konfiguraci site ssh klientem.

```
ssh -o PermitLocalCommand=yes -o LocalCommand='dhcpcd -b %T' -o Tunnel=ethernet -w any:any root@10.11.17.35 'ip link set $SSH_TUNNEL master vmbr0 up'
```

Takova konfigurace je vhoda i pro kombinaci s autossh, protoze dhcp je spusteno ssh klientem, takze se automaticky restartne dhcp pri restartu ssh.

WireGuard+Geneve

https://en.wikipedia.org/wiki/Generic_Network_Virtualization_Encapsulation

Server

```
[Interface]
Address = 10.11.17.123/24
...
PostUp = ip link add gnv0 type geneve id 1234 remote 10.11.17.124
PostUp = ip link set gnv0 up
#PostUp = ip addr add 10.100.200.35/24 dev gnv0
PostUp = brctl addif vmbr0 gnv0
PreDown = ip link delete gnv0
```

```
[Peer]
```

```
...
```

Pozor! gnv tunel bude mit male MTU coz muze nepriznive ovlivnit dalsi interfacy v bridgi, protoze budou donuceny ho prevzit. To muze byt problem treba u veth interfacu.

Klient

```
[Interface]
```

```
Address = 10.11.17.124/24
```

```
...
```

```
PostUp = ip link add gnv0 type geneve id 1234 remote 10.11.17.123
```

```
PostUp = ip link set gnv0 up
```

```
PostUp = dhcpcd gnv0
```

```
#PostUp = ip addr add 10.100.200.32/24 dev gnv0
```

```
#PostUp = ip route add 10.10.0.0/16 via 10.10.160.1 dev gnv0
```

```
PreDown = dhcpcd --exit gnv0
```

```
PreDown = ip link delete gnv0
```

```
[Peer]
```

```
...
```

From:

<https://wiki.spoje.net/> - **SPOJE.NET**



Permanent link:

<https://wiki.spoje.net/doku.php/howto/network/wireguard?rev=1647642849>

Last update: **2022/03/18 23:34**