WireGuard

- https://www.wireguard.com/
- https://www.reddit.com/r/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 druhy L2 tunelu ma proti klasicke 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 prvni volny tap interface a prida ho do bridge vmbr0, ktera musi na serveru jiz 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@wg_ip_adresa '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. Pak staci zacatek prikazu `ssh` nahradit `autossh -M 9897`, kde 9897 je nevyuzity port vetsi nez 1024. Pro automaticky restart je nutne aby fungovalo prihlaseni bez hesla.

Cely by to pak jeste slo spoustet a vypinat z PostUp/PreDown skriptu ve wireguardu.

WireGuard+Geneve

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

Geneve je moderni p2p enkapsulace L2 over IP. Je primo v jadre a neni sifrovana. Vykonove je na tom tedy lepe nez SSH. Ale stejne jako wireguard si pridava hlavicku na urovni packetu, takze zkracuje MTU. Da se snadno nakonfigurovat formou PostUp direktiv v konfiguraci wireguardu. Narozdil od ssh se musi predkonfigurovat i na strane serveru. Na druhou stranu nepotrebuje aby mel klient na serveru pristup na root.

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]
...
```

WireGuard v restriktivních sítích

Tunelování skrz WebSocket

https://www.root.cz/clanky/websocket-jako-cesta-k-uniku-z-prilis-restriktivni-site/