WireGuard na OpenWRT (jako klient)

WireGuard je nová linuxová VPN, která vyniká svou jednoduchostí a výkonem. Najdete ho v linuxovém jádře, naše virtualizační platforma vpsAdminOS ho podporuje a má příslušný modul zavedený. Podpora Wireguardu je na OpenWRT (opensource firmware pro routery) od verze 18.06.

Pro zprovoznění wireguard na openwrt v režimu klienta (s koncovým připojením na VPS) potřebujeme nainstalovat následující balíčky ve svém OpenWRT routeru:

```
opkg update
opkg install luci-proto-wireguard luci-app-wireguard wireguard kmod-
wireguard wireguard-tools
```

Z konfigurace nutno dát pozor na firewall v kterém potřebujeme povolit provoz na libovolném portu (preferuji se držet standardního 51820):

```
uci add firewall rule
uci set firewall.@rule[-1].src="*"
uci set firewall.@rule[-1].target="ACCEPT"
uci set firewall.@rule[-1].proto="udp"
uci set firewall.@rule[-1].dest_port="51820"
uci set firewall.@rule[-1].name="Allow-Wireguard-Inbound"
uci commit firewall
/etc/init.d/firewall restart
```

- zde říkáme firewallu pro příjem (ACCEPT) jakéhokoliv (*) provozu na protokolu udp pod portem 51820 s vlastním názvem pravidla (jde vidět z webového rozhraní následně).

Pokračujeme k vytvoření vlastní zóny ve firewallu (především kvůli praktičnosti při starání se o provoz v budoucnu, zapojení napřímo se každopádně nedoporučuje).

```
uci add firewall zone
uci set firewall.@zone[-1].name='wg'
uci set firewall.@zone[-1].input='ACCEPT'
uci set firewall.@zone[-1].forward='ACCEPT'
uci set firewall.@zone[-1].output='ACCEPT'
uci set firewall.@zone[-1].masq='1'
# Add the WG interface to it
uci set firewall.@zone[-1].network='wg0'
# Forward WAN and LAN traffic to/from it
uci add firewall forwarding
uci set firewall.@forwarding[-1].src='wg'
uci set firewall.@forwarding[-1].dest='wan'
uci add firewall forwarding
uci set firewall.@forwarding[-1].src='wg'
uci set firewall.@forwarding[-1].dest='lan'
uci add firewall forwarding
uci set firewall.@forwarding[-1].src='lan'
uci set firewall.@forwarding[-1].dest='wg'
```

```
uci add firewall forwarding
uci set firewall.@forwarding[-1].src='wan'
uci set firewall.@forwarding[-1].dest='wg'
uci commit firewall
/etc/init.d/firewall restart
```

- vytváříme zónu s názvem wg pro provoz v obou směrech, forward a masquerading, připojujeme k interface (viditelné poté z webUI) a následně nastavujeme forward provozu tak aby šel přes wireguard nikoliv přes standardní upstream - na závěr provedeme commit (uložení změn) a restart firewallu.

Vytoříme interface později viditelný z webového rozhraní

```
uci set network.wg0="interface"
uci set network.wg0.proto="wireguard"
uci set network.wg0.private_key="<<privátní klíč klienta>>"
uci set network.wg0.listen_port="51820"
uci add_list network.wg0.addresses='<<cidr rozsah ipv6 adres, pokud chceme
použít>>'
uci add_list network.wg0.addresses='<cidr rozsah ipv4 adres, pokud chceme
použít>>'
# Save the changes
uci commit network
/etc/init.d/network reload
```

Následně je potřeba ve webovém rozhraní openwrt vlézt do interfaces > wg0 (náš nový interface wireguardu) a dovyplnit chybějící položky - především endpoint host, Allowed IP (bacha to je většinou 0.0.0.0/0 - jiná je adresa klienta nastavená už na druhé straně tunelu - serveru), MTU, v sekci peerů vytvořit peer (tj. server kde běží wireguard a přes který to chceme provozovat).