

# Tunelování IPv6

vpsFree.cz provozuje vlastní tunelovací server, prostřednictvím kterého je možné získat IPv6 tunel do míst, kam dosud IPv6 zavedeno není.

## Motivace

Šestého června 2017 byla [ukončena činnost tunelovací platformy SixXS](#). Ta jako jediná poskytovala tunelovací server v Praze, který bylo možné použít i bez veřejné IPv4 adresy. Ačkoli je argumentace SixXS pochopitelná, jsou situace, kdy jednoduše není možné požádat poskytovatele o IPv6 konektivitu a často ani nelze změnit poskytovatele za jiného.

Pokud je k dispozici veřejná IPv4 adresa, je možné zařídit tunel od [HE.net](#), který funguje rychle a spolehlivě. Naše služba se tedy zaměřuje hlavně na situace, kdy v místě není ani veřejná IPv4 adresa. Bohužel, software `sixxsd`, který tvořil serverovou část tunelovací platformy SixXS a dokázal efektivně obsluhovat stovky tunelů, ~~nebyl nikdy uvolněn jako Open Source~~ [dlouho nebyl zveřejněn](#). Bylo tedy třeba hledat jiné řešení.

## Řešení pomocí OpenVPN

K tunelování IPv6 provozu používáme OpenVPN verze 2.4 s vypnutým šifrováním a autentizací provozu – to z důvodu nedostatku výkonu na straně klienta. Používá se UDP provoz na standardním portu 1194. Každý klient se autentizuje certifikátem. Každému klientovi je **staticky** přidělena jedna spojovací IPv6 adresa a podsít' o délce prefixu /48.

Klientský certifikát je platný jeden rok. Před uplynutím jeho platnosti je třeba požádat o vydání nového. Záměrem tohoto nepohodlného opatření je, aby každý uživatel **nejméně jednou ročně napsal svému poskytovateli připojení dotaz na stav podpory IPv6**.

## Jak zprovoznit tunel

1. Napište svému ISP dotaz ohledně podpory IPv6.
2. Požádejte o tunel prostřednictvím e-mailu na [ipv6tun@vpsfree.cz](mailto:ipv6tun@vpsfree.cz).
3. Obdržíte konfigurační soubor pro OpenVPN klienta.
4. Upravte soubor podle své potřeby.
5. Nakonfigurujte svůj router tak, aby do domácí sítě přiděloval nějaké adresy z přidělené podsítě. (Konfigurační soubor obsahuje ukázkou konfigurace pro OpenWRT)

## Příklad konfigurace OpenVPN pro OpenWRT

V tomto případě je ukáзка přímo v dodaném konfiguračním souboru. Konfigurační soubor stačí uložit tak, jak je (s příponou `.conf`) do `/etc/openvpn/` (je třeba mít nainstalovaný balík `openvpn-openssl`). A nadefinovat službu:

[/etc/config/openvpn](#)

```
config openvpn custom_config
    option enabled 1
    option config /etc/openvpn/ipv6tun-XXX.conf
```

Dále je potřeba vytvořit nové logické rozhraní:

[/etc/config/network](#)

```
config interface 'ipv6tun'
    option ifname 'tunipv6'
    option proto 'static'
    option ip6addr '<adresa konce tunelu>/64'
    option ip6gw '<adresa brány>'
    option ip6prefix '<přidělený prefix>/48'
```

a přidat logické rozhraní `ipv6tun` do firewallové zóny `wan`:

[/etc/config/firewall](#)

```
config zone
    option name 'wan'
    option network 'wan wan6 ipv6tun'
    option ...
```

## Řešení pomocí Wireguardu

Testujeme také použití moderního tunelovacího protokolu [WireGuard](#). Ten nabízí šifrování a autentizaci, zároveň ale také velký výkon v porovnání s OpenVPN. Používá se UDP provoz na portu 51820. Každý klient se autentizuje párem veřejného a soukromého klíče. Každému klientovi je **staticky** přidělena jedna spojovací IPv6 adresa a podsít o délce prefixu /48.

Každý tunel má nastavené datum expirace na jeden rok po zřízení, po jeho uplynutí je odkonfigurován. Pro nepřerušovaný provoz je tedy třeba požádat o prodloužení. Záměrem tohoto nepohodlného opatření je, aby každý uživatel **nejméně jednou ročně napsal svému poskytovateli připojení dotaz na stav podpory IPv6**.

## Jak zprovoznit tunel

1. Napište svému ISP dotaz ohledně podpory IPv6.
2. Vygenerujte dvojici soukromého a veřejného klíče: `$ wg genkey | tee privatekey | wg pubkey`
3. Požádejte o tunel prostřednictvím e-mailu na [ipv6tun@vpsfree.cz](mailto:ipv6tun@vpsfree.cz). Nezapomeňte připojit veřejný klíč. Prosím **neposílejte klíč v příloze, vložte ho přímo do textu zprávy**.

4. Obdržíte e-mail s příkladem konfigurace pro wg-quick a OpenWRT.
5. Doplníte do konfiguračního souboru svůj privátní klíč a nakonfigurujete svého klienta.
6. Nakonfigurujete svůj router tak, aby do domácí sítě přiděloval nějaké adresy z přidělené podsítě.

## Příklad konfiguračního souboru pro wg-quick

[/etc/wireguard/wgipv6tun.conf](#)

```
[Interface]
# FIXME: Insert your private key
PrivateKey =
Address = 2a03:3b40:200::<ID>

[Peer]
Endpoint = ipv6tun01.vpsfree.cz:51820
PublicKey = r7vzF6irpXSmkTibIHztIcfc/YzPmpyMX9LYa9z5Yw0=
AllowedIPs = ::/0
```

## Příklad konfigurace Wireguardu na OpenWRT

[/etc/config/network](#)

```
config interface 'wgipv6tun'
    option proto 'wireguard'
    option private_key 'FIXME'
    option ip6prefix '2a03:3b40:<ID>::/48'
    list addresses '2a03:3b40:200::<ID>'

config wireguard_wgipv6tun
    option endpoint_host 'ipv6tun01.vpsfree.cz'
    option endpoint_port '51820'
    option route_allowed_ips '0'
    option public_key
'r7vzF6irpXSmkTibIHztIcfc/YzPmpyMX9LYa9z5Yw0='
    list allowed_ips '::/0'

config route6 'default_v6_gw_a'
    option interface 'wgipv6tun'
    option target '::/0'
    option source '2a03:3b40:200::<ID>'

config route6 'default_v6_gw_b'
    option interface 'wgipv6tun'
    option target '::/0'
    option source '2a03:3b40:<ID>::/48'
```

## Příklad konfigurace Wireguardu pro MikroTik (verze 7)

```
/interface/wireguard/add name="wgipv6tun" mtu=1420 private-key="FIXME"  
/interface/wireguard/peers/add interface=wgipv6tun public-  
key="r7vzF6irpXSmkTibIHztIcfc/YzPmpyMX9LYa9z5Yw0=" endpoint-  
address=77.93.223.5 endpoint-port=51820 allowed-address=1::/0  
/ipv6/address/add address=2a03:3b40:200::<ID>/128 interface=wgipv6tun  
/ipv6/route/add dst-address=1::/0 gateway=wgipv6tun
```

## Povolení příchozího provozu na OpenWRT

Lze předpokládat, že pokud máte zájem o IPv6, je to proto, že se chcete vzdáleně připojovat na svá zařízení za tunelem. OpenWRT bohužel ve výchozím stavu taková spojení blokuje. Lze je ale snadno odblokovat ve firewallu. Je potřeba zvlášť povolit přístup do lokální sítě/sítí a na router samotný.

[/etc/config/firewall](#)

```
config rule  
    option name 'IPv6 forwarding'  
    option family 'ipv6'  
    option src 'wan'  
    option dest 'lan' # Eventuálně * pro všechny sítě  
    ## Pokud chcete povolit pouze dynamické porty (pro P2P služby),  
    ## odkomentujte následující řádky.  
    #option proto 'tcpudp'  
    #option dest_port '49152-65535'  
    option target 'ACCEPT'  
  
config rule  
    option name 'SSH to router over IPv6'  
    option family 'ipv6'  
    option src 'wan'  
    option proto 'tcp'  
    option dest_port '22'  
    option target 'ACCEPT'
```

From:  
<https://kb.vpsfree.cz/> - **Znalostní Báze**

Permanent link:  
<https://kb.vpsfree.cz/informace/projekty/ipv6tunel>

Last update: **2021/07/21 16:00**