



## Jak nastavit L2TP/IPSec VPN na zařízeních Mikrotik – funkční step-by-step návod (únor 2020)

09. 09. 2018 | Sítařina | 148 🗨️ | ★★★★★

Toto je funkční mnohokrát ověřený návod na zprovoznění L2TP/IPSec VPN pro připojení z Windows, Linuxu, macOS, iOSu a Androidu na vašem Mikrotiku. Přistupujete pak k zařízením v lokální síti pod lokální IP a brouzdáte po internetu pod vnější IP adresou Mikrotiku, to vše přes šifrované spojení mezi vaším zařízením a mikrotikem. Popřípadě si jen vytvoříte přídatné spojení na vzdálený Mikrotik, například pro účely jeho vzdálené správy či přístupu k lokálním IP adresám, a vnější IP adresu (pro brouzdání a stahování) si necháte původní. Tento návod je orientován jak na GUI, tak na konzoli. Jsou to původně moje

### RUBRIKY

**AKCE** (1)

**BASTLENÍ** (14)

**BLOG** (2)

**HTPC** (12)

**MINIRECENZE**  
(16)

**NEZAŘAZENÉ** (2)

**SÍŤAŘINA** (4)

### KOMENTÁŘE

{ Duben 2022 Návod zřejmě zastaralý, něco tam nesedí. Nepodařilo se nastavit, udělal jsem vše co šlo vydedukovat. Win7 se nepřipojil, hlásilo to chybu konfigurace routeru.... }

{ 5 }

**KARL** { nene bohužel není, jiné L2TP/IPSec VPN i na mikroticích mi fungují bez problému a zmíněný fuj update

zápisky, takže text není úplně uhlazený, ale na funkci to nemá vliv.

## KROK 0: WINBOX → INTERFACES → INTERFACE LIST (→ LISTS)

Toto je dodatečně přidaný krok, interface listy jsou v RouterOS dostupné od roku 2017, od té doby jsou už všechny Mikrotiky aktualizované, takže lze funkci považovat jako běžně dostupnou. Kdo konfiguroval svůj Mikrotik již před nějakou tou dobou (2018) a poté jen aktualizoval RouterOS, může mít ještě starší typ konfigurace, kde se Interface listy nepoužívaly. Stejně tak ti, co konfigurují RouterOS od píky.

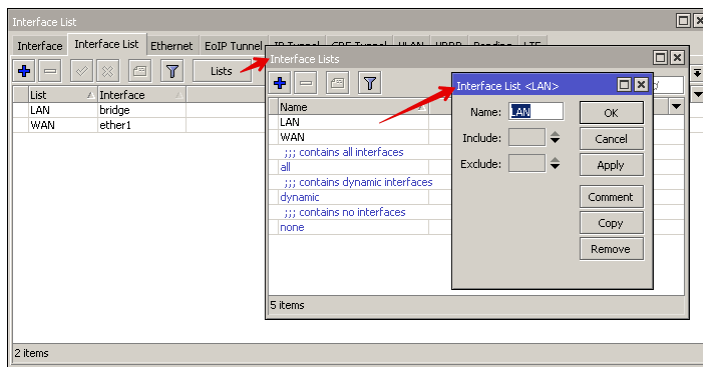
S touto funkcí se dá v nastaveních napříč celým systémem odkazovat na skupinu interfaců (interface list), nejen na jeden konkrétní interface, jak to bylo dříve. Protože my máme v každém interface listu jedinou položku (bridge1 v LAN, a ether1 ve WAN), dalo by se v našem případě bez interface listů i obejít – odkazovat se v nastaveních na interfaci bridge a ether1 přímo. Protože funkce Quick Set začala někdy od roku 2018 generovat nastavení používající Interface listy (hlavně firewall pravidla), dává smysl se toho držet a také je využívat.

```
nainstalován nemám  
}
```

```
JIŘÍ { Chyba je  
způsobena updatem  
na Win10 viz zde  
https://mspoweruser.com/microsoft-release-out-of-band-fix-for-windows-10-cant-connect-to-vpn-the-l2tp-connection-attempt-failed-error/ }
```

```
JIŘÍ {  
jiri@pavlovsky.eu }
```

```
KARL { Ahoj, díky  
za navod, na Win7  
funguje na Win10  
nikoliv. Win10  
zobrazí chybu: The  
L2TP connections  
failed because the  
security layer  
encountered a  
processing error... }
```



Zkontrolujeme tedy, zda máme v systému nastavené interface listy a zda do nich máme přiřazené interfacery. Potřebujeme dva interface listy: LAN a WAN. V LAN interface listu musí být přidány interfacery vnitřní sítě. To typicky znamená přidat bridge (název většinou bridge, nebo bridge1). Ve WAN interface listu musí být přidány interfacery sítě vnější, což bývá typicky první ethernetový port (název většinou ether1, nebo ether1-gateway).

Návod s nastavenými Interface listy spíš počítá, některé kroky v návodu ale ještě nejsou v tomto směru zaktualizované a odkazují se na interfacery přímo. To na funkci nemá vliv – aktualizují až budu zas VPN někde konfigurovat.

## KROK 1: FIREWALL PRAVIDLA

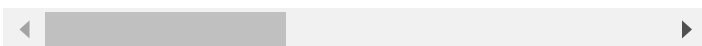
V první řadě povolíme pár pravidel na firewallu , konkrétně tyto protokoly a porty:

- Protokol UDP, port 500 pro IPsec zajišťuje první fázi připojování (protokol IKE – výměna klíčů a konfigurace spojení)
- Protokol UDP, port 1701 pro L2TP

- Protokol UDP, port 4500 pro IPsec zajišťuje mód průchodu branou NAT (IPsec NAT-Traversal mode)
- Protokol ESP (Encapsulating Security Payload) pro IPsec přidává šifrování paketů
- Protocol AH (Authentication Header) pro IPsec zajišťuje autentizaci odesílatele a příjemce

Takže se připojíme do Mikrotiku přes WinBox, spustíme konzoli a postupně povkládáme následující:

```
/ip firewall filter
add action=accept chain=input in-interface=ether1
add action=accept chain=input in-interface=ether1-gateway
add action=accept chain=input in-interface=ether2
add action=accept chain=input protocol=ip
add action=accept chain=input protocol=ipsec
```



Příkazy vkládejte do konzole ve winboxu přes right-click – vložit. Nikoliv přes Ctrl+V. Stisk Ctrl+V dost nešťastně zapne autodoplňování příkazů (commands auto-completion). V takovém případě to pak při vkládání (přes right click) mrší vkládané příkazy přidáváním nadbytečných slov. Auto-completion jde případně vypnout opětovným stiskem Ctrl+V.

Do in-interface patří vaše gateway, což je typicky ether1, nebo ether1-gateway. Je to kdyžtak vidět v Interfaces, nebo i terminálový našeptávač našeptává. Alternativně lze použít

čistší a modernější řešení: In Interface nechat prázdné a nastavit In interface list na WAN.

Potom v GUI otevřeme IP->Firewall a vše pak přesuneme nad „DROP all not coming from LAN“ pravidlo.

Kdo chce tento krok celý klikat v GUI, tak může v IP->Firewall kliknout na tlačítko [+] a ty pravidla popřidávat ručně:

```
chain:      input
protocol:   UDP
in interface: tvoje gateway (ether1 / ether2)
dst port:   500,1701,4500
action:     accept
```

```
chain:      input
protokol:   ipsec-esp
in interface: tvoje gateway (ether1 / ether2)
action:     accept
```

```
chain:      input
protokol:   ipsec-ah
in interface: tvoje gateway (ether1 / ether2)
action:     accept
```



To první trojité pravidlo lze ponechat sloučené (dst-port=500,1701,4500), nebo jej rozdělit na tři pravidla každý pro jeden port (500, 1701 a 4500). Je to jedno, odděleně se hodí pokud například hledáte příčinu problému s připojením. Můžete tak jednodušeji sledovat, kolik komunikace přiteklo jakým portem.

| #  | Action       | Chain            | Src. Address | Dest. Address  | Protocol | Src. Port | Dest. Port    | In. Interface | Out. Int. | Bytes     | Packets |
|----|--------------|------------------|--------------|----------------|----------|-----------|---------------|---------------|-----------|-----------|---------|
| 0  | pass through | forward          |              |                |          |           |               |               |           | 61.9 MB   | 66 622  |
| 1  | accept       | input            |              |                |          |           |               |               |           | 3314.6 KB | 22 936  |
| 2  | drop         | input            |              |                |          |           |               |               |           | 320 B     | 8       |
| 3  | accept       | input            |              | 1 (icmp)       |          |           |               |               |           | 0 B       | 0       |
| 4  | accept       | input            |              | 17 (udp)       |          |           | 500,1701,4500 |               |           | 3186 B    | 22      |
| 5  | accept       | input            |              | 50 (ipsec-esp) |          |           |               |               |           | 0 B       | 0       |
| 6  | accept       | input            |              | 51 (ipsec-ah)  |          |           |               |               |           | 0 B       | 0       |
| 7  | drop         | input            |              |                |          |           |               |               |           | 7.7 KB    | 127     |
| 8  | accept       | forward          |              |                |          |           |               |               |           | 0 B       | 0       |
| 9  | accept       | out ipsec policy |              |                |          |           |               |               |           | 0 B       | 0       |
| 10 | fasttrack    | forward          |              |                |          |           |               |               |           | 1479.6 KB | 11 542  |
| 11 | accept       | forward          |              |                |          |           |               |               |           | 1479.6 KB | 11 542  |
| 12 | drop         | forward          |              |                |          |           |               |               |           | 10.3 KB   | 205     |
| 13 | drop         | forward          |              |                |          |           |               |               |           | 0 B       | 0       |

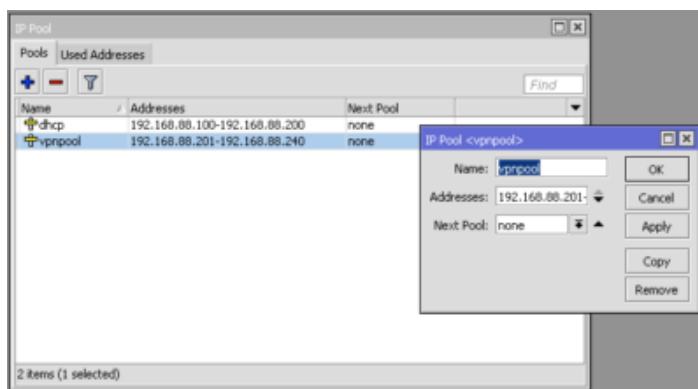
## KROK 2: IP -> POOL

IP -> Pool, zmenšíme stávající pool a ve volném místě vytvoříme pool pro VPN klienty.

Přes GUI:

1. Zmenšíme stávající pool, např. z .100-250 na .100-199
2. Vytvoříme nový pool od .200 do .250, vyhrazený klienty připojené přes VPN
3. Schválně necháme pár volných IP adres na konci rozsahu (.251 až .254).

Minimálně jednu IP totiž napevno obsadíme PPP klientem, viz následující krok.



Přes konzoli:

```
/ip pool
set dhcp ranges=192.168.88.100-192.168.88
add name=vpnpool ranges=192.168.88.201-192.168.88.254
```

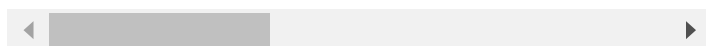


## KROK 3: PPP -> PROFILES TAB

Přidáme nový PPP profil.

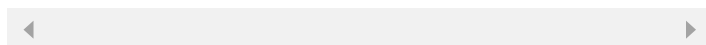
Přes konzoli:

```
/ppp profile
add name=my-l2tp-profile local-address=192.168.88.254
```



Přes GUI:

|                 |                     |
|-----------------|---------------------|
| name:           | my-l2tp-profile     |
| local address:  | 192.168.88.254      |
| remote address: | vpnpool             |
| dns server:     | 192.168.88.1        |
| change TCP MSS: | Yes                 |
| interface list: | LAN                 |
| bridge:         | žádný, nebo bridge1 |



Do Local address napíšeme volnou adresu na konci rozsahu – adresu, která není obsazena ani žádným poolem.

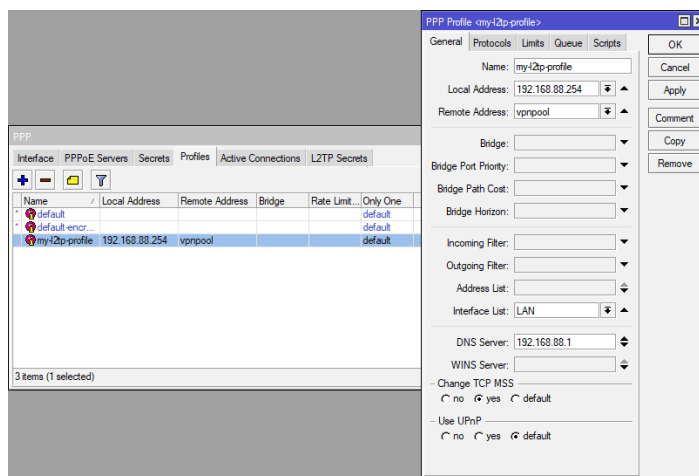
Do Remote address napíšeme pool vytvořený v předchozím kroku.

Do DNS server napíšeme IP adresu našeho routeru, tam nám DNS běží. (Pokud nám DNS běží na jiném routeru v naší LAN síti, vložíme

jeho IP.)

Do interface list vložíme LAN. Je to nutné především novějších RouterOS (2018+), kde firewall využívá interface list pro určení co je LAN a co je WAN. Toto zabezpečí, že dynamický interface, který vzniká vždy při připojení VPN klienta, se i dynamicky přidá do LAN interface listu, a tedy bude považován za součást LAN. Bez tohoto na klientovi typicky nejde DNS a nenačítá stránky. To proto, že i DNS požadavky jsou zahazovány pravidlem „DROP all not coming from LAN“.

Do bridge vložíme bridge1, pokud chceme, aby se připojený klient stal součástí LAN sítě (tzn. viděl ostatní PC a jejich služby). Pokud bude nevyplněno, dostane se VPN uživatel pouze na internet. Pokud to chcete pro různé uživatele různě, pak lze vytvořit více těchto profilů.

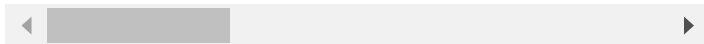


## KROK 4: PPP -> INTERFACE TAB -> [L2TP SERVER] BUTTON

Aktivujeme L2TP server.

Přes konzoli:

```
/interface l2tp-server server
set enabled=yes default-profile=my-l2tp-pr
```

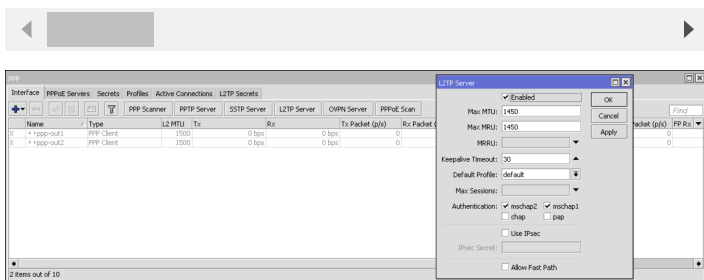


Přes GUI:

V okně PPP na záložce Interface kliknout na tlačítko L2TP Server.

Vyskočí malé okénko L2TP Server, zaškrtnout Enabled.

authentication: mschap1, mschap2  
default profile: my-l2tp-profile (profil \  
“Use IPsec”: zaškrtni a vyplň sdílené hesl



## KROK 5: IP -> IPSEC -> PEERS TAB A IDENTITIES TAB

Tento krok lze přeskočit.

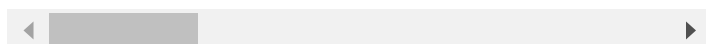
Volba “Use IPsec” z předchozího kroku vytvoří dynamické záznamy v IP -> IPsec -> Peers a IP -> IPsec -> Identities, takže není potřeba ručně nastavovat.

Pouze pokud jsi v předchozím kroku “Use IPsec” nezaškrtnul, tak bude potřeba oba

vytvořit ručně. To se hodí jen v případě, že je něco nutné nastavit nestandardně. Například je možnost omezit připojení jen z jedné konkrétní IP, ale taková věc jde typicky řešit firewallem.

Co se tam nastavuje:

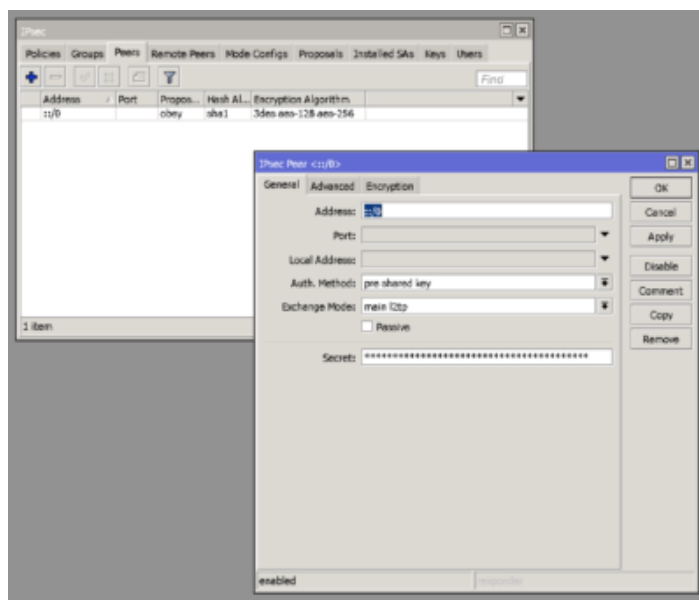
```
address: očekávaná IP adresa protistrany  
::/0 (což znamená libovolná IP a libovolný  
pokud se sem zadá konkrétní IP, pak pouze  
pokud chci omezit IP, ze které se dá připojit  
port: 500. Funguje i bez vyplněného portu.  
local address: sem nic nevyplnit (pole musí být  
auth. method: pre shared key  
exchange mode: main l2tp  
secret: sem napsat sdílené heslo pro všechny  
send initial contact: Enable  
NAT traversal: Enable  
generate policy: port override  
hash algorithm: sha1  
encryption alg.: 3des, aes128, aes256  
DH group: modp1024
```

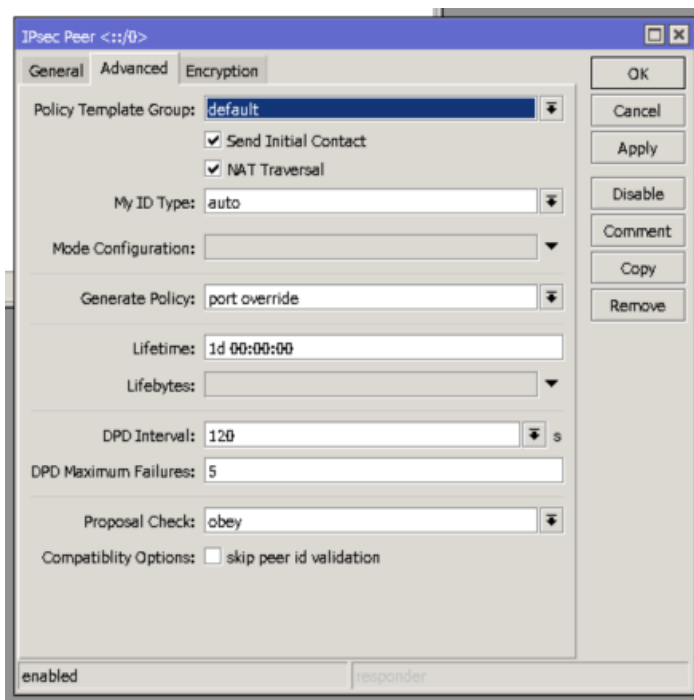
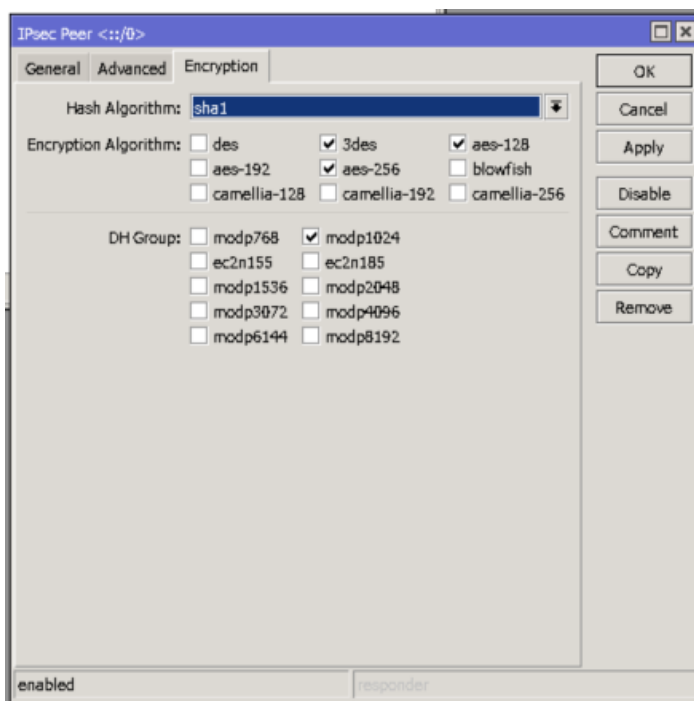


RouterOS 6.43 a starší má pouze záložku Peers a v ní hodně nastavení, rozdělena na 3 taby

RouterOS 6.38 a starší má všechna navíc všechna tato nastavení dohromady na jedné záložce

Rozhraní v RouterOS 6.44.1 a novějším je rozdělené na taby Peers a Identities, ale nastavení budou obdobná.

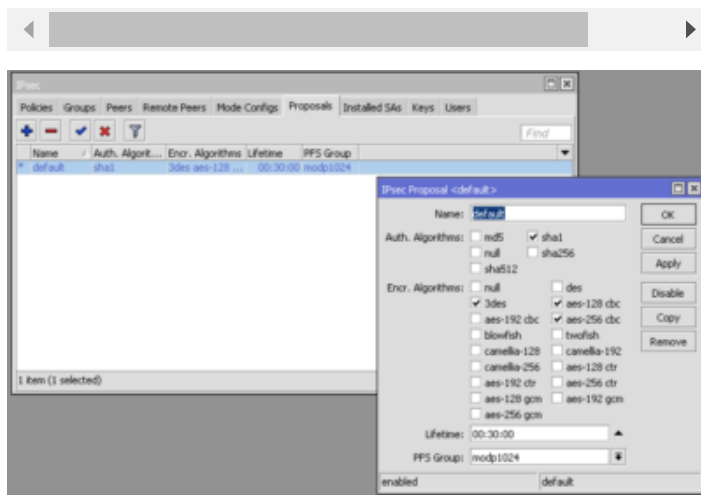




## KROK 6: IP -> IPSEC -> POLICY PROPOSALS

Upravit default položku, pokud je potřeba. V mém případě bylo vyplněno správně.

```
auth. algorithms: jen sha1
encryption algorithms: aes128, aes192, aes256
PFS group: modp1024
```



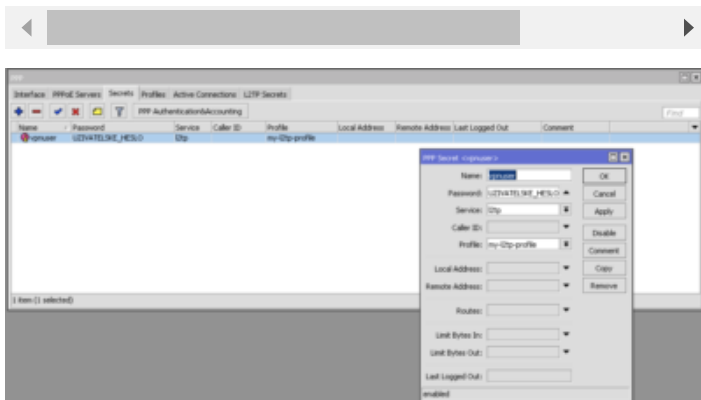
## KROK 7: VYTVOŘIT SI VPN UŽIVATELE V PPP -> SECRETS

Zde si přidáme VPN uživatele, tedy přihlašovací jméno/heslo k VPN. Pro správnou funkci stačí přidat jednoho uživatele, ale někdy je lepší přidat uživatelů víc:

a) Pokud jsou všechny zařízení jen vaše, nebo rodiny, nebo vůbec nepotřebujete vědět, kdo se připojuje, stačí mít založeného jednoho VPN uživatele. A to i v případě, že se budeme chtít připojovat z více zařízení najednou.

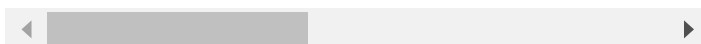
b) V případě, že dáváme přihlašovací údaje i kolegům, kamarádům, je vhodné každému určit vlastní jméno/heslo. S dalšími uživateli tedy budete vždy sdílet celkem tři autentizační údaje pro účely nastavení na jejich zařízeních: jméno/heslo zadané v tomto kroku + IPsec sdílené heslo, které stejné pro všechny. V logu je pak vidět odkud (z jakého účtu) spojení přišlo, lze sestavovat grafy a statistiky pro jednotlivé účty, atd.

```
name:      tvůj nickname, nebo cokoliv, třeba  
password: vymysli si heslo pro tohoto uživatele  
service:   l2tp  
profile:   my-l2tp-profile
```



Přes konzoli:

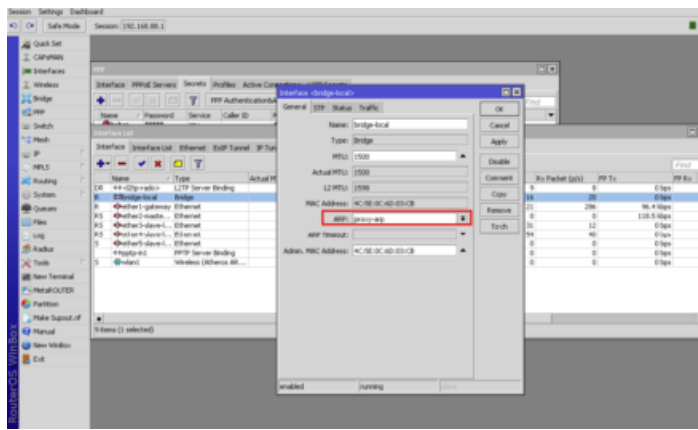
```
/ppp secret  
add name=vpnuser password="heslo-unikatni"
```



## KROK 8: ARP-PROXY NA BRIDGI

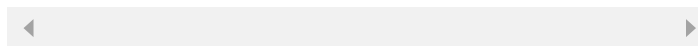
Ještě nastavíme poslední věc, a to aktivaci arp-proxy na hlavním bridgi (bridge, někdy také bridge1, či bridge-local). Když není zaplá, tak se sice dopingneme na samotný router (a připojíme na Winbox), ale už ne na ostatní zařízení v lokální síti.

Takže otevřeme Bridge -> tab Bridge -> položka bridge (popř. bridge1, bridge-local, atd.), ekvivalent je Interfaces -> tab Interface -> položka bridge (popř. bridge1, bridge-local, atd.). V dialogu stačí ARP přepnout z enabled na proxy-arp.



To samé přes konzoli:

```
/interface bridge
set bridge arp=proxy-arp
```



## KROK 9: PROFIT

Hurá, VPN hotová, můžeme očekávat aktivní připojené klienty v PPP -> Active connections.

Nejdřív se zkuste připojit z vnitřní sítě (na IP adresu routeru, tzn 192.168.88.1), až pak řešit připojení z vnějšku. Pokud máte Mikrotik připojený na nějaký „modem“/router od poskytovatele internetu, který má víc LAN portů, tak bych se notebookem připojil do toho „modemu“ a zkusil se připojit na modemem přidělenou IP adresu mikrotiku (může být například 192.168.1.117, to je vidět buď v nastavení modemu v sekci DHCP leases, nebo ve winboxu v IP -> Addresses -> dynamická položka ukazuje IP, nebo i v Quick Setu je IP vidět v kolonce IP Address.). Tím ověříme, zda firewall na mikrotiku je pro VPN průchozí.

Následně se pak se dá postoupit ještě výše a to o pokusy připojení z veřejného internetu. Na „modemu“ bude potřeba povolit nějakým způsobem přesměrování portů na adresu Mikrotiku a Mikrotiku v síti přidělit pevnou lokální IP adresu.

## TO SAMÉ, ALE POHROMADĚ V KONZOLOVÝCH PŘÍKAZECH

```
# Quick VPN setup
# Apply commands to freshly configured mikrotik

# To-do before copy-pasting these commands:
# 1) set custom shared password
# 2) set custom user name and ipsec-secret
# 3) check IP addresses, they have to match
# 4) remove "bridge=bridge1" from PPP profile
# 5) after import, check that firewall filter is enabled

/ip firewall filter
add action=accept chain=input in-interface=ether1
add action=accept chain=input in-interface=ether2
add action=accept chain=input in-interface=ether3
add action=accept chain=input protocol=ipsec
add action=accept chain=input protocol=ipsec

/ip pool
set dhcp ranges=192.168.88.100-192.168.88.199
add name=vpnpool ranges=192.168.88.201-192.168.88.254

/ppp profile
add name=my-l2tp-profile local-address=192.168.88.1

/interface l2tp-server server
set enabled=yes default-profile=my-l2tp-profile

/ppp secret
add name=vpnuser password="unique-password"

/interface bridge
set bridge arp=proxy-arp
```

## PŘIPOJÍME SE

Nyní nastavíme všechny naše zařízení. U všech připojení je jedna společná věc k volbě: buď chceme vést přes VPN tunel veškerou komunikaci – v tom případě budeme z vnějšku vidět pod IP adresou VPN brány, na kterou se připojujeme (nakonfigurovaný Mikrotik s VPN), nebo běžná komunikace zůstane beze změny a v systému se zpřístupní jen nový subnet s lokálními IP adresami vzdálené sítě.

První případ se hodí pro přístup ke zdrojům, které vyžadují konkrétní IP adresu (IP whitelist), skrytí vaší aktuální IP adresy, skrytí reálné polohy, či prostě kvůli samotnému šifrovanému tunelu, protože jste zrovna na veřejné Wi-Fi a chcete komunikaci zabezpečit. Druhý případ se hodí, pokud se chcete jenom připojit k Mikrotiku pro účely jeho správy nebo přístupu k lokálním IP adresám za ním a chcete, aby vám běžná komunikace i nadále tekla normálním způsobem plnou rychlostí.

## PŘIPOJENÍ Z WINDOWS 10

Ve Win10 je to dnes už také na pár kliků. Start – napsat VPN – najde to VPN ovládací panel, a pak už jen zadat údaje: host (vnější IP adresa routeru), preshared heslo, uživatelské jméno a heslo, a uložit.

V případě, že cílové Mikrotik zařízení, na které se připojujete, je skryté za NATem, bude ještě

nutné upravit hodnotu v registru a restartovat počítač.

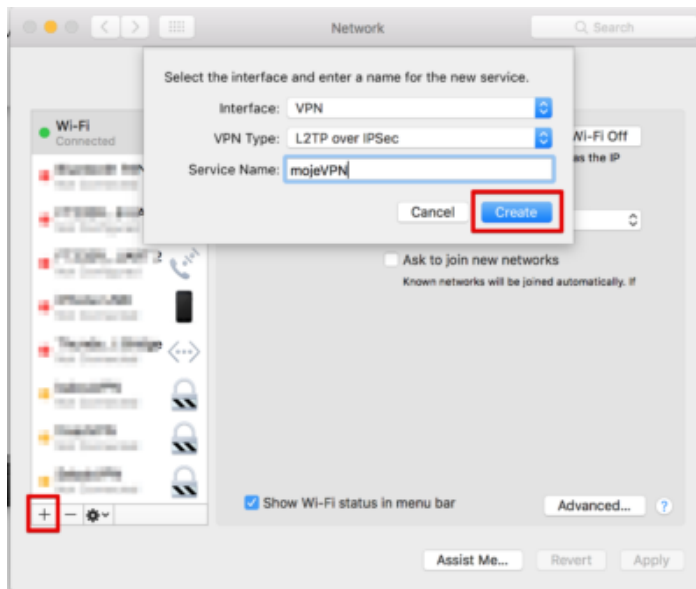
Win+R -> regedit -> OK -> větev  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\  
Services\PolicyAgent -> přidat novou hodnotu  
DWORD -> název  
AssumeUDPEncapsulationContextOnSendRule,  
hodnota 2.

Ve výchozím nastavení Windows routuje přes VPN spojení veškerou komunikaci. Pokud vám nejde o zabezpečení veškeré komunikace a chcete si zachovat stávající IP adresu, pak je nutno vejít hluboko do X-tého dialogu.

## PŘIPOJENÍ Z MACOS

- Settings → Network → tlačítko [+] vlevo dole
- Interface: VPN, VPN type: L2TP over IPSec, Service name: libovolný název; klikněte na [Create]
- Server address: vnější IP adresa routeru
- Account name: jméno uživatele
- button Authentication settings → Password: heslo uživatele, Shared secret: heslo sdílené pro všechny uživatele; [OK]
- button Advanced → checkbox Send all traffic over VPN connection  
pokud vám nejde o zabezpečení veškeré komunikace a chcete si zachovat stávající IP adresu, stačí nezaškrtnout

- Apply. Uložit, připojit!



## PŘIPOJENÍ Z IPHONU A IPADU

- Settings → General → VPN → Add VPN Configuration...
- Type: L2TP  
(je tam i volba IPSec, ale tu nevolit)
- Description: vyplnit libovolný název
- Server: vyplnit IP adresu routeru
- Account: jméno uživatele
- Password: heslo uživatele
- Secret: heslo sdílené pro všechny uživatele
- jméno uživatele
- přepínač Send all traffic nechat zapnutý  
pokud vám nejde o zabezpečení veškeré komunikace a chcete si zachovat stávající IP adresu, stačí nezaškrtnout
- Proxy nechat na Off.

- Done. Tím se uloží a nahoře máte přepínač na aktivaci, zkuste se nyní připojit.

## PŘIPOJENÍ Z ANDROIDU

Nemám po ruce žádný Android, kdo má, může dodat postup ve stylu těch předchozích a screenshoty. :-)

## CO DÁL?

VPN je tedy plně funkční a stabilní.

Dál by se někdy možná dalo rozběhat:

1. MikroTik Neighbor Discovery protocol (MNDP) pro hledání okolních mikrotiků v lokální síti
2. automatická viditelnost samby, bonjour atd.
3. mrknout jak by konfigurace vypadala pro IPv6

## STÁLE TO NEFUNGUJE?

Pokazit se může opravdu hodně věcí, sám jsem i již funkční návod musel kvůli rozličným chybám od návštěvníků mnohokrát vylepšovat. Základní rada je, zkus se nejdřív připojit z vnitřní sítě, kde je méně prvků které můžou nefungovat. Následně pak zkoušet se připojit z vnějšku na WAN port, a až nakonec se pokoušet připojit z internetu. Dále mrkni na mikrotiku do Log. Pokud to nestačí, tak zapni i podrobné logování L2TP a IPSEC těmito příkazy:

```
/system logging add prefix="L2TP_LOG ===>  
/system logging add prefix="IPSEC_LOG ===:
```



Někdy pomůžou dočasně deaktivovat drop pravidla na firewallu. Pokud můžete, mikrotik nejdřív zkoušejte konfigurovat na dobré lokalitě, kde běží pořádný internet s pevnou veřejnou IP adresou (typicky kabelový internet, nebo optika). Pokud si stále nevíte rady, nezbyvá než přidat pod článek komentář.

### **Připojení funguje, ale nedopingnu se nikam**

Viděl jsem už i případ, kdy se spojení sestavilo v pořádku, ale ve skutečnosti nefungovalo nic, nešlo se ani dopingnout nikam. Pak se ukázalo, že mi byla přidělena lokální adresa končící x.x.x.255 (např. 192.168.1.255). Nakonec byla chyba v nastavení poolu, který byl nastaven od 1 až do 255 (namísto do 254, nebo méně; v tomto návodu máme do 250). DHCP na Mikrotiku přiděluje adresy typicky od konce, a .255 je pro naše účely neplatná adresa (typicky jde o broadcast adresu).

## **ČASTÉ OTÁZKY**

### **Připojení funguje, dostanu se na internet, ale nevidím místní zařízení v LAN.**

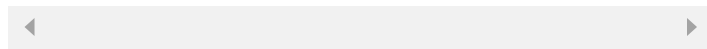
Někdo potřebuje VPN jen jako bránu do internetu, někdo chce, aby se VPN uživatelé viděli mezi sebou, a někdo chce být kompletně přítomen v LAN síti a mít tak možnost přistupovat k místním zařízením pro přístup k

webrozhraním, diskům sdíleným přes SMB, SSH službám a další.

Není problém. Pokud chceme, aby se všichni VPN uživatelé zároveň ocitli v LAN síti, pak upravíme následující:

PPP -> Profiles tab -> my-l2tp-profile:

```
interface list:  LAN
bridge:          bridge1
```



Pokud chceme jenom vybrané uživatele připojit do LAN, pak vytvoříme oddělený profil, který bude mít stejné nastavení, jen se bude lišit právě interface listem a bridgem. Bridge buď žádný (pro internet-only), nebo nějaký bridge2 (který vytvoříme pro účely propojení VPN uživatelů mezi sebou). Interface list WAN (pro internet-only), nebo LAN. Tyto profily pak přiřadíme jednotlivých uživatelům v PPP -> Secrets -> uživatel -> profile.

### **Potřebuju veřejnou statickou IP?**

Potřebuješ hlavně veřejnou IP (ať už statickou, nebo dynamickou), tzn. aby se k tobě šlo připojit z venčí.

Pokud ji nemáš, tak celý postup nemá smysl, dokud ji mít nebudeš.

ISP operátoři většinou nabízí veřejnou dynamickou IP, pokud máš stěží, nebo privátní neveřejnou, která je k ničemu. Za veřejnou IP si

nechají často zaplatit tučný měsíční poplatek, někdy v ceně základního připojení.

Přehled co operátoři nabízí je zde:

Teoreticky by ISP/operátorovi stačila jedna veřejná IPv4 pro mnoho zákazníků, jen by nabízel přeposílání několika portů, čímž by minimalizoval náklady na pořizování nedostatkových IPv4, ale v praxi to nikdo z nějakého důvodu nenabízí.

Ještě pro upřesnění, víceméně stačí mít veřejnou IP adresu i jinde, než na dané přípojce, a vytvořit si mezi přípojkou a uzlem s veřejnou tunel. To se hodí i v případě, že nechci platit zlodějský měsíční příplatek za veřejnou IP vícekrát pro víc přípojek. Nevešlo se to však do tohoto článku.

Další oblast k prozkoumání je IPv6, ale zatím čekám na větší rozšíření, nebo zájem.

### **Mám neveřejnou IP, bude mi připojení fungovat?**

Ne. Je nutná veřejná IP, aby se dalo na ni připojit zvenčí.

### **Mám veřejnou IP, bude mi připojení fungovat?**

Ano.

### **Mám veřejnou IP, ale za CGNAT (1:1 carrier-grade NATem), bude mi připojení fungovat?**

Ano.

### **Mám statickou IP, bude mi připojení fungovat?**

Nezáleží na tom, zda máš statickou IP, nebo dynamickou. Záleží, zda ta statická IP je veřejná. Pokud ano, tedy jde o veřejnou statickou IP, pak jde o ideální situaci pro připojování zvenčí.

### **Mám dynamickou IP, bude mi připojení fungovat?**

Nezáleží na tom, zda máš dynamickou IP, nebo statickou. Záleží, zda ta dynamická IP je veřejná. Pokud ano, tedy jde o veřejnou dynamickou IP adresu, pak připojení zvenčí fungovat bude. Avšak tím, že se mění, bude připojení zvenčí fungovat jen po nějakou dobu, než se stane konfigurace neaktuální. Typicky do restartu routeru v místě běžícího VPN serveru, nebo 1 den, nebo náhodnou delší dobu (u UPC například do té doby než udělají nějaký interní upgrade v síti, třeba 30 dnů až pár měsíců). Poté se nepůjde zvenčí připojit, protože na přístroji, ze kterého se připojuješ, budeš mít neaktuální IP adresu cíle. Tzn. je vždy potřeba zjistit nějak aktuální adresu, kam se připojovat, a tu si neaktualizovat v nastavení. Nic moc, pokud jsi již někde mimo lokalitu, chceš se připojit, no, a nevíš kam. Tento problém se dá řešit přes DDNS, kdy na routeru běží služba, která pravidelně aktivně informuje nějaký cizí server (např. noip.com) o své aktuální IP adrese. Vy se pak připojujete na (již pořád stejnou) textovou adresu, kterou jste získali od noip.com při prvotním nastavení. DDNS služby jsou většinou placené a jejich služby (i proto) nevyužívám, takže neporadím žádnou konkrétní službu.

### **Není pak všechno spojení zpomalené? Jak je to spojení rychlé?**

Pokud se připojujete na rychlou přípojku, tak subjektivně rozdíl nepoznáte. Ping mám dokonce prakticky beze změny. Nejčastější omezení je, že rychlost vašeho VPN downloadu

je závislá na maximálním uploadu vzdálené přípojky. U domácích připojení bývá upload často hodně škrcen. Vzdálená VDSL přípojka s 1Mbit uploadem jako VPN pro routování veškeré vaší komunikace asi není to pravé ořechové. Byť i tak může posloužit (lepší než nic). V takovém případě by bylo asi lepší využít za pár korun nějakou tu serverovou přípojku se 100Mbit uploadem (zmiňuji níže).

**Patří něco do „IP -> IPSec -> Users tab“?**

**Vypadá, že to s tím nějak souvisí.**

Odpověď: Ne.

**Patří něco do „PPP -> L2TP Secrets tab“?**

**Vypadá, že to s tím nějak souvisí.**

Odpověď: Ne.

**V logu vidím „phase1 negotiation failed due to time up“.**

- Zkontroluj krok 5 – IP -> IPsec -> Peers tab.

Máš tam správně IP adresu v peer1? Hned to první políčko Address?

Když se pokusím připojit z nepovolené IP, tak to skončí na této chybě. Takže bude nutné zadat správnou IP protistrany. Pokud tam máte dvě dvojtečky, nebo ::/0, pak je připojení povoleno ze všech IP, a problém bude jinde.

- Zkontroluj Firewall -> NAT

Nemáš tam náhodou nastavené

přesměrování portů, zrovna z rozsahu, které je využíváno VPN službou?

Jednou jsem u někoho viděl nastavené přesměrování celého range 4000-4999 do vnitřní sítě, takže to logicky kradlo data, která měla putovat do VPN funkcionality. Stačilo zrušit, nebo upravit na jiný range.

- Ani jedno nepomohlo  
Asi bude nějaký problém v tom, že se na jeden z portů nejde dostat. Myslím, že na ten 4500. Delší dobu se mi to nestalo, takže je to nutné řešit v diskuzi pod článkem.

### **Lze se připojit k VPN z více zařízení souběžně?**

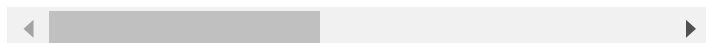
Ano. Nezáleží, zda použijete všichni stejné jméno/heslo, nebo se budete připojovat každý pod svými údaji. Nezáleží, zda se všichni připojujete z unikátních IP, nebo jste všichni skryti na NATem na stejné IP adrese.

RouterOS obsahoval dlouhá léta bug, kdy se nemohlo připojit více klientů ze stejné IP adresy. Případné připojení druhého zařízení ze stejné IP vždy vykoplo to první. Takže například dva lidé z kavárenské Wi-Fi se k takovému VPN naráz nepřipojily.

Bug byl vysvětlován jako že je to omezení protokol stacku L2TP/IPSec, který z historických důvodů, ještě před rozšířením používání NAT, nebyl navržen tak, aby toto dnes umožnil. Problém prý je ve využívání vždy stejných portů pro sestavení i udržování

spojení, a L2TP které nevidí o vrstvu níž (do IPSec). Zároveň ale bylo trochu zvláštní, že konkurence s tím problémem nemá, a také záhadná oprava problému ve firmwaru v6.47 (

l2tp - fixed multiple tunnel establishment



. Takže to nakonec asi nějak šlo. Zajímavost: připojovat ze více klienty ze stejné IP ale záhadně fungovalo už ve firmwaru v6.45.7.

Řešení před firmwarem v6.45.7: Řešení to nemá, jen příliš komplikovaný workaround – vytvoření speciálního 1:1 NATu na Mikrotiku, který překládá IP:port na unikátní/různé IP adresy, které interně předává dál protokolům L2TP/IPSec. Problematika i workaround je podrobněji popsáný zde. Reálně jediné přejít na stack IKEv2/IPSec. Někdo by mohl pomoci s prvotní konfigurací a návodem, já těžko hledám čas vše takto podrobně sepsat, to zabere kvantum času a zkoumání. Více uživatelů současně je pro mě spíš jen takový bonus, než nutnost. Kdo by to nutně potřeboval, například pro firmu, může si mě objednat, abych se tomu věnoval. Kdo se tomu věnoval sám, ocením, když mi pošle tento návod upravený pro IKEv2, zveřejním. Jinak nezbyvá než vyčkat, až si na to najdu čas i chuť.

**Lze se připojit se stejným jménem/heslem z více zařízení souběžně?**

Ano dá. Interně se pro každého klienta přidělují lokální IP adresy z poolu. Stále však platí omezení uvedené výše, tedy nutnost se k VPN připojovat z různých vnějších IP adres.

### **Lze se připojit více klienty ze stejné IP? Například mobil a notebook zároveň.**

Ano. Od firmwaru v6.47 (neoficiálně už od v6.45.7). Podrobněji viz výše.

### **Potřebuji přidávat více VPN uživatelů?**

Více uživatelských účtů potřebujete ve specifických případech:

a) VPN používá více lidí a chcete předat rozdílná jména/hesla různým lidem, abyste mohli logovat jejich přihlášení a odhlášení, přenesená data, individuálně měnit hesla či rušit účty.

b) pokud chcete přidělit pevnou lokální IP adresu některým zařízením

V tom případě vytvoříte uživatele, kterému se přidělí pevná IP, nikoli náhodná volná IP z poolu. V takovém případě bude logicky i platit pravidlo maximálně jednoho 1 připojení na tomto účtu, protože druhé připojení selže na již obsazené lokální IP adrese.

Je stále nutné dodržet podmínku, že se každý připojujete z jiné IP adresy, jak bylo vysvětleno v otázce výše.

### **Jak přidám další VPN uživatele?**

Stačí přidat více položek v kroku 7. Tzn. jděte to PPP -> Secrets a popřidávejte si více kombinací

jméno/heslo. S dalšími lidmi tedy budete vždy sdílet tři autentizační údaje: jejich vlastní jméno/heslo + jedno IPSec sdílené heslo.

Opět připomínám, toto nemá vliv na skutečnost, že lze uskutečnit jen jedno souběžné připojení z jedné IP adresy.

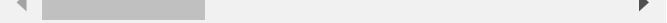
### **Jak nastavím port forwarding přes VPN?**

- V praxi bude potřeba zavést pro VPN účet pevnou interní IP adresu. Aby daný user měl po přihlášení přidělenou vždy stejnou interní IP, ne „náhodnou“ z vpnpoolu. To se nastaví v PPP -> Secrets -> <daný VPN účet> -> pole Remote address

Toto vás z principu zároveň omezí na používání jediného zařízení na jeden účet současně. Pokud se zkusíte připojit z dvou a více PC přes takto nastavený účet najednou, všechny dostanou stejnou IP a fakticky nebude nic fungovat. Ani načítání webu. Proto doporučím na stávající VPN účet nešahat, a pro tyto účely si v PPP -> Secrets vytvořit nový, oddělený účet (jméno/heslo) s pevnou IP, na který se bude připojovat vždy jen jeden PC současně.

- Dále přidáme samotné pravidlo na přesměrování portu

```
/ip firewall nat
add action=dst-nat chain=dstnat dst-add
```

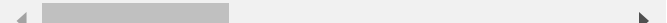


```
tzn. navenek budu vidět z <dst-address>:  
<dst-port>
```

```
a to se přesměruje na lokální <to-  
addresses>:<to-ports>
```

konkrétně například

```
/ip firewall nat  
add action=dst-nat chain=dstnat dst-add
```

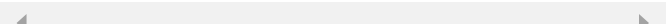


```
tzn. navenek budu vidět z  
83.201.34.120:8001  
a to se přesměruje na lokální  
192.168.88.150:80
```

### **Jak zjistím, jakou mi Mikrotik přidělil interní IP přes VPN připojení?**

- IP bude vidět v detailech aktivního VPN připojení na klientském zařízení (iPhone Settings – VPN – ikonka (i); na macOS v Settings – Networks – aktivní VPN – je vidět connect time a IP address)
- lze ji zjistit na Mikrotiku v PPP -> Interface -> <l2tp> položka double click -> záložka Status -> pole Remote address, resp.

```
/ppp active print
```



- obecně bude potřeba tu IP udělat pevnou, to se nastaví v PPP -> Secrets -> pole Remote address

**Chci lidem diktovat krásný psaný název serveru, namísto škaredé IP adresy? IP adresa se navíc může změnit, a nechce se mi pak na všech nastavených zařízeních ručně předělávat.**

No, k čemu asi tak slouží doménová jména? ;-)  
Právě k tomu! Takže si poříd' doménu, pokud nemáš, a naflákej si tam A záznamy. Hodnota A záznamu bude název subdomény a IP adresa bude adresa chtěné přípojky.

|                        |    |   |    |
|------------------------|----|---|----|
| doma.nějakádoména.cz.  | IN | A | 16 |
| chata.nějakádoména.cz. | IN | A | 16 |
| prace.nějakádoména.cz. | IN | A | 16 |



V zařízeních pak jako server uvedeš doma.nějakádoména.cz, a v případě změny cílové IP stačí vejít do nastavení DNS domény a změnit to jednou tam.

Přesněji jde o doménu + DNS hosting, ale k doméně dnes nabízí každý DNS hosting zdarma už tak automaticky, že se to tváří jakoby to byla jedna věc.

Podmínkou samozřejmě je, že vám VPN běží na pevné veřejné IP adrese, jinak byste adresu museli neustále měnit.