BEZIT – 9. cvičení

Radek Janoštík

Univerzita Palackého v Olomouci

10. 4. 2024

VPN na platformě MikroTik

- Mikrotik samozřejmě podporuje VPN, ukážeme si L2TP s IPSec
- Nastavení trochu složitější, budeme potřebovat:
  - Povolit nutné porty pro VPN na firewallu (WAN port)
  - Zajistit přiřazení IP adres klientům z VPN
  - Nastavit samotný L2TP server a IPsec
  - Nastavit přihlašovací údaje pro klienty
  - Zapnout APR-proxy na bridge

Nastavení firewallu: ip firewall filter

- Potřebujeme povolit UDP porty 500 (IKE) a 1701
- Povolit příchozí protokoly `ipsec-esp, ipsec-ah`
- Nezapomenout přesunout pravidla nad pravidlo, které zahazuje příchozí komunikaci

```
[admin@MikroTik] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
...
 5    chain=input action=accept protocol=udp in-interface=ether1 dst-port=500

 6    chain=input action=accept protocol=udp in-interface=ether1 dst-port=1701

 7    chain=input action=accept protocol=ipsec-esp in-interface=ether1

 8    chain=input action=accept protocol=ipsec-ah in-interface=ether1

 9    ;;; defconf: drop all not coming from LAN
      chain=input action=drop in-interface-list=!LAN
...
```

Přiřazení IP adres

- Zmenšíme pool IP adres současného DHCP poolu

  ```
  ip pool set dhcp ranges=192.168.88.2-192.168.88.200
  ```

- Vytvoříme nový pool pro klienty VPN

- Rozsah záměrně nedáváme úplný

  ```
  ip pool add name=vpn ranges=192.168.88.201-192.168.88.253
  ```

L2TP server

- Vytvoříme nový PPP profil: PPP → Profile

```
ppp profile add name=l2tp local-address=192.168.88.254
            remote-address=vpn dns-server=192.168.88.1
            change-tcp-mss=yes interface-list=LAN bridge=bridge
```

- Nastavíme L2TP server: ppp → Interface → L2TP server

```
interface l2tp-server server set enabled=yes default-profile=l2tp
           use-ipsec=yes ipsec-secret="SuperTajnyPresharedKey"
           authentication=mschap1,mschap2
```

- Nastavíme parametry IPSec: ip → ipsec → proposals

```
ip ipsec proposal set default auth-algorithms=sha1
         enc-algorithms=aes-256-cbc,aes-192-cbc,aes-128-cbc
         lifetime=30m pfs-group=modp1024
```

Přihlašovací údaje a ARP proxy

- Jednotlivé uživatele můžeme vytvářet v ppp → secrets

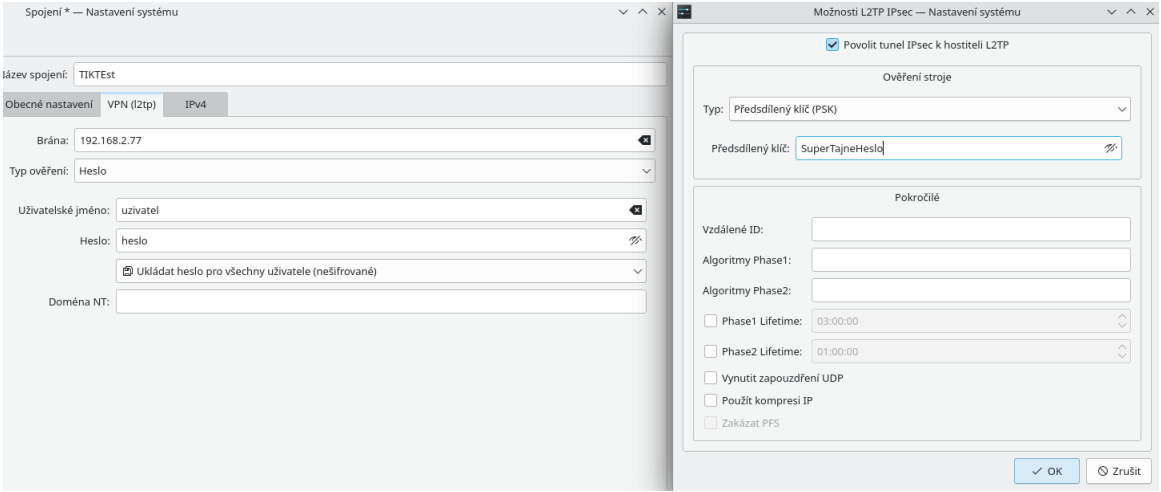
```
ppp secret add name=uzivatel password="uzivatelovoHeslo" profile=l2tp
          service=l2tp
```

- Zapneme ARP proxy na bridge

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

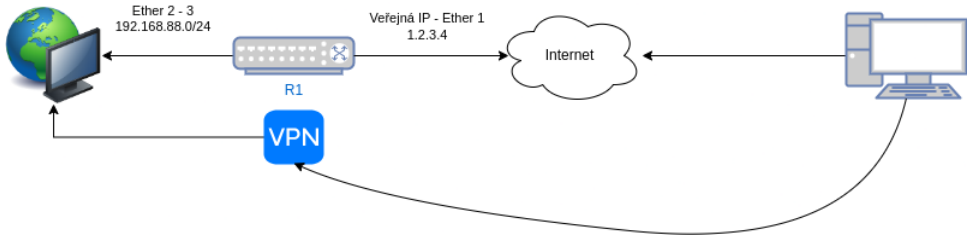
- Nyní již máme server nastavit, nastavíme klienta

Nastavení klienta



Úkol – Nastavení VPN na MikroTik jako brána do vnitřní sítě

- Simulujte obdobné nastavení



- Nastavte router tak, aby sloužil jako VPN brána
- Klienti, kteří se se na ni připojí se budou jevit, jakoby byli ve vnitřní síti
- Využijte L2TP a IPsec
- Odevzdání – přímá ukázka
- Nebo screenshoty nastavení PC (ip a), ping do vnitřní sítě, nastavení VPN na klientovi