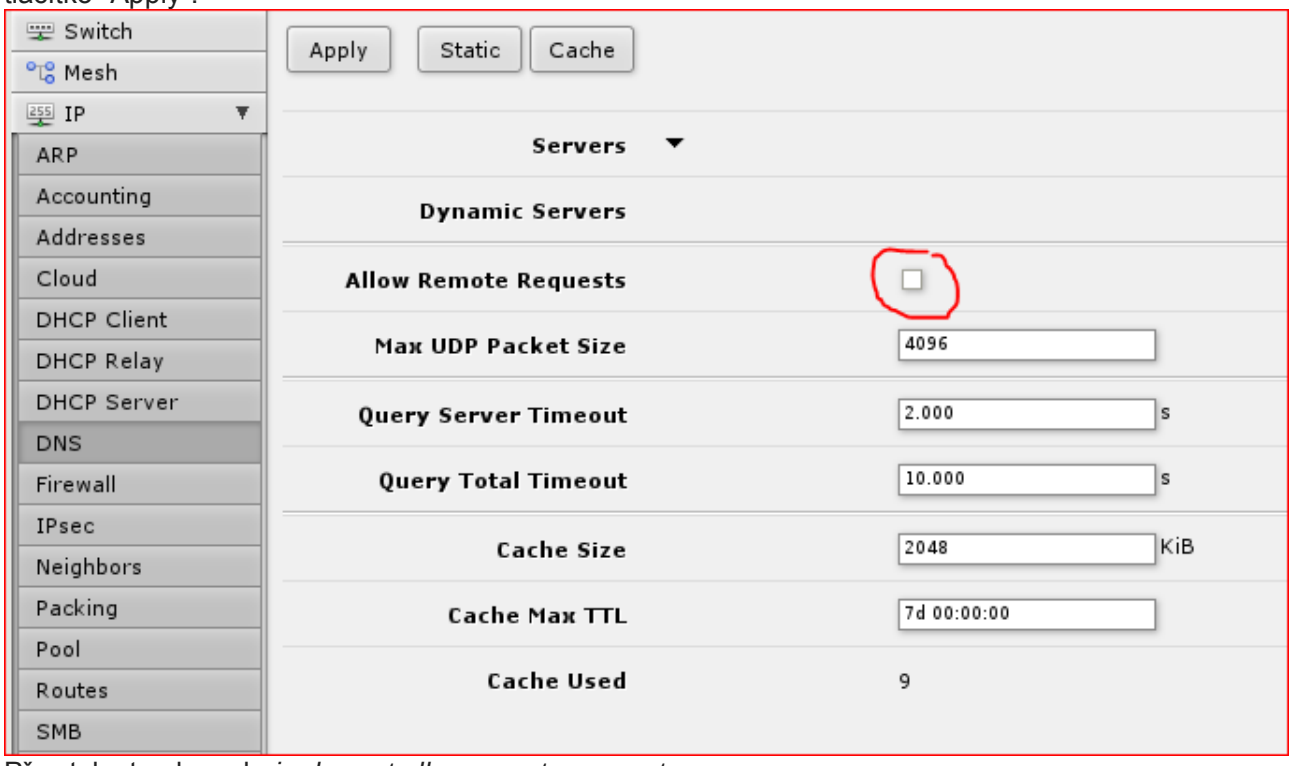
Návody

Pro splnění podmínek umožňující členství v projektu Fenix je potřeba zajistit detekci a likvidaci zdrojů útoku typu DNS amplification (zákaz nespravovaných otevřených resolverů, implementace response rate limiting) v přiděleném adresním prostoru. Níže je návod pro správnou konfiguraci na nejvíce užívaných zařízeních.

1 Mikrotik - konfigurace

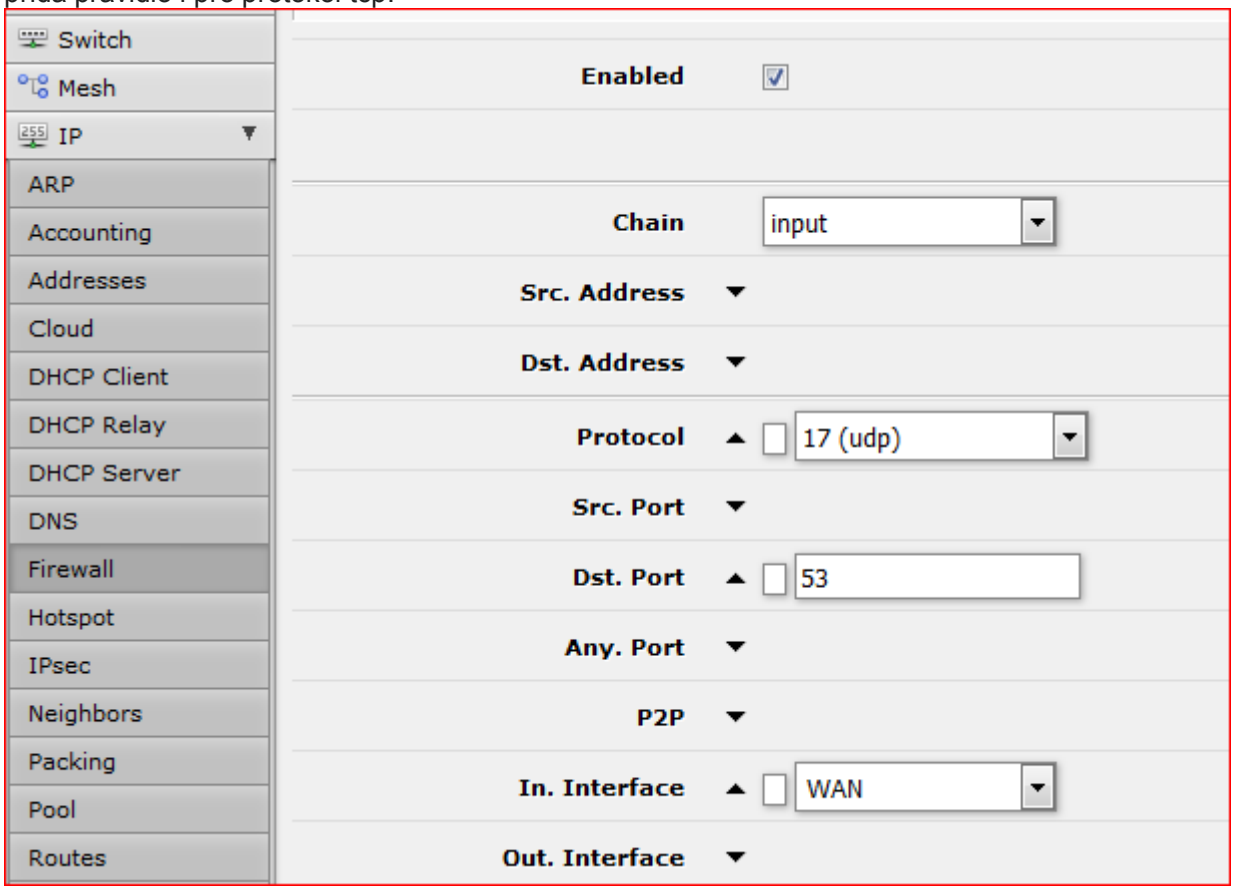
Varianta 1
Úplné zakázání služby na RB (routerboardu) - přes webové rozhraní nebo winbox - v levé liště menu rozbalit nabídku "IP" a v podnabídce "DNS" odškrtnout políčko "Allow Remote Requests" → poté tlačítko "Apply".

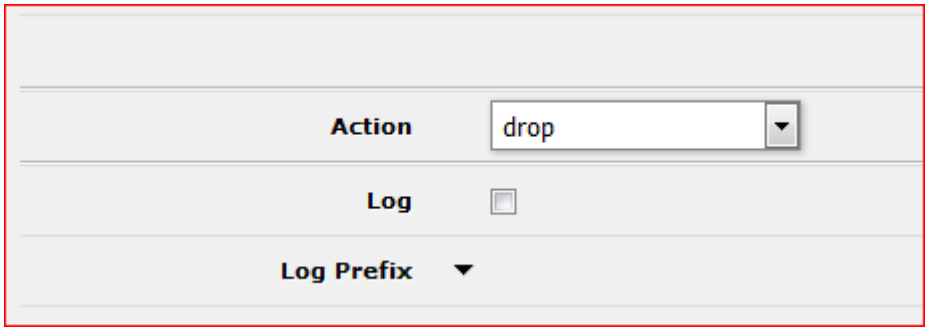


Přes telnet nebo ssh: *ip dns set allow-remote-requests=no*
Tato varianta má ale tu nevýhodu, že RB přestane fungovat jako DNS resolver i pro vnitřní síť, což nevadí, pokud mají koncové stanice nastavené jiné DNS než RB.

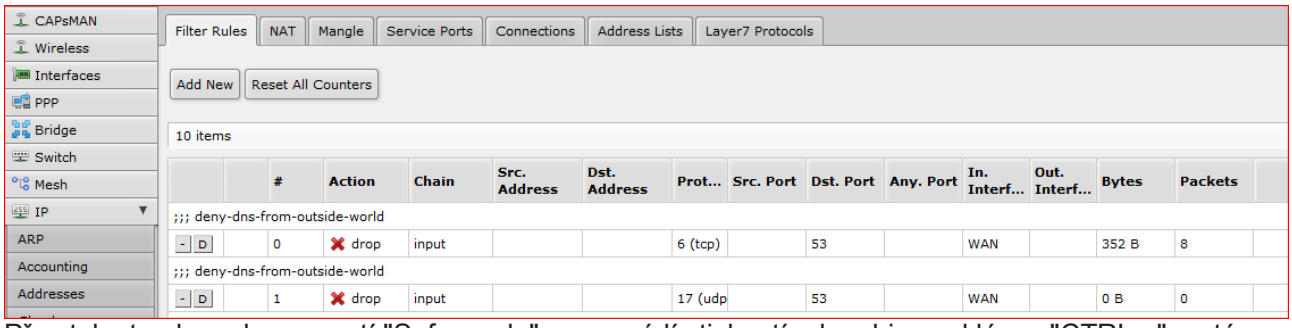
Varianta 2
Zakázání portu 53, UDP a TCP - nastavením filtru na venkovní interface RB. Tuto variantu doporučuji dělat v "Safe modu", pro případ, že by se "něco nepovedlo".
Zapnutí "Safe modu" ve webovém rozhraní nebo ve winboxu - na levé liště stisknout tlačítko "Safe Mode". Dále v levé liště rozbalit nabídku "IP", podnabídku "Firewall" a v záložce "Filter Rules" použít tlačítko "Add New".
Stačí vyplnit pole "Chain" hodnotou "input", pole "Protocol" hodnotou "17 (udp)", pole "Dst.Port" hodnotou "53", pole "In.Interface", kde je nutné vybrat venkovní rozhraní a pole "Action" hodnotou

"drop". Pole "Action" je až téměř na konci formuláře, je nutné použít posuvník. Stejným způsobem se přidá pravidlo i pro protokol tcp.





Pravidla se vytvoří jako poslední, pro správnou funkčnost je ho potřeba je přesunout myší v seznamu nahoru, ideálně do pozice 0, což se provede přetažením myší. Pokud je vše v pořádku, tak se opět stiskne tlačítko "Safe mode", tím se konfigurace uloží.
Takto vypadají správně nastavená pravidla:



Přes telnet nebo ssh - zapnutí "Safe mode" se provádí stisknutím kombinace kláves "CTRL-x", poté se přepneme do konfigurace filtru příkazem "*/ip firewall filter*" a přidáme pravidlo takto: *add chain=input action=drop protocol=udp dst-port=53 comment=deny-dns-from-inet in-interface=ether1-gateway* (místo ether1-gateway zvolíme správné pojmenování WAN portu) a obdobně pravidlo pro tcp. Příkazem "*print*" si vypíšeme seznam pravidel, nově přidaná pravidla budou jako poslední. Přesun v seznamu nahoru se provede příkazem "*move*", tzn. např. pokud má nově vytvořené pravidlo pořadové číslo 15, dáme příkaz *move 15 0*. To přesune pravidlo s číslem 15 místo pravidla s číslem 0 a celý seznam se o jednu pozici posune, nemusíme se bát, že by se pravidlo číslo 0 přepsalo. Stejně tak přesuneme i druhé pravidlo. Příkazem "print" si ověříme, že jsou nyní nově vytvořená pravidla na prvních místech

```
Flags: X - disabled, I - invalid, D - dynamic
 0    ;;; open-dns
      chain=input action=drop protocol=tcp in-interface=WAN dst-port=53 log=no log-prefix=""

 1    ;;; open-dns
      chain=input action=drop protocol=udp in-interface=WAN dst-port=53 log=no log-prefix=""
```

a pokud je vše v pořádku, tak opětovným stiskem kláves "CTRL-x" uvolníme "Safe mode" a konfigurace je uložena.