

# 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".

The screenshot shows the Mikrotik WinBox interface for DNS configuration. On the left is a sidebar menu with categories: Switch, Mesh, IP, and SMB. Under 'IP', sub-menus include ARP, Accounting, Addresses, Cloud, DHCP Client, DHCP Relay, DHCP Server, DNS (selected), Firewall, IPsec, Neighbors, Packing, Pool, Routes, and SMB. The main area has buttons for 'Apply', 'Static', and 'Cache'. Below these are sections for 'Servers' and 'Dynamic Servers'. The 'Allow Remote Requests' checkbox is circled in red. Other settings include 'Max UDP Packet Size' (4096), 'Query Server Timeout' (2.000 s), 'Query Total Timeout' (10.000 s), 'Cache Size' (2048 KiB), and 'Cache Max TTL' (7d 00:00:00). The 'Cache Used' is shown as 9.

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 nevádí, 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.

The screenshot shows the configuration of a Firewall rule in Mikrotik WinBox. The left sidebar lists various services, with 'Firewall' selected. The main configuration area is as follows:

- Enabled:**
- Chain:** input
- Src. Address:** (empty dropdown)
- Dst. Address:** (empty dropdown)
- Protocol:** 17 (udp)
- Src. Port:** (empty dropdown)
- Dst. Port:** 53
- Any. Port:** (empty dropdown)
- P2P:** (empty dropdown)
- In. Interface:** WAN
- Out. Interface:** (empty dropdown)

This close-up shows the bottom part of the Firewall rule configuration:

- Action:** drop
- Log:**
- Log Prefix:** (empty dropdown)

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:

#	Action	Chain	Src. Address	Dst. Address	Prot...	Src. Port	Dst. Port	Any. Port	In. Interf...	Out. Interf...	Bytes	Packets
10 items												
;;; deny-dns-from-outside-world												
0	drop	input			6 (tcp)		53		WAN		352 B	8
;;; deny-dns-from-outside-world												
1	drop	input			17 (udp)		53		WAN		0 B	0

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.