Mikrotik RouterOS:

Problematika výměnných sítí

Obsah

Úvod

Výměnné sítě, neboli sítě typu peer to peer (P2P) jsou postrachem nejen mediálních vydavatelství, ale také provozovatelů Internetových sítí. Necháme stranou právní aspekty P2P. Nad tím ať se přou Majors se zastánci lidských práv a svobod a podíváme se na způsoby, jak se s datovým provozem, který P2P generují, vypořádat. Je to totiž krajně nepříjemné, když 10% procent zaměstnanců generuje 90% veškerého zatížení firemního spoje do Internetu.

Stopování P2P provozu

RouterOS od verze 2.8 obsahuje funkci vystopování P2P provozu (tzv. P2P connection tracker). Ten umožňuje zacházet s P2P provozem ve třech úrovních:

- Měření datových toků, které generují P2P
- Řízení datových toků P2P
- Zákaz P2P komunikace

Podrobně si všechny tři možnosti probereme v samostatných kapitolách. Nyní se pojďmě podívat, které P2P protokoly RouterOS rozeznává:

- BitTorrent
- Blubster
- DirectConnect (DC++, MLDonkey)
- eDonkey (eDonkey 2000, eMule, xMule, Shareaza, MLDonkey)
- Fasttrack (Kazza a jeho klony – např. KazzaLite, Grokster, iMesh)
- GNUtella (Shareaza, XoLoX, GNUcleus, BearShare, LimeWire, Morpheus, Phex atd.)
- GNUtella 2 (Shareaza, MLDonkey)

Klientských programů samozřejmě existuje stále více. Jedná se však vesměs o programy využívající jednu z výše uvedených výměnných sítí, nejčastějí Fasttrack a GNUtella.

Funkci Connection Tracking zapínáme přes

```
/ip firewall connection tracking
```

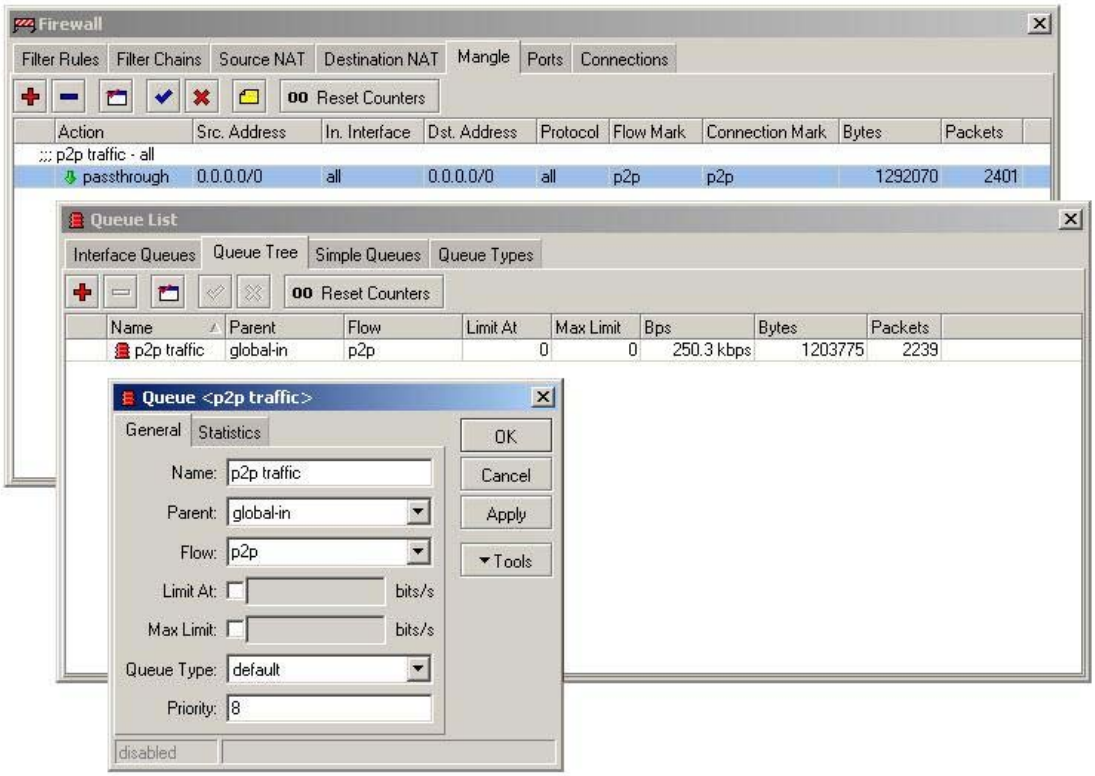
Nejedná se o prosté filtrování cílových portů, takže budete-li provoz sledovat síťovým snifferem, zaznamenáte komunikaci prvních několik paketů P2P, pak již nastupují Vámi zvolená pravidla.

Měření datových toků P2P

Dříve, než se pustíte do více či méně tvrdých restrikcí, je vhodné zjistit, na kolik P2P zatěžují Vaši síť. K tomu slouží Traffic Marking, neboli značkování paketů. Nastavujeme jej v

```
/ip firewall mangle
```

Volíme zde konkrétní P2P protokol, jehož provoz budeme měřit. V našem případě budeme chtít zjistit veškerý P2P provoz, takže zvolíme `all-p2p`. Action zvolíme `Passthrough`. Zdrojovou a cílovou IP necháme 0/0, neboť měříme celkový průtok v součtu obou směrů. Nic nám však nebrání rozdělit tok na příchozí (pak zadáváme do `source address` adresu vnitřní sítě) a odchozí (pak zadáváme adresu vnitřní sítě do `destination address`). Pokud naše vnitřní síť obsahuje více než jednu síť, kterou bysme mohli obsáhnout do jedné masky, pak zadáme přesně tolik pravidel do `firewall mangle`, kolik máme takovýchto sítí. Stejným znakem těchto sítí pak bude `Flow Mark` a `Connection Mark`, kam zadáme například `p2p-in`, resp. `p2p-out`. V našem, níže uvedeném případě, však máme pouze jedno pravidlo obsahující vešekerý traffic, kterému jsme nastavili Marky na značku `p2p`.



Jakmile správně nadefinujeme Firewall Mangle, okamžitě můžeme vidět počet přenesených bajtů a paketů týkající se P2P provozu.

My bychom však rádi viděli průtok nejen jako sumu přenesených bajtů či paketů, ale i jeho okamžitou hodnotu vyjádřenou v bitech/vteřinu. K tomu nám poslouží Queue Tree, kterou si pro náš účel vytvoříme. Výše uvedený obrázek ukazuje nastavení zmíněné Queue Tree, které používá námi definovanou značku Flow p2p a tudíž ošetřuje veškeré pakety, které jsme touto značku označili ve Firewall Mangle.

Pokud se týká zpracování p2p statistik, zobrazením toku v bitch/vteřinu jsme ještě nevyčerpali všechny naše možnosti. RouterOS disponuje SNMP MIB, které obsahuje mimo jiné, také Queues. Jednoduchý způsobem pak můžeme zjistit konrétní OID našeho queue:

```
Terminal vt102 detected, using multiline input mode
[admin@NV40] > queue
[admin@NV40] queue> tree
[admin@NV40] queue tree> print oid
Flags: X - disabled, I - invalid, D - dynamic
 0    name=.1.3.6.1.4.1.14988.1.1.2.2.1.2.16777657
      flow=.1.3.6.1.4.1.14988.1.1.2.2.1.3.16777657
      bytes=.1.3.6.1.4.1.14988.1.1.2.2.1.5.16777657
      packets=.1.3.6.1.4.1.14988.1.1.2.2.1.6.16777657
```

To nám dává nepřeberné množství možností, jak tyto hodnoty zpracovat, například ve formě slušivého MRTG grafu. Více k problematice viz zmíněné Howto.

Řízení datových toků P2P

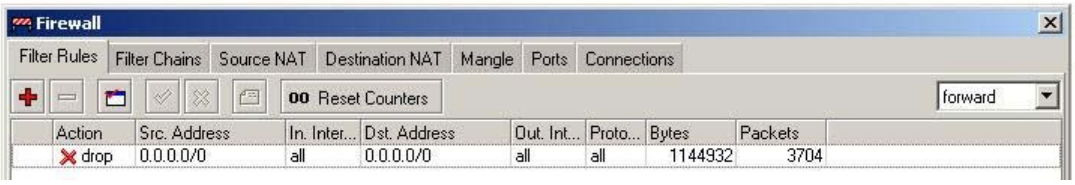
Pokud jste pročetli předchozí kapitolu o měření datových toků, pak již pro Vás není žádný problém datový tok P2P řídit podle svého uvážení. Ukázali jsme si totiž, kterak označené pakety zpracovat v Queue Tree. Když pohlédnete na obrázek z předchozí stránky, jistě si povšimnete dvou hodnot, které jsme v Qeue nezadali, jedná se o Limit At a Max limit. Ano, zde zadáváme rychlost v bitech za vteřinu, která se bude pro danou queue uplatňovat. Veškerá P2P komunikace se pak bude tvářit jako velká sdílená linka. To Vám možná nebude úplně vyhovovat, proto můžeme využít ponteciálu protokolu PCQ (per connection queue).

Zákaz P2P komunikace

Zatímco ISP by měli postupovat obezřetněji ve snaze omezovat své uživatele, v případě vnitropodnikové sítě zřejmě není co řešit a veškerou P2P komunikaci bude žádoucí rovnou zakázat.

K tomu nám slouží

`/ip firewall rule forward`



V zadání pravidla je pro nás důležitá záložka Advanced, kde specifikujeme P2P komunikaci (opět vybíráme jednotlivé P2P protokoly nebo všechny pomocí volby `p2p-all`).

Dále specifikujeme akci (Action). Zadáme-li `drop`, P2P pakety budou zahazovány bez posílání ICMP zprávy o odmítnutí. Naopak akce `reject` pro každeý zahozený paket vygeneruje ICMP zprávu o zamítnutí. V obou případech však dojde ke znemožnění P2P komunikace ve Vaší síti.