

# Membatasi akses internet berdasarkan quota dan waktu akses dengan menggunakan iptables

By Henry Saptono <[boypyt@gmail.com](mailto:boypyt@gmail.com)>

Maret 2011

“*Emang gak ada matinye nih Linux !*”, ungkapan ini tentunya sangat wajar, kenapa demikian?, karena sistem linux yang dikenal banyak orang, bukan saja berbiaya murah, namun juga begitu *powerfull*, dapat diandalkan untuk menjadi infrastruktur jaringan dengan berbagai fungsi. Misalnya untuk firewall, di linux telah disediakan mekanisme firewall yaitu iptables yang umumnya merupakan modul pada kernel linux. Iptables dikembangkan oleh netfilter project ([www.netfilter.org](http://www.netfilter.org)).

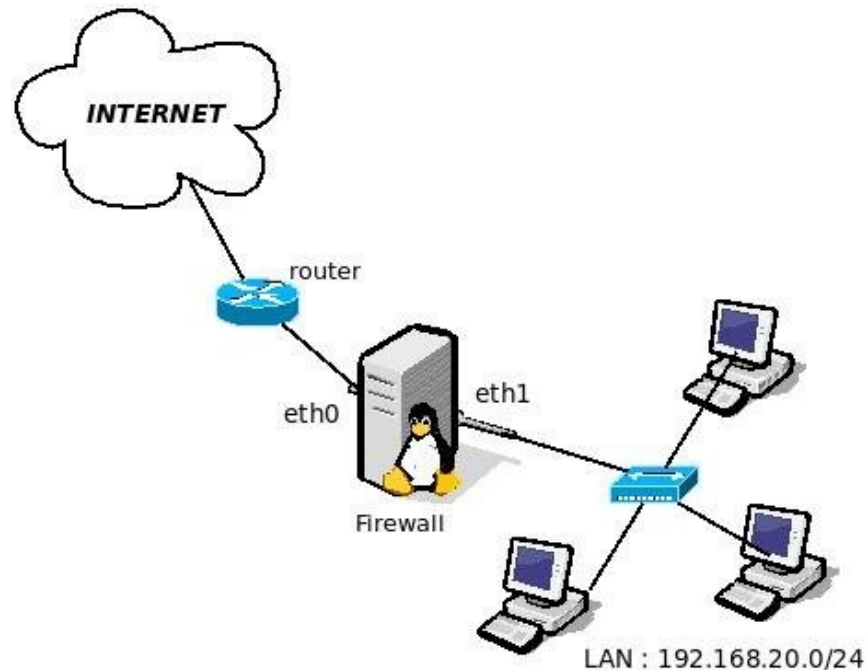
Ternyata iptables memiliki dukungan ekstensi/modul yang sangat variatif dan *powerfull*. Dengan iptables Anda bukan saja menerapkan firewall (*packet filtering*) namun lebih dari itu, Anda dapat menerapkan NAT(*Network Address Translation*) dan PAT (*Port Address Translation*), Anda juga dapat mengatur pembatasan akses internet berdasarkan quota dan waktu akses. Bagi Anda pengelola RT/RW net, atau ISP kecil kecilan tentunya butuh mekanisme pembatasan akses internet yang dapat berdasarkan quota dan waktu akses. Anda tidak perlu mengeluarkan kocek yang cukup mahal untuk membeli perangkat khusus yang dapat melakukan hal tersebut. Cukup menggunakan perangkat komputer biasa yang diinstal sistem operasi linux, kemudian dengan melakukan konfigurasi iptables, maka semuanya sudah bisa dilakukan.

Terkait kebutuhan pembatasan akses internet berdasarkan quota dan waktu akses maka penulis kali ini akan mencoba membahasnya, penulis menggunakan solusi iptables dalam upaya pembatasan akses internet tersebut. Ekstensi/modul iptables yang akan digunakan adalah modul **quota** dan modul **time**. Dalam pembahasan ini penulis menggunakan sistem operasi Linux Ubuntu 10.04 (kernel 2.6.32-21-generic ). Dalam melakukan konfigurasi pembatasan akses internet berdasarkan quota dan waktu ini penulis menggunakan tool iptables bawaan distribusi Linux Ubuntu 10.04.

## **Skenario**

Untuk memudahkan pembahasan, penulis membuat skenario sebagai berikut:

- Skema topologi jaringan tampak pada gambar-1.



Gambar-1. Skema Topologi Jaringan

- Jaringan lokal (LAN) memiliki alamat jaringan 192.168.20.0/24.
- Komputer Firewall linux memiliki dua buah network controller yaitu eth0 dan eth1. eth0 terhubung ke router (internet), dan eth1 terhubung ke jaringan lokal (LAN).
- Komputer Firewall berfungsi juga sebagai gateway/internet sharing
- Kebijakan Firewall linux adalah mengizinkan semua komputer pada LAN mengakses jaringan internet dan juga mengizinkan LAN mengakses komputer firewall.
- Akses dari router(internet) ke komputer firewall dan ke LAN ditolak.
- Pembatasan akses internet yang diterapkan pada firewall terhadap akses yang berasal dari LAN adalah sebagai berikut:
  - Pembatasan berdasarkan quota diterapkan pada komputer tertentu yaitu komputer bernomor ip **192.168.20.101** dan komputer **192.168.20.102**. **Quota** yang diberikan untuk komputer 192.168.20.101 dan komputer 192.168.20.102 adalah sebesar **100MB**. Jadi jika quota telah tercapai maka komputer 192.168.20.101 dan 192.168.20.102 tidak akan bisa lagi mengakses internet.
  - Pembatasan akses internet untuk komputer 192.168.20.101 dan 192.168.20.102 juga diterapkan berdasarkan **waktu akses**, yakni waktu akses internet dari hari **senin** sampai dengan **minggu**, mulai pukul **08:00** sampai dengan pukul **17:30**. Jadi jika waktu akses dilakukan diluar ketentuan waktu tersebut maka komputer 192.168.20.101 dan 192.168.20.102 tidak akan dapat mengakses internet.

## Langkah-langkah Konfigurasi

### Konfigurasi gateway/Internet sharing

Langkah awal dalam upaya pembatasan akses internet adalah tentunya menentukan nomor IP untuk setiap network controller (eth0 dan eth1) yang terpasang pada komputer firewall. Yang perlu menjadi catatan adalah pada komputer firewall, default gateway diatur ke alamat IP dari router yang terhubung ke komputer firewall (melalui eth0). Disisi komputer klien pada LAN diatur default gateway-nya ke alamat IP komputer firewall (ip pada eth1). Untuk penomoran alamat IP komputer firewall ini silahkan Anda tentukan sendiri (sesuaikan dengan skenario pada gambar-1).

Langkah selanjutnya adalah melakukan konfigurasi gateway/internet sharing, agar komputer firewall linux dapat meneruskan traffic IP dari LAN ke internet. Berikut ini langkah langkahnya:

- Mengaktifkan ip forwarding, ketiklah perintah berikut:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Atau:

```
# sysctl w net.ipv4.ip_forward=1
```

yang perlu dicatat adalah perintah perintah tersebut bersifat sementara, agar permanen tulislah kembali perintah perintah tersebut kedalam file /etc/rc.local.

- Mengaktifkan IP Masquerade. Diasumsikan rule firewall saat ini memiliki default policy ACCEPT untuk semua jenis traffic (*no firewall*). Ketiklah perintah berikut ini untuk mengaktifkan ip masquerade:

```
# iptables -F
```

```
# iptables -F -t nat
```

```
# iptables -F -t mangle
```

```
# iptables -X
```

```
# iptables -t nat -A POSTROUTING -s 192.168.20.0/24 -o eth0  
-j MASQUERADE
```

### Konfigurasi awal firewall

Langkah berikutnya adalah melakukan konfigurasi awal firewall. Untuk itu ketiklah beberapa perintah berikut:

```
# iptables -P INPUT DROP
```

```
# iptables -P FORWARD DROP
```

kedua perintah diatas menyebabkan default policy untuk chain INPUT dan FORWARD menjadi DROP

```
# iptables -A INPUT -s 192.168.20.0/24 -j ACCEPT
# iptables -A INPUT -m state --state ESTABLISHED,RELATED -j
ACCEPT
```

kedua perintah diatas menunjukkan akses ke komputer firewall yang berasal dari jaringan 192.168.20.0/24 diijinkan.

```
# iptables -N loc2net
# iptables -N net2loc
```

kedua perintah diatas menunjukkan dibuatnya dua buah chain baru yaitu chain loc2net dan net2loc

```
# iptables -A FORWARD -i eth0 -o eth1 -j net2loc
# iptables -A FORWARD -i eth1 -o eth0 -j loc2net
```

kedua perintah diatas menunjukkan bahwa traffic ip yang masuk dari eth0 dan keluar melalui eth1 akan dimasukkan ke chain net2loc. Dan traffic ip yang masuk dari eth1 dan keluar melalui eth0 akan dimasukkan ke chain loc2net.

## Konfigurasi pembatasan akses berdasarkan kuota dan waktu

Langkah terakhir adalah mengatur firewall agar melakukan pembatasan akses internet berdasarkan kuota dan waktu akses. Kebijakan pembatasannya sesuai dengan skenario yang telah disebutkan diatas.

Untuk itu buatlah rule rule firewall yang akan melakukan pembatasan akses internet berdasarkan kuota dan waktu akses dengan menggunakan perintah iptables seperti berikut :

```
# iptables -I net2loc 1 -m quota -d 192.168.20.101 --quota
100000000 -m time --timestart 8:00 --timestop 17:30 --weekdays
Mon,Tue,Wed,Thu,Fri,Sun,Sat -j ACCEPT
# iptables -I net2loc 2 -m quota -d 192.168.20.102 --quota
100000000 -m time --timestart 8:00 --timestop 17:30 --weekdays
Mon,Tue,Wed,Thu,Fri,Sun,Sat -j ACCEPT
```

Kedua perintah diatas menunjukkan traffic yang datang dari internet menuju komputer 192.168.20.101 dan 192.168.20.102 dibatasi akses internetnya berdasarkan kuota sebesar 100MB atau waktu akses yaitu senin sampai minggu mulai pukul 08:00 sampai 17:30.

```
# iptables -A net2loc -j LOG --log-prefix "QUOTA EXCEED OR TIME
EXPIRE"
```

Perintah diatas menunjukkan semua traffic yang tidak match dengan rule-rule firewall sebelumnya pada chain net2loc akan di catat dalam log (/var/log/messages) dengan log prefix "QUOTA EXCEED OR TIME EXPIRE"

```
# iptables -A loc2net -s 192.168.20.0/24 -j ACCEPT
```

Perintah diatas menyatakan bahwa semua akses internet dari jaringan 192.168.20.0/24 diijinkan.

Agar seluruh konfigurasi firewall yang telah dilakukan bersifat permanen, maka lakukan perintah berikut ini:

```
# iptables-save > /etc/iptables.cfg
```

kemudian agar setiap kali komputer firewall booting, rule rule firewall yang tersimpan dalam file /etc/iptables.cfg dijalankan secara otomatis, maka tambahkan baris perintah berikut ini kedalam file /etc/rc.local, tepatnya diatas (sebelum) baris perintah 'exit 0':

```
iptables-restore -c /etc/iptables.cfg  
exit 0
```

**Untuk** melakukan uji coba, silahkan Anda coba melakukan download file dari internet pada komputer 192.168.20.101 atau 192.168.20.102 yang berukuran lebih besar dari 100MB, atau cobalah mengakses internet pada jam sebelum 08:00 atau setelah jam 17:30. Selamat mencoba.