

Memantau Penggunaan Bandwidth dengan iptables

By Henry Saptono <boypyt@gmail.com>

Desember 2009

Anda membutuhkan tool atau software untuk memungkinkan Anda memantau total penggunaan bandwidth terutama penggunaan bandwidth internet oleh jaringan lokal Anda ? Jika Anda menggunakan linux jangan khawatir banyak sekali tool atau software untuk maksud tersebut yang dibuat oleh komunitas open source di linux, sebut saja tool seperti **bandwidthd**, **vnstat**, **netwatch**, **iftop** dan lain lain. Yang menarik bagi penulis adalah kita dapat menggunakan tool **iptables** (default terinstall) yang selama ini diketahui adalah tool untuk mensetup firewall dan *network address translation* di linux, namun dapat juga digunakan untuk memantau atau memonitor penggunaan bandwidth. Hal ini dikarenakan iptables juga menyediakan fitur melakukan penghitungan total atau jumlah packet dan byte. Hanya saja tentunya Anda harus membuat terlebih dahulu rule-rule firewall yang Anda maksudkan untuk dapat menghitung total packet dan byte yang diterima dari internet dan yang dikirim ke internet dari jaringan lokal Anda.

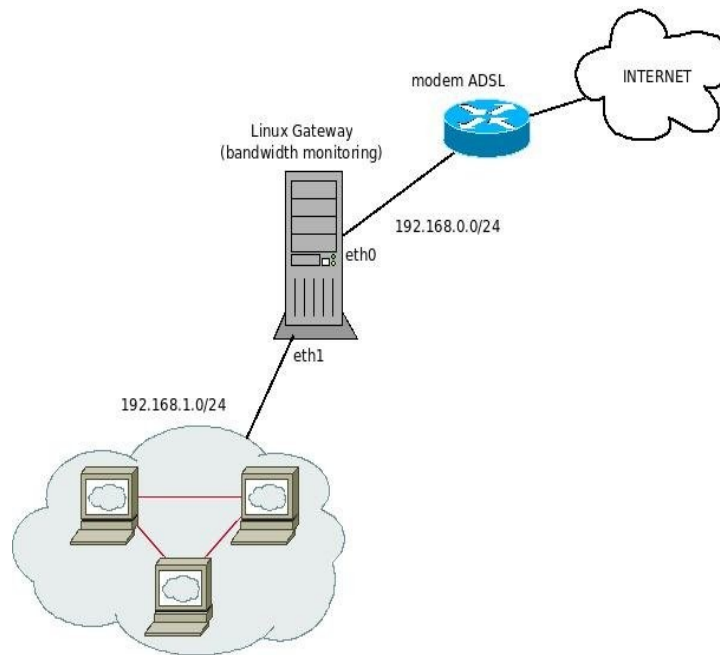
Dengan cara seperti itu maka Anda harus menggunakan sistem linux sebagai gateway atau internet connection sharing bagi jaringan lokal Anda, dan pada gateway linux tersebutlah Anda harus mensetup rule -rule firewall untuk melakukan bandwidth monitoring menggunakan iptables. Dalam artikel kali ini penulis ingin menjelaskan secara singkat bagaimana kita dapat melakukan monitoring penggunaan bandwidth internet berdasarkan service tertentu seperti HTTP, SMTP, POP3, DNS, dan SSH. Dalam artikel ini penulis menggunakan sistem linux distribusi CentOS 5.3, namun jika Anda menggunakan distribusi linux yang lainnya pada prinsipnya hampir sama.

Skenario

Untuk memudahkan penjelasan maka penulis membuat skenario sebagai berikut:

- Internet akses menggunakan broadband akses internet yaitu ADSL
- Jaringan lokal terhubung ke internet melalui sebuah komputer gateway dengan sistem operasi CentOS 5.3. Dengan kata lain sistem linux CentOS 5.3 berperan sebagai internet sharing.
- Komputer gateway linux memiliki dua buah network interface yaitu eth0 dan eth1. Dimana eth0 terhubung dengan modem ADSL (jaringan yang menuju internet), sedangkan eth1 terhubung dengan jaringan lokal. Jaringan lokal memiliki network address 192.168.1.0/24 sedangkan jaringan antara gateway dan modem ADSL adalah 192.168.0.0/24.
- Monitoring bandwidth berdasarkan services yaitu service HTTP,SMTP,POP3,DNS dan SSH. Monitoring dilakukan untuk traffic download dan upload dari jaringan lokal ke internet.

Untuk memberikan gambaran yang cukup jelas mengenai layout jaringan tersebut maka penulis membuat gambar diagram jaringan seperti tampak pada gambar-1.



Gambar-1. Diagram Jaringan

Kemudian bagaimanakah langkah langkahnya untuk menerapkan bandwidth monitoring menggunakan iptables pada komputer gateway linux tersebut. Untuk itu berikut akan dijelaskan langkah-langkahnya.

Langkah Konfigurasi

Konfigurasi gateway

Komputer gateway diasumsikan sudah dikonfigurasi jaringan untuk eth0 dan eth1 nya. Langkah konfigurasi pertama adalah mengkonfigurasi komputer linux agar berfungsi sebagai gateway atau internet sharing, yaitu dengan menjalankan perintah berikut untuk mengaktifkan ip forwarding:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
# echo "echo 1 > /proc/sys/net/ipv4/ip_forward" >> /etc/rc.local
```

Atau:

```
# sysctl -w net.ipv4.ip_forward=1
# echo "sysctl -w net.ipv4.ip_forward=1" >> /etc/rc.local
```

Atau dapat juga dengan cara mengedit file **/etc/sysctl.conf** dan set parameter **net.ipv4.ip_forward = 1**

Diasumsikan rule firewall saat ini memiliki default policy ACCEPT untuk semua jenis traffic dan belum ada chain baru yang dibuat oleh user. Langkah selanjutnya mengaktifkan nat atau ip masquerade, dengan perintah berikut:

```
# service iptables stop
# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
# service iptables save
```

```
# chkconfig iptables on
```

Jika Anda menggunakan distribusi lain terutama non keluarga redhat seperti ubuntu, gunakan perintah berikut ini untuk melakukan ip masquerade:

```
# iptables -F
# iptables -t nat -F
# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
# iptables-save > /etc/myiptables.cfg
# sed -i 's/exit 0//' /etc/rc.local
# echo "iptables-restore < /etc/myiptables.cfg" >> /etc/rc.local
# echo "exit 0" >> /etc/rc.local
```

Sampai disini komputer gateway linux baru berfungsi sebagai gateway dan internet sharing. Anda dapat melihat total penggunaan bandwidth dari internet Anda dengan perintah iptables sebagai berikut:

```
# iptables -nL -v
```

Namun perintah iptables diatas belum dapat memberikan gambaran secara rinci mengenai penggunaan bandwidth internet yang dilakukan oleh jaringan lokal.

Mendefinisikan rule firewall untuk monitoring bandwidth

Langkah berikutnya adalah membuat rule firewall untuk memungkinkan kita memantau statistik atau total penggunaan bandwidth internet yang dilakukan oleh jaringan lokal berdasarkan service tertentu sebagaimana disebutkan dalam skenario.

Langkah pertama dalam membuat rule firewall adalah membuat chain baru dengan nama "DOWNLOAD" dan "UPLOAD" seperti berikut ini:

```
# iptables -N DOWNLOAD
# iptables -N UPLOAD
# iptables -nL
```

Setelah mendefinisikan chain baru , selanjutnya mendefinisikan rule-rule firewall untuk mengklasifikasikan traffic FORWARD menjadi traffic UPLOAD dan DOWNLOAD. Langkahnya sebagai berikut:

```
# iptables -A FORWARD -s 192.168.1.0/24 -o eth0 -j UPLOAD
# iptables -A FORWARD -d 192.168.1.0/24 -i eth0 -j DOWNLOAD
```

Selanjutnya membuat rule-rule firewall untuk menyesuaikan traffic UPLOAD dan DOWNLOAD dengan service HTTP, SMTP, POP3, DNS, dan SSH, seperti berikut ini:

```
# iptables -A UPLOAD -p tcp -s 192.168.1.0/24 -dport 80
# iptables -A UPLOAD -p tcp -s 192.168.1.0/24 -dport 25
# iptables -A UPLOAD -p tcp -s 192.168.1.0/24 -dport 110
# iptables -A UPLOAD -p tcp -s 192.168.1.0/24 -dport 53
# iptables -A UPLOAD -p udp -s 192.168.1.0/24 -dport 53
# iptables -A UPLOAD -p tcp -s 192.168.1.0/24 -dport 22
```

```
# iptables -A DOWNLOAD -p tcp -d 192.168.1.0/24 -dport 80
# iptables -A DOWNLOAD -p tcp -d 192.168.1.0/24 -dport 25
# iptables -A DOWNLOAD -p tcp -d 192.168.1.0/24 -dport 110
```

```
# iptables -A DOWNLOAD -p tcp -d 192.168.1.0/24 -dport 53
# iptables -A DOWNLOAD -p udp -d 192.168.1.0/24 -dport 53
# iptables -A DOWNLOAD -p tcp -d 192.168.1.0/24 -dport 22
```

Setelah rule rule firewall dibuat jangan lupa untuk menyimpan rule yang ada dengan menjalankan perintah berikut ini:

```
# service iptables save
```

Untuk distribusi linux Ubuntu sebagai berikut:

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

Melihat penggunaan bandwidth upload dan download

Selesai melakukan konfigurasi, selanjutnya dapat kita lakukan pemantauan bandwidth.

Untuk melihat total bandwidth upload dan download perintahnya sebagai berikut:

```
# iptables -nL FORWARD -v
```

Untuk melihat rincian bandwidth download setiap service perintahnya sebagai berikut:

```
# iptables -nL DOWNLOAD -v
```

Untuk melihat rincian bandwidth upload setiap service perintahnya sebagai berikut:

```
# iptables -nL UPLOAD -v
```