Dengan berbagai metode kita dapat mengukur besar keluar-masuknya data tiap komputer dalam jaringan kita. Salah satu cara yang sederhana dan mudah dikerjakan adalah dengan menggunakan iptables dan MRTG. Iptables hanya digunakan untuk menghitung besar data yang masuk untuk tiap-tiap komputer dalam jaringan, dan hasilnya ditampilkan dengan menggunakan MRTG. Dengan begitu kita tidak perlu menginstall server snmp di tiap komputer, namun masih bisa mendapatkan gambaran umum aktifitas koneksi tiap komputer dengan jaringan lain.

Di sini diasumsikan bahwa jaringan kita beralamat 10.11.12.0/24, pengukuran dilakukan di gateway dengan alamat 10.11.12.1.

1. Instalasi

Program yang kita butuhkan di sini tidak begitu banyak, dan biasanya pada beberapa distro linux program-program ini sudah disertakan di CD. Bila tidak ada, beberapa program inilah yang harus anda download dan anda install.

1. MRTG, dapat didownload dari http://www.ee.ethz.ch/~oetiker/webtools/mrtg/
2. iptables(versi > 1.2.6), dapat didownload dari http://www.netfilter.org
3. Apache web server, dapat didownload dari http://httpd.apache.org (web server lain juga bisa)

Ikuti petunjuk instalasi yang disertakan pada tiap-tiap program, biasanya ada pada file README dan INSTALL.

2. Iptables

Untuk bisa mengetahui jumlah keluar/masuknya paket data untuk suatu komputer kita harus menghitungnya secara terpisah yaitu untuk yang masuk dan untuk yang keluar. Bila kita akan mengamati sepuluh komputer, maka setidaknya harus ada 20 rule iptables. Chain yang digunakan untuk mengamati adalah chain FORWARD.

Untuk memudahkan pengamatan & parsing nilai hitungan iptables kita dapat menambahkan masing-masing 2 chain kosong yang menjadi target rule sehingga memudahkan kita dalam

menjalankan grep, misal dengan menggunakan nama komputer yang kita beri tambahan -in dan -out.

```
root:~# iptables -N yudhistira-in
root:~# iptables -N yudhistira-out
root:~# iptables -A FORWARD -d 10.11.12.2 -j yudhistira-in
root:~# iptables -A FORWARD -s 10.11.12.2 -j yudhistira-out

root:~# iptables -N anoman-in
root:~# iptables -N anoman-out
root:~# iptables -A FORWARD -d 10.11.12.3 -j anoman-in
root:~# iptables -A FORWARD -s 10.11.12.3 -j anoman-out

root:~# iptables -N bagong-in
root:~# iptables -N bagong-out
root:~# iptables -A FORWARD -d 10.11.12.4 -j bagong-in
root:~# iptables -A FORWARD -s 10.11.12.4 -j bagong-out

root:~# iptables -nvxL FORWARD
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts  bytes target         prot opt in  out  source       destination
0     0     yudhistira-in  all  --  *   *    0.0.0.0/0    10.11.12.2
0     0     yudhistira-out all  --  *   *    10.11.12.2   0.0.0.0/0
0     0     anoman-in      all  --  *   *    0.0.0.0/0    10.11.12.3
0     0     anoman-out     all  --  *   *    10.11.12.3   0.0.0.0/0
0     0     bagong-in      all  --  *   *    0.0.0.0/0    10.11.12.3
0     0     bagong-out     all  --  *   *    10.11.12.3   0.0.0.0/0
```

Di atas dapat kita lihat bahwa kalau kita ingin mengambil besar data(dalam bytes) output iptables -nvxL FORWARD dapat kita *pipe* kan ke grep dan mengambil nilai kolom kedua dari output yang dihasilkan oleh grep.

```
root:~# iptables -nvxL FORWARD | grep bagong-in
0      0     bagong-in     all      --      *      *      0.0.0.0/0       10.11.12.3
root:~# iptables -nvxL FORWARD | grep bagong-in | awk '{print $2}'
0
```

Untuk memudahkan kita dalam memasukkan nilainya ke MRTG kita bisa membuat script kecil seperti ini:

```
#!/bin/sh
paketIN=`/sbin/iptables -nvxL FORWARD | grep &quot;$1-in&quot; | awk '{print $2}'`
paketOUT=`/sbin/iptables -nvxL FORWARD | grep &quot;$1-out&quot; | awk '{print $2}'`
echo $paketIN
echo $paketOUT
```

Pemakaiannya hanyalah dengan cara menuliskan nama scriptnya dengan 1 parameter yaitu [nama komputer], misalnya scriptbacatrafik.sh bagong. Script ini akan mencetak nilai bytes yang keluar dari jaringan kita yang berasal dari komputer "bagong". Angka ini diambil dari iptables, sehingga kata bagong atau apa pun itu harus anda sesuaikan dengan nama chain yang anda gunakan di iptables.

3. MRTG

Nilai yang dimasukkan ke mrtg haruslah berpasangan, pertama untuk in dan kedua untuk out. Nilai ini dapat diambil dari SNMP, dapat pula diambil dari nilai eksekusi program tertentu. Contoh *mrtg.cfg* yang mengambil nilai dari script yang tadi kita buat dapat dilihat di bawah ini.

```
WorkDir: /var/www/mrtg

Target[anoman]: `/usr/local/sbin/scriptbacatrafik.sh anoman`
Title[anoman]: Anoman
PageTop[anoman]: <h1>Anoman</h1>
MaxBytes[anoman]: 1250000
YLegend[anoman]: Bytes/s
ShortLegend[anoman]: B/s
LegendI[anoman]:  Traffic in
LegendO[anoman]:  Traffic out
Legend1[anoman]: Traffic in Bytes per Second

Target[bagong]: `/usr/local/sbin/scriptbacatrafik.sh bagong`
Title[bagong]: bagong
PageTop[bagong]: <h1>bagong</h1>
MaxBytes[bagong]: 1250000
YLegend[bagong]: Bytes/s
ShortLegend[bagong]: B/s
LegendI[bagong]:  Traffic in
LegendO[bagong]:  Traffic out
Legend1[bagong]: Traffic in Bytes per Second

Target[yudhistira]: `/usr/local/sbin/scriptbacatrafik.sh yudhistira`
```

```
Title[yudhistira]: yudhistira
PageTop[yudhistira]: <h1>yudhistira</h1>
MaxBytes[yudhistira]: 1250000
YLegend[yudhistira]: Bytes/s
ShortLegend[yudhistira]: B/s
LegendI[yudhistira]:  Traffic in
LegendO[yudhistira]:  Traffic out
Legend1[yudhistira]: Traffic in Bytes per Second
```

Setelah file konfigurasi selesai, jalankan indexmaker untuk membuat file index.html MRTG.

```
root:~# indexmaker /path/file/mrtg.cfg > /var/www/mrtg/index.html
```

Bila apache telah berjalan, cobalah untuk membuka *http://10.11.12.1/mrtg/* untuk melihat hasilnya.

4. Pengembangan

Dengan cara pengukuran yang persis sama anda dapat pula mengukur besarnya keluar masuk paket per layanan misal web, ftp, smb, domain, dan sebagainya. Pengukuran dilakukan dengan menggunakan iptables, hanya saja kita tidak mendefinisikan alamat IP per komputer. Yang kita definisikan adalah protokol(TCP/UDP/ICMP) beserta nomor portnya, serta network address jaringan kita seperti contoh di bawah ini.

```
root:~# iptables -N www-in
root:~# iptables -N www-out
root:~# iptables -A FORWARD -d 10.11.12.0/24 -p tcp --dport 80 -j www-in
root:~# iptables -A FORWARD -s 10.11.12.0/24 -p tcp --sport 80 -j ww-out

root:~# iptables -N ftp-in
root:~# iptables -N ftp-out
root:~# iptables -A FORWARD -d 10.11.12.0/24 -p tcp --dport 20:21 -j ftp-in
root:~# iptables -A FORWARD -s 10.11.12.0/24 -p tcp --sport 20:21 -j ftp-out
```

Contoh rule iptables di atas berguna untuk menghitung:

1. Besar paket data yang kita dapatkan dari webserver yang berasal dari luar jaringan kita.
2. Besar paket data request ke webserver di luar jaringan kita.
3. Besar paket data yang kita download melalui ftp yang berasal dari luar jaringan kita.
4. Besar paket data upload melalui ftp ke luar jaringan kita.

Edit mrtg.cfg untuk memasukkan hasil perhitungan iptables untuk kedua port yang baru.

```
Target[www]: `/usr/local/sbin/scriptbacatrafik.sh www`
  Title[www]: www
  PageTop[www]: <h1>www</h1>
  MaxBytes[www]: 1250000
  YLegend[www]: Bytes/s
  ShortLegend[www]: B/s
  LegendI[www]:  Traffic in
  LegendO[www]:  Traffic out
  Legend1[www]: Traffic in Bytes per Second

    Target[ftp]: `/usr/local/sbin/scriptbacatrafik.sh ftp`
  Title[ftp]: ftp
  PageTop[ftp]: <h1>ftp</h1>
  MaxBytes[ftp]: 1250000
  YLegend[ftp]: Bytes/s
  ShortLegend[ftp]: B/s
  LegendI[ftp]:  Traffic in
  LegendO[ftp]:  Traffic out
  Legend1[ftp]: Traffic in Bytes per Second
```

Selamat mencoba, semoga sukses. (Kamas Muhammad, http://www.sokam.or.id)

5. Referensi

1. Dokumentasi MRTG
2. Berbagai tutorial iptables
3. man iptables

Kamas Muhammad [illegible]). Terima