

Analisis Efektifitas Bandwidth Menggunakan Ipcop (Studi Kasus : Balai Besar Teknologi Energi)

Viva Arifin¹, R. Inge Fitriana²

¹Jurusan Teknik Informatika UIN Syarif Hidayatullah Jakarta; viva_arifin@uinjkt.ac.id

²Jurusan Teknik Informatika UIN Syarif Hidayatullah Jakarta; freezyfizz@gmail.com

Abstrak — Pada Balai Besar Teknologi Energi (B2TE) kerap mengalami masalah koneksi. Masalah koneksi dapat mengganggu jalannya aktifitas komunikasi. Untuk menanggulangi masalah tersebut, maka perlu adanya pengaturan bandwidth. Salah satu pengaturan bandwidth yang dapat menurunkan beban bandwidth adalah menggunakan pemakaian dua jalur modem ADSL. Pada IPCop pembatasan bandwidth menggunakan Advanced Proxy yaitu dengan download throttling. Pada B2TE total bandwidth pada jaringan antarmuka GREEN adalah 2 Mbps, kemudian dibatasi setiap host/pengguna untuk mengunduh adalah 512 Kbps. Begitu juga pada jaringan antarmuka BLUE bandwidth yang disediakan adalah 512 Kbps, dan untuk setiap pengguna dibatasi untuk mengunduh adalah 512 Kbps. Traffic shaping digunakan untuk membatasi kecepatan lajur. Maksimal kecepatan dibatasi hanya sampai 1 Mbps, sedangkan untuk mengunduh 512 Kbps. Hal ini untuk mencegah para pengguna mengunduh data secara berlebihan yang mengakibatkan pemborosan bandwidth.

Kata kunci : Bandwidth, IPCop

Abstract — At the Center for Energy Technology (B2TE) often experience connection problems. Connection problems can disrupt the communication activities. One of such problems, hence the need for bandwidth settings. One of the settings that can reduce the load of bandwidth bandwidth usage is to use two ADSL modem lines. Restrictions on bandwidth using IPCop Advanced Proxy is to download throttling. At B2TE total bandwidth on the network interface GREEN is 2 Mbps, then limited each host / user to download is 512 Kbps. So also the BLUE network interface bandwidth provided is 512 Kbps, and for each user is limited to 512 Kbps download. Traffic shaping is used to limit the speed lane. Limited to a maximum speed of 1 Mbps, while for mengunduh 512 Kbps. This is to prevent users to download data in excess resulting in wastage of bandwidth.

Keywords: Bandwidth, IPCop

1. PENDAHULUAN

Bandwidth internet di Indonesia saat ini sangatlah mahal disebabkan minimnya bandwidth internasional yang disediakan oleh pemerintah, sehingga suatu perusahaan harus dapat secara bijak menggunakan bandwidth yang tersedia dengan sebaik mungkin. Dengan bandwidth tersebut harus bisa melayani ratusan pengguna yang ingin menggunakan internet secara bersamaan. Jika tidak diatur, kemungkinan besar lalu lintas dan bandwidth akan penuh ketika digunakan oleh beberapa pengguna sekaligus, maka diperlukan suatu sistem manajemen lalu lintas dan bandwidth dengan menggunakan IPCop sebagai alatnya. IPCop adalah suatu distribusi Linux yang digunakan sebagai alat yang memiliki kemampuan untuk mengatur bandwidth dalam jaringan lokal

2. LANDASAN TEORI

a. Definisi Analisis

Analisis adalah suatu kegiatan untuk memahami seluruh informasi yang terdapat pada suatu kasus, mengetahui isu apa yang sedang terjadi, dan

memutuskan tindakan apa yang harus segera dilakukan untuk memecahkan masalah.

b. Konsep Bandwidth

Istilah *bandwidth management* sering dipertukarkan dengan istilah *traffic control*, yang dapat didefinisikan sebagai pengalokasian yang tepat dari suatu bandwidth untuk mendukung kebutuhan atau keperluan aplikasi atau suatu layanan jaringan. Istilah *bandwidth* dapat didefinisikan sebagai kapasitas atau daya tampung suatu *channel* komunikasi (medium komunikasi) untuk dapat dilewati sejumlah arus informasi atau data dalam satuan waktu tertentu. Umumnya *bandwidth* dihitung dalam satuan bit, kbit atau bps (*byte per second*). Pengalokasian *bandwidth* yang tepat menjadi salah satu metode dalam memberikan jaminan kualitas suatu layanan jaringan atau yang biasa disebut dengan istilah *Quality Of Services* (Saptono, 2010).

Bandwidth sebagai salah satu media yang menentukan performa dari suatu jaringan karena *bandwidth* merupakan media pembawa informasi. *Bandwidth* menjadi faktor batasan dalam transfer data,

hal ini dapat terjadi disebabkan kemampuan dari suatu perangkat jaringan yang tidak mendukung atau kesalahan dalam penggunaannya. Contoh : Sebuah PC memiliki NIC dengan spesifikasi 10/100 kbps, terkoneksi kedalam jaringan menggunakan media kabel UTP dan *bandwidth internet* yang dimiliki adalah sebesar 32 Kbps, dan user akan mengirim data sebesar 100 KB maka yang terjadi adalah data yang dikirim akan memakan waktu yang cukup lama untuk sampai pada komputer tujuan.

Bandwidth sebagai media yang membawa paket data dalam suatu jaringan. Transfer data yang terjadi tergantung dari jarak, waktu, dan perangkat yang digunakan, misalkan sebuah komputer desktop memiliki NIC dengan kemampuan mengirim data sebesar 100 Mbps namun bukan berarti data yang mengalir 100 Mbps. Hal ini disebut sebagai *throughput* dan dipengaruhi oleh beberapa faktor seperti : Perangkat Jaringan, Tipe atau jenis data yang mengalir, Topologi Jaringan, Jumlah pengguna dalam jaringan, Jumlah komputer, Komputer server, Kondisi power (listrik)

c. Sistem Operasi Linux Ubuntu

Ubuntu merupakan salah satu distribusi Linux yang berbasis Debian. Proyek Ubuntu resmi disponsori oleh *Canonical Ltd* yang merupakan perusahaan milik seorang kosmonot asal Afrika Selatan Mark Shuttleworth. Nama Ubuntu diambil dari nama sebuah konsep ideologi di Afrika Selatan, "Ubuntu" berasal dari bahasa kuno Afrika, yang berarti "rasa perikemanusiaan terhadap sesama manusia".

Tujuan dari distribusi Linux Ubuntu adalah membawa semangat yang terkandung di dalam Filosofi Ubuntu ke dalam dunia perangkat lunak.

Ubuntu adalah Sistem operasi lengkap berbasis Linux, tersedia secara bebas dan mempunyai dukungan baik yang berasal dari komunitas maupun tenaga ahli profesional.

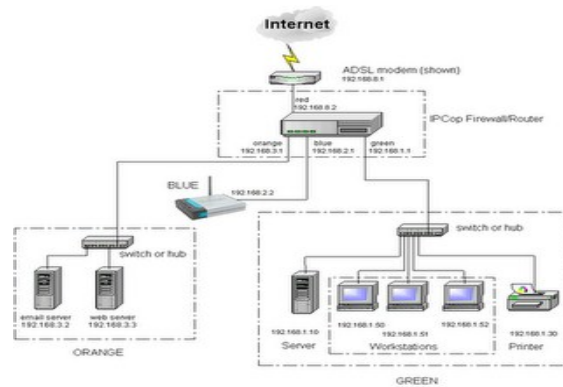
d. IPCop

IPCop adalah suatu distribusi *open source* Linux yang menyediakan fitur *simple-to-manage firewall appliance* berbasis perangkat keras PC.

IPCop juga merupakan suatu *stateful firewall* dibuat berdasarkan pada Linux *netfilter framework*. IPCop sangat sederhana, dan memiliki fitur *user-managed* atau pengaturan pengguna untuk mekanisme peningkatan keamanannya. Bahkan cenderung mudah dipahami untuk yang para pemula, dan handal untuk yang sudah berpengalaman. "The Bad Packet Stop Here" merupakan slogan yang diusung untuk menjadikan IPCop sebagai *firewall* yang handal.

e. Konfigurasi IPCop

Jaringan antarmuka atau *Network interface* IPCop terdefinisi atas empat macam yaitu RED, GREEN, BLUE dan ORANGE.

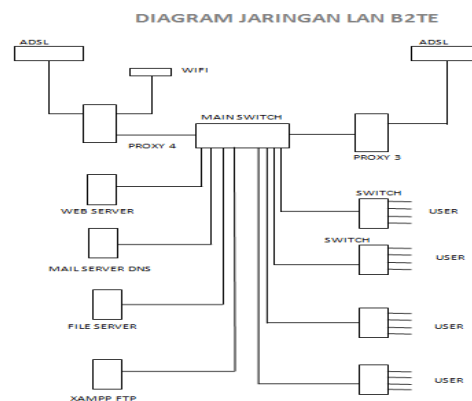


Gambar 1. Contoh Konfigurasi RED, ORANGE, BLUE, GREEN

3. IMPLEMENTASI IPCop

a. Topologi Jaringan B2TE

Jaringan di B2TE menggunakan topologi *STAR*. Sebuah *main switch* dengan kapasitas 1 GB menghubungkan 2 buah *proxy server*, *web server*, *mail server*, *file server*, *xampp* dan *ftp*. Satu port terhubung dengan sebuah konverter *fiber optic-RJ45* dan port-port lainnya terhubung dengan empat buah *switch* yang masing-masing terhubung dengan pengguna di bagian divisi berbeda di B2TE.



Gambar 2. Topologi Jaringan di B2TE

Terdapat dua jalur modem ADSL di B2TE yang masing-masing sebesar 2 MB dihubungkan dengan komputer yang berfungsi sebagai *proxy server*. *Proxy server* digunakan sebagai *gateway* atau jembatan dari terjadinya transaksi data antara *internet* (modem) dan jaringan lokal. Penggunaan *proxy server* bertujuan agar *web browser* tidak langsung mengakses halaman *web*, namun dengan *queue* atau antrian. Seperti sebuah *cache*, *proxy server* dapat menyimpan halaman *web* yang pernah diakses untuk kemudian jika ada yang mengakses halaman tersebut lagi, *web* tersebut dapat diakses dengan lebih cepat. Hal ini juga berpengaruh terhadap *bandwidth* yang digunakan, terutama disaat pemakaian pengguna yang bersamaan karena dapat menghemat pemakaian *bandwidth*. Aplikasi yang digunakan sebagai *proxy server* adalah IPCop, sebuah sistem operasi berbasis linux.

Pada Gambar 2. terhubung dengan jaringan *wi-fi*. Jaringan ini telah tersedia dan dikelola oleh kawasan

PUSPIPTEK, sehingga B2TE tidak ikut mengontrol jaringan ini.

Seorang pengguna hendak mengakses *web* B2TE dengan alamat 118.96.8.xxx port 80. Secara umum port ini akan di blok oleh *server* untuk mengurangi akses yang tidak diinginkan. Namun port tersebut beserta email dan ftp, yaitu port 443 dan 21 telah dimodifikasi pada IPCop agar dapat di akses oleh jaringan eksternal.

Keuntungan menggunakan dua jalur modem adalah *Fail Over Redudancy*, yaitu jika satu jalur down atau rusak, maka semua pengguna akan di arahkan ke jalur yang lainnya karena masih berfungsi baik. Penggunaan dua jalur ADSL ini juga bermanfaat menurunkan beban *bandwidth* dari sekian banyaknya pengguna.

b. Fitur-fitur IPCop

Untuk mengakses IPCop cukup dengan memasukkan alamat IP yang terhubung dengan jaringan antarmuka GREEN atau *hostname* dari IPCop *server*, yaitu port 445 (menggunakan *https/secure*) atau 81 (dialihkan ke 445). Untuk akses IPCop di B2TE telah dimodifikasi portnya, sehingga menjadi <https://118.96.8.xxx:4445>.

Untuk mengganti port tersebut menggunakan *command line*:

```
$/usr/local/bin/setreservedports 4445
```



Gambar 3. Tampilan Home IPCop

c. Tampilan Fitur-fitur IPCop

1. SSH Client (Gambar 4)

Memperbolehkan IPCop diakses dari jaringan eksternal. Jika fitur ini diaktifkan, maka IPCop akan dapat diakses secara *remote* dari jaringan luar. Pada gambar 4, *Port default* untuk *SSH Client* IPCop adalah 222.

2. Services (Gambar 5)

Pada gambar 5, menampilkan layanan apa saja yang sedang berjalan dan yang tidak berjalan beserta besarnya pemakaian layanan pada jaringan lokal B2TE.

3. Memory/swapfile (Gambar 6)

Pada gambar 6, menampilkan besar, ukuran, dan pemakaian RAM *cache* dan *Swap* pada IPCop.

4. Disk Usage (Gambar 7)

Menampilkan besar penggunaan ruang penyimpanan pada IPCop. Pada gambar 7, memperlihatkan alat penyimpanan /dev/root yang diakses dari /(root) dengan kapasitas 8084 MB telah terpakai 6009 MB, sehingga persentase menjadi 76% pemakaian.

5. Routing Table (Gambar 8)

Pada gambar 8 terlihat daftar tabel *routing* yang masuk melewati IPCop

6. Tabel ARP (Gambar 9)

Pada gambar 9, mengidentifikasi *MAC address* dari *host* tujuan untuk menghubungkan jaringan lokal dengan jaringan luar.

7. Traffic Graph (Gambar 10)

Menunjukkan grafik dari lalu lintas masuk dan keluar. Setiap jaringan antarmuka masing-masing ditampilkan terpisah. Setiap gambar menampilkan grafik lalu lintas per hari, minggu, bulan dan tahun dengan mengklik gambar tersebut. Pada gambar 10, menunjukkan grafik lalu lintas pemakaian per hari yang mulai meningkat dari pukul 8.00 hingga 20.00.

8. Proxy Graph (Gambar 11)

Menampilkan lalu lintas melalui layanan *proxy* IPCop. Informasi yang ditampilkan berguna untuk melihat apakah ukuran *proxy* sesuai dengan beban yang berjalan. Pada gambar 11, memperlihatkan informasi berupa tanggal dan waktu grafik dibuat, durasi analisis, kecepatan, tanggal dan waktu mulai dan berhenti grafik, dan domain

9. Connections Menu (Gambar 12)

IPCop menggunakan Linux Netfilter atau fasilitas *IPTables firewall* untuk memelihara *firewall* tetap terjaga, yang berguna menelusuri koneksi yang menuju dan berasal dari seluruh alamat jaringan antarmuka IP, berdasarkan tujuan dan asal alamat IP dan port, sebagaimana status dari koneksi itu sendiri. Pada gambar 12, menunjukkan protokol yang digunakan, sumber dan tujuan berakhirnya paket. Untuk melihat DNS lookup klik pada sebuah alamat IP.

10. Dialup (Gambar 13)

Digunakan jika akses *internet* menggunakan modem analog, ISDN atau koneksi DSL. B2TE menggunakan jalur Speedy sebagai koneksi *internet*. Fitur *Dialup* memindahkan *dial up* dari modem Speedy ke dalam IPCop agar memudahkan koneksi akses eksternal. Disebut juga dengan PPPoE.

Keterangan pada gambar 13, [a] Inisiasi layanan ISP yang digunakan adalah Speedy, [b] Untuk memindahkan *dialup* ke IPCop masukkan nama pengguna dari Speedy beserta *password* yang telah mereka berikan, gunakan metode PAP or CHAP, [c] lalu masukkan DNS primer dan sekunder dari Speedy tersebut

11. Hostname (Gambar 14).

Pada DNS *proxy* di IPCop kita dapat memasukkan nama-nama *host* yang ingin kita monitor secara manual dalam jaringan lokal. Bisa berupa perangkat lokal atau perangkat *internet* yang ingin kita ambil alih. Pada gambar 14, terdapat daftar alamat IP beserta *hostname* serta domain yang telah dibuat oleh B2TE yang di monitor sendiri oleh B2TE.

12. Traffic shaping (Gambar 15)

Mengizinkan kita untuk memberi prioritas pada perpindahan lalu lintas IP melalui *firewall*, atau

disebut juga dengan *WonderShaper* yang dibuat untuk memperkecil waktu jeda ketika melakukan ping, memastikan SSH merespon dengan baik ketika dalam keadaan sedang mengunduh ataupun sedang mengunggah. Pada Gambar 15, kecepatan *downlink* dibatasi hingga 1024 kbit/sec sedangkan kecepatan *uplink* dibatasi hingga 512 kbit/sec.

13. *Advanced proxy* (Gambar 16)
Sebuah *add-ons* atau fitur tambahan untuk menggantikan fitur bawaan IPCop yaitu *Web Proxy server*. *Proxy server* akan membuat *cache* dari halaman *internet* yang pernah dibuka sebelumnya, sehingga jika ada 3 komputer mengakses halaman *web* yang sama maka hanya dibutuhkan satu paket yang ditransfer dari *internet*. Hal ini dapat menghemat *internet* akses di jaringan B2TE. Pada gambar 16, hanya diaktifkan pada lajur jaringan GREEN yaitu jaringan lokal. Port dan *email* admin perlu diisi agar mudah menangani jika terjadi masalah.
14. *Cache management* (Gambar 17)
Pada gambar 17 untuk menentukan besar ruang *disk memory* dan *harddisk* yang dipakai untuk penyimpanan halaman *web cache* pada *Advanced Proxy*.
15. *Time Restriction* (Gambar 18)
Admin dapat membatasi pemakaian *internet* pada hari dan jam tertentu dengan mencentang hari dan jam yang ingin ditentukan dengan *Time Restriction*. Pada gambar 18, akses 24 jam setiap hari tanpa transfer limit (batasan transfer) namun ada pembatasan mengunduh untuk jaringan GREEN sebesar 2048 kbit/s dan jaringan BLUE 512 kbit/s.
16. *URL filter* (Gambar 19)
Digunakan untuk memblokir tema dari situs-situs yang tidak ingin para pengguna untuk dapat mengaksesnya. Pada gambar 19, dengan mencentang tema yang dipilih seperti porno, edukasi dewasa dan jual-beli.
17. *URL Filter Access Control* (Gambar 20)
Jika ada pengguna yang mencoba mengakses situs-situs yang tidak diijinkan akan keluar pesan seperti pada gambar 20.
18. *Port forwarding* (Gambar 21)
Router berbasis NAT seperti IPCop menolak semua permintaan data yang berasal langsung dari *internet*. Hal ini untuk menjaga LAN komputer tetap aman dari akses yang tidak diinginkan. Di B2TE terdapat beberapa layanan lokal seperti *web server*, *FTP server*, *mail server*, *File server*. *Port forwarding* meneruskan permintaan untuk layanan *internet* yang telah ditentukan, misalnya *web server* kepada mesin atau PC tertentu pada jaringan. Akses *internet* menjadi aman dan lebih mudah dikontrol. Pada gambar 21, menunjukkan port-port yang akan boleh diteruskan beserta alamat tujuannya.
19. *Proxy logs* (Gambar 22)
Pada gambar 22, menampilkan file-file yang telah dibuat *cache* dari *web proxy server*
20. *Firewall logs* (Gambar 23)

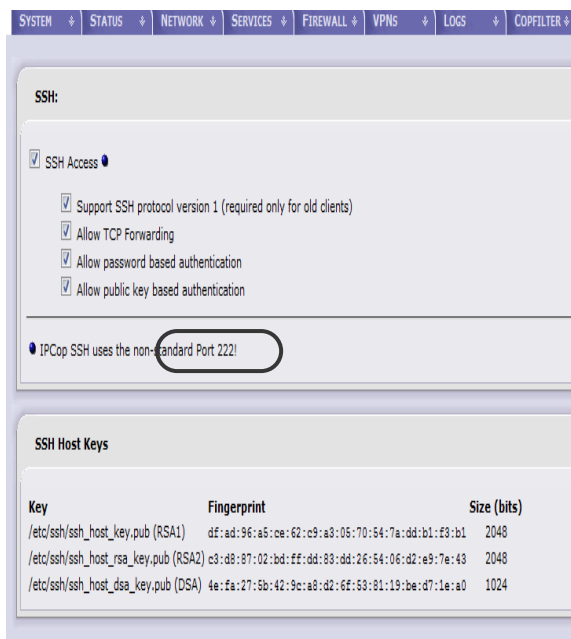
Pada gambar 23, menampilkan paket data yang diblok oleh IPCop *firewall*, waktu kejadian, IP sumber dan IP tujuan, port tujuan, dan protokol yang digunakan paket tersebut.

21. *URL Filter logs* (Gambar 24)
22. *System logs* (Gambar 25)
Kita dapat melihat catatan sistem. Setiap kategori dapat dilihat pada menu dropdown:
[1]. IPCop – tampilan standar IPCop seperti profil data PPP dan sambungan terhubung atau terputus dari modem *dialup*.
[2]. RED – lalu lintas yang melewati tampilan tersebut yang membawa PPP kepada IPCop. Termasuk didalamnya data string yang dikirim, dan yang diterima dari modem dan jaringan antarmuka lainnya. Merupakan sumber yang sangat berguna ketika situasi gagal tersambung.
[3]. DNS – menampilkan log aktifitas *dnsmasq*, bagian dari layanan penyedia domain.
[4]. *DHCP server* – menampilkan log aktifitas *DHCP server* pada IPCop.
[5]. SSH – menampilkan rekaman pengguna yang *log in* dan *log out* IPCop *server* lewat jaringan via antarmuka SSH.

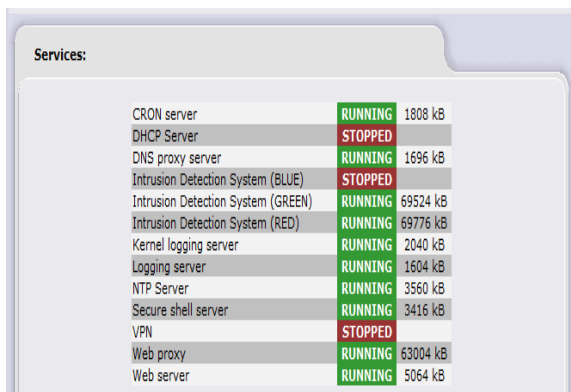
4. ANALISIS PEMAKAIAN BANDWIDTH

1. Terbatasnya sumber *bandwidth* yang dimiliki B2TE, maka dibutuhkan suatu pengaturan dari penggunaan *bandwidth* tersebut. IPCop sebagai OS *Router* digunakan untuk membantu melakukan pengaturan penggunaan pengguna *bandwidth* dan sebagai alat pengawas lalu lintas penggunaan pengguna *bandwidth*. IPCop diharapkan dapat memberikan informasi kepada *administrator* dalam pengaturan penggunaan *bandwidth*.
2. Pada B2TE pemakaian *bandwidth* dapat dilihat pada menu Status – *Traffic Graph*.
Pada gambar 26, contoh lalu lintas pemakaian *bandwidth* di B2TE.
[a]. Warna biru menandakan lalu lintas yang masuk dalam byte per detik. Lalu lintas terbesar terjadi antara jam 10.00 hingga jam 20.00.
[b]. Warna hijau menandakan lalu lintas yang masuk.
3. Pada gambar 27, adalah tampilan lalu lintas per minggu, bulan, dan tahun 2011. Menunjukkan besarnya *bandwidth* yang terpakai selama berlangsung, dan pemakaian terbesar hingga 300 Kbps.
4. Pada gambar 28, Tampilan GREEN *Traffic* per tahun
5. Pada gambar 29, TCP Access Grafik *Proxy*, menunjukkan tampilan pemakaian grafik di B2TE.
6. Pada gambar 30, TCP Transfer dan Rata-rata Durasi Grafik *Prox*. Keterangan dari Gambar 30 pemakaian akses TCP beserta *cache* yang dihasilkan. Dari sini terlihat pemakaian *bandwidth* yang efektif. Kemudian gambar dibawah transfer TCP dan total durasi pemakaian keseluruhan TCP yang berjalan pada B2TE.

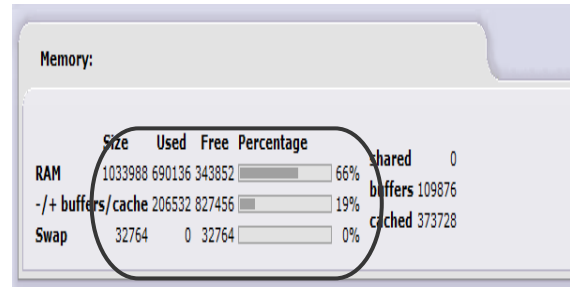
7. Pada gambar 31 *Download Throttling*, Pembatasan *bandwidth* dapat dilihat pada menu *Advanced Proxy* di bagian *download throttling* seperti pada Gambar 31 Pada B2TE total *bandwidth* pada jaringan antarmuka GREEN adalah 2 Mbps, kemudian dibatasi setiap *host/pengguna* untuk mengunduh adalah 512 Kbps. Begitu juga pada jaringan antarmuka BLUE *bandwidth* yang disediakan adalah 512 Kbps, dan untuk setiap pengguna dibatasi untuk mengunduh adalah 512 Kbps.
8. Pada gambar 32 *Traffic shaping*, maksimal kecepatan dibatasi hanya sampai 1 Mbps, sedangkan untuk mengunggah 512 Kbps. Hal ini untuk mencegah para pengguna mengunduh data secara berlebihan yang mengakibatkan pemborosan *bandwidth*.



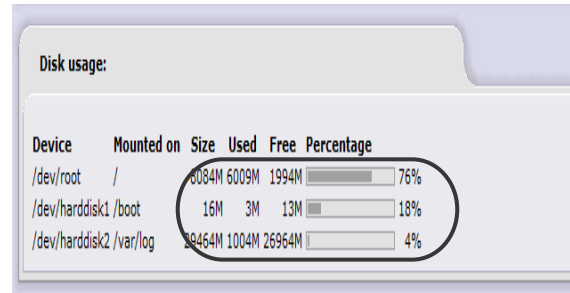
Gambar 4. SSH Client yang diaktifkan



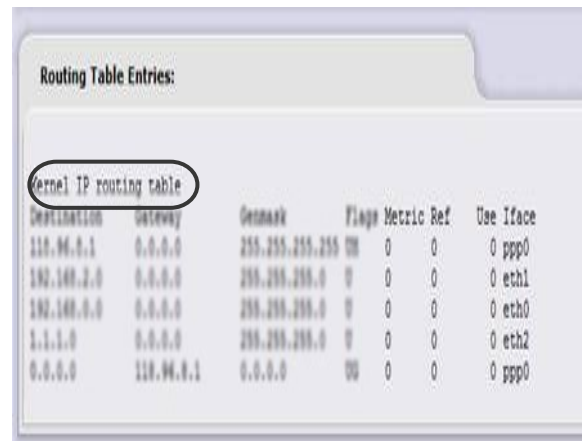
Gambar 5. Services yang berjalan pada IPCop B2TE



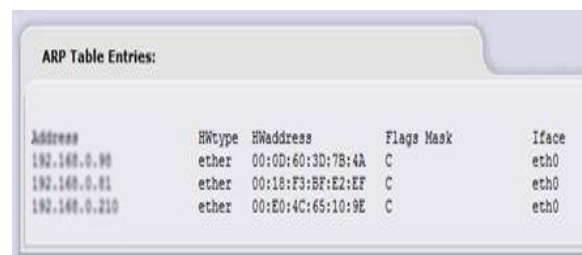
Gambar 6. Pemakaian memory pada menu



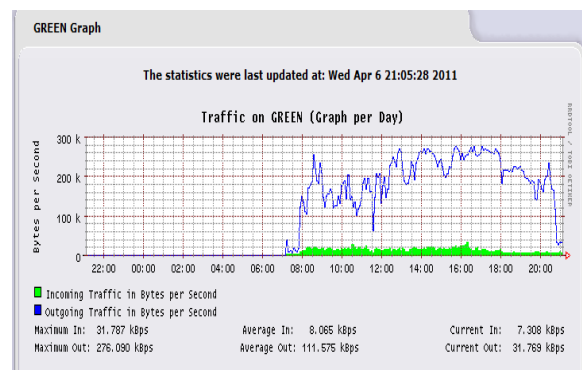
Gambar 7. Disk Usage



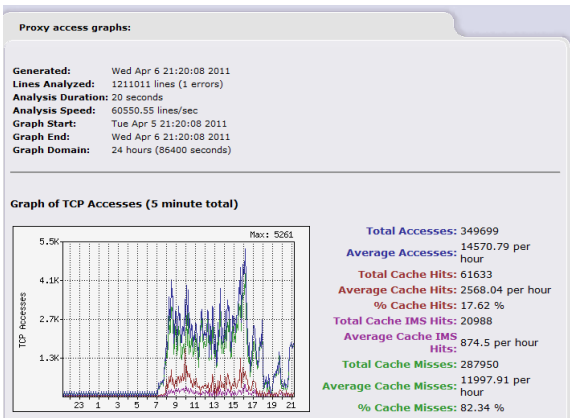
Gambar 8. Routing Table



Gambar 9. ARP Table Entries



Gambar 10. Grafik Lalu lintas per hari



Gambar 11. Grafik Proxy

Current hosts:

Host IP address	Hostname	Domain name	Action
192.168.0.9	b2te	bppt.go.id	<input checked="" type="checkbox"/>
192.168.0.9	kamera	b2te.bppt.go.id	<input checked="" type="checkbox"/>
192.168.0.8	mail	b2te.bppt.go.id	<input checked="" type="checkbox"/>
192.168.0.9	pinjam	b2te.bppt.go.id	<input checked="" type="checkbox"/>
192.168.0.9	putaka	b2te.bppt.go.id	<input checked="" type="checkbox"/>
192.168.0.9	repo	b2te.bppt.go.id	<input checked="" type="checkbox"/>
192.168.0.2	server/b2te	local	<input type="checkbox"/>
192.168.0.9	time	b2te.bppt.go.id	<input checked="" type="checkbox"/>
192.168.0.9	webserver	b2te.bppt.go.id	<input checked="" type="checkbox"/>
192.168.0.9	www	b2te.bppt.go.id	<input checked="" type="checkbox"/>

Legend: Enabled (click to disable) Disabled (click to enable) Edit Remove

Gambar 14. Hostname

Legend: LAN INTERNET DMZ Wireless IPCop VPN

Protocol	Expires (Secs)	Connection Status	Original Source IP:Port	Original Dest. IP:Port	Expected Source IP:Port	Expected Dest. IP:Port	Marked	Use
udp (17)	27		0.0.0.0:68	255.255.255.255:67	255.255.255.255:67	0.0.0.0:68	(UNREPLIED)	1
tcp (6)	17	TIME_WAIT	118.96.8.238:41179	79.140.171.9:80	79.140.171.9:80	118.96.8.238:41179	(ASSURED)	1
tcp (6)	25	TIME_WAIT	118.96.8.238:41178	79.140.171.9:80	79.140.171.9:80	118.96.8.238:41178	(ASSURED)	1
tcp (6)	26	TIME_WAIT	118.96.8.238:41179	79.140.171.9:80	79.140.171.9:80	118.96.8.238:41179	(ASSURED)	1
tcp (6)	23	TIME_WAIT	118.96.8.238:41183	79.140.171.9:80	79.140.171.9:80	118.96.8.238:41183	(ASSURED)	1
tcp (6)	105	TIME_WAIT	118.96.8.238:41087	79.140.171.9:80	79.140.171.9:80	118.96.8.238:41087	(ASSURED)	1

Gambar 12. Connections Menu

Settings:

Traffic Shaping

Downlink speed (kbit/sec): 1024

Uplink speed (kbit/sec): 512

Save

Add service

Priority: Medium Port: Protocol: TCP Enabled:

Add

Traffic shaping services

Priority	Port	Protocol	Action
High	3128	tcp	<input checked="" type="checkbox"/>
Medium	21	tcp	<input checked="" type="checkbox"/>

Gambar 15. Traffic shaping

Profiles: Profile: 1. Speedy Select Delete Restore

Connection: Interface: PPPoE Refresh
 USB: usb-ohci
 Idle timeout (mins, 0 to disable): 0
 Connect on IPCo restart: Connection debugging:

Reconnection: Manual Persistent Dial on Demand
 In case reconnection fails, switch to profile: 1. Speedy
 Dial on Demand for DNS: Maximum retries: 10
 Holdoff time (in seconds): 30

Additional PPPoE settings: Service name: Speedy Concentrator name: Speedy

Authentication: User name: 123456789012@server Password: ***** Script name: Method: PAP or CHAP

DNS: Automatic Manual
 Primary DNS: 202.130.196.155 Secondary DNS: 202.134.0.155
 Profile name: Speedy Save

Legend: This field may be blank.

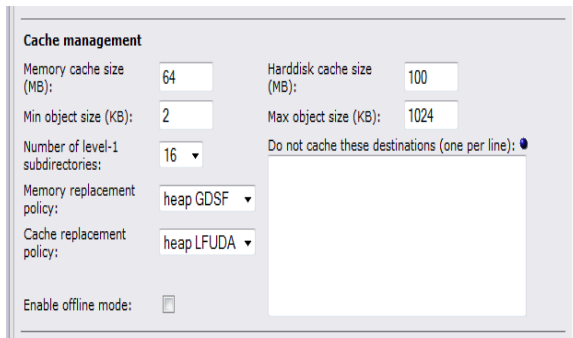
Gambar 13. Dialup

advanced web proxy modification LUSCA_HEAD

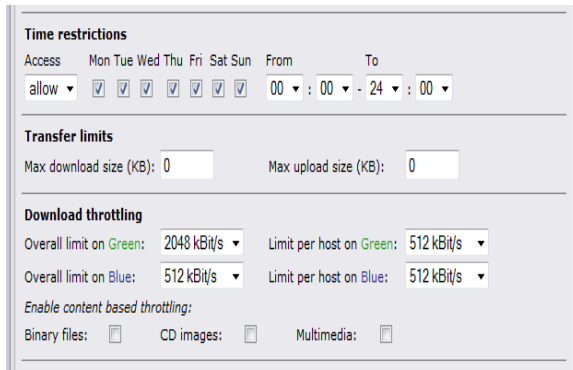
Common settings

Enabled on Green: Proxy port: 3128
 Transparent on Green: Visible hostname: Proxy3
 Enabled on Blue: Cache administrator: admin@b2te.bppt.go.id
 Transparent on Blue: e-mail: Error messages language: English
 Suppress version information: Error messages design: IPCop
 Squid Cache version: [LUSCA_HEAD Build by KEBLUX]

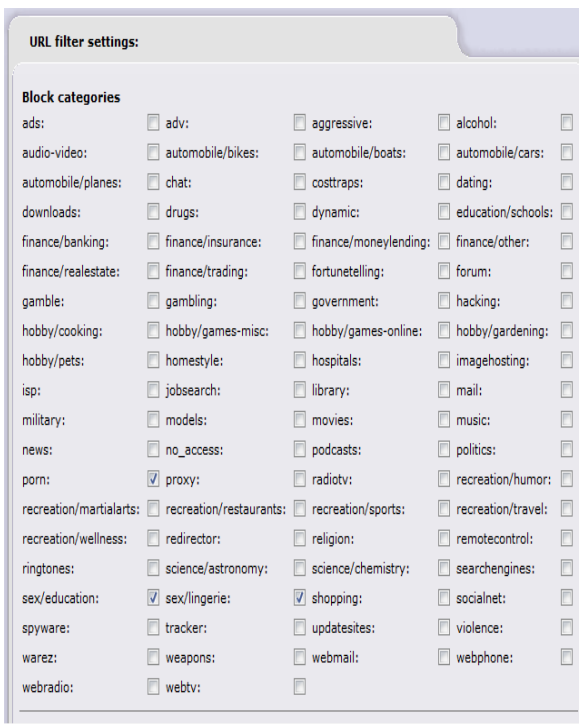
Gambar 16. Advanced Proxy



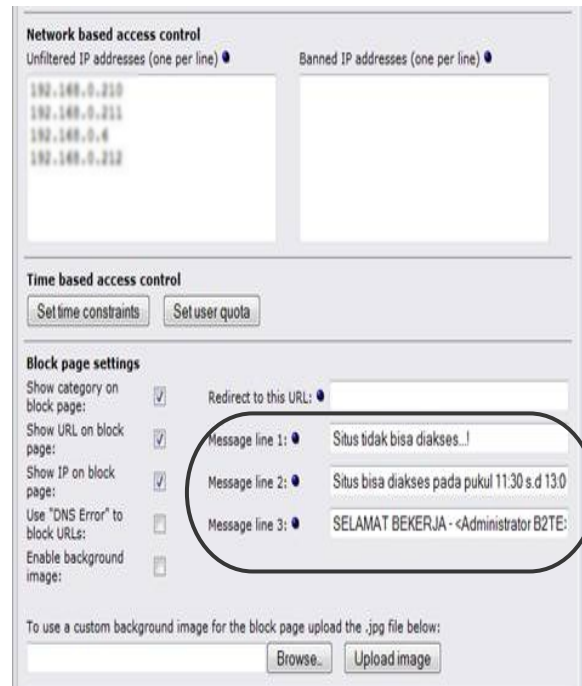
Gambar 17. Cache Management



Gambar 18. Time Restriction



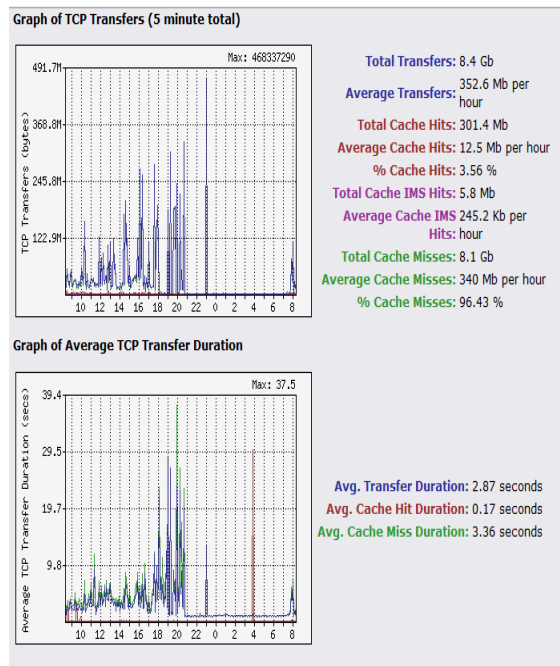
Gambar 19. URL Filter Setting



Gambar 20. URL Filter Access Control



Gambar 21. Port forwarding



Gambar 28. TCP Transfer dan Rata-rata Durasi Grafik Proxy

Time restrictions

Access: allow
 Mon: Tue: Wed: Thu: Fri: Sat: Sun:
 From: 00:00 To: 24:00

Transfer limits

Max download size (KB): 0 Max upload size (KB): 0

Download throttling

Overall limit on Green: 2048 kBit/s Limit per host on Green: 512 kBit/s
 Overall limit on Blue: 512 kBit/s Limit per host on Blue: 512 kBit/s

Enable content based throttling:
 Binary files: CD images: Multimedia:

Gambar 29. Download Throttling

Settings:

Traffic Shaping
 Downlink speed (kbit/sec): 1024
 Uplink speed (kbit/sec): 512

Add service

Priority: Medium Port: Protocol: TCP Enabled:

Traffic shaping services

Priority	Port	Protocol	Action
High	3128	tcp	<input checked="" type="checkbox"/> <input type="checkbox"/>
Medium	21	tcp	<input checked="" type="checkbox"/> <input type="checkbox"/>

Gambar 30. Pembatasan Download pada Traffic shaping

- Keunggulan dari IPCop yang utama adalah *Port Forwarding*, dimana dengan ini seorang admin dapat mengakses jaringan lokal dari jaringan eksternal.
- Untuk lebih menjamin keamanan, *monitoring* dan efektifitas pembagian *bandwidth internet* maka bisa dirancang mekanisme pengaksesan *internet* melalui *tunnel* khusus seperti VPN atau lainnya.
- Bisa dikembangkan *web interface* kondisi lalu lintas dan penggunaan *bandwidth internet* secara umum agar pengguna bisa melihat dan memantau kondisi jaringan. Hal ini dimaksudkan untuk memberikan informasi kepada pengguna tentang ada waktu kapan jaringan penuh sehingga diharapkan bisa merubah pola atau waktu pengaksesan *internet* oleh pengguna.

DAFTAR PUSTAKA

- Dempster, Barrie, 2006, *Configuring IPCop Firewalls*, Published by Packt Publishing
- Geier, Jim. 2005, *Wireless Networks First-Step*, ANDI Yogyakarta, Jakarta
- Jhonsen, Jhon Edison, 2005, *CCNA : Membangun Wireless LAN*, PT Elex Media Komputindo, Jakarta
- Kurniawan, Davit, 2008, *TCP/IP Bagian 1*, Prasimax Technology Development Center, Jakarta
- Mulyana, Edi S. 2005, *Pengenalan Protokol Jaringan Wireless Komputer*, ANDI Yogyakarta, Jakarta
- Poerwo, Doddy, 2005, *Aplikasi Manajemen Bandwidth Akses Internet Pada Local Area Network*, Tugas Akhir STT Telkom, Bandung.
- Purbo, Onno W dan Taufan, Riza, 2002, *Manajemen Jaringan TCP/IP*, Elex Media Komputindo, Jakarta
- Rangkuti, 2005, *Jaringan Komputer*, LSP Telematika, Jakarta
- <http://www.ipadd.de/binary-v14.html>, (akses : 15 April 2011)
- <http://www.ipcop.org/index-pn.php>, (akses : 18 April 2011)

5. KESIMPULAN

- IPCop sebagai manajemen sumber *bandwidth* mampu memberikan jaminan kepada pengguna untuk mendapatkan sumber *bandwidth* yang sesuai dengan kebutuhan *bandwidth* B2TE.