Jurnal Sarjana Teknik Informatika
Volume 3 Nomor 1, Februari 2015
e-ISSN: 2338-5197

ANALISIS PERANCANGAN FIREWALL PAKET FILTERING DAN PROXY SERVER UNTUK OPTIMASI BANDWIDTH (Studi Kasus di Lab Riset Universitas Ahmad Dahlan Kampus 3)

[1]Yanuar Dwi Jatmiko Wismoaji, [2]Imam Riadi

[1]Program Studi Teknik Informatika
[2]Program Studi Sistem Informasi
Universitas Ahmad Dahlan
Prof. Dr. Soepomo, S.H., Janturan, Umbulharjo, Yogyakarta 55164
[1]Email: yanuarjunetz@gmail.com
[2]Email: imam_riadi@uad.ac.id

ABSTRAK

Masalah keamanan menjadi salah satu aspek penting dari sebuah jaringan komputer. Pada jaringan di laboratorium riset UAD ditemukan beberapa masalah antara lain adanya situs yang mengandung pornografi yang masih dapat diakses di laboratorium riset UAD dan kecepatan akses yang belum dibatasi pada download file selain digunakan untuk kegiatan praktikum. Berdasarkan permasalahan tersebut, jaringan laboratorium riset UAD perlu dibangun sistem yang dapat memblokir situs-situs yang tidak berhubungan dengan praktikum yang memakan data besar dan juga mampu membatasi kecepatan akses download file, sehingga penggunaan bandwidth dapat dioptimalkan.

Tahapan dalam penelitian ini terbagi menjadi beberapa langkah yang terdiri dari pengumpulan data, analisis kondisi saat ini, perancangan arsitektur firewall, implementasi, pengujian dan rekomendasi. Tahapan pembangunan sistem terdiri dari perancangan topologi jaringan yang digunakan, perancangan firewall paket filtering dan manajemen bandwidth yang menggunakan squid dan IPTables. Pengujian sistem dilakukan dengan uji kelayakan pada saat sebelum dan sesudah diterapkannya firewall dan proxy server.

Berdasarkan hasil pengujian menggunakan metode uji kelayakan pada sistem didapatkan hasil bahwa sebanyak 78% responden menyatakan setuju, 20% menyatakan sangat setuju dan 2% menyatakan kurang setuju. Kesimpulan yang didapat dari hasil pengujian tersebut, bahwa firewall paket filtering yang diterapkan mampu memblokir situs pornografi yang masih dapat diakses serta manajemen bandwidth yang diterapkan dapat mengontrol penggunaannya jadi lebih optimal untuk praktikum.

Kata Kunci: Jaringan, Firewall, Paket Filtering, Optimasi, Bandwidth, Proxy Server

 e-ISSN: 2338-5197

1. PENDAHULUAN

Masalah keamanan termasuk dalam salah satu aspek penting dari sebuah sistem informasi, seperti pada jaringan komputer.Terhubungnya LAN (*Local Area Network)* atau komputer ke Internet membuka potensi adanya lubang keamanan *(security hole)* yang membuka celah untuk merusak kinerja sistem. Instansi pendidikan saat ini menggunakan laboratorium sebagai sarana pendidikannya seperti halnya laboratorium riset UAD. Pada laboratorium riset UAD diterapkan jaringan untuk media praktikum bagi mahasiswa.

Masalah keamanan seringkali menjadi permasalahan utama pada jaringan komputer khususnya pada laboratorium riset UAD. Permasalahan yang ada di antaranya ditemukannya beberapa situs pornografi yang masih dapat diakses dan belum adanya pembatasan *bandwidth* pada *download* file selain yang digunakan untuk praktikum sehingga penggunaannya belum optimal. Berdasarkan masalah tersebut, maka dilakukan suatu penelitian untuk memblokir situs *pornografi* dan memanajemen penggunaan *bandwidth*.

2. KAJIAN PUSTAKA

Berdasarkan penelitian yang dilakukan oleh Riko, 2010, Teknik Informatika, Universitas Ahmad Dahlan Yogyakarta. Menjelaskan sistem yang dibangun menggunakan *firewall layer* 7 dan *traffic shaping* untuk membangun manajemen *bandwidth* dengan judul : implementasi *firewall* menggunakan layer 7 protokol untuk manajemen *bandwidth* [1].

Penelitian yang dilakukan Alfin Hikmaturokhman, 2010, Teknik Informatika, Sekolah Tinggi Telkom Bandung. Menjelaskan sistem yang dibangun menggunakan metode *traffic filtering* yang dapat mengijinkan ataupun menolak *traffic* data yang masuk dengan judul : analisis perancangan dan implementasi *firewall*dan *traffic filtering* menggunakan CISCO *router* [2].

Penelitian yang dilakukan Ariefati Wiratama, 2010, Teknik Informatika, Universitas Islam Negeri Syarif Hidayatullah Jakarta. Menjelaskan sistem yang dibangun menggunakan *statefull firewall* dengan arsitektur *dual-homed host* yang menggunakan dua alamat IP dan dua *interface* dengan judul : penerapan *statefull firewall* pada arsitektur *dual-homedhost* [3].

Penelitian yang dilakukan Friza Rahmat, 2010, Sistem Informasi, Sekolah Tinggi Manajemen Informatika dan Komputer Amikom Yogyakarta. Menjelaskan sistem yang dibangun menggunakan *delay pools* untuk manajemen *bandwidth* pada *download* file dengan ekstensi tertentu dan *streaming* video dengan judul : membangun manajemen *bandwidth wireless* menggunakan *squid delay pools* [4].

2.1 Firewall

Firewall digunakan untuk melindungi, dengan cara menyaring, membatasi atau bahkan menolak suatu atau semua hubungan segmen pada jaringan pribadi dengan jaringan luar yang bukan bagian ruang lingkupnya yang diterapkan baik terhadap *hardware*, *software* ataupun sistem itu sendiri. *Firewall* paket *filtering* termasuk salah

 e-ISSN: 2338-5197

satu jenis teknologi keamanan yang digunakan untuk mengatur paket-paket apa saja yang diizinkan masuk ke dalam sistem atau jaringan dan paket-paket apa saja yang diblokir [5].

2.2 Algoritma KMP (Knuth-Morris-Pratt)

Algoritma *Knuth-Morris-Pratt* termasuk dalam algoritma pencarian *string* yang mencari dengan cara menghitung dimulai dari ketidakcocokan ditemukan, berdasarkan hasil tersebut akan dihitung awal pencarian selanjutnya pada letak karakter berikutnya. Algoritma ini termasuk jenis *Exact String Matching Algorithm* yang melakukan pencocokan *string* secara tepat berdasarkan urutan dan susunan karakter dalam *string* [6].

2.3 *Bandwidth* dan Manajemen *Bandwidth*

Bandwidth diartikan sebagai kapasitas atau daya tampung kabel *ethernet* agar dapat dilewati trafik paket data dalam jumlah tertentu. *Bandwidth* juga bisa berarti jumlah konsumsi paket data per satuan waktu dinyatakan dengan satuan *bit per second* (bps). *Bandwidth Management* digunakan untuk *management* dan mengoptimalkan berbagai jenis jaringan dengan menerapkan layanan *Quality Of Service* (QoS) untuk menetapkan tipe-tipe lalu lintas jaringan [7].

2.4 Squid

Squid termasuk salah satu program *proxy server* yang dapat mengimplementasikan *caching* untuk beberapa protokol aplikasi Internet seperti HTTP, FTP, dan Gopher, sedangkan *proxy server* berguna untuk menjembatani klien dengan *server gateway* sebelum berkomunikasi dengan Internet. *Delay pools* digunakan untuk membatasi *bandwidth* yang dikonsumsi klien, *delay pools* juga termasuk opsi untuk menspesifikasikan banyaknya jumlah *pool* yang digunakan untuk membatasi jumlah *bandwidth* dari ACL tertentu [8].

3. METODE PENELITIAN

3.1 Metode Pengumpulan Data
3.1.1 Studi Observasi

Metode pengumpulan data dilakukan dengan pengamatan secara langsung pada jaringan laboratorium riset UAD mengenai kinerja jaringannya dari *bandwidth* yang digunakan serta akses situs web.

3.1.2 Metode *Interview*

Metode pengumpulan data melakukan wawancara langsung kepada narasumber dengan mengajukan pertanyaan mengenai *bandwidth* dan hak akses situs web.

 e-ISSN: 2338-5197

3.1.3 Studi Literatur

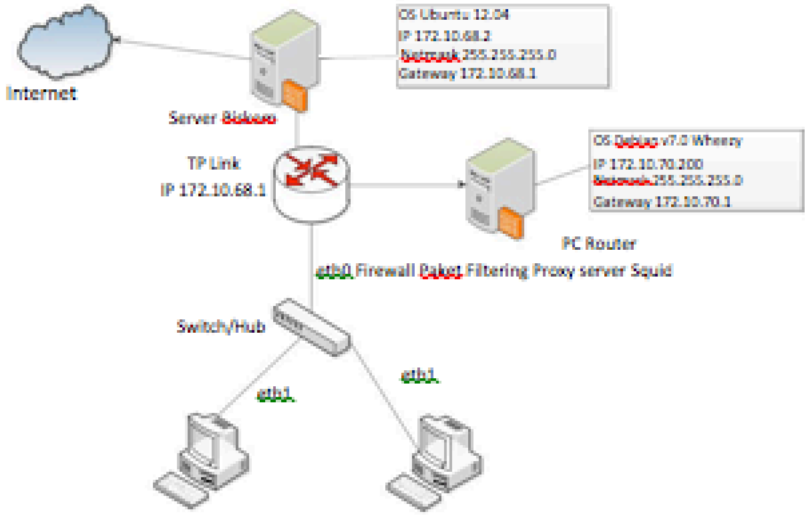
Metode pengumpulan data pada studi pustaka yang dilakukan dengan mencari, membaca dan mengumpulkan dokumen sebagai referensi seperti buku, artikel dan literatur.

4. HASIL DAN PEMBAHASAN

4.1 Perancangan Sistem

4.1.1 Perancangan Arsitektur *Firewall* Paket *Filtering*

Arsitektur *firewall* ini terdiri dari klien dan *server*, klien terdiri dari komputer yang ada di laboratorium riset UAD dan Biskom UAD yang bertindak sebagai *server*. Klien akan dihubungkan dengan *router* yang telah diimplementasikan *firewall* paket *filtering* dan manajemen *bandwidth delay pools* yang penggambaran arsitekturnya dapat dilihat pada Gambar 1.



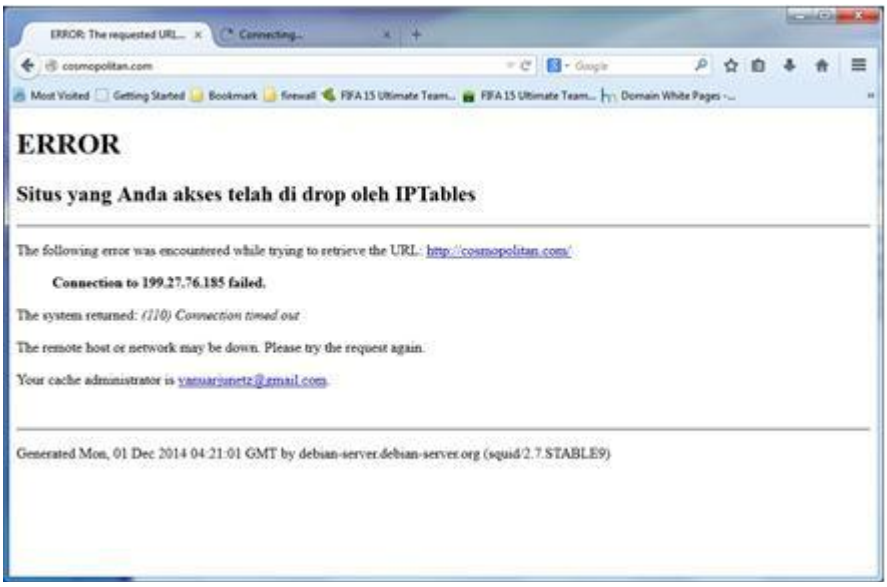
Gambar 1 Perancangan arsitektur *firewall*

4.2 Implementasi

4.2.1 Firewall Paket Filtering

Firewall paket *filtering* yang dibangun menggunakan dua metode antara lain *drop* menggunakan *IPTables* dan pencocokan *string* menggunakan algoritma KMP. Hasil pemblokiran menggunakan metode *drop IPTables* dapat dilihat pada Gambar 2.

 e-ISSN: 2338-5197



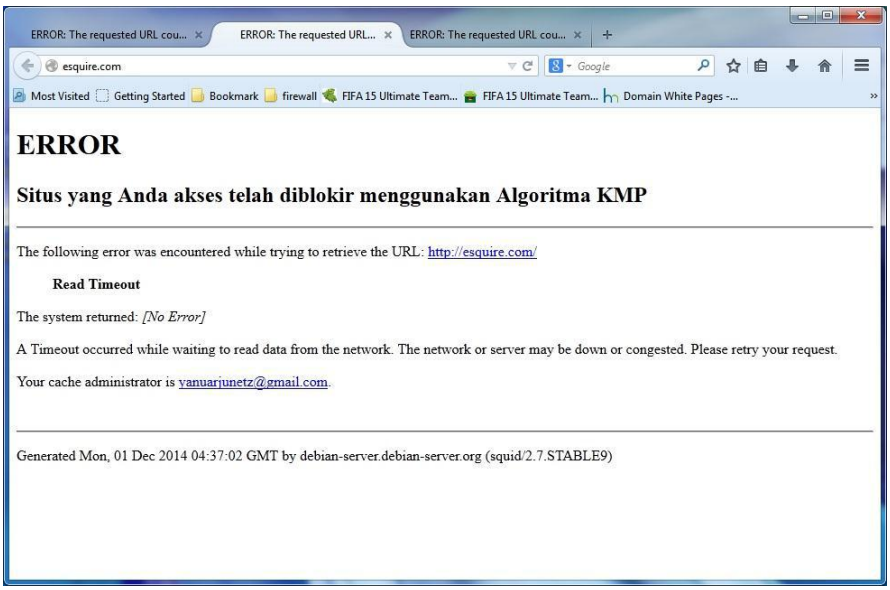
Gambar 2 Hasil blokir metode *drop IPTables*

```
~# iptables -A OUTPUT -d 199.27.76.185 -j DROP
~# iptables -A OUTPUT -d 31.192.116.24 -j DROP
~# iptables -A OUTPUT -d 87.83.27.65 -j DROP
~# iptables -A OUTPUT -d 202.78.200.25 -j DROP
~# iptables -A OUTPUT -d 210.210.179.69 -j DROP
~# iptables -A OUTPUT -d 110.92.25.198 -j DROP
~# iptables -A OUTPUT -d 103.11.40.102 -j DROP
~# iptables -A OUTPUT -d64.38.230.2 -j DROP
```

Listing 1 Blokir alamat IP dari situs web pada *IPTables*

Listing 1 menjelaskan *IPTables* akan memblokir paket data yang keluar menuju alamat situs yang sudah didefinisikan. Perintah yang digunakan *drop* sehingga paket data yang menuju situs tersebut langsung ditolak oleh kernel untuk diproses lebih jauh dan tidak mengirimkan informasi tambahan baik kepada *server* maupun klien.

Metode pemblokiran yang kedua menggunakan pencocokan *string* algoritma KMP. Hasil pemblokirannya dapat dilihat pada Gambar 3 dan kode programnya pada Listing 2.



Gambar 3. : Hasil blokir situs menggunakan algoritma KMP

 e-ISSN: 2338-5197

```
~# iptables -A INPUT -m string --algo kmp --string esquire.com -j REJECT
~# iptables -A FORWARD -m string --algo kmp --string esquire.com -j REJECT
~# iptables -A INPUT -m string --algo kmp --string xhamster.com -j REJECT
~# iptables -A FORWARD -m string --algo kmp --string xhamster.com -j REJECT
~# iptables -A INPUT -m string --algo kmp --string xvideos.com -j REJECT
~# iptables -A FORWARD -m string --algo kmp --string xvideos.com -j REJECT
~# iptables -A INPUT -m string --algo kmp --string pururin.com -j REJECT
~# iptables -A FORWARD -m string --algo kmp --string pururin.com -j REJECT
```

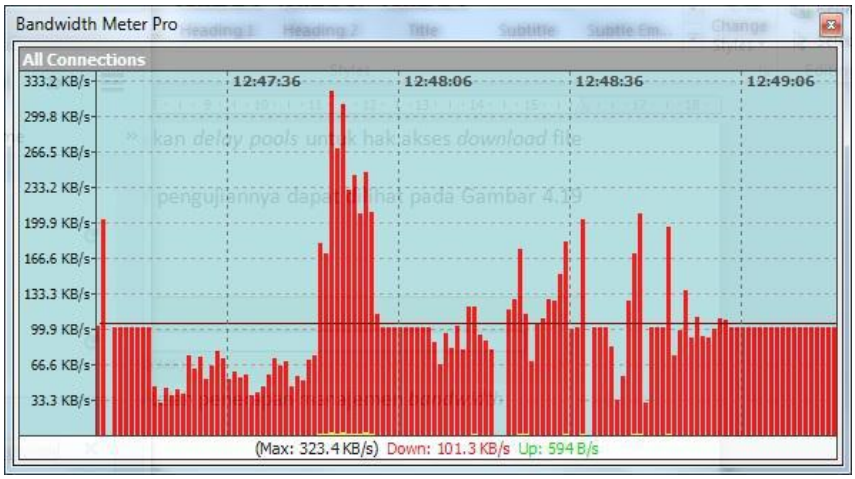
Listing 2 Blokir situs menggunakan pencocokan *string*

Listing 2 *menjelaskan* tentang *IPTables* akan menolak akses menuju situs web yang sudah didefinisikan dengan mencocokkan string pada inputan situs web di *browser.* Perintah pemblokiran menggunakan *reject* karena *firewall* akan menolak paket dan memberitahukan pesan *error* kepada klien, serta tidak menghabiskan *bandwidth* Internet karena akan langsung menolak akses.

4.2.2 Manajemen *Bandwidth Delay Pools*

Manajemen *bandwidth* yang dibangun diimplementasikan di dalam *squid.* Aturan-aturan di *squid* menggunakan ACL (Access Control List). ACL terdiri atas aturan-aturan dan kondisi yang menentukan trafik jaringan dan menentukan proses nantinya akan dilewatkan atau tidak. ACL inilah yang akan digunakan untuk implementasi dalam pembangunan *delay pools.* Untuk hasil penerapan *delay pools* dapat dilihat pada Gambar 4 dan 5.

Gambar 4. Pembatasan *bandwidth* pada ekstensi file tertentu

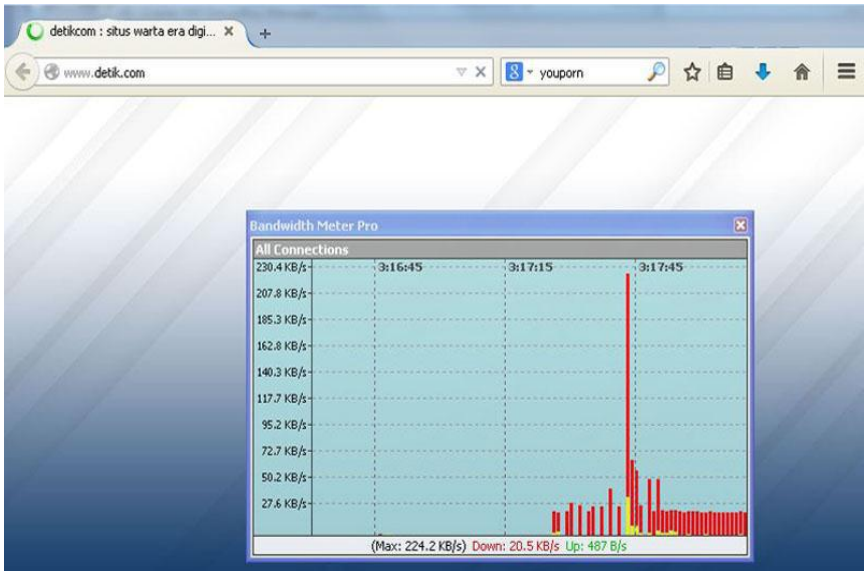


Gambar 5. Pembatasan *bandwidth* pada *download* file

Pada gambar 4 dan 5 tersebut didapatkan bahwa kecepatan *download* untuk file dengan ekstensi .iso sebesar 100 KBps, sedangkan untuk hasil pembatasan *bandwidth* pada jam tertentu sebesar 20 KBps seperti pada Gambar 6 dan implementasiannya pada Listing 3.

 e-ISSN: 2338-5197

4.2.3 Pengujian



Gambar 6. : Pembatasan bandwidth pada waktu tertentu

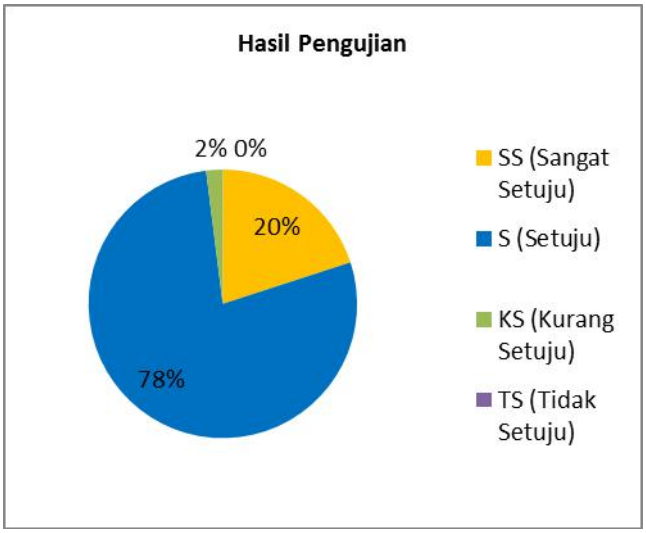
```
acl download url_regex -i http ftp .exe .iso .rar
.zip .mp4 .avi .msi .flv .apk .001 .$ acl praktikum time
SMTWHFA 08:00-12:00 http_access allow download
http_access allow praktikum http_access deny all
delay_pools 2
delay_class 1 1 delay_parameters 1 20000/20000
delay_access 1 allow praktikum delay_access 1 deny all
delay_class 2 2
delay_parameters 2 -1/-1 100000/10240000 delay_access 2
allow download delay_access 2 deny all
```

Listing 3. :Implementasi Manajemen bandwidth Delay Pools

Listing 3 menjelaskan ACL yang digunakan untuk implementasi *delay pools* yang terlebih dahulu diberikan hak akses ijinnya menggunakan `http_acces`. ACL dengan nama praktikum yang menggunakan format waktu dari jam 08:00 – 12:00 akan terkena perlambatan *bandwidth* sebesar 20 KBps yang berlaku untuk mengunduh maupun *browsing*. ACL dengan nama download yang berisi ekstensi file tertentu akan terkena perlambatan kecepatan akses apabila ukuran file yang diunduh lebih dari 10 MB maka *bandwidth* yang didapatkan sebesar 100 KBps.

Pengujian program dengan cara mengamati keluaran (*output*) program yang dilihat dari hasil akses situs web dan penggunaan *bandwidth*. Pengujian yang dilakukan pada sistem ini menggunakan uji kelayakan pada keadaan sebelum dan sesudah diterapkannya sistem. Dari evaluasi yang dilakukan oleh klien terhadap sistem, dapat diperoleh presentasi penilaian pengujian bahwa sangat setuju = 20 %, setuju = 78 %, dan kurang setuju = 2 %. Hasil pengujian dapat dilihat pada Gambar 7.

 e-ISSN: 2338-5197



Gambar 7. Hasil pengujian sistem

5. KESIMPULAN

Firewall paket filtering yang dikembangkan dengan memblokir situs menggunakan metode *drop IPTables* dan pencocokan *string* algoritma KMP. Manajemen *bandwidth* yang dibangun dengan membatasi kecepatan akses untuk mengunduh file pada ekstensi tertentu dan *download* maupun *browsing* pada jam tertentu. Pengujian sistem menggunakan uji kelayakan yang hasilnya didapatkan bahwa sangat setuju = 20 %, setuju = 78 %, dan kurang setuju = 2 %. Berdasarkan pengujian tersebut dapat disimpulkan bahwa sistem layak dan direkomendasikan untuk diterapkan di laboratorium riset UAD, serta sistem mampu menangani permasalahan mengenai situs *pornografi* yang masih dapat diakses dan penggunaan *bandwidth* yang belum optimal untuk praktikum.

6. DAFTAR PUSTAKA

[1] Riko. 2010. "*Implementasi Firewall Menggunakan Layer 7 Protokol Untuk Manajemen Bandwith"*. Yogyakarta: Skripsi Informatika UAD.

[2] Hikmaturokhman dkk, Alfin. 2010. "*Analisis Perancangan Dan Implementasi Firewall Dan Traffic Filtering Menggunakan CISCO Router"*. Bandung: Skripsi Sekolah Tinggi Telkom.

[3] Wiratama, Ariefati. 2010. "*Penerapan Stateful Firewall Pada Arsitektur Dual-Homed Host"*. Jakarta: Skripsi UIN Syarif Hidayatullah.

[4] Rahmat, Friza. 2010. "*Membangun Manajemen Bandwidth Wireless Menggunakan Squid Delay Pools"*. Yogyakarta: Skripsi STMIK Amikom.

[5] Purbo, Onno W. 2004."*Firewall : Security Internet"*.Jakarta : penerbit Elex Media Computindo.

[6] Wibowo, Kevin. 2011. "*Perbandingan Algoritma Knuth-Morris-Pratt dan Algoritma Boyer-Moore dalam Pencarian Teks di Bahasa Indonesia dan Inggris"*. Bandung : Skripsi ITB Bandung.

 e-ISSN: 2338-5197

[7] Wijaya, Alfon Indra. 2013. "*Manajemen Bandwidth Dengan Metode HTB (Hierarchical Token Bucket) Pada Sekolah Menengah Pertama Negeri 5 Semarang"*. Semarang : Skripsi Universitas Dian Nuswantoro.

[8] Rafiudin, Rahmat. 2009. "*Squid Koneksi Anti Mogok"*. Yogyakarta : penerbit Andi.