Metode *Access Control List* sebagai Solusi Alternatif Seleksi Permintaan Layanan Data pada Koneksi Internet

S.N.M.P. Simamora[1], Nina Hendrarini[2], Erika Lya Umi Sitepu[3]

[1,2,3]Program Studi Teknik Komputer Politeknik Telkom, Bandung
[1] sns@politekniktelkom.ac.id, [2] nina2bdg@yahoo.com , [3]eriqa_belover07@yahoo.com

Abstrak

Metode *Access Control List* merupakan salah satu teknik selektivitas permintaan sambungan dalam komunikasi data untuk mengijinkan atau sebaliknya, sejumlah paket data dari suatu *host-computer* menuju ke tujuan tertentu. Hasil dari riset ini telah membuktikan proses *filtering* dan selektivitas permintaan panggilan/sambungan dalam keamanan akses jaringan ke *internet* pada infrastruktur sebuah LAN (*Local Area Network*) dengan cara terpusat, dengan menyediakan metode *filtering* berbasiskan *Access Control List*, serta model jaringan *intranet* berbasis *Access Control List* yang telah dapat menyaring identifikasi perangkat berdasar IP-*Address* dan MAC-*Address* serta seletivitas permintaan layanan data berdasarkan URL yang dikunjungi.

Kata kunci: *access control list*, IP-*address*, URL (*uniform resources locator*), *filtering*, MAC *address*

Abstract

Method of Access Control List is one of selectivity technique in data communication connection request to allow or vice versa, a number of data packets from a host-computer go to a specific destination. The results of this research has proven the process of filtering and selectivity request a call / connection in the network access security infrastructure to the Internet on a LAN (Local Area Network) with a centralized manner, by providing a filtering method based Access Control List, as well as intranet model based Access Control List which has been able to filter based device identification and the MAC-Address IP-Address and seletivitas demand data services based on URL visited.

Keywords: physical-address, IP-address, URL (uniform resources locator), filtering, ACL.

1. Pendahuluan

Saat ini jaringan *internet* semakin meningkat kegunaannya dikalangan masyarakat. Mulai dari kalangan sekolah, kantor, perusahaan maupun masyarakat biasa sudah menggunakan sistem jaringan komputer. Tujuannya agar *user* dapat saling berkomunikasi antara satu dengan yang lainnya. Hal ini memicu orang-orang yang tidak bertanggungjawab untuk melakukan hal-hal yang dapat mengganggu sistem keamanan komunikasi data dalam sebuah jaringan. Misalnya saja mencuri informasi, atau sekedar iseng-iseng saja. Hal tersebut membuat kita harus berhati-hati dan cermat dalam menentukan suatu sistem keamanan komunikasi data dalam sebuah jaringan.

Sistem keamanan jaringan menjadi faktor yang sangat penting untuk dipertimbangkan bagi seorang *administrator* jaringan, dan berbagai upaya dilakukan dalam mengamankan jaringan dari ancaman dan serangan baik oleh *hacker* maupun penyebaran virus. *Access Control List* (ACL) merupakan salah satu alternatif upaya untuk mengamankan jaringan komputer [5]. ACL yang dibuat dengan baik dapat dijadikan dasar sistem keamanan jaringan komputer. Pada riset ini akan dibahas tentang konsep kontrol akses yang dilakukan ACL pada sebuah *proxy server* disertai dengan contoh implementasi dari ACL tersebut.

Untuk dapat mengakses jaringan *wireless* maka setiap perangkat komputer harus mendaftarkan alamat *Media Access Control* (MAC)-nya kepada *administrator* [2] yang nantinya akan dimasukkan kedalam ACL yang diatur pada *squid proxy server*. Selain MAC *Address*, dalam penelitian ini juga akan menambahkan parameter lain dalam proses otorisasi seperti *filtering* IP dan pemblokiran beberapa URL dalam akses jaringan komputer. ACL nantinya akan bekerja memberikan otoritas kepada perangkat komputer yang akan terhubung dengan jaringan yang ada.

Terkait dengan hal tersebut diatas, penelitian ini dilakukan untuk mengkaji langkah-langkah yang perlu dilakukan untuk memberikan hak akses ke jaringan berdasarkan MAC *address* komputer agar dapat membangun komunikasi data ke komputer lain, serta langkah-langkah untuk melakukan *blocked-access* terhadap sebuah *website* yang diakses oleh *client* berdasarkan *restricted-list* URL.

Dalam melakukan kajian terhadap hal-hal yang telah disebutkan sebelumnya, dalam penelitian ini kami melakukan analisa dan pengujian *Access Control List* (ACL) sebagai salah satu solusi alternatif keamanan setiap permintaan koneksi perangkat *client* ke jaringan *backbone* serta

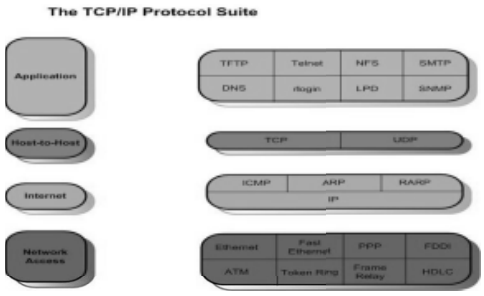
melakukan uji pemblokiran ke beberapa URL (*Uniform Resources Locator*), atau situs tertentu dalam sebuah jaringan.

Pengujian dilakukan dengan mempertimbangkan hal-hal berikut ini:

a. Identifikasi perangkat menggunakan MAC *Address*.
b. Jenis IP yang digunakan hanya untuk klasifikasi IP *static*.
c. Aspek keamanan hanya sebatas mengeksplorasi pemanfaatan penggunaan MAC *Address* sebagai salah satu metode dalam *user controlling access* ke jaringan.
d. *Tools* yang digunakan adalah Squid Proxy Server yang akan menguji *selective process* menggunakan parameter: MAC *Address*, URL, dan IP *Address*.
e. Pengujian hanya dilakukan pada *platform* Sistem Operasi Linux.
f. Tidak menguji untuk implikasi dari serangan.
g. Pengujian hanya dilakukan pada jaringan *intranet*.
h. Pengujian hanya dilakukan pada arsitektur metode akses *user multipoint to point*.
i. ACL yang digunakan hanya yang terdapat dalam *tools Squid Proxy Server*.

2. Kajian Pustaka

2.1 Lapisan-lapisan TCP/IP



Gambar 1. Skema *TCP/IP Layers*[4]

Deskripsi dari setiap lapisan tersebut adalah sebagai berikut [4]:

a. Lapisan *Application*: lapisan ini bertanggung jawab dalam menyediakan akses kepada aplikasi terhadap jaringan TCP/IP. Protokol-protokol yang berjalan pada lapisan ini adalah protokol *Dynamic Host Configuration Protocol* (DHCP), *Domain Name System* (DNS), *Hypertext Transfer Protocol* (HTTP), *File Transfer Protocol* (FTP), *Telnet*, *Simple Mail Transfer Protocol* (SMTP), *Simple Network Management Protocol* (SNMP).
b. Lapisan *Transport* (*Host-to-Host*): lapisan ini bertanggung jawab dalam membuat komunikasi antara aplikasi atau antar dua *host*, dengan cara membuat sebuah sesi *connection-oriented* atau dengan menyebarkan sebuah *connectionless broadcast.* Protokol-protokol yang berjalan pada lapisan ini adalah protokol *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP).
c. Lapisan *Internet*: lapisan ini bertanggung jawab dalam melakukan *routing* dan pembuatan paket IP (dengan menggunakan teknik *encapsulation*). Protokol-protokol yang berjalan pada lapisan ini adalah *Internet Protocol* (IP), *Address Resolution Protocol* (ARP), *Internet Control Message Protocol* (ICMP), serta *Internet Group Management Protocol* (IGMP).
d. Lapisan *Network Access*: lapisan ini bertanggung jawab dalam meletakkan *frame-frame* data di atas media jaringan. Protokol yang berjalan dalam lapisan ini adalah beberapa arsitektur jaringan lokal (seperti halnya Ethernet atau Token Ring), serta layanan teknologi WAN *Plain Old Telephone Service* (POTS), *Integrated Services Digital Network* (ISDN), *Frame Relay*, dan *Asynchronous Transfer Mode* (ATM).

2.2 Proxy-*server*

Proxy server adalah sebuah *server* yang menjembatani *client* dengan sebuah *server gateway* sebelum berkomunikasi dengan *internet* atau *extranetwork* lain. Melalui *proxy server*, maka situs-situs yang sering dikunjungi akan terasa semakin cepat diakses *user*, karena telah tersimpan didalam *cache proxy*. Selain itu, *proxy server* juga berfungsi untuk melakukan otentikasi *user*, memblokir situs-situs tertentu, dan sebagainya.

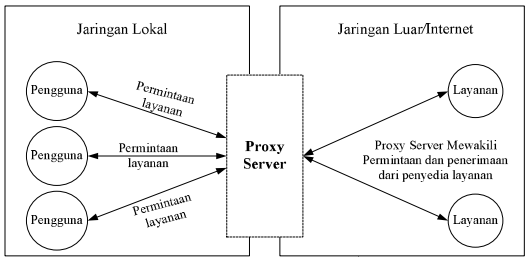
Fungsi utama dari *proxy-server* adalah:

a. *Connection Sharing*; konsep dasarnya adalah seorang pengguna (*client*) tidak langsung berhubungan dengan jaringan luar atau *internet*, tetapi harus melewati suatu *gateway*, yang bertindak sebagai batas antara jaringan lokal dan jaringan luar.
b. *Filtering*; bekerja pada layer aplikasi sehingga berfungsi sebagai *firewall packet filtering* yang digunakan untuk melindungi jaringan lokal dari serangan atau gangguan yang berasal dari jaringan *internet* dengan melakukan *filtering* atas paket yang lewat dari dan ke jaringan-jaringan yang dihubungkan ke *internet*.
c. *Caching*; mekanisme *caching* akan menyimpan obyek-obyek yang merupakan hasil permintaan (*request*) dari dari para pengguna, yang didapat dari *internet* atau kunjungan protokol HTTP, dan disimpan dalam ruang disk yang disediakan (yang disebut *cache*).

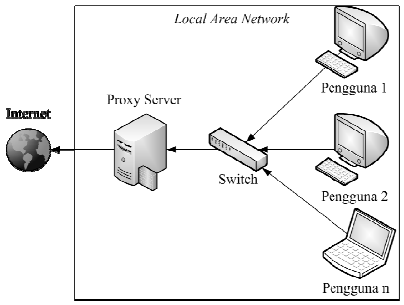
2.3 Squid Proxy

Squid adalah salah satu aplikasi *caching proxy* untuk *client web*, seperti *Hyper-text Transfer Protocol* (HTTP), *Hyper-text Transfer Protocol Secure* (HTTPS), *File Transfer Protocol* (FTP), dan

layanan sejenis lainnya dalam *proxy server* [2]. Squid merupakan *software proxy* yang banyak dipakai dan dapat diperoleh secara gratis. Squid juga dapat digunakan untuk mengendalikan pemakaian *bandwidth* berdasarkan ekstensi *file-file* tertentu, menyaring situs-situs yang boleh diakses. Hal ini terwujud dengan melakukan *caching* halaman *web* dan menggunakan ulang halaman yang sering dikunjungi.



Gambar 2. Fungsi dari *Proxy Server* Antara Pengguna dan Penyedia Layanan



Gambar 3. Posisi dari *Proxy Server* Antara Pengguna dan Penyedia Layanan

2.4 ACL (*Access Control List*)

ACL adalah daftar *device* yang berisi MAC *Address* yang diberi hak untuk mengakses sebuah jaringan[3]. Daftar ini memberitahu *router* paket-paket mana yang akan diterima atau ditolak. ACL membuat keputusan berdasarkan alamat asal, alamat tujuan, protokol, dan nomor *port*. ACL sangat membantu dalam pengontrolan lalu lintas dalam akses sebuah jaringan. Mekanisme dasar ACL yakni menyaring paket yang tidak diinginkan ketika komunikasi data berlangsung sehingga menghindari permintaan akses maupun paket data yang mencurigakan dalam akses keamanan sebuah jaringan[3].

Fungsi dari *Access Control List* (ACL) adalah:

a. Membatasi trafik jaringan dan meningkatkan unjuk kerja jaringan. Misalnya, dengan mem-*block* trafik video, yang dapat menurunkan beban jaringan, sehingga meningkatkan kerja jaringan.
b. Mampu memberikan dasar keamanan untuk akses ke jaringan. Misalkan *host* A tidak diijinkan akses ke jaringan privat institusi; namun *host* B diijinkan.
c. Memberi keputusan terhadap jenis trafik mana yang akan dilewatkan atau di-*block* melalui *interface router*. Misalkan trafik *e-mail* dilayani sementara trafik *Facebook* di-*block* dalam waktu yang ditentukan.
d. Mengontrol daerah-daerah (*cells*) dimana *client* dapat mengakses jaringan.
e. Memilih *host-host* yang diijinkan atau di-*block* akses ke segmen jaringan. Misalkan, ACL mengijinkan atau mem-*block* FTP atau HTTP.

2.4.1 MAC *Address*

Media Access Control Address adalah sebuah alamat jaringan yang diimplementasikan pada Lapisan *Network Access*[4] yang dapat merepresentasikan sebuah *node* tertentu dalam jaringan. MAC *Address* merupakan alamat yang unik yang memiliki panjang 48-bit (6 byte) yang mengidentifikasikan sebuah komputer, *interface* dalam sebuah *router*, atau *node* lainnya dalam jaringan. Dalam sebuah komputer, MAC *Address* ditetapkan ke sebuah kartu jaringan (*Network Interface Card*, NIC) yang digunakan untuk menghubungkan komputer yang bersangkutan ke sebuah jaringan.

2.4.2 Internet *Protocol Address* (IP *Address*)

Alamat IP adalah alamat logika yang diberikan pada sebuah perangkat jaringan[1]. IP *Address* yang digunakan dalam suatu komputer harus unik dan tidak boleh sama dengan yang lain. Alamat IP terdiri dari deretan angka biner antar 32-bit sampai 128-bit yang dipakai sebagai alamat identifikasi untuk tiap komputer *host* dalam jaringan komputer. Panjang dari angka ini adalah 32-bit (IPv4 atau IP versi 4), dan 128-bit (IPv6 atau IP versi 6) yang menunjukkan alamat dari komputer tersebut pada jaringan komunikasi data berbasis TCP/IP.

2.4.3 URL (*Uniform Resources Locator*)

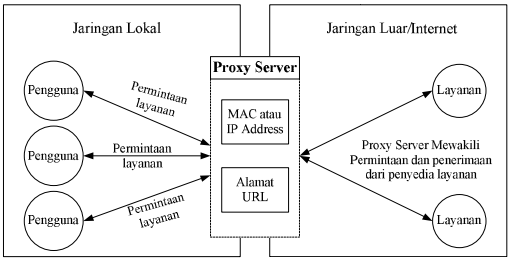
Uniform Resources Locator (URL) adalah sebuah rangkaian karakter yang membentuk suatu "*pathname*" untuk mengidentifikasikan sebuah dokumen atau gambar dalam sebuah *web*.

URL terdiri dari beberapa bagian, seperti:[4]

a. Bagian pertama URL dikenal sebagai protokol atau disebut pula http:// yang merupakan singkatan dari *Hyper-text Transfer Protocol*.
b. Bagian kedua dari URL dikenal sebagai nama domain, domain mewakili nama *server* yang sedang berhubungan dengan internet.
c. Bagian ketiga dari URL disebut dengan *directory path* yang merupakan area khusus dimana domain-domain berada.

d. Bagian keempat dari URL disebut nama *file* dokumen, yakni menentukan *file* khusus yang sedang diakses yang biasanya adalah sebuah *file* HTML, gambar, suara dan sebagainya.

3. Analisis dan Perancangan



Gambar 4. Model Konseptual Penelitian

3.1 Analisis Spesifikasi Kebutuhan

Pemanfaatan ACL sebagai salah satu solusi alternatif keamanan dalam akses sebuah jaringan pada suatu institusi atau lembaga. Penelitian ini menggunakan pemodelan jaringan untuk mensimulasikan sistem *filtering* MAC *Address*, IP *Address* dan pemblokiran beberapa situs yang akan menggunakan sebuah sebuah server *proxy* dimana didalamnya telah di-*install*-kan sebuah *tools* Squid Proxy Server yang terdiri dari satu komputer untuk *proxy server* serta beberapa komputer berfungsi sebagai *client* untuk melakukan pengujian terhadap kinerja ACL.

TABEL 1
SPESIFIKASI PERANGKAT LUNAK

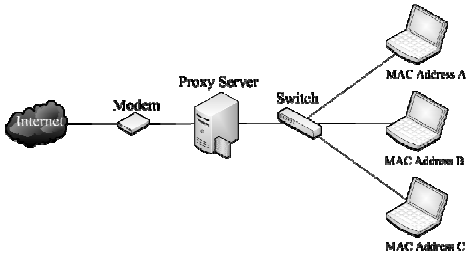
No.	Perangkat Lunak	*Proxy Server*	*Client*
1.	Sistem Operasi	Linux Ubuntu 9.10	Windows
2.	Aplikasi	Squid	Mozilla Firefox
3.	*Editor*	Gedit	Word,Notepad

TABEL 2
SPESIFIKASI PERANGKAT KERAS

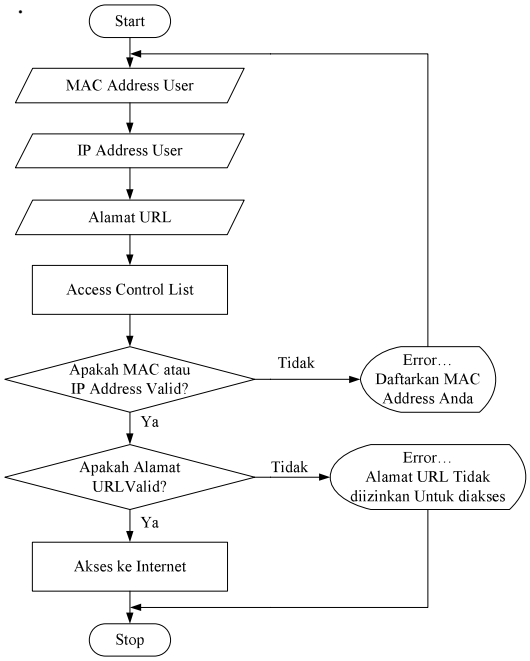
No.	Perangkat Keras	*Proxy Server*	*Client*
1.	*Motherboard*		Intel Core Duo
2.	*Processor*	Intel Pentium 4 CPU 3.00 GHz	Pentium 4 CPU 3.00 GHz
3.	RAM	DDR RAM 512 MB PC3200	DDR RAM 512 MB
4.	*Hard Disk*	Seagate Baraccuda SATA-40GB	Seagate Baraccuda 40GB
5.	LAN *Card*	OnBoard 100Mbps	a. OnBoard 100Mbps b. NIC Allied Telesyn AT2500TXL/ RTL8139D 100Mbps
6.	Monitor	Samsung Sync Master 740n 14”	Samsung Sync Master 740n 14”

3.2 Model Arsitektur Jaringan

Dari Gambar 5, terlihat model arsitektur jaringan yang diharapkan dapat membantu *administrator* untuk menjalankan ACL, sebagai salah satu solusi yang mendasar, untuk menjaga keamanan dalam mengakses jaringan



Gambar 5. Model Arsitektur Jaringan yang Dibangun



Gambar 6. *Flowchart* Sistem yang Akan Dibangun

4. Implementasi dan Pengujian

4.1 Konfigurasi ACL pada *Proxy Server*

Konfigurasi Squid:

```
http_access deny porn
#MAC yg d perbolehkan
ACL MAC arp
"/etc/squid/blokMAC.txt"http_access allow
MAC
#or
#IP yang di perbolehkan ACL IP src
"/etc/squid/blokIP.txt"http_access allow IP
http_access deny manager http_access allow
purge localhosthttp_access deny purge
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
```

```
http_access allow localhost
#http_access allow localnet
#http_access allow !auth_user
```

TABEL 3
DAFTAR TABEL PENGUJIAN

No.	MAC *Address* yang Terdaftar	IP *Address* yang Terdaftar	URL yang diblok
1.	00:1e:ec:16:d8:a6	192.168.2.10	www.playboy.com
2.	00:1f:3c:00:c5:79	192.168.2.7	www.facebook.com
3.	00:24:81:66:45:2f	192.168.2.6	www.17tahun.com

4.2 Pengujian File Konfigurasi

Skenario pengujian untuk melihat implikasi pembatasan akses *user* ke *back-bone jaringan*, dimana dengan melakukan pembatasan beberapa hal sebagai berikut:

a. Jumlah *host-computer* aktif sebelum *restricted-access* diaktifkan: 10
b. Jumlah *host-computer* aktif setelah *restricted-access* diaktifkan: 8
c. *Host-computer* yang di-*restricted* untuk 10x pengujian adalah sama.
d. Uji-coba dilakukan pada sebuah *file video* format *.flv dengan durasi 2.50 menit dengan kapasitas 12,982KB
e. Kapasitas kanal diamati dengan *speed*: 1.0Mbps
f. Pengujian dilakukan secara berulang untuk *file* yang sama sebanyak 10x dengan selang setiap pengujian: 60 detik.
g. Pengujian menggunakan *tools*: Sothink Web Video Downloader.
h. Akses ke Jaringan Publik *internet* menggunakan koneksi modem *wireless* Esia – Wimode.

TABEL 4
PENGARUH PEMBATASAN AKSES DENGAN ALOKASI *BIT-RATE* DATA YANG TERSEDIA

	***Bit-rate* data telah tersimpan (KBps)**		***ratio* (KBps)**
	Sebelum *restricted*	**Setelah *restricted***	
	2.5	2.9	0.4
	3.4	3.9	0.5
	3.7	4.2	0.5
	3.4	3.9	0.5
	4.4	4.8	0.4
	3.6	4.0	0.4
	3.5	4.0	0.5
	4.2	4.6	0.4
	4.7	5.2	0.5
	3.5	3.9	0.4
Rata-rata	3.69	4.14	0.45

1KB = 8Kbit

5. Penutup

Beberapa hal yang dapat disimpulkan berdasar hasil pengujian adalah sebagai berikut:

a. Metode *Access Control List* dengan *tools* Squid Proxy Server dapat menyediakan dan memberikan hak akses kepada pengguna jaringan berdasarkan MAC *Address* dan IP *Address*; dengan demikian membantu seorang *Network Administrator* jaringan mengamankan akses jaringan.
b. Menyediakan *restricted-access list* pada media *cache website* yang tidak dapat digunakan oleh *client* dalam mengakses sebuah jaringan. Ini terlihat pada sejumlah URL yang dilakukan pemblokiran
c. Metode *Access Control List* (ACL) dengan *tools* Squid Proxy Server dalam *proxy server* hanya dapat dikonfigurasi dengan parameter MAC *Address*, IP *Address*, dan pembatasan alamat *Uniform Resources Locator* (URL).

Daftar Pustaka

[1] Hantoro, Gunadi, D., *Wi-Fi (Wireless LAN) Jaringan Komputer Tanpa Kabel*, Bandung: Informatika Bandung, 2009.
[2] Hill, Brian, *CISCO - The Complete Reference*, California: McGraw-Hill, 2002,
[3] Rafiudin, R., *SQUID*, Yogyakarta: ANDI-Offset, 2008.
[4] *Squid Configuration Directive ACL*. http://www.Squid-cache.or.id/info.php/. Diunduh tanggal 19 February 2010.
[5] Simamora, S.N.M.P., WLAN Implementation in High-floor Indoor Office Building for Communication Successfull Solution, Proceeding of International Conference on Open Source for Higher Education (ICOSic), Sebelas Maret University (UNS), Solo, 2010, halaman : 135 -. 138.
[6] Stallings, William, *Komunikasi Data Dan Komputer Jaringan Komputer*, Jakarta: Salemba Teknikam, 2002.