PERANCANGAN LAYER-7 PACKET FILTERING PADA JARINGAN KOMPUTER UNIVERSITAS ATMA JAYA MAKASSAR

Arnold Nasir[1)]
[1]Prodi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Atma Jaya Makassar
Alamat e-mail:arnold_nasir@outlook.com

ABSTRACT

Penggunaan Internet bervariasi, mulai dari mencari dan bertukar informasi, sebagai media untuk bisnis dan komunikasi, serta memfasilitasi publikasi atau promosi. Untuk memenuhi kebutuhan penggunaan Internet, banyak pengembang perangkat lunak mulai mengembangkan berbagai aplikasi, seperti BitTorent, FileZilla, dll. Sayangnya, beberapa aplikasi tidak dikembangkan untuk mematuhi peraturan pelabuhan tertentu yang membuatnya rentan terhadap serangan akses jarak jauh. Serangan semacam ini biasanya dieksploitasi oleh pengguna yang tidak dikenal, kebanyakan dikenal sebagai peretas untuk mendapatkan akses dalam sistem internal di mana aplikasi sedang diinstal. Oleh karena itu, sebagai tanggapan untuk mengukur balik ancaman semacam itu terhadap organisasi, diperlukan untuk menerapkan metode penyaringan yang dapat mengklasifikasikan paket yang masuk dan keluar dari jaringan, bersama dengan mencapai bandwidth arbitrase..

Keywords: *Firewall, Jaringan Komputer,Layer-7 Protocol, Packet Filtering*

1. PENDAHULUAN

Perkembangan teknologi jaringan komputer berbasis Internet saat ini kian pesat. Hal ini ditandai dengan bertambahnya pengguna Internet setiap tahunnya. Dari data yang diperoleh[1] jumlah pengguna Internet di Indonesia pada tahun 2014 mencapai 83,7 juta orang dan diprediksi pengguna Internet pada tahun 2016 mencapai 102,8 juta orang. Penggunaan Internet pun beragam, mulai dari pencarian dan pertukaran informasi, media komunikasi dan bisnis, serta memfasilitasi proses promosi dan publikasi. Untuk memenuhi kebutuhan akan penggunaan Internet, para pengembang software mulai mengembangkan beberapa aplikasi, seperti BitTorrent, FileZilla, dan sebagainya. Sayangnya, beberapa aplikasi yang dikembangkan tidak menggunakan pengaturan port standar sehingga beberapa aplikasi tersebut vulnerable terhadap remote access sehingga kerap dieksploitasi oleh para cracker untuk dapat masuk kedalam jaringan internal. Guna mengatasi masalah tersebut maka perlu diterapkan sebuah metode filtering yang dapat mengklasifikasikan paket-paket yang masuk dan keluar pada sebuah jaringan serta arbitrase bandwith dengan port non-standar dan standar.

Ada sejumlah layanan jaringan yang memerlukan klasifikasi paket, seperti routing, access-control di firewall, routing berbasis kebijakan, dan pengaturan Quality of Service (QoS). Dalam setiap kasus sangatlah penting untuk menentukan tindakan yang perlu dilakukan terhadap setiap paket masuk dan alur mana sebuah paket masuk akan diteruskan, misalnya apakah akan diteruskan atau paket tersebut di drop, kemana paket tersebut diteruskan, kelas layanan apa paket masuk tersebut harus terima. Fungsi kategorisasi dilakukan oleh flow classifier (disebut juga packet classifier) yang mengoperasikan sebuah set aturan dimana masing-masing aliran mematuhi setidaknya satu aturan. Aturan mengklasifikasikan alur yang mana sebuah paket akan diteruskan berdasarkan isi dari header packet(s). Misalnya, alur bisa didefinisikan oleh nilai-nilai tertentu dari sumber dan tujuan alamat IP, dan dengan nomor port transportasi tertentu. Selain itu, alur bisa dengan sederhana didefinisikan oleh prefix tujuan dan rentang nilai port.

Bentuk paling sederhana dan paling terkenal dari packet classifier digunakan dalam routing datagram IP, di mana setiap aturan menentukan prefix tujuan, dan selanjutnya

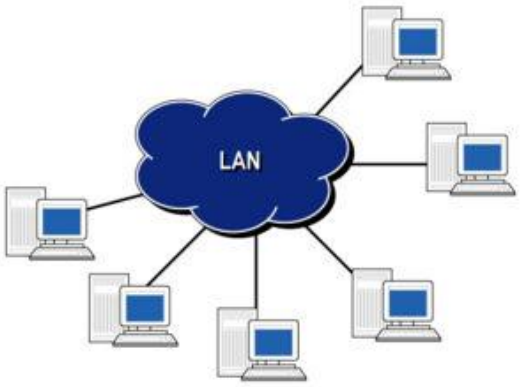
menentukan alamat IP dari next-hop dimana paket harus dialihkan. Proses klasifikasi membutuhkan menentukan prefix terpanjang yang sesuai dengan alamat tujuan paket tersebut.

Ada beberapa keuntungan yang dapat diperoleh dengan menerapkan packet classifier pada sebuah jaringan perusahaan. Pertama, efisiensi dalam penggunaan bandwith dapat lebih ditingkatkan. Hal ini dikarenakan packet classifier menganalisa setiap paket data yang masuk maupun keluar sehingga jika terdapat aplikasi yang berjalan di belakang layar dan meminta untuk menginginkan pembaharuan/update maka hal tersebut dapat dicegah. Kedua, dengan menerapkan packet classifier maka dapat memonitor penggunaan bandwith setiap user pada sebuah jaringan. Ketiga, packet classifier mampu memantau apabila terdapat aplikasi yang tergolong malware yang ingin meminta untuk terkoneksi dengan server diluar jaringan perusahaan. Hal ini umum ditemukan mengingat malware merupakan client-side application yang beroperasi dengan cara membuat suatu jaringan penghubung dengan server diluar jaringan perusahaan kemudian cracker dapat masuk kedalam jaringan tersebut.

2. TINJAUAN PUSTAKA

2.1 *Local Area Network* (LAN)

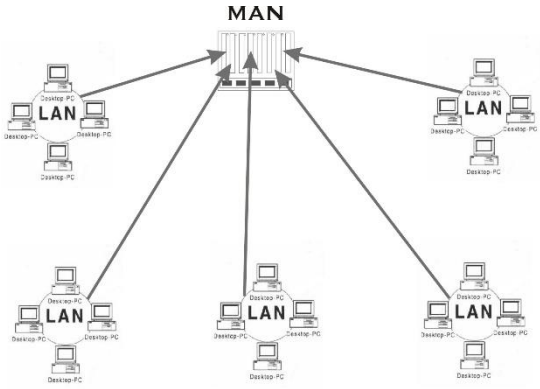
Local Area Network atau yang lebih dikenal dengan istilah LAN merupakan jaringan yang memiliki daerah jangkauan yang relatif kecil, seperti dalam sebuah perusahaan atau jaringan yang terdapat didalam sebuah rumah.



Gambar 1. Local Area Network (LAN)

2.2 Metropolitan Area Network (MAN)

Metropolitan Area Network atau sering pula disebut dengan istilah MAN merupakan jaringan komputer yang terdiri atas dua atau lebih LAN dalam satu area geografis. Sebagai contoh, sebuah bank tentu terhubung dengan Kantor Cabang Utama (KCU) bank tersebut.



Gambar 2. Metropolitan Area Network (MAN)

2.3 Routerboard Mikrotik

Routerboard Mikrotik atau yang lebih dikenal dengan sebutan Mikrotik merupakan sebuah perangkat jaringan komputer yang berfungsi layaknya sebuah router maupun switch. Mikrotik sendiri amat populer digunakan pada instansi berskala kecil hingga besar dengan harga yang relatif murah bila dibandingkan router dengan merek ternama, seperti Cisco. Meski harga yang relatif murah, namun Mikrotik memiliki fitur yang lengkap, antara lain:

a. Address List: Pengelompokan IP Address berdasarkan nama.
b. Interface : Gerbang trafik keluar atau masuk ke mikrotik atau Ethernet
c. Asynchronous: Mendukung serial PPP dial-in / dial-out, dengan otentikasi CHAP, PAP, MSCHAPv1 dan MSCHAPv2, Radius, dial on demand, modem pool hingga 128 ports.
d. Bonding: Mendukung dalam pengkombinasian beberapa antarmuka ethernet ke dalam 1 pipa pada koneksi cepat.
e. Bridge: Mendukung fungsi *bridge spinning tree*, *multiple bridge interface*, *bridging firewalling*.
f. Data Rate Management: QoS berbasis HTB dengan penggunaan burst, PCQ,

RED, SFQ, FIFO queue, CIR, MIR, limit antar peer to peer.

g. DHCP: Mendukung DHCP tiap antarmuka; DHCP Relay; DHCP Client, multiple network DHCP; static and dynamic DHCP leases.
h. Firewall dan NAT : Mendukung pemfilteran koneksi peer to peer, source NAT dan destination NAT. Mampu memfilter berdasarkan MAC,IP address, range port, protokol IP, pemilihan opsi protokol seperti ICMP, TCP Flags dan MSS.
i. Hotspot: Hotspot gateway dengan otentikasi RADIUS. Mendukung limit data rate, SSL, HTTPS.
j. MNDP: MikroTik Discovery Neighbour Protokol, juga mendukung Cisco Discovery Protokol (CDP).
k. Monitoring / Accounting: Laporan *Traffic* IP, log, statistik graph yang dapat diakses melalui HTTP.
l. Proxy: Cache untuk FTP dan HTTP proxy server, HTTPS proxy; transparent proxy untuk DNS dan HTTP; mendukung protokol SOCKS; mendukung parent proxy; static DNS.
m. Routing: Routing statik dan dinamik; RIP v1/v2, OSPF v2, BGP v4.
n. Synchronous: V.35, V.24, E1/T1, X21, DS3 (T3) media ttypes; sync-PPP, Cisco HDLC; Frame Relay line protokol ; ANSI-617d (ANDI atau annex D) dan Q933a (CCITT atau annex A);Frame Relay jenis LMI.
o. Tool: Ping, Traceroute; bandwidth test; ping flood; telnet; SSH; packet sniffer; Dinamik DNS update.

Untuk mengakses dan melakukan proses pengaturan/konfigurasi Mikrotik dapat ditempuh dengan dua cara: yang pertama ialah dengan mengakses via web browser kemudian mengetikkan alamat IP default dari Mikrotik, dan kedua ialah dengan mengakses via aplikasi bernama Winbox.

2.4 Kajian Penelitian Sejenis

Adapun beberapa penelitian sejenis yang dijadikan sebagai acuan pada penelitian ini antara lain:

a. M. Agreindra Helmiawan (2018) [2]
Penelitian ini berjudul: Internet Positif dengan Metode Web Filtering Layer 7 Pada Jaringan Wireless (Study Case Hotspot RT4 CIpeuteuy Baru Sumedang). Penelitian ini membahas mengenai penggunaan layer 7 filtering untuk membantu menciptakan kondisi pengggunaan internet yang positif dengan memblokir konten-konten internet yang dianggap negatif. Penelitian ini dilakukan pada hotspot RT4 RW6 Cipeuteuy yang hasilnya mampu mengurangi penggunaan bandwidth pada kawasan tersebut.
b. Arif Hidayat (2018)[3]
Penelitian ini berjudul: Comparative Analysis of Mikrotik Site Filter Using Address List Techniques, Layer7 Protocols, Web Proxy, Mangle and DNS Static. Penelitian ini berfokus pada berbagai macam teknik filtering yang dibenamkan pada Mikrotik. Kemudian dilakukan pengujian terhadap jenis-jenis filtering tersebut agar didapatkan bentuk output yang optimal. Disamping itu, penelitian ini juga memberikan hasil terkait pola yang didapati dari tiap-tiap jenis filtering yang digunakan dalam percobaan ini.

3. METODOLOGI PENELITIAN

Penelitian ini dikembangkan dengan menggunakan metode eksperimental. Secara umum kegiatan penelitian ini dibagi menjadi 2 tahapan utama, yakni tahap perancangan dan tahap evaluasi. Pada tahapan perancangan, pengusul pertama-tama akan memantau dan menganalisa kondisi traffic pada jaringan komputer Universitas Atma Jaya Makassar. Lamanya kegiatan observasi ini dijadwalkan selama kurang lebih dua (2) minggu dan dapat diperpanjang apabila jumlah layanan aplikasi yang berjalan pada jaringan universitas bertambah. Setelah diperoleh data yang terkait dengan penggunaan aplikasi, maka selanjutnya dilakukan proses perancangan packet classifier guna mengatur arus paket data yang mengalir baik dari luar maupun dari dalam jaringan universitas. Perancangan packet classifier berlangsung selama 2-3 bulan, tetapi dapat berlangsung lebih lama jika didapati aplikasi baru yang berjalan pada jaringan universitas. Nantinya packet

classifier tersebut akan bertindak sebagai filter dan membatasi penggunaan akses sebuah aplikasi, terutama jika aplikasi tersebut merupakan aplikasi yang membutuhkan koneksi Internet untuk dapat beroperasi.

Setelah packet classifier diimplementasikan maka selanjutnya akan masuk pada tahap evaluasi, dimana pada tahap ini pengusul akan mengevaluasi hasil implementasi dari packet classifier. Hasil evaluasi ini nantinya akan memproyeksikan jumlah paket data yang berhasil ditolak ataupun diizinkan untuk masuk kedalam atau keluar dari jaringan universitas. Data tersebut nantinya dapat melihat aplikasi-aplikasi yang menggunakan koneksi Internet, sehingga peluang untuk menemukan aplikasi malware yang berada pada jaringan universitas semakin besar. Disamping itu, dengan adanya data evaluasi yang diperoleh dapat menjadi referensi untuk pengaturan load balance pada jaringan universitas.

3.1 Lokasi Penelitian

Sesuai dengan judul dari kegiatan penelitian ini maka lokasi penelitian akan dilakukan pada Universitas Atma Jaya Makassar.

3.2 Analisis Data

Proses pengumpulan data dilakukan dengan metode observasi dan wawancara. Observasi dilakukan terhadap backbone pada jaringan universitas yang berpusat di Fakultas Teknologi Informasi (FTI) UAJM. Dari FTI, pengusul tentunya dapat melihat dengan jelas traffic yang masuk dan keluar dari jaringan universitas. Selanjutnya, pengusul akan mengambil sampling traffic kemudian dianalisa guna mendapatkan aplikasi serta layanan yang masuk ataupun keluar dari jaringan universitas. Sementara itu, untuk kegiatan proses wawancara pengusul akan mewawancarai beberapa pihak yang dianggap mengetahui aplikasi ataupun layanan yang dijalankan oleh pihak universitas pada jaringan public maupun private.

Hasil dari implementasi visualisasi ini kemudian akan diuji kembali apakah telah sesuai dengan konsep algoritma stacking images yang telah dirancang pada tahap sebelumnya. Pengujian juga dilakukan dengan melihat keterkaitan antar gambar yang ditampilkan apakah telah sesuai dengan yang ada di lapangan

4. HASIL DAN PEMBAHASAN

4.1 Analisa Kebutuhan

Dalam tahapan ini terdapat beberapa kegiatan yang dilakukan terkait perancangan *rules and policy* yang nantinya digunakan pada Layer-7 Protocol di lingkungan UAJM. Agar Layer-7 Protocol dapat bekerja tepat dan sesuai dengan kebutuhan UAJM, maka dilakukan kegiatan observasi terhadap kondisi jaringan komputer, utamanya mengenai *traffic* penggunaan Internet. Hal ini dilakukan untuk memberikan gambaran yang jelas terhadap kondisi jaringan maupun layanan pada UAJM saat ini.

4.1.1 Observasi

Kegiatan observasi sendiri dijadwalkan untuk dilakukan selama dua (2) minggu, kemudian ditambah seminggu untuk mendapatkan data traffic jaringan selama satu (1) bulan.

Adapun hasil observasi yang diperoleh adalah sebagai berikut:

a. Jumlah pengguna jaringan komputer di lingkungan UAJM adalah sebesar 1.600 orang yang terdiri atas dosen, karyawan, dan mahasiswa. Dari ketiga kategori pengguna tersebut, dosen dan karyawan merupakan pengguna yang diprioritaskan sehingga diberikan bandwidth jaringan yang lebih besar bila dibandingkan dengan mahasiswa. Alasan mengapa dosen dan karyawan diberikan bandwidth yang lebih besar ialah untuk mendukung kegiatan pekerjaan mereka, seperti pembayaran pajak via online, mengunggah materi kuliah, mengunggah hasil penelitian pada jurnal online, dsb. Disamping itu, dosen dan karyawan dapat mengakses fasilitas Internet di berbagai lokasi namun bagi mahasiswa yang ingin memanfaatkan layanan Internet hanya dapat mengaksesnya pada Computing Center dan perpustakaan.
b. Pengguna jaringan komputer di lingkungan UAJM umumnya menggunakan jaringan komputer untuk berbagai jenis aktivitas, antara lain mengakses SIA, mencari informasi

berupa jurnal atau buku, mengunduh dan mengunggah materi kuliah.

c. Adapun aktivitas penggunaan yang diamati lebih difokuskan pada penggunaan layanan Internet dimana layanan tersebut sering dikeluhkan oleh para pengguna di lingkungan universitas. Dari hasil observasi yang dilakukan, beberapa informasi yang didapatkan antara lain:
d. Untuk aktivitas browsing, situs yang sering dikunjungi oleh pengguna antara lain google.com, yahoo.com, lldikti9.ristekdikti.go.id, kemdikbud.go.id, forlap.dikti.go.id, uajm.ac.id (beserta subdomain didalamnya). Selain itu, tidak jarang ditemukan berbagai website plugin yang berjalan pada beberapa pengguna sehingga mengakibatkan pengguna tidak hanya mengakses situs yang diinginkan melainkan adapula situs yang terakses dan berjalan dibelakang layar, contohnya baidu pc clean.
e. Untuk aktivitas lokal, layanan yang digunakan umumnya untuk mengakses SIA, dan Kios Akademik.
f. Untuk aktivitas download, jenis file yang sering diunduh antara lain Portable Document Format (.pdf), office file types (.doc/.docx, .xls, .ppt/.pptx). Selain itu ada pula file gambar dengan format .jpg dan .png. Umumnya gambar-gambar tersebut terunduh pada saat sebuah website diakses, kemudian ditampilkan pada web browser pengguna. Untuk file dengan ukuran besar (diatas 50 MB), file yang sering diunduh merupakan file installer sebuah aplikasi/program. Adapun file installer yang diunduh merupakan proses yang disadari oleh pengguna, tetapi bisa juga proses tersebut berjalan tanpa sepengetahuan pengguna. Perlu diketahui, bahwa apabila seorang pengguna melakukan proses pengunduhan sebuah file yang berukuran besar maka dampaknya dapat dirasakan langsung oleh pengguna yang berada pada jaringan tersebut.

4.2 Perancangan Rules Packet Classifier

Tahapan selanjutnya dalam proses analisa kebutuhan adalah merancang *packet classifier* yang sesuai dengan kondisi yang ada di lingkungan UAJM. Dengan adanya perangkat Mikrotik yang digunakan sebagai router, maka tidaklah sulit untuk menentukan jenis *packet classifier* yang tepat. Salah satunya adalah dengan menggunakan L7 Protocols.

Secara umum L7 dapat melakukan beberapa kegiatan, seperti melakukan pengaturan pemblokiran terhadap *incoming traffic*, atau melakukan perubahan bentuk *traffic* dengan menetapkan *IP packets* dari sebuah arus data spesifik menuju proses antrian (*queue*).

Dari hasil observasi dan sampling yang telah dilakukan maka dapat digambarkan perancangan prioritas packet classifier sebagai berikut:

Tabel 1. *Rules* pada L7

No	Jenis Packet	Tindakan
1	*In → .exe*	Queue/Block
2	*In → .pdf*	Allow
3	*In → .jpg*	Allow
4	*In → .png*	Allow
5	*In → .html*	Allow
6	*In → .php*	Allow
7	*In → .rar*	Queue/Block
8	*In → .zip*	Queue/Block
9	*In → .mp4*	Block
10	*In → .iso*	Block

Seperti yang terlihat pada Tabel 1, L7 akan mengalihkan bahkan tidak mengijinkan pengguna untuk melakukan pengunduhan file dengan tipe .exe, .rar, .zip, dan .mp4. Hal ini bertujuan untuk menghindari pemakaian *bandwidth* yang berlebihan pada salah satu pengguna sehingga mengakibatkan pengguna lain terganggu pada saat menggunakan layanan Internet.

Rules yang telah dirancang nantinya akan diubah kedalam bentuk regexp (Regular Expression) POSIX yang digunakan untuk mencocokkan pola. Sebagai contoh, jika user ingin melakukan perubahan *traffic* terhadap paket rdp (Remote Desktop Protocol = jenis paket yang dapat mengkoneksikan seseorang dengan komputer lain dengan tampilan grafis) maka perintah dimasukkan sebagai berikut:

```
/ip firewall layer7-protocol
add name=rdp
regexp="rdpdr.*cliprdr.*rdpsnd"
```

Tabel 2. Daftar regexp

No	Regexp value	Tipe file
1	"\\.(exe)"	.exe
2	"\\.(rar)"	.rar
3	"\\.(zip)"	.zip
4	"\\.(mp4)"	.mp4
5	"\\.(iso)"	.iso

4.3 Konfigurasi Firewall Filter

Setelah melakukan proses perancangan jenis paket yang akan diizinkan maupun diblokir, maka proses selanjutnya adalah melakukan konfigurasi Firewall Filter agar sinkronisasi antara packet classifier dan Firewall dapat berjalan.Misalkan pada contoh sebelumnya dilakukan packet classifier terhadap paket rdp, maka selanjutnya dilakukan proses konfigurasi firewall.

Setelah melakukan proses konfigurasi terhadap Firewall maka paket rdp nantinya akan ditolak oleh Mikrotik apabila terdeteksi pada jaringan.

Konfigurasi firewall untuk setiap tipe file pada Tabel 3 adalah sebagai berikut:

Tabel 3. Konfigurasi Firewall

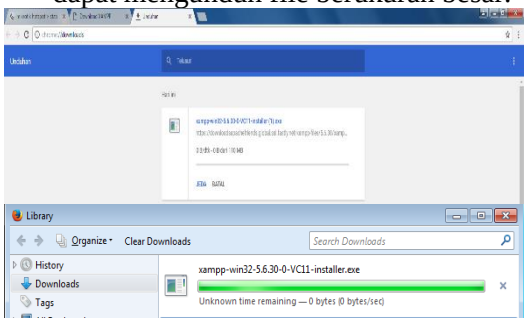
```
#add .iso
add action=mark-connection
chain=prerouting comment="iso
DOWNS" disabled=no layer7-
protocol="Extension \" .iso \"" new-
connection-mark="iso DOWNS"
passthrough=yes protocol=tcp
add action=mark-packet
chain=postrouting comment=""
connection-mark= "iso DOWNS"
disabled=no new-packet-mark=iso
passthrough=no protocol=tcp

#add .mp4
add action=mark-connection
chain=prerouting comment="mp4
DOWNS" disabled=no layer7-
protocol="Extension \" .mp4 \"" new-
connection-mark="mp4 DOWNS"
passthrough=yes protocol=tcp
add action=mark-packet
chain=postrouting comment=""
connection-mark="mp4 DOWNS"
disabled=no new-packet-mark=mp4
passthrough=no protocol=tcp
```

4.4 Implementasi Pada Mikrotik Router

Setelah melakukan proses konfigurasi, maka selanjutnya dilakukan percobaan untuk melihat hasil dari penerapan L7. Untuk itu, dilakukan simulasi dengan menggunakan 8 buah komputer yang akan melakukan proses pengunduhan file instalasi aplikasi dengan jenis file .exe berukuran 110 MB. Dari pengujian didapati hasil sebagai berikut:

1. Dari 8 PC tidak ada satu pun yang berhasil mengunduh file yang ditujukan.
2. L7 berhasil mendeteksi paket data dan melakukan pemblokiran terhadap file yang hendak diunduh.
3. Stabilitas layanan Internet pada jaringan terjaga karena tidak ada pengguna yang dapat mengunduh file berukuran besar.



Gambar 1 File dengan ekstensi tertentu gagal diunduh

5. KESIMPULAN

Kesimpulan yang dapat diperoleh dari penelitian ini adalah dengan menggunakan L7 Protocol sebagai packet classifier merupakan salah satu cara yang dapat ditempuh untuk membatasi penggunaan bandwidth dalam jaringan. Selain itu, L7 Protocol dapat pula digunakan untuk mengubah alur tipe data spesifik sehingga mengurangi kemungkinan malware untuk dapat menyebar pada jaringan komputer di lingkungan UAJM.

6. DAFTAR PUSTAKA

[1] Hidayat, A.2018. *Comparative Analysis of Mikrotik Site Filter Using Address List Techniques, Layer7 Protocols, Web Proxy, Mangle and DNS Static* [online]. Dapat diakses pada : https://www.researchgate.net/publication/327963385

[2] Helmiawan, M. Agreindra.2018. *Internet Positif dengan Metode Web Filtering Layer 7 Pada Jaringan Wireless (Study Case Hotspot RT4*

Cipeuteuy Baru Sumedang) [online]. Dapat diakses pada https://www.researchgate.net/publication/328138592

[3] Norton Peters. (1999). *Complete Guide to Networking*. Sams, India.

[4] P. KOMINFO, *"Pengguna Internet Indonesia Nomor Enam Dunia", Website Resmi Kementerian Komunikasi dan Informatika RI, 2014*. [Online]. Dapat diakses pada https://kominfo.go.id/content/detail/4286/pengguna-internet-indonesia-nomor-enam-dunia/0/sorotan_media

[5] Murch, R.2012, *Project Management: Best Practices for IT Professionals*, Ed.1, Prentice Hall, New Jersey.

[6] Sutanta, Edy, (2005). *Komunikasi Data dan Jaringan*, Graha Ilmu,Yogyakarta.