ANALISIS KINERJA PACKET FILTERING BERBASIS MIKROTIK ROUTERBOARD PADA SISTEM KEAMANAN JARINGAN

Ari Muzakir
Fakultas Ilmu Komputer, Program Studi Teknik Informatika
Universitas Bina Darma
Email: arimuzakir@binadarma.ac.id

Maria Ulfa
Fakultas Vokasi, Program Studi Teknik Komputer
Universitas Bina Darma
Email: maria.ulfa@binadarma.ac.id

ABSTRAK

Pada penelitian ini fokus pada ujicoba kinerja jaringan komputer dari sisi sistem keamanan jaringan. Ujicoba sendiri dilakukan pada jaringan komputer yang ada di Laboratorium Komputer di Universitas Bina Darma menggunakan sistem operasi Mikrotik. Adapun hasil akhir yang diharapkan melalui penelitian ini yaitu untuk melihat secara komprehensif kemampuan *packet filtering* yang terdapat di *mikrotik routerboard* dalam mengatasi masalah keamanan jaringan komputer. Keamanan jaringan yang dimaksud adalah kemampuan pada proses pemblokiran URL *http* dan *https*. Pada ujicoba yang dilakukan, *filtering rule* mampu melakukan blok *url* yang ada pada *protocol HTTP* maupun *HTTPS* yang mana membuktikan bahwa kinerja dari *filtering rule* cukup baik. Dalam menganalisis kinerja *packet filtering* menggunakan *tool network packet anayzer* Wireshark dengan cara melakukan capture paket yang lewat didalam jaringan dan menampilkan semua informasi secara detil. Hasil akhir yang didapatkan dalam proses simulasi sistem keamanan jaringan menggunakan *wireshark* adalah setiap paket yang dikirim tidak dapat dibaca (*blokir*) baik pada *protocol* http maupun https. Kinerja dari *tool*s disebuah *router* mikrotik tidak menjamin keamanan yang baik, efektivitas keamanan tergantung pada kemampuan administrator dalam mengkonfigurasi sebuah keamanan tersebut.

Kata kunci: *packet filtering*; sistem keamanan jaringan; *microtik routerboard;* analisis kinerja jaringan.

ABSTRACT

In this research focus on testing the performance of computer networks from the side of the network system. Experiments performed using Mikrotik operating system on a computer network that is in the Computer Laboratory at the University of Bina Darma. The purpose of this program is to find out the filtering capability of the routerboard microtic in solving computer network problems.Network security is the ability to block http and https URLs. In the experiments carried out, the filtering rule is able to block urls that exist in both http and https protocols which prove that the performance of the filtering rule is quite good. In analyzing packet filtering performance using the Wireshark anayzer network packet tool by capturing packets that pass in the network and display all the information in detail. The final result obtained in the network security system simulation process using Wireshark is that each packet sent cannot be read (blocked) on both http and https protocols. The performance of the tools on a microtic router does not guarantee good security, the effectiveness of security depends on the ability of the administrator to configure a security.

Keywords: *packet filtering; network security system; mikrotik routerboard.*

1. PENDAHULUAN

Kemajuan teknologi pada saat ini memaksa seluruh jaingan komputer yang ada saat ini untuk mampu menunjukkan bahwa model sistem keamanan terus dianggap masih sangat penting bagi pengguna yang menginginkan suatu keamanan baik dari dalam maupun dari luar jaringan dikarenakan *internet* merupakan sebuah media jaringan komputer yang memiliki akses sangat terbuka di dunia. Sehingga akibat yang harus ditanggung adalah jaminan keamanan dari pengguna yang terhubung secara langsung kedalam jaringan *internet* tersebut. Berbagai bentuk serangan bahkan ancaman baik secara langsung maupun tidak langsung akan memberikan dampak pada aktifitas yang terjadi pada jaringan internet tersebut, sehingga utnuk memberikan proteksi terhadap berbagai bentuk kemungkinan terjadi serangan dalam jaringan tersebut maka

dibutuhkan suatu mode keamanan seperi *firewall*. *Firewall* sendiri merupakan konsep dari sistem keamanan yang terdapat pada sistem operasi. Sistem operasi pada suatu jaringan komputer merupakan media pengatur sumber daya yang mana memberikan keamanan atau proteksi pada jaringan tersebut, serta menjadikontrol pengguna untuk selalu dapat tersambung pada sumber jaringan [1]. Sedangkan *Firewall* dikonfigurasi untuk dapat mencegah akses yang tidak diharapkan kedalam jaringan baik dari dalam maupun luar.

Firewall mempunyai dua komponen penting yaitu *router* dan *application gateway*[2]. *Router* adalah *hardware* yang mempunyai *software* sendiri untuk membangun suatu benteng yang menjadi pertahanan untuk jaringan, sedangkan *application gateway* adalah *software* khusus untuk mengamati paket yang keluar dan masuk. Kemampuannya dalam menjalankan keamanan terdiri atas *packet filtering* dan *proxy services*. *Packet filtering* merupakan aksi yang dilakukan suatu alat atau *software* yang secara ketat mengontrol pemilihan aliran dari suatu paket yang berisi informasi yang didapat dari suatu jaringan [3][4].

Pada penelitian ini menggunakan sistem operasi *mikrotik*. *Mikrotik router* adalah salah satu sistem operasi yang dapat digunakan sebagai *router* jaringan yang handal, mencakup berbagai fitur lengkap untuk jaringan komputer. Selain itu *Mikrotik* dapat juga berfungsi sebagai *firewall* [2][5]. Melalui penelitian ini akan melakukan analisis kinerja dari sistem keamanan jaringan yaitu *packet filtering* untuk mengetahui kinerja didalam melakukan pemblokiran akses (*url* dan domain *block*). Tujuan dari penelitian ini adalah melakukan perancangan sistem keamanan menggunakan *packet filtering* sebagai *firewall* dengan menggunakan mikrotik *routerboard*, kemudian melakukan analisis kinerja untuk mengetahui kemampuan didalam *firewall*.

2. METODOLOGI PENELITIAN

Dalam menjalankan penelitian ini menerapkan model eksperimen, dimana dimulai dari pembentukan dan pemeliharaan kelompok, kontrol, memberikan keputusan yang terjadi, mengontrol pada setiap faktor-faktor yang relevan, melakukan perubahan yang diizinkan, dan pada akhirnya adalah monitoring terhadap hasil pengukuran tersebut [6]. Adapun penelitian model eksperimen ini dilakukan melalui beberapa tahapan yaitu:

a) Persiapan yaitu melakukan observasi terhadap objek yang akan diteliti, pengumpulan kebutuhan yang berkaitan dengan teori-teori dan konsep, menentukan variabel penelitian, dan membuat desain model.
b) Pelaksanaan yaitu melakukan ujicoba atau penelitian, pengumpulan data-data hasil ujicoba, melakukan analisis sampai pada penyusunan laporan hasil.
c) Kesimpulan yaitu diperoleh hasil akhir dari pengamatan dan ujicoba yang dapat digunakan sebagai bahan keputusan.

2.1 Analisis

Sebelum melakukan analisis *packet filtering* dalam sistem keamanan jaringan, ada beberapa tahap yang akan dilakukan oleh penelitian diantaranya:

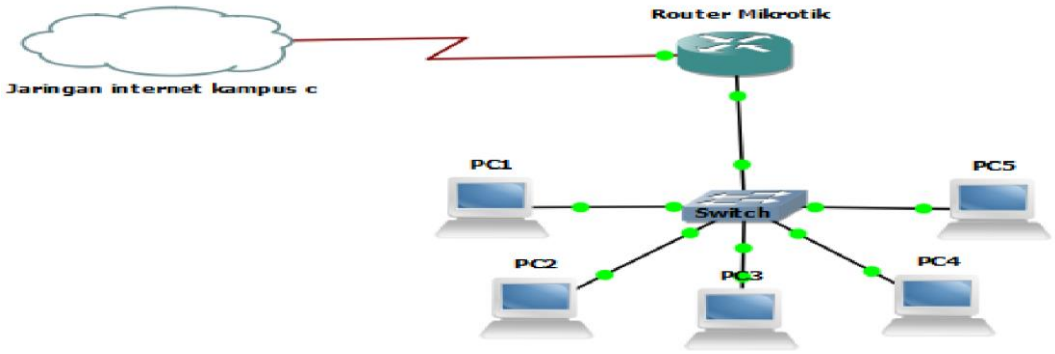
a) Konfigurasi *router mikrotik* dan *client* sehingga dapat *connect* ke *internet* (*internet services provider*) yang terhubung ke *server* [7].
b) Konfigurasi *router mikrotik* untuk menerapkan *packet filtering*.
c) Melakukan tes perbandingan variabel (URL *block* dan Domain *block*) pada *packet filtering* [8].

2.2 Perancangan Topologi Jaringan

Pada penelitian ini peneliti menggunakan peralatan yaitu *router*, *switch*, kabel *straight*, dan 5 personal komputer. Pada penelitian melakukan *monitoring* secara langsung pada *router* yang selanjutnya proses implementasi dilakukan pada komputer dengan memakai aplikasi *winbox*. Pada komputer *server* serta *client* akan terkoneksi langsung melalui jaringan *intranet* dengan *subneting* yang sama, dan masing-masing komputer *client* diberi IP *addres* pada tabel 1 dibawah ini:

Tabel 1. IP Address jaringan LAN pada laboratorium cisco 1

No	*Nama*	*IP Address*	*Subnetmask*
1	*Personal komputer (PC)*	*192.168.10.2/24 -192.168.10.6/24*	255.255.255.0
2	*Router MikroTik*	*Gateway: 192.168.10.1/24*	255.255.255.0

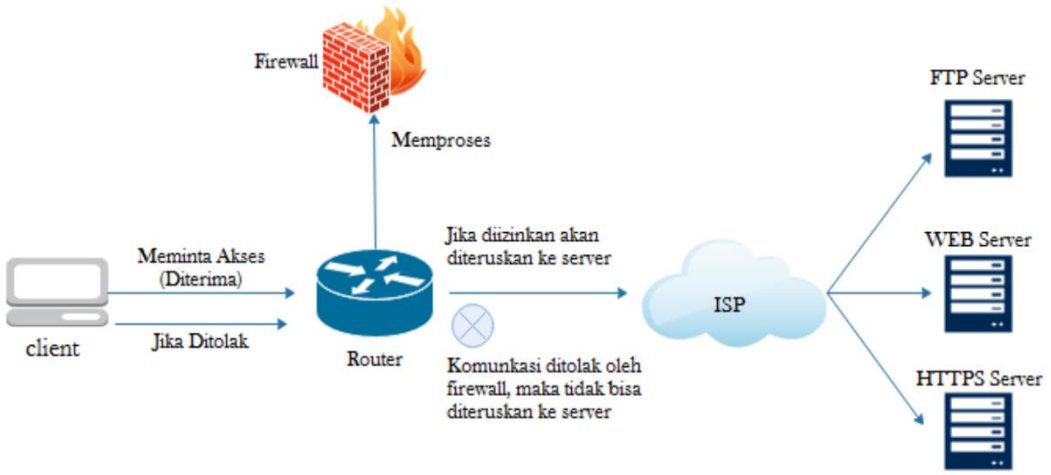


Gambar 1. Perancangan Topologi Jaringan

Pada gambar 1 tersebut menunjukkan bahwa perancangan topologi menggunakan komputer core i3 dengan sistem operasi windows pada Laboratorium Cisco 1 Kampus C Universitas Bina Darma, masing-masing memiliki 25 PC *client* disetiap ruangan yang terhubung dengan *switch* dan menggunakan *router mikrotik*, dimana peneliti hanya menggunakan 5 PC, 1 switch dan *router mikrotik* sebagai bahan penelitian pada Laboratorium cisco 1.

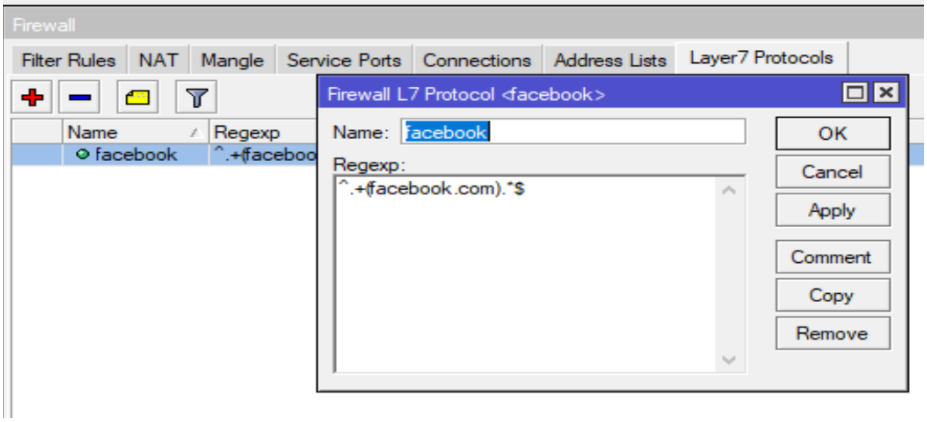
2.3 Perancangan Firewall Filtering

Setiap paket yang memasuki atau meninggalkan jaringan akan dikonfigurasi baik diterima atau ditolak sesuai dengan aturan yang ditentukan oleh pengguna [8]. *Packet filtering* ini dalam hal transparansi kepada pengguna sudah cukup baik, namun beberapa hal sulit untuk dilakukan konfigurasi. Pada gambar 2 berikut memperlihatkan perancangan dari *packet filtering*.



Gambar 2. Perancangan *Packet filtering*

Untuk mem-*block* situs-situs yang dirasa tidak diharapkan untuk ditampilkan oleh *client* seperti facebook, youtube, dan *website* lainnya, *mikrotik* sendiri menyediakan fitur *acces control list* (ACL). Fitur ini berfungsi untuk memberikan akses permintaan atau memblokir *traffic* dari *ip address* tertentu dan untuk mengatur *traffic* berdasarkan *source* / *destination* ip *address* dan *port* [9]. Dapat dikatakan bahwa ACL sendiri terbukti dapat menangani berbagai kondisi yang terjadi pada *firewall*. Dengan memasukan ip atau domain *website* yang ingin di *block* pada menu layer 7 *protocol*: contohnya seperti facebook.com, sebuah *client* tidak dapat mengakses *website* tersebut. Caranya adalah dengan memasukan script ^.+(facebook.com).*$ yang dimana script tersebut bertujuan untuk memasukkan *list* target yang ingin di *block*. Berikut ini pada gambar 3 adalah tampilan menu *layer* 7 *protocol* .



Gambar 3. Ujicoba Menu *Layer* 7 *Protocol*

Dari ujicoba pada Gambar 3 diatas, *firewall* dapat melakukan *blocking* terhadap *website* yang telah dimasukkan yang mana untuk selanjutnya adalah melakukan *filter rules*. Pada *filter rules* terdapat *menu chain* yaitu suatu perintah lanjutan untuk mem-*block website* yang ditargetkan dengan perintah antara lain *chain forward, chain input,* dan *chain oputput* [10].

Perintah *chain* tersebut terdapat di dalam *mikrotik* yang dapat mem-*block* atau membatasi hak akses suatu *client* untuk mengakses *website* target yang diberi perintah *chain* tersebut. Berikut ini adalah tampilan dari menu filter *rules* yang terdapat dalam *mikrotik router* OS. Setelah perintahh chain diterapkan, maka untuk menjalankan proses selanjutnya adalah dengan melakukan perintah perintah *action drop*. Perintah *action drop* adalah perintah yang digunakan untuk membuang paket data yang tersimpan pada *client* melalui perangkat *router*. Proses ini dilakukan secara diam-diam agar tidak diketahui, dengan mengirimkan pesan penolakan ICMP (*Internet Control Message Protocol*), sehingga ketika *client* mengirimkan pesan *ping* dari CMD, maka hasilnya adalah *request time out* (RTO).

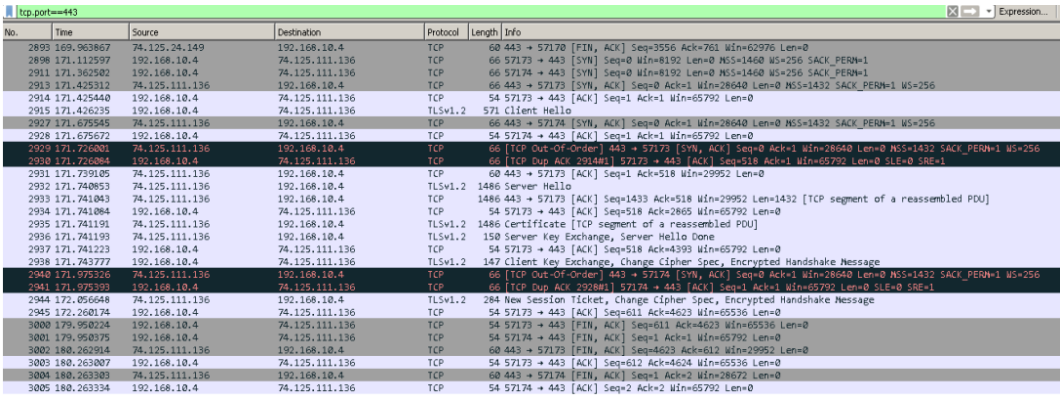
3. HASIL DAN PEMBAHASAN

Sistem keamanan *filtering rule* dapat memblokir akses *protocol* http maupun *https* serta kinerja sistem keamanan *filtering* mampu melakukan *blokir* terhadap beberapa akses ke situs *web* tertentu.

3.1 Analisis Kinerja Packet Filtering

Pada proses analisa sistem keamanan jaringan, firewall bertindak sebagai tempat dilakukannya pemfilteran satu layer yang menerapkan metode firewall packet filtering. Metode ini melakukan filtering paket data berdasarkan parameter yang sudah ditentukan sebelumnya. Cara kerja metode ini berada pada level IP paket data serta membuat keputusan tindakan yang kemudian akan memberikan akses atau menolak. Sehingga metode ini hanya didesain untuk mamp u mengontrol setiap paket data yang lewat berdasarkan alamat asal, tujuan, port yang digunakan serta tipe informasi yang terdapat dalam paket tersebut. IP *firewall* sangat aman namum dapat mengabaikan sejumlah *log* yang mungkin penting.

Network Filter memiliki lima rantai utama yang dapat digunakan yaitu *prerouting*, *postrouting*, *input*, *forward*, dan *output*. Setiap paket yang tiba pada *iptables* akan melalui rantai *prerouting*. Disini paket akan mengalami perubahan yang sesuai. Dari sini, paket akan masuk ke keputusan *routing*. Jika paket ditujukan untuk *host* itu sendiri, maka akan diteruskan ke rantai *input*, namun jika paket ditujukan untuk *host* lain, maka paket akan diteruskan ke rantai *forward*. Paket yang masuk ke rantai *input* akan diproses oleh *host* lokal. Jika kemudian ada paket yang keluar, maka paket akan masuk ke rantai *output*. Paket yang berasal dari *forward* dan *output* kemudian akan masuk ke rantai *post-routing* sebelum akhirnya paket benar-benar meninggalkan *host*. Ketika paket masuk melewati *firewall*, paket filter akan langsung menginspeksi *header* setiap paket, kemudian mencocokan dengan kebijakan dan peraturan yg diterapkan pada paket filter, paket akan lewat jika memang di izinkan, sedangkan paket akan di tolak apabila paket tersebut tidak memenuhi syarat pada paket filter. Pada gambar 4 berikut merupakan contoh hasil setelah diterapkannya pemblokiran akses maka *wireshark* tidak dapat membaca *https* yang *ip add* 157.240.13.35 yaitu facebook.com yang sebelumnya sudah diterapkan pada *router mikrotik* RB201 1iL-RM, serta hasil pengujian pemblokiran beberapa situs setelah proses konfigurasi dibandingkan dengan sistem keamanan *web proxy* pada tabel 2.



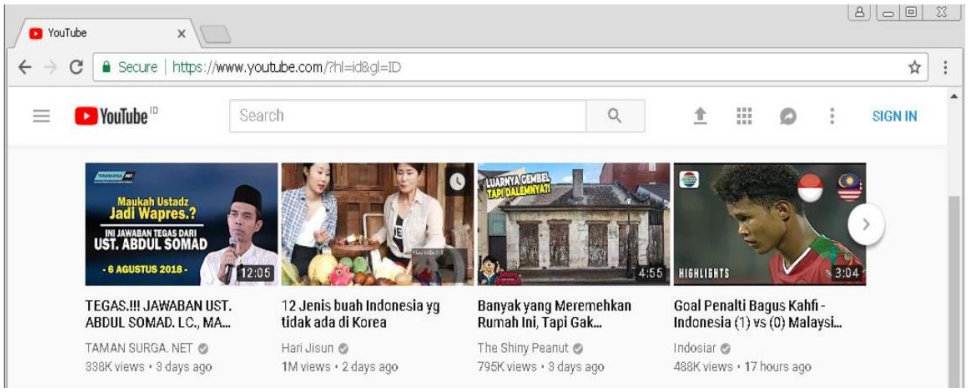
Gambar 4. Hasil Penerapan Pemblokiran Akses Dengan Aplikasi *Wireshark*

Tabel 2. Hasil Pemblokiran Situs *Web*

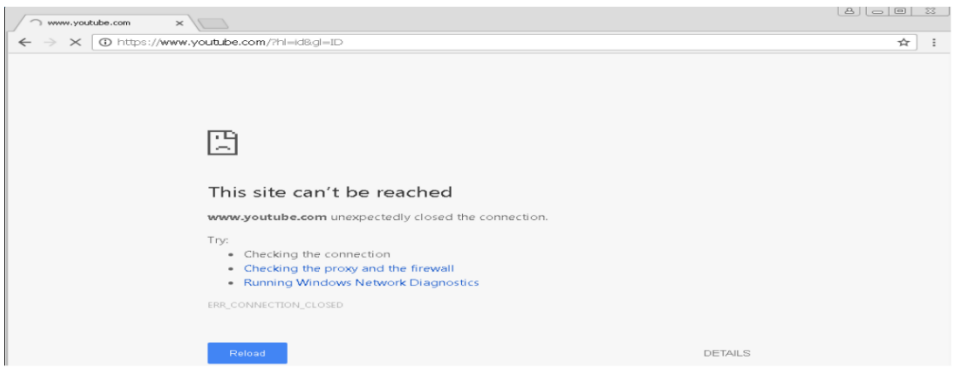
No	*URL (http/https)*	*Filtering rule*	*Web Proxy*
1	*yahoo.com*	*Deny*	*Deny*
2	*id.portalgaruda.org*	*Deny*	*Deny*
3	*sisfo.binadarma.ac.id*	*Deny*	*Deny*
4	*youtube.com*	*Deny*	*Allow*
5	*playboy.com*	*Deny*	*Deny*
6	*facebook.com*	*Deny*	*Allow*

3.2 Pengujian Hasil

Untuk mengetahui keberhasilan dari beberapa tahapan konfigurasi yang telah dilakukan, maka perlu dilakukan ujicoba. Ujicoba yang dilakukan yaitu pemblokiran *url* dan domain ada *filtering rule* dalam sistem keamanan jaringan. Pada gambar 4 dan 5 berikut menunjukkan hasil ujicoba.



Gambar 4. Akses *url* dari youtube.com secara normal (tanpa *filtering rule*)



Gambar 5. Akses *url* dari youtube.com dengan sistem pemblokiran (*filtering rule*)

4. KESIMPULAN

a) Adapun tujuan dari penelitian ini adalah untuk mengetahui kemampuan *packet filtering* dalam melakukan *bloking* terhadap suatu situs *web*, kemudian hasilnya adalah metode ini dapat diterapkan untuk sistem keamanan jaringan.
b) Dalam menganalisis kinerja *packet filtering* menggunakan *tool network packet anayzer wireshark* dengan cara melakukan *capture* paket yang lewat didalam jaringan dan menampilkan semua informasi secara detil.
c) Dengan melakukan konfigurasi dan ujicoba sistem keamanan jaringan ini membuktikan bahwa kinerja dari *filtering rule* cukup baik dalam memblok akses *web protocol http* dan *https*.

DAFTAR PUSTAKA

[1] T. Listyorini and R. Meimaharani, "NETWORKING OPERATING SYSTEM (NOS) BERBASIS SIMULASI," *J. SIMETRIS*, vol. 9, no. 1, pp. 181–188, 2018.
[2] M. Grennan, "Firewall and Proxy Server HOWTO," *Linux Doc. Proj.*, p. 40, 2000.
[3] Rodiah, "Perbandingan Cara Kerja Packet Filtering Dan Proxy Services Sebagai Firewall Pada Keamanan Jaringan," *UG J.*, vol. 6, no. 11, 2012.
[4] J. Boutet, "Use offense to inform defense . Find flaws before the bad guys do.," *SANS Inst.*, 2010.
[5] A. Hikmaturokhman, A. Purwanto, and R. Munadi, "Analisis Perancangan Dan Implementasi Firewall Dan Traffic Filtering Menggunakan Cisco Router," *Semin. Nas. Inform.*, 2010.
[6] A. Muzakir and C. D. Kusmindari, "Design of Push-Up Detector Applications Using Quality Function Development and Anthropometry For Movement Error Detection," *Sci. J. Informatics*, vol. 5, no. 2, pp. 248–257, 2018.
[7] A. P. N. Permana and R. Firmansyah, "Distribusi Jaringan Menggunakan Routing Ospf," *J. SIMETRIS*, vol. 9, no. 1, pp. 519–532, 2018.
[8] L. H. Chen and W. C. Ko, "Fuzzy approaches to quality function deployment for new product design," *Fuzzy Sets Syst.*, vol. 160, no. 18, pp. 2620–2639, 2009.
[9] P. Silitonga and I. S. Morina, "Analisis Qos (Quality Of Service) Jaringan Kampus Dengan Menggunakan Microtic Routerboard (Studi Kasus : Fakultas Ilmu Komputer Unika Santo Thomas S.U)," *J. TIMES*, 2014.
[10] I. Riadi, "Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik Pendahuluan Landasan Teori," *JUSI, Univ. Ahmad Dahlan Yogyakarta*, 2011.