In Search

p-ISSN: 2085-7993
e-ISSN:2580 -3239
Volume 17 No. 02, November 2018

PERANCANGAN PENGAMANAN *FIREWALL* PADA JARINGAN LAN MENGGUNAKAN METODE *PACKET FILTERING*

Kurnia[1],Eko Agus Darmadi [2]
Politeknik Tri Mitra Karya Mandiri, Karawang, Indonesia
Email: niamansur03@gmail.com,ekoagus.darmadi@gmail.com

Abtrak

Firewall adalah tools dalam jaringan komputer yang berfungsi untuk pengamanan pada sebuah sistem jaringan internet. *Firewall* merupakan salah satu bagian dari keamanan jaringan (termasuk keamanan internet) yang paling mudah untuk diimplementasikan pada jaringan komputer apapun, serta mudah untuk dikonfigurasi secara manual. *firewall* berfungsi untuk melindungi setiap komputer *user* dari serangan konten-konten berbahaya yang tidak diinginkan. Perancangan ini bertujuan untuk membuat suatu batasan pengaksesan data pada jaringan internet yang tidak diizinkan dengan menggunakan sebuah *software packet filtering*. *Packet filtering* mampu memblokir paket data berdasarkan kriteria tertentu seperti protokol yang digunakan dan berbagai karakteristik protokol. Dari perancangan *firewall* pada jaringan LAN menggunakan metode *packet filtering* yang telah dibuat, diharapkan *packet filtering firewall* mampu menghentikan paket data yang tidak diizinkan sesuai dengan yang diharapkan. Serta untuk menjadi referensi dalam menentukan pembuatan sistem keamanan jaringan.

Kata kunci: Firewall, Paket data, Jaringan LAN, Packet filtering.

Abstract

Firewall is tools in a computer network that serves to secure an internet network system. Firewall is one part of network networks (including internet internet) which is most easily implemented on any computer network, and is easy to manually configure. The firewall serves to protect every computer user from attacks of unwanted harmful content. This design aims to limit the access of data on internet networks that cannot be used by using a filtering software package. Packet filtering is able to delete data packets based on different criteria. From designing a firewall on a LAN network using the packet filtering method that has been created, it is expected that packet filtering firewalls can stop data packets that are not as expected. And to be a reference in determining the making of a network system.

Keywords: Firewall, Data Package, LAN Network, Packet filtering.

p-ISSN: 2085-7993
e-ISSN:2580 -3239
Volume 17 No. 02, November 2018

1. PENDAHULUAN

Firewall merupakan salah satu bagian dari keamanan jaringan (termasuk keamanan internet) yang paling mudah untuk diimplementasikan pada jaringan komputer apapun, serta mudah untuk dikonfigurasi secara manual. Pada jaringan LAN, *firewall* berfungsi untuk melindungi setiap komputer *user* dari serangan konten-konten berbahaya yang tidak diinginkan. Dapat juga untuk menjaga keamanan jaringan komputer termasuk data-datanya.[1]

Pada instalasi jaringan LAN, selain memperhatikan keamanan juga memerlukan suatu cara/teknik dalam hal memelihara (*maintenance*) keamanan. Penerapan teknologi *packet filtering* pada *firewall* jaringan sangat diperlukan. Hal ini berguna untuk membatasi *resource* yang ada digunakan secara benar dan untuk menjadi referensi dalam menentukan pembuatan sistem keamanan jaringan.[2]

Dalam *firewall*, selain mampu diterapkan *packet filtering* sebagai pemeliharaan (*maintenance*) keamanan, juga dapat diterapkan suatu metode yang bekerja ketika *firewall* secara acak menutup semua *port* terhadap hak akses *user* yang telah diberi izin untuk mengaksesnya. Metode *port knocking* mampu membuka suatu *port* yang telah ditutup *firewall* dengan catatan *user* mengetahui *knocking* dari *port* tersebut. Selanjutnya ketika teknik pemeliharaan (*maintenance*) pada jaringan telah dirasa sesuai yang diharapkan, maka setelah itu jaringan perlu terfokus pada peningkatan keamanan. Salah satunya melalui sistem otentikasi pengguna jaringan tersebut.[3]

Pada perancangan pengamanan firewall ini, penulis menggunakan metode *packet filtering firewall* yang dapat menghentikan paket data yang tidak diizinkan. *Packet filtering* telah terbukti menjadi alat yang berguna untuk menempatkan kontrol akses ke lalu lintas *IP*. *Packet filtering* yang dapat digunakan untuk memblokir paket data berdasarkan kriteria tertentu seperti protokol yang digunakan dan berbagai karakteristik protokol.[3]

Hasil yang diharapkan dari perancangan pengamanan *firewall* pada jaringan LAN menggunakan metode *packet filtering* dapat mengaplikasikan *firewall* yang telah dibuat. Apakah *packet filtering firewall* dapat menghentikan paket data yang tidak diizinkan sesuai dengan yang diharapkan. Serta untuk menjadi referensi dalam menentukan pembuatan sistem keamanan jaringan.[2]

2. TINJAUAN PUSTAKA

2.1 Keamanan Jaringan Komputer

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Sering kali urutan keamanan berada diurutan kedua atau bahkan diurutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila mengganggu performa sistem, seringkali keamanan dikurangi atau bahkan ditiadakan. Terhubungnya LAN atau komputer ke internet membuka potensi adanya lubang keamanan yang tadinya bisa ditutup dengan mekanisme keamanan secara fisik. Ini sesuai dengan pendapat bahwa kemudahan mengakses informasi berbanding terbalik dengan tingkat keamanan sistem informasi itu sendiri.

Keamanan informasi adalah bagimana kita dapat mencegah penipuan atau mendeteksi adanya penipuan di sebuah sistem berbasis informasi, dimana informasiinya sendiri tidak memiliki arti fisik. Keamanan jaringan menurut Mariusz Stawowski dalam jurnalnya "*The principles of network security design*", adalah keamanan jaringan yang utama sebagai pelindungan sumber daya sistem terhadap ancaman yang berasal dari luar jaringan. Keamanan komputer digunakan untuk mengontrol resiko yang berhubungan dengan penggunaan komputer. Keamanan

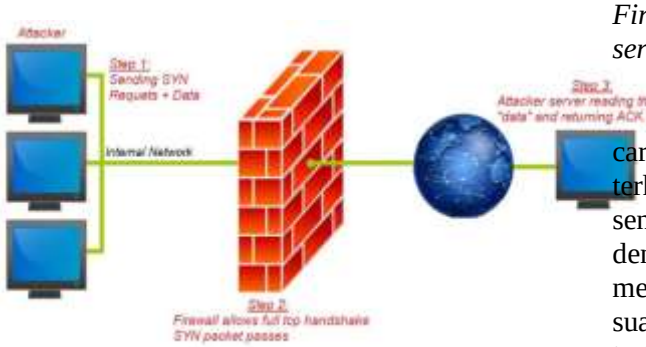
p-ISSN: 2085-7993
e-ISSN:2580 -3239
Volume 17 No. 02, November 2018

komputer yang dimaksud adalah keamanan sebuah jaringan (internet).[4]

2.2 Pengertian Local Area Network (LAN)

Menurut Nasmul Irfan, ST dalam bukunya yang berjudul *"Pengenalan dan InstalasiJaringan"* menjelaskan bahwa Jaringan *Local Area Network* (LAN) adalah jaringan yangdibatasi oleh area yang relatif kecil, umumnya dibatasi oleh area lingkungan seperti sebuah perkantoran di sebuah gedung atau sebuah sekolah dan biasanya tidak jauh dari sekitar 1 km persegi.
Local Area Network (LAN) memberikan banyak keuntungan kepada pengguna, diantara keuntungan tersebut ialah dapat saling berbagi informasi dan sumber daya. *Local Area Network* (LAN) juga merupakan jaringan komputer berkecepatan tinggi yang cakupan wilayahnya cukup kecil.[5]

2.3 Firewall



Gambar 2.1 Firewall

Firewall adalah alat untuk mengimplementasikan kebijakan security (*security policy*). Sedangkan kebijakan security, dibuat berdasarkan perimbangan antara fasilitas yang disediakan dengan implikasi *security*-nya. Semakin ketat kebijakan *security*, semakin kompleks konfigurasi layanan informasi atau semakin sedikit fasilitas yang tersedia di jaringan. Sebaliknya, dengan semakin banyak fasilitas yang tersedia atau sedemikian sederhananya konfigurasi yang diterapkan, maka semakin mudah orang orang 'usil' dari luar masuk kedalam sistem (akibat langsung dari lemahnya kebijakan *security*).

Dalam dunia nyata, *firewall* adalah dinding yang bisa memisahkan ruangan, sehingga kebakaran pada suatu ruangan tidak menjalar ke ruangan lainnya. Tapi sebenarnya *firewall* di Internet lebih seperti pertahanan disekeliling benteng, yaitu mempertahankan terhadap serangan dari luar. Gunanya:

1) memba tasi gerak orang yang masuk ke dalam jaringan internal
2) memba tasi gerak orang yang keluar dari jaringan internal
3) menceg ah penyerang mendekati pertahanan yang berlapis

Jadi yang keluar masuk *firewall* harus *acceptable*. *Firewall* merupakan kombinasi dari *router*, *server*, dan *software* pelengkap yang tepat.

Firewall merupakan suatu cara/sistem/mekanisme yang diterapkan baik terhadap *hardware* , *software* ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah *workstation*, *server*, *router*, atau *local area network* (LAN).[1]

2.4 Pake Data

Paket data adalah entitas dasar dari semua sistem komunikasi. Keamanan jaringan demikian berarti keamanan dari paket data. Sebuah paket data adalah blok yang paling dasar komunikasi yang melibatkan aliran *streamline* terbatas replika

p-ISSN: 2085-7993
e-ISSN:2580 -3239
Volume 17 No. 02, November 2018

lainnya untuk mengirimkan informasi dari satu perangkat ke perangkat lainnya. Sebuah paket data yang terkandung dalam segmen data yang menimpan informasi lain seperti protokol yang digunakan, tujuan *hardware* alamat dan lain-lain. Singkatnya, identitas setiap paket yang datang dari sumber tidak bisa diandalkan dapat dideteksi dengan mempelajari isinya. Manajemen trafik data, pengukuran trafik jaringan komputer dan *sniffing* adalah beberapa produk dari *packet capture*, *packet capture* juga digunakan sebagai basis untuk berbagai macam sistem keamanan. [6] , [7]

2.5 Paket Filter

Informasi yang ditransmisikan pada jaringan dalam bentuk "paket", dengan kata lain informasi dibagi menjadi potongan-potongan kecil pada sumbernya, ditransmisikan dan kembali berkumpul pada penerima akhir. *Firewall* memeriksa bagian yang relevan dari sebuah paket dan hanya memungkinkan orang-orang yang sesuai dengan konfigurasi yang akan berhasil dikirim. Inilah sebabnya, beberapa paket yang tepat dikonfigurasi salah yang ditolak oleh *firewall.* Dalam kasus *firewall proxy*, lalu lintas tidak pernah mengalir langsung antara jaringan. Sebaliknya, *proxy repackages* permintaan dan tanggapan. Tidak ada host internal dapat diakses secara langsung dari jaringan eksternal dan tidak ada *host eksternal* secara langsung dapat diakses oleh *host internal*. Pekerjaan utama dari firewall adalah *Packet Filtering*, yang mengontrol akses dengan memeriksa paket berdasarkan isi dari *header* paket. [8] , [9]

Salah satu cara untuk menerapkan *firewall* adalah untuk memanfaatkan apa yang disebut *packet filtering*. *Packet filtering* telah terbukti menjadi alat yang berguna untuk menempatkan kontrol akses ke lalu lintas *IP*. *Packet filtering* yang dapat digunakan untuk memblokir paket data berdasarkan kriteria tertentu seperti protokol yang digunakan dan berbagai karakteristik protokol. Data sebagai sumber dan alamat tujuan, UDP dan TCP, *port* asal dan tujuan dapat digunakan dalam keputusan penyaringan. Metode ini juga banyak digunakan dalam sistem monitoring jaringan, dengan menerapkannya pengguna dapat memantau aktifitas pada jaringan setiap saat. [7] , [10]

2.6 IP Addres

Menurut Safrizal (2005:110) "*IP Address* merupakan pengenal yang digunakan untuk memberi alamat pada tiap-tiap komputer dalam jaringan". Sedangkan "Format *IP address* adalah bilangan 32 bit yang tiap 8 bit-nya dipisahkan oleh tanda titik".[11]

IP Address sebenarnya terdiri dari dua bagian, yaitu : *Network ID* dan *Host ID*. *Network ID* menentukan alamat dari suatu jaringan komputer dan *Host Id* menentukan alamat dari suatu komputer (*host*) dalam suatu jaringan komputer. *IP Address* memberikan alamat lengkap dari suatu komputer (*host*) yang merupakan gabungan dari nama *Network Id* dan Nama *Host ID*. Hal ini mirip dengan pemberian nama jalan dan nomor rumah pada sistem pemberian alamat rumah.

Apabila suatu organisasi memiliki *IP Address* dengan Network Id 222.124.14.0 memerlukan lebih dari satu *network* Id, maka organisasi tersebut harus mengajukan permohonan ke IANA (Internet *Assigned Number Authority*) untuk mendapatkan *IP Address* baru. Permasalahan saat ini adalah persediaan *IP Address* sangat terbatas, karena banyaknya perusahan *dotcom* yang membuat situs-situs di internet. Untuk mengatasi permasalahan yang ada dan menghindari mengajukan *IP Address* yang baru ke IANA, dibuatlah suatu metode untuk memperbanyak *Network ID* dari suatu *Network ID* yang telah dimiliki sebelumnya. Metode ini sering disebut dengan istilah *Subnetting*, yaitu mengorbankan sebagian *Host ID* untuk digunakan dalam membuat *Network ID* tambahan.[2]

p-ISSN: 2085-7993
e-ISSN:2580 -3239
Volume 17 No. 02, November 2018

3. PEMBAHASAN DAN HASIL

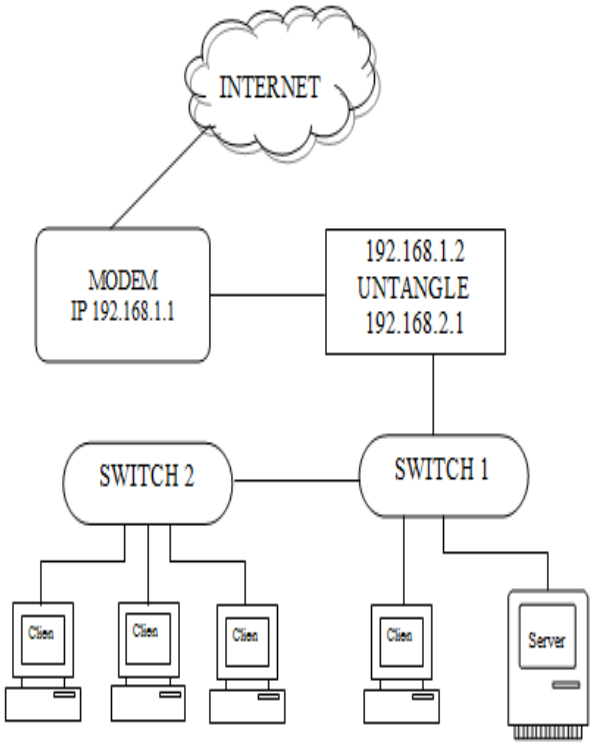
3.1 Manajemen Jaringan Usulan

Berikut ini penulis mencoba menggambarkan dan merancang sistem jaringan usulan terhadap jaringan LAN. Adapun rancangan sistem jaringan usulannya sebagai berikut.

3.1.1 Topologi Jaringan

Topologi jaringan merupakan sebuah pola rancang bangun untuk membentuk sebuah arsitektur jaringan.[2] Dalam rancangan jaringan usulan yang penulis rancang menggunakan topologi jaringan LAN. Dalam pengamanan *firewall* pada jaringan LAN, penulis menambahkan sebuah sistem *Packet Filtering* yang nantinya digunakan sebagai pendeteksi sekaligus pemutusan paket data yang tidak diijinkan. Dengan cara menambah 1 unit komputer yang nantinya digunakan sebagai *router* tambahan, yang nantinya akan di install *software Untangle*. *Router* itu nantinya akan berfungsi sebagai *firewall* (dinding pemisah) yang akan melindungi jaringan internal (*private*/LAN) dari ancaman bahaya jaringan eksternal (*public*/WAN/Internet).

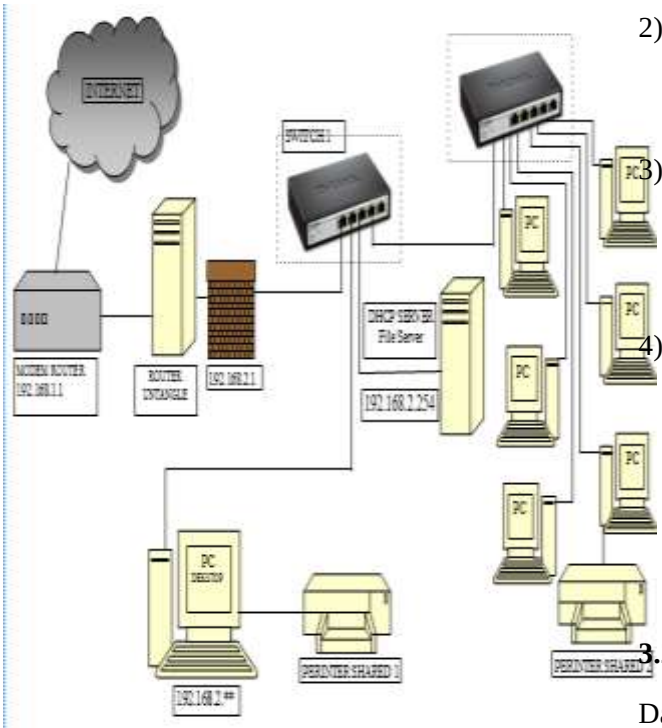
Berdasarkan rancangan jaringan usulan ini maka *IP Address* pada jaringan internal (*private*/ LAN) harus diubah dan tidak lagi menggunakan 192.168.1.xxx. *IP Address* yang penulis sarankan disini masih menggunakan *IP Address* kelas C, karena jumlah banyaknya *user* pada jaringan internal(*private*/LAN) masih bisa dibilang sedikit dan untuk *IP Address* jaringan internal (*private*/LAN) yang baru adalah 192.168.2.xxx. Jadi IP Address yang digunakan adalah 192.168.1.xxx untuk jaringan eksternal(public/WAN/Internet) dan 192.168.2.xxx untuk jaringan internal(*private*/ LAN).



Gambar 3.1 Topologi rancangan jaringan usulan

p-ISSN: 2085-7993
e-ISSN:2580 -3239
Volume 17 No. 02, November 2018

3.1.2 Skema Jaringan



Gambar 3.2 Skema jaringan

Gambar yang di atas adalah skema jaringan usulan yang telah penulis rancang untuk mengamankan jaringan komputer. Pada skema jaringan usulan penulis menambahkan untangle sebagai *router* tambahan dan sekaligus penulis menggunakan sebagai *firewall* (dinding pemisah) yang nantinya berguna untuk mengamankan jaringan internal (*private*/LAN) dari jaringan *external* (publik/WAN/internet).

Adapaun fitur-fitur yang terdapat pada skema jaringan usulan yang telah penulis rancang untuk mengamankan jaringan komputer yaitu sebagai berikut.

1) Pada jaringan usulan kita dapat menjadikan *router untangle* sebagai *firewall* sehingga proses lalu-lintas data dari *internet* ke LAN atau sebaliknya menjadi lebih aman dan cepat.
2) Dengan *untangle* penyetingan *firewall* menjadi lebih berlapis baik di-*filter* dari segi *port, url* ataupun *ip address.*
3) Dapat melakukan penyetingan *untangle* dari komputer *server* atau *client* dengan menggunakan aplikasi *web browser IE, Mozilla Firefox*, dll.
4) Dapat memblok/mem-*filter* situs-situs yang dapat menurunkan kinerja karyawan, dengan mengaktifkan *web blocker* dan dapat mengamankan jaringan internal dari virus atau ancaman lainnya dengan mengaktifkan *virus blocker*, *spyware blocker, phish blocker.*

3.2 Keamanan Jaringan

Dalam keamanan jaringan disini penulis merancang sebuah keamanan jaringan dengan metode *packet filtering firewall* yang nantinya berguna untuk mengamankan jaringan internal (*private*/LAN).

Dalam merancang sebuah keamanan jaringan dengan metode *packet filtering firewall* terdapat 3 tahapan, yaitu:

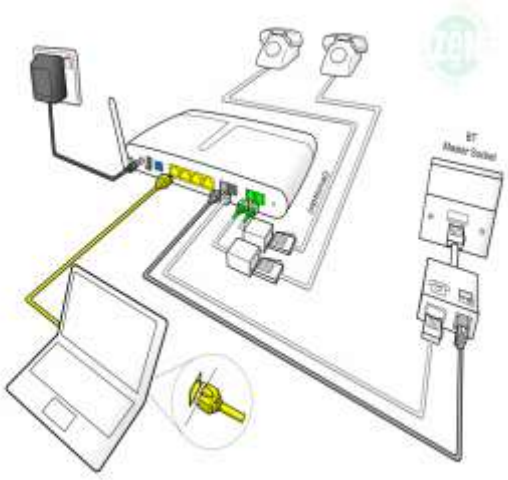
1) Instalasi dan men-*setting* software untangle *Software Untangle* memberikan tampilan simulasi yang cukup mudah dimengerti selain itu dapat mengakses langsung ke *router untangle* melalui *web browser.*

p-ISSN: 2085-7993
e-ISSN:2580 -3239
Volume 17 No. 02, November 2018

Gambar 3.3 Aplikasi Untangle

2) Setting router

Men-*setting* router merupakan pengaturan awal, yaitu pengaturan untuk membuat untangle menjadi Router OS.



Gambar 3.4 Setting router

3) Setting *Packet Filtering Firewall* pada Aplikasi *Untangle*

Pengaturan selanjutnya adalah mem-*filter* akses internet jaringan itu sendiri, karena banyak hal-hal yang sangat berbahaya yang beredar luas di *internet*, khususnya : Virus. banyak aplikasi *untangle* yang dapat digunakan dalam mem-*filter* jaringan, semua itu tergantung kebutuhan pada jaringan tersebut. Adapun pengaturan yang penulis *setting* disini adalah *Firewall*, *Web Blocker*, *Virus Blocker*, *Spyware Blocker*, *Phish Blocker*, *Attack Blocker*.

3.3 Hasil Perancangan

1. Dari hasil perancangan ini sistem dapat bekerja memblok atau mem-*filter* situs-situs yang dapat menurunkan kinerja karyawan, dengan mengaktifkan *web blocker* dan dapat mengamankan jaringan internal dari virus atau ancaman lainnya..

2. Firewal l merupakan tembok api yang bekerja melindungi komputer dari serangan virus atau segala ancaman dari jaringan internet.

3. Dalam perancangan ini packet filtering digunakan untuk membatasi pengakses internet. Packet filtering bekerja sebagai penyaring data yang di izinkan dan yang tidak di izinkan.

4. KESIMPULAN

Dari hasil perancangan pengamanan *firewall* pada jaringan LAN menggunakan metode *packet filtering firewall*, maka dapat ditarik kesimpulan antara lain:

1) Penera pan teknologi *packet filtering firewall* jaringan sangat diperlukan untuk membatasi *resource* yang ada digunakan secara benar dan untuk menjadi referensi dalam menentukan pembuatan sistem keamanan jaringan.

p-ISSN: 2085-7993
e-ISSN:2580 -3239
Volume 17 No. 02, November 2018

2) *Softwa re Untangle* memberikan tampilan simulasi yang cukup mudah dimengerti selain itu dapat mengakses langsung ke *router untangle* melalui *web browser*.

3) *Untang le* sangat berguna dan memiliki fitur yang lengkap dalam me-*manage* dan mengamankan jaringan mulai dari skala LAN hingga WAN.

DAFTAR PUSTAKA

[1] M. Van Busten, "Optimalisasi Firewall Pada Jaringan Skala Luas," no. Jaringan Komputer, hal. 1–23, 2009.

[2] S. N. Khasanah, "Keamanan Jaringan Dengan Packet Filtering Firewall (Studi Kasus PT.SUKSES BERKAT MANDIRI JAKARTA)," *Jurnal Khatulistiwa Informatika*, vol. IV, hal. 182–192, 2016.

[3] M. A. A. Gobel, Suyoto, dan T. Suselo, "Analisa Dan Pengembangan Sistem Peringatan Keamanan Jaringan Komputer Menggunakan Sms Gateway Dan Paket Filter," *Seminar Nasional Teknologi Informasi dan Komunikasi 2014 (SENTIKA 2014)*, hal. 382–388, 2014.

[4] E. N. Hartiwati, "Keamanan Jaringan Dan Keamanan Sistem Komputer Yang Mempengaruhi Kualitas Pelayanan Warnet," hal. 27–33.

[5] Moch Linto Herlambang. 2008. *Panduan Lengkap Menguasai Router Masa Depan Menggunakan MIKROTIK ROUTER OS*. Yogyakarta:Andi Offset.

[6] Suri and Brata. 2012. Comparative Study of Network Monitoring Tools: *International Journal of Innovative Technology and Exploring Engineering*, vol.1, no.3, pp. 63-65.

[7] Aluvala. 2011. Inter-domain Packet Filters to Control IP-Forging: *Research Journal of Computer Systems Engineering – An International Journal*, vol. 2, no. 2, pp. 67-72.

[8] Lindqvist, J. et all. 2010. Enterprise Network Packet Filtering for Mobile Cryptographic Identities: *International Journal of Handheld Computing Research*, vol.1, no.1, January , pp. 79-94.

[9] Arai, M. 2012. TCP/IP Visualization Systems with a Packet Capturing Function: *International Journal of Information and Education Technology*, vol.2, no.4 , 291-293.

[10] Al-Mukhtar, M.M. 2012. Development of a Flexible Real-Time Monitor for an Enterprise Network: *International Jurnal of Computer Applications*. vol.42, no. 21, pp. 42-47.

[11] Safrizal, Melwin. 2005. *Pengantar Jaringan Komputer*. Yogyakarta:ANDI.