ANALISIS DAN OPTIMASI DARI SIMULASI KEAMANAN JARINGAN MENGGUNAKAN FIREWALL MIKROTIK STUDI KASUS DI TAMAN PINTAR YOGYAKARTA

Efrahim Sinyo Rio Ola Balen Langobelen[1], Rr. Yuliana Rachmawati[2], Catur Iswahyudi[3]
Program Studi Informatika, Fakultas Teknologi Industri
Institut Sains & Teknologi AKPRIND Yogyakarta
Email: [1]rioola@gmail.com, [2]yuliana@akprind.ac.id, [3]catur@akprind.ac.id

ABSTRACT

The research objective to be achieved from this research is to conduct an analysis of network security simulations that are adapted to the network topology in Taman Pintar Yogyakarta by utilizing various features that exist in the proxy such as firewalls and other network security support features in Taman Pintar Yogyakarta.

The methodology used in this study uses the Prepare Plan Design Operate and Optimize (PPDIOO) concept, which is the Life Cycle methodology that is continuously carried out in the process of network development and implementation. This method is very suitable to be used in the development of network security systems because network security is constantly developing along with the rapid development of technology.

In general, this study produced a configuration for the Taman Pintar Yogyakarta computer network security system using a Mikrotik router firewall which included configurations for firewalls, service port management and filter configurations for Bridges. This research applies four firewall configurations which are functioned to block user activity or attacks from outside which can endanger the network security system. These configurations are blocking the use of VPN applications, blocking the use of torrent applications, blocking DDOS attacks and disguising port scanning using NMAP.

Keywords*: Microtic, Simulation, Network Security,* Taman Pintar Yogyakarta*.*

INTISARI

Tujuan penelitian yang hendak dicapai dari penelitian ini adalah melakukan analisis dari simulasi kemanan jaringan yang disesuaikan dengan topologi jaringan di Taman Pintar Yogyakarta dengan memanfaatkan berbagai fitur yang ada pada Mikrotik seperti firewall dan fitur pendukung keamanan jaringan lainnya di Taman Pintar Yogyakarta.

Metodologi yang digunakan dalam penelitian ini menggunakan konsep Prepare Plan Design Implement Operate and Optimize (PPDIOO) yaitu metologi Life Cycle yang secara berkesinambungan terus dilakukan dalam proses pengembangan dan implementasi jaringan. Metode ini sangat cocok digunakan dalam pengembangan sistem keamanan jaringan karena keamanan jaringan setiap saat terus berkembang seiring dengan cepatnya perkembangan teknologi.

Secara umum penelitian ini menghasilkan konfigurasi untuk sistem keamanan jaringan komputer Taman Pintar Yogyakarta mengunakan firewall router Mikrotik yang meliputi konfigurasi untuk firewall, pengelolaan service port serta konfigurasi filter untuk Bridge. Penelitian ini menerapkan empat konfigurasi firewall yang difungsikan untuk memblokir aktivitas pengguna atau serangan dari luar yang dapat membahayakan sistem keamanan jaringan. Konfigurasi tersebut yaitu blokir penggunaan aplikasi geratis VPN, blokir penggunaan aplikasi torrent, blokir seragan DDOS serta melakukan penyamaran untuk scaning port menggunakan NMAP.

Kata Kunci: Mikrotik, Simulasi, Keamanan Jaringan, Taman Pintar Yogyakarta.

PENDAHULUAN

Perkembangan dunia telekomunikasi saat ini sangat pesat seiring dengan peningkatan kebutuhan layanan yang cepat dan efisien. Begitu juga dengan komunikasi data, mulai dari koneksi antar dua komputer hingga jaringan komputer. Jaringan komputer saat ini merupakan suatu layanan yang sangat dibutuhkan. Jaringan komputer mempunyai manfaat yang lebih dibandingkan dengan komputer yang berdiri sendiri. Jaringan komputer memungkinkan pemakaian secara bersama baik penggunaan data, perangkat lunak dan peralatan. Sehingga kelompok kerja dapat berkomunikasi lebih efektif dan efisien. Tentunya dalam pembangunan jaringan komputer kualitas akan keamanan jaringan merupakan hal yang paling utama.

Keamanan jaringan yang dimaksud adalah bagaimana suatu jaringan mampu mengamankan jaringannya sendiri.
Segala bentuk ancaman yang datang baik langsung maupun tidak langsung akan mengganggu kegiatan yang sedang berlangsung dalam jaringan komputer. Dalam rangka melindungi kemungkinan serangan-serangan tersebut perlu di terapkan konsep firewall. Dimana firewall dirancang untuk mencegah akses yang tidak diinginkan yang datang baik dari internal maupun external jaringan. Penerapan konsep firewall terlihat cukup sederhana yaitu bila ada traffic yang datang dan menuju suatu jaringan, firewall kemudian akan melakukan pemeriksaan serta control terhadap traffic tersebut kemudian dikirimkan ke tujuannya.
Kemanan jaringan yang ada di Taman Pintar Yogyakarta masih membutuhkan pengembangan agar terbaharui dengan perkembangan teknologi dan mampu meminimalisir segala bentuk serangan yang mungkin bisa masuk ke dalam sistem jaringan. Menyikapi keamanan tersebut dipandang perlu untuk menerapkan kebijakan teknis yang digunakan untuk mengelola user, yakni mencegah akses yang tidak perlu yang nantinya dapat membebani jaringan.
MikroTik router adalah salah satu sistem operasi yang dapat digunakan sebagai router jaringan yang handal, mencakup berbagai fitur lengkap untuk jaringan dan wireless. Selain itu MikroTik dapat juga berfungsi sebagai firewall. Melalui penelitian ini dengan judul “Analisis dan Optimasi dari Simulasi Keamanan Jaringan Menggunakan Firewall Mikrotik Studi Kasus di Taman Pintar Yogyakarta” akan dibahas bagaimana merancang sistem keaman jaringan komputer dengan menerapkan konsep firewall berbasis Miktorik dengan tujuan dapat mengurangi resiko ancaman yang akan mengganggu aktifitas yang yang sedang berlangsung, disesuaikan dengan kondisi di Taman Pintar Yogyakarta.

TINJAUAN PUSTAKA

Penelitian ini dikembangkan dari beberapa literatur dan pustaka sebagai referensi pembuatan aplikasi antara lain Keamanan Jaringan Dengan Firewall Filter Berbasis Mikrotik Pada Laboratorium Komputer STIKOM Bali oleh (Mardiyana, 2015). Penelitian ini mengenai bagaimana cara memperkuat kinerja firewall agar sistem keamanan dan data komputer di Laboratorium Program Diploma D-III Sistem Informasi menjadi lebih baik. Selain dari itu penelitian ini juga mengenai bagaimana mengatasi celah keamanan yang memungkinkan malware dan serangan dari luar. Hasil dari penelitian ini yaitu rancangan jaringan komputer yang sesuai untuk diterapkan dalam sistem gateway sekaligus sebagai firewall yang menerapkan packet filtering dimana metode package filtering akan mengatur semua paket baik yang menuju, melewati atau akan dituju oleh paket tersebut. packet tersebut akan diatur apakah akan di terima, diteruskan atau di tolak.

Rancang Bangun Sistem Jaringan Menggunakan Mikrotik Pada Novilla Boutique Resort oleh (Hidayat, 2017). Penelitian ini mengenai manajemen bandwidth internet agar terbagi rata kepada seluruh pengguna ketika banyak pengguna melakukan akses internet secara bersamaan serta peningkatan keamanan untuk memudahkan memantau penggunannya. Penelitian ini fokus ke perancangan jaringan, konfigurasi IP, topologi dan implementasinya. Serta pengoptimalan bandwidth dan serta firewall yang ada. Hasil dari penelitian ini yaitu perancangan sistem jaringan yang ditujukan untuk melakukan pembagian bandwidth jaringan internet agar masing-masing user bisa memperoleh bandwidth secara adil sesuai dengan banyaknya pengguna aktif. Selain dari itu semua interface dapat di monitor dengan baik di dalam mikrotik, terutama interface yang menuju internet.

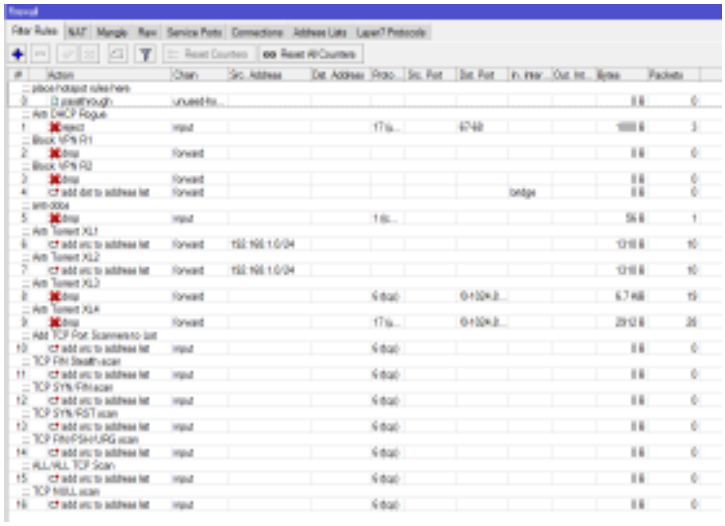
Implementasi Keamanan Jaringan Dengan Metode Firewall Filtering Menggunakan Mikrotik oleh (Astari, 2018). Penelitian ini mengenai agaimana cara merancang dan membangun keamanan jaringan pada kawasan sekolah menggunakan Mikrotik untuk mencegah dampak negatif dari internet berupa situs yang berbau dewasa dan media sosial agar menciptakan belajar mengajar yang kondusif. Hasil dari penelitian ini yaitu konfigurasi sistem keamanan jaringan menggunakan Mikrotik dengan metode Firewall Filtering. Sistem ini melakukan pemfilteran menggunakan layer 7 protokol untuk memblokir situs yang berbau konten dewasa maupun media sosial yang terindikasi memuat konten pornografi berdasarkan keywords.

Dari beberapa pustaka tersebut dapat disimpulkan untuk pengembangan penelitian yang akan dikerjakan antara lain dari penelitian yang dikerjakan oleh (Mardiyana, 2015) akan dilakukan penambahan filter pada router, agar router memiliki sistem keamanan yang memproteksi diri sendiri seperti serta ditambahkan beberapa konfigurasi untuk meminimalisir kesalahan yang mungkin terjadi akibat penambahan perangkat oleh client. Kemudian pengembangan dari penelitian (Hidayat, 2017) akan dilakukan penambahan perangkat berupa access point yang digunakan untuk melakukan penguatan signal wifi sehingga dapat dijangkau dengan baik oleh

semua pelanggan yang berada di Novilla Boutique Resort. Sedangkan dari penelitian (Astari, 2018) akan dilakukan Pengembangan mengenai penambahan fitur pengamanan dengan menerapkan hotspot server pada jaringan internet public sehingga pengguna dapat terkontrol melalui satu pintu akses.

PEMBAHASAN

Sistem keamanan jaringan berbasis mikrotik dibangun dengan menerapkan beberapa *rule firewall*. Berikut ini akan dibahas beberapa penangan keamanan untuk mengamankan sistem jaringan computer.



Gambar 1 *Firewall List*

Blokir External VPN

VPN eksternal bekerja dengan menyembunyikan IP lokal dan menggantikan dengan IP dari VPN, sehingga pengguna bisa membuka website atau aplikasi tertentu yang terblokir. Dilansir dari VPNMentor, kebanyakan aplikasi VPN gratis bakal menampilkan iklan yang berasal dari pihak ketiga. Tidak hanya itu, aplikasi VPN juga membagikan data dan kebiasaan berinternet pengguna kepada pihak ketiga. Oleh sebab itu penggunaan VPN sangat berbahaya bagi jaringan dan harus di blokir supaya pengguna tidak bisa menggunakannya.

Gambar 2 Contoh Aplikasi VPN Geratis

Langkah pertama penanganan aplikasi VPN yaitu harus mengetahui terlebih dahulu *port, protocol*, atau IP *Server* dari apps tersebut. Jika dilakukan *torch*, maka terlihat dst-port=443 dengan IP *Server* yang selalu berubah, sehingga sulit untuk blokir menggunakan dua opsi tersebut.

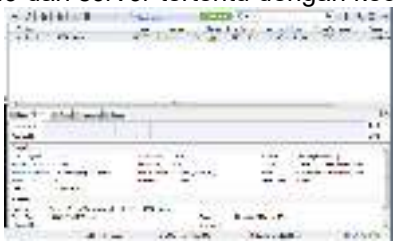
Gambar 3 Contoh Hasil Torch dari Aplikasi VPN

Gambar 4 menampilkan grafik informasi kinerja *firewall* ketika sedang melakukan proses pemblokiran terhadap aktivitas pengguna yang mengaktifkan aplikasi VPN.

Gambar 4 Grafik informasi kinerja *firewall* pemblokir VPN

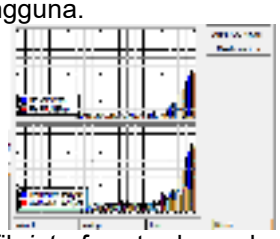
Blokir Penggunaan Aplikasi *Torrent*

Penggunaan aplikasi *torrent* memang menyediakan berbagai jenis program, film, foto, vidio, hingga *ebook* berbayar sekalipun bisa didapatkan dengan mudah dan gratis. Media ini juga memungkinkan seseorang dapat berbagi *file* (*file sharing*) dengan orang lain tanpa perlu men-*download*-nya secara sekaligus. Gambar 5 menampilkan contoh aplikasi *torent* yang berhasil melakukan *download* sebuah *file* dari *server* tertentu dengan kecepatan 716.3 kB/s



Gambar 5 Aplikasi Torrent Sedang Berjalan

Gambar 6 menampilkan grafik interface yang sedang berada pada port pengguna yang sedang menjalankan aplikasi torrent. Pada gambar tersebut terlihat ada pergerakan meningkat dimana terjadi proses *downloading* oleh pengguna.



Gambar 6 grafik *interface* terdampak aplikasi tertentu

Gambar 7 menampilkan kegiatan mengunduh sebuah *file* menggunakan aplikasi torrent yang sudah terblokir oleh *firewall*. Pada gambar tersebut ditampilkan progress bar dengan warna coklat dan pada *download speed* juga tidak tampil pergerakan, artinya *firewall* memblokir koneksi pada aplikasi ini.

Gambar 7 contoh aplikasi *torrent* terblokir *firewall*

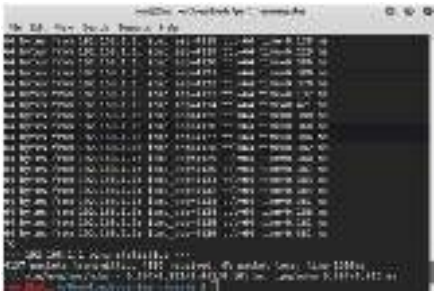
Gambar 8 menampilkan grafik proses dari firewall anti torrent yang sedang bekerja memblokir aktivitas download menggunakan file torrent. Pada gambar tesebut terlihat ada pergerakan yang sedikit mengingkat, hal tersebut menandakan *firewall* berhasil memblokir kegiatan *download* tersebut.

Gambar 8 Grafik Firewall Anti Aplikasi *Torrent*

Anti DDOS

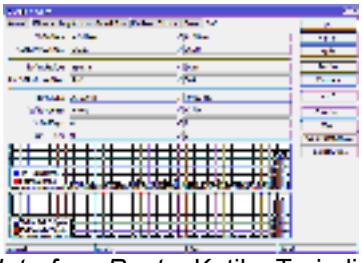
Gambar IV.25 menampilkan contoh serangan *flooding* melalui *protocol* icmp atau sring dikenal dengan *Distributed Denial of Service* (DDOS) dengan menggunakan layanan TCP port 53. Pada gambar tersebut ditampilkan serangan ditujukan ke ip *router* atau *gateway* dari jaringan Taman Pintar Yogyakarta. Serangan yang dilancarkan sukses dengan total *requested reply* 515152 kali.

Gambar IV.25 berikut. Jika tidak dihentikan maka sistem jaringan akan *down atau bisa juga mati total* (perangkat jaringan seperti *router* akan *collapse*). Serangan ini memang menjadi momok sejak jaman dulu sampai sekarang. Serangan yang cukup besar belum lama ini yaitu pada sistem jaringan milik twitter.



Gambar 9 Contoh serangan DDOS dengan LOIC App

Gambar IV.26 menampilkan *traffic* dari *interface* router yang terkoneksi dengan penyerang. Pada gambar ditampilkan dua buah grafik yang pertama menjelaskan *bandwidth* yang digunakan oleh *interface* tersebut, sedangkan grafik yang dibawah merupakan paket yang diterima oleh *router*. TX dan Rx menggunakan protokol yang diimplementasikan dalam sebuah perangkat bernama UART (Universal *Asynchronaus Receiver* / Transmitter). Rx adalah jalur penerimaan data (perpindahan data) dari satu komputer ke komputer lain. Rx biasa disebut received, yang berguna menangkap data yang dikirim oleh transmitter (Tx). Tx disebut transmit yang berfungsi untuk mengirim data/mengeluarkan data, atau merupakan jalan yang dilalui dalam mengirim data antar *device*. data akan dikirim melalui Tx (transmitter) dan di ujung lainnya data akan diterima melalui Rx (*Received*).



Gambar 10 *Traffic Interface Router* Ketika Terjadi Serangan *Flooding*

Gambar IV.29 menampilkan contoh serangan flooding dengan *protocol* icmp yang gagal karena sudah diatasi oleh *firewall*. Pada statistic terlihat 383 paket dikirim dalam waktu 6,2 detik akan tetapi paket yang diterima 0. Dengan demikian *firewall* sudah bisa mengatasi serangan ini dengan baik.

Gambar 11 Contoh Serangan DDOS yang sudah terblokir *firewall*

Gambar IV.30 menampilkan grafik proses dari firewall anti DDOS yang sedang bekerja memblokir aktivitas DDOS menggunakan perintah *ping*. Pada gambar tesebut terlihat ada pergerakan yang cukup signifikan mengingkat, hal tersebut menandakan *firewall* berhasil memblokir kegiatan *ping* DDOS tersebut.

Gambar 12 Grafik *Firewall* Ketika Memblokir DDOS

Analisis Keamanan Jaringan

Analaisis yang dilakukan pada penelitian ini yaitu dengan melakukan penetrasi ke berbagai perangkat yang terhubung jaringan. Berikut merupakan hasil penetrasi yang telah dilakukan uji coba.

1) Penetrasi Pada Perangkat *Router*

Gambar IV.31 menampilkan hasil penetrasi keamanan jaringan dengan menggunakan NMap Pada perangkat *Router*. Pada gambar tersebut dapat dilihat ada 5 buah *port* yang terbuka. Dari keterangan *service port* yang ditampilkan tidak ada yang menunjukkan adanya *port* yang berbahaya, dengan demikian perangkat ini cukup aman pada sistem jaringan.

Gambar 13 Hasil Penetrasi Kemanan Jaringan dari Perangkat *Router*

2) Penetrasi Pada Perangkat *Server*

Gambar IV.33 menampilkan hasil penetrasi keamanan jaringan dengan menggunakan NMap pada perangkat *Access Point*. Pada gambar tersebut dapat dilihat ada 16 buah *port* yang terbuka. Dari keterangan *service port* yang ditampilkan ada beberapa port yang memerlukan pengamanan, dengan demikian port-port tersebut harus ditutup.

Gambar 14 Hasil Penetrasi dari Perangkat *Server*

Gambar IV.34 menampilkan hasil optimasi terhadap perangkat *server* yang memiliki banyak *port* terbuka. Dapat dilihat perangkat *server* sekarang hanya memiliki 5 *port* yang terbuka.

Gambar 15 Hasil Penetrasi dari Optimasi Perangkat *Server*

PEMBAHASAN

Berikut ini merupakan hasil beberapa kali pengujian yang dilakukan pada beberpa fitur kemanan yang telah diterapkan. Pengujian pertama dilakukan pada Hasil penetrasi ke seluruh perangkat yang terhubung dengan jaringan komputer Taman Pintar Yogyakarta.

Tabel 1 Hasil Pengujian Penetrasi Jaringan

NO	Perangkat	Jumlah Port Terbuka	Hasil Analisis
1.	*Router*	5	Aman
2.	*Access Point*	1	Aman
3.	*Server*	16	Perlu Pengamanan

Setelah dilakukan optimasi jaringan dengan menutup *port-port* yang terbuka didapat hasil pengujian seperti ditampilkan pada tabel 2 berikut:

Tabel 2 Hasil Pengujian Penetrasi Jaringan Setelah Optimasi

NO	Perangkat	Jumlah Port Terbuka	Hasil Analisis
1.	*Router*	5	Aman
2.	*Access Point*	1	Aman
3.	*Server*	5	Aman

Pengujian kedua dilakukan pada keamanan jaringan untuk mencegah pengguna mengakses *file torrent* seperti terlihat pada Tabel 3.

Tabel 3 Hasil Pengujian *Firewall* Anti *Torrent*

NO	*Link Torrent*	Aplikasi	Hasil
1.	open.acgtracker.com	UTorrent	Tidak Terblokir
2.	babytorrent.com	Tribler Torrent	Tidak Terblokir
3.	bangumi.moe	Tixati Torrent	Tidak Terblokir
4.	piratebay.cloud	Deluge Torrent	Tidak Terblokir
5.	bangumi.moe	UTorrent	Tidak Terblokir

Hasil optimasi dari pengamanan aplikasi *torrent* cukup memuaskan karena *firewall* telah berhasil memblokir semua serangan. Aktivitas *download* ataupun *upload* yang menggunakan *torrent* semua ditolak hal terebut telah dilakukan uji coba beberapa kali pada beberapa link *torrent* dengan berbagai macam sumber *torrent* seperti ditampilkan pada tabel 4 berikut ini.

Tabel 4 Hasil Pengujian *Firewall* Anti *Torrent*

NO	*Link Torrent*	Aplikasi	Hasil
1.	open.acgtracker.com	UTorrent	Sukses Terblokir
2.	babytorrent.com	Tribler Torrent	Sukses Terblokir
3.	bangumi.moe	Tixati Torrent	Sukses Terblokir
4.	piratebay.cloud	Deluge Torrent	Sukses Terblokir
5.	bangumi.moe	UTorrent	Sukses Terblokir

Pengujian ketiga dilakukan pada keamanan jaringan untuk mencegah terjadi serangan DDOS seperti terlihat pada Tabel 5.

Tabel 5 Hasil Pengujian *Firewall* Anti DDOS Sebelum Optimasi

NO	Jaringan	Beban	Lama	Hasil
1	Wired LAN 1	40 kb	2.15 menit	Tidak Terblokir
2	Wifi	40 kb	2.41 menit	Tidak Terblokir
3	Wired LAN 2	40 kb	2.32 menit	Tidak Terblokir
4	Wifi 2	40 kb	2.10 menit	Tidak Terblokir

Hasil optimasi jaringan untuk kemanan anti DDOS dapat dilihat pada Tabel 6 berikut ini. Seperti yang ditampilkan pada data tabel aktivitas DDOS dapat tertanggulangi dengan baik oleh *router* hal tersebut karena *firewall* dapat memblokir *protocol* icmp untuk melakukan kegiatan yang membahayakan ini.

Tabel 6 Hasil Pengujian *Firewall* Anti DDOS Sebelum Optimasi

NO	Jaringan	Beban	Lama	Hasil
1	Wired LAN 1	40 kb	3.15 menit	Blokir Sukses
2	Wifi	40 kb	4.41 menit	Blokir Sukses
3	Wired LAN 2	40 kb	5.32 menit	Blokir Suskes
4	Wifi 2	40 kb	5.10 menit	Blokir Sukses

KESIMPULAN

Berdasarkan hasil pembahasan dalam bab sebelumnya, dapat diambil kesimpulan yaitu:

1. Ananlisis dan Optimalisasi sistem keamanan jaringan pada Taman Pintar Yogyakarta dapat dilaksanakan dengan baik. Menerapkan metodologi PPDIO penelitian ini melakukan beberapa konfigurasi kemanan jaringan yang meliputi konfigurasi untuk *firewall*, pengelolaan *service port* serta konfigurasi *filter* untuk *Bridge*. Hal tersebut dipaparkan secara jelas dalam hasil dan pembahasan penelitian ini yang dilengkapi dengan ujicoba kasus dari masing-masing pembahasan.
2. Penelitian ini selain melakukan pengamanan juga menerapkan beberapa konfigurasi yang difungsikan mencegah adanya beberapa kesalahan. Seperti penerapan anti *rogue* DHCP yang mungkin saja terjadi akibat penambahan perangkat pada client tanpa sepengetahuan administrator. Dengan fungsi tersebut maka sistem jaringan tetap berjalan dengan baik tanpa terjadi gangguan khususnya gangguan akibat *rogue* DHCP.

Saran

Saran yang dapat dilakukan untuk pengembangan dalam penelitian selanjutnya antara lain:

1. Saran untuk pengembangan selanjutnya agar mampu melakukan blokir terhadap virus atau malware yang mungkin bisa masuk ke dalam sistem jaringan akibat penularan dari salah satu komputer client yang terinfeksi.
2. Saran yang kedua yaitu dikembangkan sistem yang mamapu melakukan pendeteksian serangan terhadap jaringan secara live, sehingga dapat langsung ditangani atau diputus agar tidak menjalar kemana-mana atau melakukan kerusakan yang lebih parah.
3. Saran selanjutnya yaitu dengan meningkatkan keamanan agar sistem jaringan terhindar dari berbagai serangan yang dapat melumpuhkan sistem jaringan sperti menambah *rule* pada *firewall* atau konfigurasi pendukung lainnya.

Selain dari itu perlu dikembangkan lagi mengenai *load balancing* yaitu mendistribusikan beban trafik pada dua atau lebih jalur koneksi secara seimbang, agar trafik dapat berjalan optimal, memaksimalkan *throughput*, memperkecil waktu tanggap dan menghindari *overload* pada salah satu jalur koneksi.

DAFTAR PUSTAKA

Astari, A. A. (2018). Implementasi Keamanan Jaringan Dengan Metode Firewall Filtering Menggunakan Mikrotik, Jurnal Elektronik Universitas Nusantara PGRI Kediri. Kediri, Jawa Timur: Universitas Nusantara PGRI Kediri.

Hidayat, A. (2017). Rancang Bangun Sistem Jaringan Menggunakan Mikrotik Pada Novilla Boutique Resort. Pangkalpinang: STIMIK ATMA LUHUR.

Mardiyana, I. (2015). Keamanan Jaringan Dengan Firewall Filter Berbasis Mikrotik Pada Laboratorium Komputer STIKOM Bali. Konferensi Nasional Sistem & Informatika 2015, 804-807.