

Implementasi dan Perbandingan Firewall Security Menggunakan Mikrotik dan M0n0wall Pada Local Area Network

Hendra H Sinaga¹, Prof. Dr. Opim Salim Sitompul², M. Umar Saleh T, ST³

Program Studi Ekstensi SI Ilmu Komputer

Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Sumatera Utara

Jalan Universitas No. 9 Kampus USU Medan 20155

Email : hendra_h_sinaga@usa.com

opim@usu.ac.id

m.umar@usu.ac.id

Abstrak— Dalam sebuah jaringan istilah “firewall” adalah tembok api, yang berperan sebagai pembatas jaringan luar yang terkoneksi dengan internet. Dengan pesatnya perkembangan internet, dapat memberikan dampak positif bagi kita sebagai penyedia layanan informasi dan komunikasi, selain itu internet juga dapat memberikan dampak negatif sekaligus ancaman bagi penggunanya. Sehingga akses jaringan kita dengan internet harus dibatasi oleh sebuah pembatas yang dikenal dengan firewall. Bertujuan untuk implementasi sistem *firewall security* menggunakan *mikrotik* dan *m0n0wall* pada *local area network*. *Firewall* merupakan suatu perangkat keamanan jaringan yang memperperkenalkan berbagai bagian ruas jaringan untuk melaksanakan komunikasi antara satu dengan yang lainnya sesuai dengan definisi kebijakan keamanan yang telah diterapkan sebelumnya. *firewall* peka terhadap kesalahan konfigurasi dan kegagalan untuk menerapkan kebijakan, sehingga diperlukan tambahan atau peningkatan keamanan lain. Oleh karena itu, konfigurasi *firewall* yang digunakan dalam *Mikrotik* dan *M0n0wall* harus dilakukan secara hati-hati, sehingga organisasi seharusnya dapat bertahan dengan mengurangi kerapuhan dan gangguan baru. Dalam Perancangan *Firewall* pada *mikrotik* dan *m0n0wall* pada *local area network* menggunakan *paket filtering*, *NAT*, *transparent proxy*, *application* dan *port address* yang dapat mengurangi ancaman dan gangguan yang terjadi pada *local area network*. Diperlukan usaha kerja keras untuk memelihara semua sistem di dalam cara mengamankan dan tidak semata-mata mengandalkan pada *firewall* untuk menghentikan ancaman keamanan tersebut.

Kata Kunci : *Filter Packet*, *NAT*, *Transparent proxy*, *Application* dan *Port Address*.

I. PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi jaringan komputer saat ini menunjukkan bahwa sistem keamanan sangatlah penting bagi suatu sistem jaringan komputer yang terhubung dengan jaringan luar atau *Internet*. Karena *Internet* merupakan sebuah jaringan komputer yang sangat terbuka di dunia, konsekuensi

yang harus di tanggung adalah bagaimana jaminan sebuah keamanan bagi jaringan yang terhubung dengan *Internet*.

Dalam *Local Area Network* diketahui bahwa setiap sistem jaringan komputer yang terhubung tidak ada jaminan sebuah keamanan. Di dalam mengimplementasikan komponen dari sistem keamanan jaringan seperti *firewall* yang berfungsi untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak semua hubungan/kegiatan suatu segemen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat berupa sebuah *workstation*, *server*, *router*, atau LAN (*Local Area Network*) (Paulus, 20120).

Banyak masalah yang sering terjadi pada *Local area network* dikarenakan sering terjadi *Backdoor*, *Port Scan*, *Virus* dan *Malware*, *Hacker/Cracker*, *Denial Of Service (Dos/DDos)*. Akibat dari kelemahan sistem keamanan yang ada di *Local area network*. Hal ini bukan hanya merugikan satu bidang, bahkan semua bidang yang terhubung pada *Local area network* (Wijaya, H. 2009).

Oleh karena itu metode untuk menangani masalah yang terjadi pada jaringan *Local area network* yaitu:

- a) *Packet filtering* dan analisis
- b) *Port address*
- c) *Ip address*
- d) *Protocol (TCP/UDP)*
- e) *Keyword*
- f) *Application*

Di dalam *Mikrotik firewall* di setting untuk mengamankan packet yang akan di kirim ke router (Rafiudin, R. 2006). Di dalam *Mikrotik* terdapat juga fungsi *NAT* atau *Network Address Translation* yang digunakan :

- a. Untuk pembatasan akses secara langsung dan melindungi *traffic* yang akan keluar dari *router*
- b. Hanya *user* atau *group* tertentu
- c. Hanya *protocol* tertentu
- d. Hanya beberapa aplikasi dan sumber daya
- e. Waktu akses dan akses dari tempat tertentu

Ada dua jenis firewall sebagai berikut :

- a. *Personal Firewall*
- b. *Network Firewall*

Firewall umumnya terdiri dari bagian *filter* dan bagian *gateway*. Filter berfungsi untuk membatasi akses, mempersempit gerak, atau untuk memblokir kelas *traffik* tertentu. agar keamanan Jaringan *Local area network* lebih terjamin dan efektif (Rafiudin, R. 2006).

B. Rumusan Masalah

Dari latar belakang diatas dapat disimpulkan beberapa pokok permasalahan, diantaranya :

1. Keamanan jaringan yang terhubung dengan *Internet* sangat rentan terkena serangan.
2. Pengimplementasian komponen dari sistem keamanan jaringan seperti *firewall*.
3. Sering terjadi pencurian data hingga serangan berupa *virus, backdoor, hacker, port scan, dan Dos/Ddos*.

Maka dapat dirumuskan masalah yang harus ditanggulangi yaitu bagaimana membangun sistem keamanan yang terhubung dengan jaringan agar tidak terjadi gangguan dan serangan pada *Local area network* (Listianto, V. 2011).

C. Batasan Masalah

Untuk menghindari penyimpangan pembahasan dari tujuan awal maka diperlukan batasan masalah skripsi ini adalah sebagai berikut :

- a) *Mikrotik* yang akan digunakan adalah *Mikrotik* versi 2.9.27.
- b) *M0n0wall* yang akan digunakan adalah *M0n0wall* versi 1.33
- c) *Modem* yang digunakan adalah TPLink TL-MR3420.
- d) Meningkatkan keamanan LAN *Mikrotik* dan *M0n0wall*

D. Tujuan Penelitian

Adapun yang menjadi tujuan dari penelitian ini adalah

- a) Perancangan strategi sistem keamanan *Local area network* berbasis *firewall*.
- a) Mengimplementasikan keamanan *firewall* pada *Local area network*.
- b) Membuat sistem jaringan yang terjamin keamanan dan terkendali.

II. TINJAUAN TEORI

A. Jaringan Komputer

Sebuah rangkaian yang terdiri dua atau lebih komputer yang dapat berhubungan satu dengan yang lain yang secara bersama-sama membentuk sebuah jaringan agar dapat saling berkomunikasi, bertukar data dan *resource*. Pada model komputer *stand alone* (masing-masing berdiri sendiri) setiap proses bertukar data harus melalui mekanisme pemindahan data melalui media penyimpan *eksternal* misal CD, *Flash Disk, Eksternal Hardisk* dan lain-lain (Arifin, 2005).

B. Jenis Jaringan

Jaringan komputer dapat dikelompokkan berdasarkan luas area yang dapat dijangkau. Secara umum jaringan komputer terbagi menjadi 3 jenis, yaitu *Local Area Network (LAN)*, *Metropolitan Area Network (MAN)*, dan *Wide Area Network (WAN)* (Dharmo Oetomo, 2008). Topologi jaringan adalah bentuk perancangan jaringan baik secara fisik maupun secara logik yang digunakan untuk membangun sebuah jaringan komputer (Windy, 2012). Topologi jaringan menggambarkan struktur dari suatu jaringan, atau bagaimana sebuah jaringan didesain. Topologi yang dimaksud antara lain topologi Bus, topologi Ring, topologi Star.

C. Protokol Jaringan Komputer

Model (OSI) *Open Systems Interconnection* diciptakan oleh (ISO) *International Organization for Standardization* yang menyediakan kerangka logika terstruktur bagaimana proses komunikasi data berinteraksi melalui jaringan. Standard ini dikembangkan untuk industri komputer agar komputer dapat berkomunikasi pada jaringan yang berbeda secara efisien (Oscar rachman, 2009).

D. TCP/IP (Transmission Control Protocol / Internet Protocol)

TCP/IP (Transmission Control Protocol/ Internet Protocol) adalah sekumpulan protokol yang didesain untuk melakukan fungsi-fungsi komunikasi data seperti pada LAN(*Local Area Network*) dan WAN(*Wide Area Network*). TCP/IP terdiri atas sekumpulan protokol yang masing-masing bertanggung jawab atas bagian-bagian tertentu dari komunikasi data. Pemodelan empat layer TCP/IP (Rafiudin, 2006).

E. IP (Internet Protocol)

IP Address/Alamat IP merupakan pengenalan yang digunakan untuk member alamat pada tiap-tiap computer dalam jaringan. Alamat IP merupakan representasi dari 32 bit bilangan biner yang ditampilkan dalam bentuk desimal dengan dipisahkan oleh tanda titik. Alamat IP terdiri atas *network ID* dan *host ID*. *Network ID (NetID)* merupakan nomor *network*, sedangkan *host ID* mengidentifikasi *host* dalam suatu *network*. Contoh valid dari alamat IP adalah 10.150.0.2 (Whindy, 2012).

F. Subnetting

Subnetting adalah proses membagi atau memecah sebuah *network* menjadi beberapa *network* yang lebih kecil atau yang sering di sebut subnet. Dengan *subnetting*, pengguna dapat menentukan jumlah *host* yang akan digunakan di dalam jaringan. Bila pengguna hanya punya 5 *host*, tapi subnetmask kita tidak kita set sesuai dengan jumlah *host*, maka paket data yang masuk ke jaringan akan *dibroadcast* ke seluruh alamat IP (*host*), walaupun *host* itu pada kenyataannya tidak pernah ada.

G. Pengalokasian IP Address

Terdapat beberapa aturan dasar dalam penggunaan *network ID* dan *host ID*, yaitu:

1. *Network ID* 127.0.0.0 tidak dapat digunakan karena IP tersebut merupakan alamat loopback dari system local.
2. *Host ID* tidak boleh semua bitnya di set 1, (contoh klas A: 10.255.255.255) karena akan diartikan sebagai alamat broadcast. *ID broadcast* merupakan alamat yang mewakili seluruh anggota jaringan. Pengiriman paket ke alamat ini akan menyebabkan paket ini didengarkan oleh semua anggota paket jaringan tersebut.
3. *Network ID* dan *host ID* tidak boleh sama dengan 0 (seluruh bit diset 0 seperti 0.0.0.0), karena IP *address* dengan *host ID* 0 diartikan sebagai alamat jaringan. Alamat jaringan adalah alamat untuk menunjuk suatu jaringan dan tidak menunjukkan suatu host.
4. *Host ID* harus unik dalam suatu jaringan. Artinya, dalam satu jaringan, tidak boleh ada dua *host* dengan *host ID* yang sama.

IP Private yang dapat digunakan dalam jaringan local, yaitu: 10/8, 172.16.0.0/12, 192.168.0/16, 224.0.0.0/4 (class D multicast), 240.0.0.0/5 (class E research) karena IP ini tidak dipergunakan (di-publish) di internet[5].

H. Gateway

Gateway adalah sebuah perangkat yang digunakan untuk menghubungkan satu jaringan komputer dengan satu atau lebih jaringan komputer yang menggunakan protokol komunikasi yang berbeda sehingga informasi dari satu jaringan komputer dapat diberikan kepada jaringan komputer lain yang protokolnya berbeda (Sofyan, 2009).

I. Sejarah Mikrotik

Mikrotik RouterOS™ adalah sistem operasi yang dirancang khusus untuk *network router*. Mikrotik adalah perusahaan kecil berkantor pusat di Latvia, bersebelahan dengan Rusia, pembentukannya diprakarsai oleh John Trully dan Arnis Riekstins. John Trully yang berkebangsaan Amerika Serikat bermigrasi ke Latvia dan berjumpa Arnis yang sarjana Fisika dan Mekanika di sekitar tahun 1995. Tahun 1996 John dan Arnis mulai *me-routing* dunia (visi Mikrotik adalah *me-routing* seluruh dunia).

J. Pengertian Mikrotik

Mikrotik merupakan sistem operasi *linux base* yang dirancang secara khusus untuk keperluan *networking*. Didesain untuk memberikan kemudahan bagi penggunaannya. Mikrotik dapat dilihat seperti *Winbox*. *Winbox* merupakan perangkat lunak untuk *me-remote* mikrotik dalam GUI (*Graphic User Interface*) sehingga user dengan mudah dapat mengakses dan mengkonfigurasi *router* sesuai kebutuhan dengan mudah, efektif, dan efisien Selain itu instalasi dapat dilakukan pada standard PC (*Personal Computer*) (Ari Sujarwo, 2009).

K. Sejarah M0n0wall

Buechler Chris menyatakan *m0n0wall* merupakan *embedded firewall* berbasis *freeBSD* yang ringan dan mudah penggunaannya. *m0n0wall* adalah proyek yang ditujukan untuk menciptakan *firewall*, lengkap paket perangkat lunak, bila digunakan bersama dengan PC, menyediakan semua fitur penting dari kotak *firewall* komersial (termasuk kemudahan penggunaan) di sebagian kecil dari harga (software gratis). *m0n0wall* didasarkan pada versi awal dari *FreeBSD*, bersama dengan *web server* (Chris, 2008).

Dengan fitur yang sedemikian lengkap *m0n0wall* dapat menjadi solusi yang cepat untuk membangun *firewall* karena proses instalasinya yang tidak memakan waktu lama, menghemat biaya dan relatif aman.

Salah satu fungsi *router* adalah memberikan hak akses pada *client*, dan kali ini saya mencoba menuliskan hasil dari implementasi menggunakan *router m0n0wall*, yaitu bagaimana melakukan setting di *Ruler Firewall m0n0wall* untuk mengatur hak akses *client* dalam mengakses Internet (Buechler, 2008).

III. ANALISIS DAN PERANCANGAN

A. Analisis Sistem

Masalah keamanan merupakan hal yang sangat penting dalam jaringan komputer, terutama dalam jaringan *Local area network*. Firewall merupakan sebuah perangkat dasar yang dibutuhkan untuk membatasi akses dari luar jaringan.

Masalah yang sering terjadi pada *Local area network* seperti :

- a) Remote login → layanan yang memberikan jalan bagi orang-orang untuk melakukan koneksi ke sebuah sistem komputer dan mengendalikannya secara remote dalam beragam bentuk
- b) Aplikasi-aplikasi “backdoor” → program – program yang dirancang spesial untuk memberi jalan bagi siapa pun untuk melakukan akses remote terhadap sebuah sistem target. Program-program ini biasanya memanfaatkan bug-bug yang digunakan sistem target.
- c) Denial of service → ini merupakan sebuah bentuk serangan, dikenal dengan DoS. Seorang attacker berusaha membebani jaringan atau sistem target dengan trafik-trafik dalam sejumlah extra
- d) Virus/Malware → virus merupakan bentuk pelanggaran paling populer dan paling tua dalam dunia komputer. Virus tidak lain adalah program kecil yang dapat mengopi dirinya sendiri ke komputer-komputer.
- e) Port Scan → Sebuah mekanisme yang dapat digunakan untuk mengakses sistem, aplikasi, atau jaringan, selain dari mekanisme yang umum digunakan (melalui proses *logon* atau proses autentikasi lainnya).

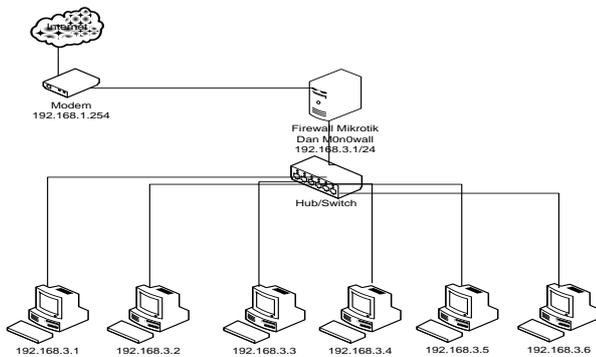
B. Topologi Yang Sedang Berjalan

Topologi jaringan yang digunakan pada LAN adalah topologi star, karena setiap komputer client akan terhubung

langsung dengan server menggunakan switch, dimana switch tersebut berfungsi sebagai konsentrator antara server dengan workstation.

C. Topologi Yang Sedang Berjalan

Server tersebut membentuk sebuah jaringan Internet dimana server bertindak sebagai penyedia fasilitas yang dibutuhkan workstation (client) dalam *Local area network*. Berikut gambar skema perancangan jaringan Lan :



Gambar 1 Sekema Firewall LAN

D. Sistem Yang Sedang Berjalan

a) **Packet filter:** Tampak pada setiap paket memasuki atau meninggalkan jaringan dan menerima atau menolaknya berdasarkan aturan yang ditetapkan pengguna. Packet filtering cukup efektif dan transparan bagi pengguna. Firewall packet filtering memiliki tiga aturan (policy), yaitu:

- 1) **INPUT**
Mengatur paket data yang memasuki firewall dari arah intranet maupun internet
- 2) **OUTPUT**
Mengatur paket data yang keluar dari firewall ke arah intranet maupun internet.
- 3) **FORWARD**
Mengatur paket data yang melintasi firewall dari arah internet ke intranet maupun sebaliknya

Secara umum, firewall biasanya menjalankan fungsi sebagai berikut:

a) Analisa dan filter paket

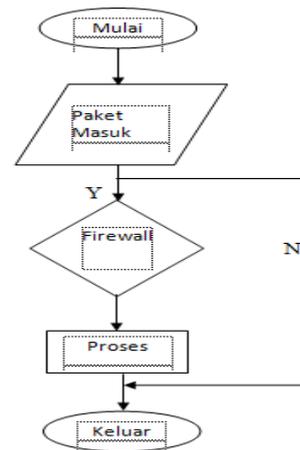
Data yang dikomunikasikan lewat protokol di internet, dibagi atas paket-paket. Firewall dapat menganalisa paket ini, kemudian memperlakukannya sesuai kondisi tertentu.

b) Bloking isi dan protokol

Firewall dapat melakukan bloking terhadap isi paket yang keluar dan masuk ke jaringan tersebut.

c) Autentikasi koneksi

Firewall umumnya memiliki kemampuan untuk menjalankan autentikasi identitas user, integritas dari satu session, dan melapisi transfer data pada jaringan



Gambar 2 Flowchart Firewall

Ada beberapa parameter yang digunakan untuk menentukan koneksi LAN yang diizinkan lewat atau tidak. Aada tiga macam yaitu:

- b) **ACCEPT** Akses diterima dan diizinkan melewati firewall.
- c) **REJECT** Akses ditolak, koneksi dari komputer klien yang melewati firewall langsung terputus, biasanya terdapat pesan "Connection Refused". Target Reject tidak menghabiskan bandwidth internet karena akses langsung ditolak, hal ini berbeda dengan DROP.
- d) **DROP** Akses diterima tetapi paket data langsung dibuang oleh kernel, sehingga pengguna tidak mengetahui kalau koneksinya dibatasi oleh firewall, pengguna melihat seakan - akan server yang dihubungi mengalami permasalahan teknis.

E. Masalah Yang Dihadapi Pada Sistem

Masalah yang sering terjadi pada packet Filtering Router antara lain:

- a) Kabel yang menghubungkan antara switch dengan komputer-komputer yang kadang putus atau tidak tersambung ke komputer yang ada, dan untuk mencari kabel yang terputus tersebut cukup sulit.
- b) Koneksi data dan internet juga dirasakan agak lambat dan terkadang sering *disconnect*.
- c) Komputer server terkadang juga sering mengalami *hang* dan sering terkena virus
- d) Tidak ada pembagian *bandwidth* pemakaian internet dan tidak menggunakan *proxy server*.
- e) *Firewall* hanya didalam windows xp dan security yang kurang baik.

F. Solusi Yang Ditawarkan

Untuk mengatasi masalah-masalah yang dihadapi pada *Local area network* seperti yang telah dijelaskan di atas, maka dibutuhkan solusi yang dapat mengatasi serangan yang terjadi pada *Local area network*. Berdasarkan analisis pada sistem yang sedang berjalan dan jaringan dan komputer, penulis menyimpulkan bahwa dibutuhkan keamanan sebuah jaringan dan mampu memfilter semua paket dan memblok semua port-

port yang kemungkinan terjadi serangan pada LAN menjadi lebih efisien.

Solusi yang di tawarkan adalah:

- Membuat server agar dapat mengatur jaringan
- Pembagian kinerja PC server menjadi lebih baik dan efisien.
- Adanya PC Server *Mikrotik dan Monowall* yang mengatur seluruh jaringan LAN.
- Maintenance* lebih mudah.
- Adanya pembagian *bandwidth* upload dan download yang teratur dan menggunakan *transparent proxy Mikrotik dan Monowall*
- Menggunakan *firewall dan security router mikrotik dan monowall* yang handal.

G. Perancangan Sistem

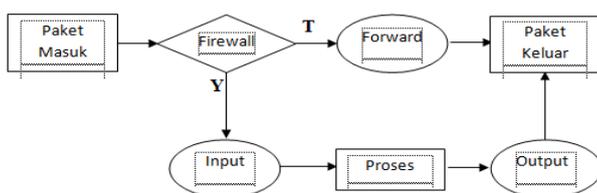
Sistem operasi yang dirancang berupa paket filtering firewall dan memblok semua port-port yang kemungkinan terjadi serangan pada LAN menjadi lebih efisien dan efektif.

Packet Filtering adalah tipe firewall yang diaplikasikan dengan cara mengatur semua packet IP baik yang menuju, melewati atau akan dituju oleh packet tersebut. Pada tipe ini packet tersebut akan diatur apakah akan di terima dan diteruskan atau di tolak.

Tipe Firewall yang akan digunakan :

- Packet filter:** Tampak pada setiap paket memasuki atau meninggalkan jaringan dan menerima atau menolaknya berdasarkan aturan yang ditetapkan pengguna. Packet filtering cukup efektif dan transparan bagi pengguna.
- Server proxy:** Memotong semua pesan yang masuk dan keluar jaringan. Server proxy secara efektif menyembunyikan alamat jaringan benar.

H. Alur Kerja Firewall



Gambar 3 Alur Kerja Firewall

Ketika ada paket data yang masuk ke jaringan atau komputer maka Firewall akan mengecek header dari paket data tersebut. Kemudian firewall akan menentukan apakah data paket ini bisa diteruskan atau tidak. Jika tidak maka akan ada pemblokiran, jika diijinkan maka paket data ini akan diteruskan sesuai mekanisme jaringan tersebut sehingga sampai ke komputer yang dimaksud (Rafiudin, 2006).

IV. IMPLEMENTASI DAN PENGUJIAN

A. Spesifikasi Sistem

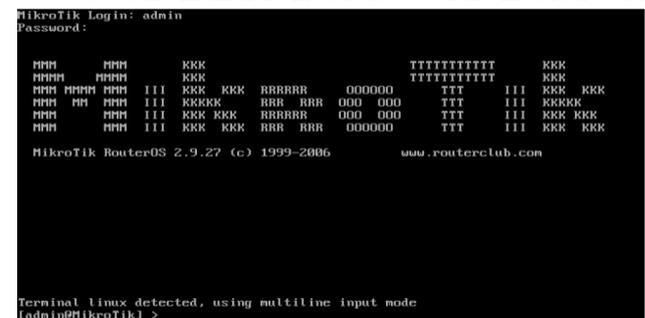
Pada tahap ini dilakukan pada sebuah PC Server (OS Mikrotik dan Monowall, PC client terbagi dalam 10 titik agar dapat mengimplementasi sistem yang meliputi spesifikasi sistem untuk perangkat keras dan perangkat lunak pada sistem jaringan LAN.

B. Rancangan Implementasi

Perangkat keras yang dibutuhkan yaitu PC server, PC client, Router, Switch, Modem TP-Link Mr 3420 wireless router dan notebook. PC server merupakan komputer yang digunakan untuk me-routing jaringan dengan sistem operasi mikrotik sedangkan PC client di sini merupakan komputer yang digunakan sebagai client

C. Implementasi Perangkat Lunak (Software)

PC router diinstall melalui CD instalasi mikrotik melalui booting CD-ROM, ukuran filenya hanya sekitar 15MB. Kemudian mikrotik akan memulai memformat seluruh isi harddisk dan memulai instalasi. Setelah instalasi selesai,

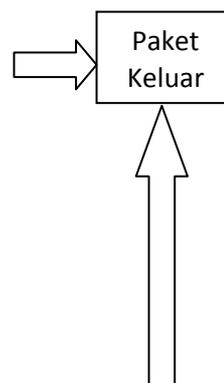


sistem akan melakukan *reboot*, dan PC router dengan sistem operasi mikrotik siap digunakan

Gambar 4 Tampilan Awal Mikrotik

D. Perangkat Lunak Mikrotik

Mikrotik RouterOS™ adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer biasa menjadi *router network*. *Winbox loader* seperti pada gambar berikut:





Gambar 5 Tampilan Winbox

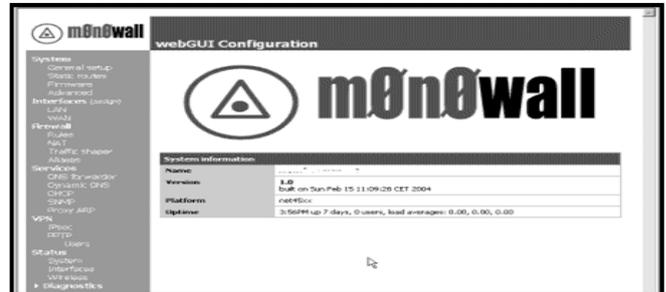
Gambar 8 Konfigurasi NAT Firewall

E. Perangkat Lunak M0n0wall

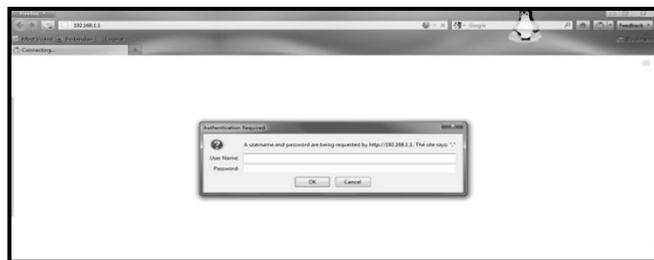
PC router diinstall melalui CD instalasi m0n0wall melalui booting CD-ROM, ukuran filenya hanya sekitar 15MB. Kemudian m0n0wall akan memulai memformat seluruh isi *harddisk* dan memulai instalasi. Setelah instalasi selesai, sistem akan melakukan *reboot*, dan PC *router* dengan sistem operasi mikrotik siap digunakan

H. Konfigurasi IP Address M0n0wall

M0n0wall sangat sederhana, untuk menggunakan konfigurasi. Masukkan alamat IP m0n0wall ke dalam kotak Alamat pada web browsers m0n0wall dan akan diminta untuk user dan Password.



Gambar 9 Halaman M0n0wall



Gambar 6 Tampilan Web Gui M0n0wall

F. Konfigurasi Operating System

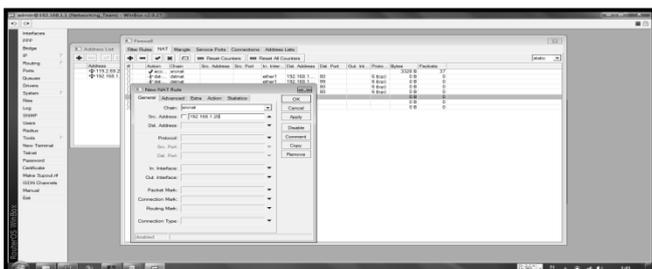
Untuk mengkonfigurasi mikrotik pada awal pemakaian di PC *router*, digunakan terminal login CLI (command line interface). Kemudian set nama interface ethernet dan alamat IP Mikrotik dengan perintah:

```
interface set ether1 name=speedy
interface set ether2 name=Networking_Team
ip address add address 192.168.1.254/24 interface=speedy
ip address add address 192.168.1.1/24 interface=Networking_Team
```

Sekarang mikrotik telah mempunyai alamat IP yang dapat di akses dari jaringan Networking_Team yaitu 192.168.1.1

G. Konfigurasi NAT Firewall Mikrotik

Network Address Translation atau yang lebih biasa disebut dengan NAT adalah salah satu fasilitas router untuk meneruskan paket dari IP asal ke IP tujuan.



I. Hasil Pengujian Sistem

Hasil Pengujian Filter Virus Menggunakan Mikrotik dan M0n0wall



Gambar 10 Website yang mengandung Virus di block

J. Perbandingan Operating Sistem

Dengan menggunakan topologi dan ujicoba implementasi sistem baru pada usulan pemecahan masalah yang telah dilakukan, yaitu:

Perbandingan Mikrotik :

1. Mikrotik adalah sistem operasi yang dirancang untuk menjadi router,
2. pemrosesan data dimana data yang pertama masuk akan terlebih dahulu di proses sampai selesai kecuali request tersebut mengalami keadaan time out dimana request tidak dapat dilayani sampai waktu yang ditentukan
3. Koneksi secara simultan dalam jumlah yang banyak akan membebani resource memori
4. Semakin banyak aturan firewall akan semakin membebani resource hardware pada komputer yang terinstall mikrotik

- Aturan pada mikrotik yang seringkali saling tumpang tindih (kesalahan konfigurasi oleh admin).
- Mikrotik khusus untuk melayani routing sesuaikan Konfigurasi dengan kondisi hardware router.

Perbandingan Menggunakan M0n0wall

- M0n0wall adalah sistem operasi yang dirancang untuk menjadi router,
- Koneksi yang berlebihan dalam jumlah yang banyak akan membebani resource memori.
- Semakin banyak aturan firewall akan semakin membebani resource hardware pada komputer yang terinstall mikrotik
- Aturan pada m0n0wall yang seringkali saling tumpang tindih(kesalahan konfigurasi oleh admin).
- Kinerja PC Router menjadi lebih baik dan stabil. Setelah adanya PC router dengan mikrotik yang mengendalikan seluruh jaringan komputer.

- Dapat memberikan hak akses, membangun sistem keamanan secara berlapis, membuat satu jalur masuk akses data, menggunakan metode paket filtering.
- Keamanan jaringan komputer dengan firewall mikrotik dan m0n0wall berkaitan dengan jenis fasilitas apa yang akan disediakan bagi para pemakai, sejauh mana level resiko keamanan yang bisa diterima, serta berapa banyak waktu dan biaya yang tersedia.
- Hasil Implementasi dan Perbandingan sistem keamanan jaringan pada LAN menggunakan Mikrotik lebih mudah penggunaanya.

B. Saran

Adapun saran-saran yang diberikan untuk pengembangan lebih lanjut terhadap Implementasi dan Perbandingan *Firewall Mikrotik* dan *M0n0wall* pada *Local Area Network* yaitu:

- Keamanan Jaringan dapat ditingkatkan dengan menerapkan *firewall \ filter* pada tiap gateway, serta untuk gateway utama dapat menggunakan firewall dengan *filter* biasa.
- Meningkatkan keamanan jaringan tidak hanya menggunakan *firewall filter*, namun lebih baik juga dengan menggunakan script firewall yang terupdate.

TABEL 1
PERBANDINGAN MENGGUNAKAN MIKROTIK DAN
MONOWALL

Mikrotik	M0n0wall
Adanya router mikrotik yang mengatur seluruh jaringan	Tidak adanya Pengaturan jaringan keseluruhan
Maintenance Lebih Mudah	Maintenance Lebih Rumit
Adanya pembagian <i>bandwidth</i> upload dan download yang teratur dan menggunakan <i>transparent proxy</i> mikrotik.	Tidak dapat membagi <i>bandwith</i> yang teratur.
Menggunakan <i>firewall</i> dan <i>security</i> router mikrotik yang handal.	Pengaturan firewall yang bersifat manual, membutuhkan waktu yang lama.
Update script firewall lebih mudah	Update firewall dengan manual
Lebih mudah pengaturannya	Lebih rumit pengaturannya

V. KESIMPULAN

A. Kesimpulan

Adapun kesimpulan yang di dapat dari analisis, perancangan, implementasi dan pengujian pada Mikrotik dan BrazilFW dalam memfilter situs porno penulis dapat menarik kesimpulan sebagai berikut :

- Keamanan jaringan komputer bertujuan untuk memaksimalkan sumber daya yang ada untuk mengamankan sistem jaringan komputer pada titik-titik yang tepat sehingga lebih efisien.
- Sistem *firewall* pada mikrotik dan m0n0wall dapat membantu menaggulangi masalah yang terjadi pada local area network.

DAFTAR PUSTAKA

- Athailah. 2012, "Kontrol dan Amankan Koneksi Internet di Jaringan", Jakarta: PT.Elex Media Komputindo.
- Alan, N. 2001, "Small Business Solutions for Networking", Jakarta: PT.Gramedia
- Budi, S. dan Dharma. O. 2008, "Konsep dan Perancangan Jaringan Komputer", Yogyakarta: Andi
- Belovin, S. Cheswick, W. 2005. "Network Firewalls", IEEE Communications Magazine.
- Buechler, C. 2008, *M0n0wall Handbook* : M0n0wall Documentation Project.
- Gunawan, M. F. Ari, S. dan Sofyan, W. L. 2009. "Pelatihan Jaringan Komputer", Magelang: DKK Magelang.
- Gin-gin, Y. dan Oscar, R. 2009, "Router teknologi, Konsep, Konfigurasi dan Troubleshooting" Bandung: Informatika
- Hardana, dan Irvantino, I. 2011, "Konfigurasi Wireless Routerboard Mikrotik", Yogyakarta: Andi.
- Harijanto, P. 2008, "Firewall Melindungi jaringan dari Ddos menggunakan Linux dan Mikrotik", Yogyakarta: Andi.
- Jufriadif, N. "Firewall Sebagai Pengaman Internet", Jurnal Akadimika, ISSN 0854-4336 Vol. 7 No. 2 : Oktober 2003, Hal 14-20.
- Kustanto, dan Saputro. 2008, "Membangun Server Internet dengan MikroTik OS", Yogyakarta: Gava Media.
- Linto H, M. 2009 "Membangun Sharing Koneksi Internet di Windows Mikrotik, Linux dan OpenBSD", Yogyakarta: Andi.
- Linto, H. M. dan Azis, C. L. 2008, "Panduan Lengkap Menguasai Router Masa Depan Menggunakan MikroTik RouterOS™", Yogyakarta: Andi.
- Listianto, V. 2011. "Teknik Jaringan Komputer", Jakarta: Prestasi Pustaka Publisher.
- Odum, W. 2005. "Computer Networking First-Step" Yogyakarta: Penerbit Andi
- Rafudin, R. 2006 "Membangun Firewall dan Traffic Filtering", Yogyakarta: Andi.
- Rafudin, R. 2006 "IP Routing dan Firewall Dalam Linux", Yogyakarta: Andi
- Setiawan, D. Vol 3-2008, "Kajian Penanganan Serangan DoS di Internet" Jurnal Generic, ISSN No: 1907-4093.
- Whindy, Y. 2012. "Kontrol dan Amankan Koneksi Internet di Jaringan", Jakarta: PT.Elex Media Koputindo.
- Wijaya, H. 2011, "Belajar Sendiri Cisco DSL Router ASA Firewall dan VPN", Jakarta: PT Elex Media Komputindo.
- Wiliam, S. 2002, "Komunikasi Data dan Komputer Jaringan Komputer", Jakarta: Salemba Teknika dan Pearson Education Asia.

Paulus, Y. J. 2012, "*Computer Networking, Pengaturan Jaringan, Keamanan Jaringan, Koneksi dan sharing, Troubleshooting Jaringan*", Yogyakarta: Andi.