Jurnal Tugas Akhir

Analisis dan Implementasi *Firewall* dengan *Metode Stateful Multilayer Inspection* Pada *Mikrotik Router OS*

Zohan Aris Pribadi
Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang

Abstrak

Kebutuhan sistem keamanan jaringan komputer baik untuk sistem informasi atau komputer yang terhubung dengan jaringan internet, sangat rentan sekali terhadap penyusupan, pencurian data serta penyalahgunaan informasi oleh orang yang tidak bertanggung jawab. Sehingga upaya untuk melindungi sistem tersebut sangat dibutuhkan. Firewall merupakan salah satu solusi perlindungan jaringan komputer dalam mencegah adanya tindakan tersebut. metode yang di terapkanpun bermacam-macam meliputi Circuit Level gateway, Application level gateway, dan Packet Filtering firewall. Sebagai contoh adalah metode Packet Filtering, lalu lintas data akan di filter pada layer network meliputi IP Address dan Port, akan tetapi semakin meningkatknya kebutuhan keamanan, maka dibutuhan suatu keamanan yang dapat menginspeksi lebih dari satu lapisan protokol jaringan didalam satu sistem, sedangkan untuk menerapkan keamanan tersebut dibutuhkan suatu infrastruktur dan perangkat yang tidak murah. Sehingga diperlukan suatu perangkat dan sistem keamanan firewall yang ekonomis,efisien sekaligus mampu bekerja secara optimal untuk melindungi jaringan komputer. Metode Stateful Multilayer Inspection Firewall merupakan sebuah metode yang dapat menggabungkan keunggulan metode-metode firewall lainya dalam satu sistem. Mikrotik merupakan salah satu Operating System yang mempunyai fitur unggulan, salah satunya adalah sebagai Firewall. Laporan tugas akhir ini akan menguraikan aktifitas dan produk yang dihasilkan pada masing-masing tahap pengembangan. Analisis dan implementasi firewall multilayer ini akan menghasilkan sebuah metode keamanan berlapis dengan meningkatkan pemfilteran yang lebih selektif, kemudahan administrasi sistem dan pengelolaanya. Pada tahap akhir pengembangan metode firewall, hal-hal apa yang telah dilakukan dan apa yang belum dilakukan pada pengembangan firewall ini akan diulas dan di evaluasi pada bagian akhir laporan ini.

Kata Kunci : firewall, Packet Filtering, stateful multilayer inspection, mikrotik

1. Pendahuluan

1.1 Latar Belakang

Firewall merupakan salah satu solusi perlindungan jaringan komputer dalam mencegah serangan dan penyusupan yang dapat membahayakan kerahasiaan data serta kerusakan pada infrastruktur suatu jaringan[8]. Mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan 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)[6]. Pada masing-masing jenis *firewall* tersebut, masih terdapat suatu kekurangan yaitu *software firewall* yang memakan sumber daya dari komputer (CPU, memory, ruang disk) sehingga dapat menyebabkan inkompatibilitas pada sistem operasi, sedangkan *hardware firewall* cenderung lebih mahal dan

konfigurasi yang sangat sulit dibandingkan dengan *software firewall,* dengan demikian dibutuhkan suatu sistem firewall yang mampu berjalan dalam satu sistem yang efisien.

Beberapa metode *firewall* diantaranya adalah *Circuit Level gateway, Application level gateway, Packet Filtering firewall*[2]. Karena teknologi konvensional atau metode pemfilteran *firewall* tersebut hanya melakukan inspeksi pada level tertentu saja, maka untuk memberikan keamanan secara spesifik, dibutuhkan suatu metode keamanan berlapis. Pada metode pemfilteran satu layer metode yang diterapkan umumnya menggunakan metode firewall *packet filtering,* metode tersebut berfungsi sebagai translasi jaringan komputer dari jaringan luar kedalam jaringan lokal dan inspeksi berdasarkan *port, IP address, dst-address, src-address, src-port, dst-port* pada *layer network, routers* adalah bentuk umum dari metode *packet filtering firewall* ini. Untuk memenuhi kebutuhan keamanan pada segmen jaringan komputer secara efektif dan aman dibutuhkan suatu *firewall* yang dapat menerapkan keamanan berlapis yang dapat menginspeksi di banyak layer protokol jaringan.

Metode *Stateful Multilayer Inspection Firewall* merupakan sebuah metode firewall yang menggabungkan keunggulan dari *Packet Filtering*, *NAT Firewall*, *Circuit-Level Firewall* dan *Proxy Firewall* dalam satu sistem. Sehingga tingkat keamanan pada metode ini secara spesifik dapat melindungi keamanan infrastruktur komputer pada segmen jaringan pribadi secara selektif. *Mikrotik* merupakan salah satu *Router Operating System* yang mempunyai banyak fitur, salah satunya adalah sebagai *Router* dan *Firewall*[6]. Dalam penelitian ini penulis menganalisa kelemahan dan kekurangan pada metode firewall sebelumnya dan menerapkan metode baru dengan menggunakan metode *Stateful Multilayer Inspection* pada *Mikrotik Router OS.*

Berdasarkan latar belakang permasalahan tersebut maka penulis memilih judul: "Analisis dan Implementasi *Firewall* dengan metode *Stateful Multilayer Inspection* pada *Mikrotik Router OS*". Adanya penelitian ini agar didapatkan suatu analisa firewall yang aman dengan tingkat keamanan berlapis serta menghasilkan penerapan metode *Stateful Multilayer Inspection Firewall* pada *Mikrotik Router OS.*

1.2 Rumusan Masalah

Berdasarkan uraian di atas maka penulis mengambil rumusan masalah sebagai berikut "Bagaimana Menganalisa dan menerapkan *firewall* untuk mendapatkan analisa kelemahan dan kekurangan yang dimiliki pada metode sebelumnya sehingga didapatkan suatu sistem keamanan yang baik yang dapat diterapkan pada Mikrotik Router OS dengan menggunakan metode *Stateful Multilayer Inspection Firewall"*.

1.3 Batasan Masalah

Untuk menghindari penyimpangan dari judul dan tujuan yang sebenarnya serta keterbatasan pengetahuan yang dimiliki penulis, maka penulis membuat ruang lingkup dan batasan masalah yaitu :

1. Menganalisa metode keamanan jaringan komputer dalam penerapan Firewall menggunakan metode *Stateful Multilayer Inspection* pada *Mikrotik Router OS* untuk meningkatkan keamanan yang sudah tersedia dengan menerapkan konsep multilayer pada satu sistem.

2. Penerapan metode *Stateful Multilayer Inspection Firewall* ini tidak sampai pada penerapan aplikasi yang digunakan oleh layanan server yang berada di dibelakang *firewall*.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah untuk menganalisa kelemahan yang dimiliki pada metode satu layer kemudian menerapakan metode baru yaitu dengan menggunakan metode *Stateful Multilayer Inspection* pada *Mikrotik Router OS* secara efisien,mudah dikelola dan selektif.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini antara lain :

1. Menghasilkan keamanan pada jaringan pribadi dari hal yang membahayakan infrastruktur jaringan atau penyalahgunaan hak akses dari jaringan luar dengan memanfaatkan *Mikrotik Router OS* sebagai *firewall*.
2. Menghasilkan keamanan pada infrastruktur jaringan pribadi dengan penyaringan *multilaye*r, sehingga lalu lintas data yang masuk dan keluar dapat di inspeksi secara lebih selektif untuk menghindari dari penyalahgunaan informasi, pencurian data dan perusakan terhadap sistem informasi serta infrastruktur jaringan komputer.
3. Memberikan kemudahkan dalam pengelolaan administrasi firewall dengan menggunakan *Winbox* pada *Mikrotik Router OS.*

2. Kajian Pustaka

2.1 Keamanan Jaringan Komputer

Tujuan utama dari keamanan sistem adalah memberikan jalur yang aman antar-entitas yang saling bertukar informasi dan untuk menyediakan perlindungan data. Insiden keamanan jaringan komputer adalah suatu aktivitas yang berkaitan dengan jaringan komputer, di mana aktifitas tersebut memberikan implikasi terhadap keamanan.

2.2 Jenis Serangan terhadap Keamanan

Pada dasarnya, menurut jenisnya, serangan terhadap suatu data dalam suatu jaringan dapat dikategorikan menjadi 2, yaitu :

a. Serangan Pasif *(Passive Attacks)*

Serangan pasif adalah serangan pada sistem autentikasi yang tidak menyisipkan data pada aliran data (*data stream),* tetapi hanya mengamati atau memonitor pengiriman informasi ke tujuan. Informasi ini dapat digunakan di lain waktu oleh pihak yang tidak bertanggung jawab. Serangan pasif yang mengambil suatu unit data dan kemudian menggunakanya untuk memasuki sesi autentikasi dengan berpura-pura menjadi user autentik/ asli disebut dengan *replay attack.* Beberapa informasiautentikasi seperti password atau data *biometric* yang dikirim melalui transmisi elektronikdapat direkam dan kemudian digunakan untuk memalsukan data yang sebenarnya. Serangan pasif ini sulit untuk dideteksi karena penyerang tidak melakukan perubahan data. Oleh sebab itu untuk mengatasi serangan pasif ini lebih ditekankan pada pencegahan daripada pendeteksiannya.

b. Serangan Aktif (*Active Attacks)*

Serangan aktif adalah serangan yang mencoba memodifikasi data, mencoba mendapatkan autentikasi, atau mendapatkan autentikasi dengan mengirimkan paket-paket data yang salah ke data stream atau dengan memodifikasi paket-paket yang melewati data stream. Kebalikan dari serangan pasif, serangan aktif sulit untuk dicegah karena untuk melakukannya dibutuhkan perlindungan fisik untuk semua

fasilitas komunikasi dan jalur-jalurnya setiap saat. Yang dapat dilakukan adalah mendeteksi dan memulihkan keadaan yang disebabkan oleh serangan ini.

2.3 Model OSI

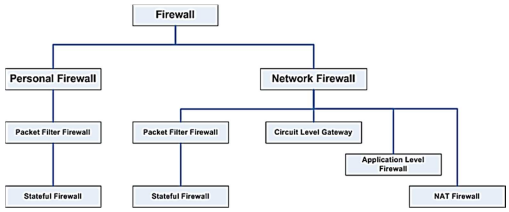
Model OSI ditetapkan oleh sebuah badan standar internasional yang bernama *International Standards Organization (ISO)* pada tahun 1947. Standar semacam ini perlu untuk menjaga interoperabilitias antar peralatan yang dibuat oleh pabrik yang berbeda-beda. Model OSI menetapkan 7 lapis proses, yaitu Application layer, Presentation layer, Session layer, Transport layer, Network layer, Data-link layer dan Physical layer

2.4 Protokol

Protokol adalah sebuah standar aturan yang mengatur alat-alat dalam jaringan komputer sehingga dapat saling berkomunikasi satu sama lain, dapat berhubungan satu sama lain dan dapat melakukan perpindahan data satu sama lain. Protokol dapat diterapkan pada perangkat keras (hardware), perangkat lunak (software) dan kombinasi keduanya.

2.5 Definisi Firewall

Firewall merupakan suatu cara atau 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 segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan lingkupnya. Segmen tersebut dapat merupakan *sebuah workstation, server, router, atau local area network* (LAN)



2.6 Fungsi Firewall

Berdasarkan definisi diatas Fungsi umum firewall adalah :

1. Mengatur dan mengontrol lalu lintas jaringan
2. Melakukan autentikasi terhadap akses
3. Melindungi sumber daya dalam jaringan privat
4. Mencatat semua kejadian, dan melaporkan kepada administrator

2.7 Karakteristik Firewall

Berikut ini adalah karakteristik dari sebuah *firewall* :

1. Seluruh hubungan/kegiatan dari dalam ke luar, harus melewati firewall. Hal ini dapat dilakukan dengan cara memblok/membatasi baik secara fisik semua akses terhadap jaringan lokal, kecuali melewati firewall. Banyak sekali bentuk jaringan yang memungkinkan agar konfigurasi ini terwujud.
2. Hanya kegiatan yang terdaftar/dikenal yang dapat melewati/melakukan hubungan, hal ini dapat di lakukan dengan mengatur *policy* pada konfigurasi keamanan lokal. Banyak sekali jenis *firewall* yang dapat di pilih sekaligus berbagai jenis *policy* yang di tawarkan.
3. *Firewall* itu sendiri haruslah kebal atau relatif kuat terhadap serangan/kelemahan. Hal ini berarti penggunaan sistem yang dapat dipercaya dan dengan sistem yang relatif aman.

2.8 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 yang protokolnya berbeda

2.9 Winbox

Winbox adalah sebuah utility yang digunakan untuk melakukan remote ke server mikrotik dalam mode GUI (*Graphical User Interface).*

2.10 Nmap

(Network Mapper) adalah sebuah aplikasi atau tool yang berfungsi untuk melakukan *port scanning*. Nmap dibuat oleh Gordon Lyon, atau lebih dikenal dengan nama Fyodor Vaskovich. Aplikasi ini digunakan untuk meng-audit jaringan yang ada. Dengan menggunakan tool ini, kita dapat melihat host yang aktif, port yang terbuka, Sistem Operasi yang digunakan, dan feature-feature scanning lainnya. Pada awalnya, *Nmap* hanya bisa berjalan di sistem operasi Linux, namun dalam perkembangannya sekarang ini, hampir semua sistem operasi bisa menjalankan Nmap

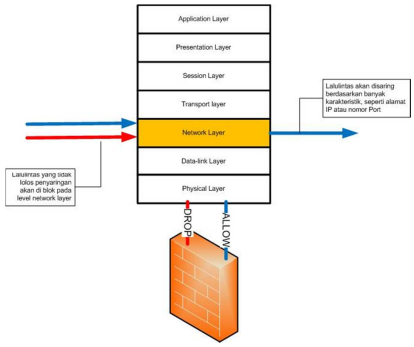
2.11 Wireshark

Wireshark adalah penganalisis paket gratis dan sumber terbuka. Perangkat ini digunakan untuk pemecahan masalah jaringan, analisis, perangkat lunak dan pengembangan protokol komunikasi, dan pendidikan. Awalnya bernama Ethereal, pada Mei 2006 proyek ini berganti nama menjadi *Wireshark* karena masalah merek dagang.

3. Hasil dan Implementasi

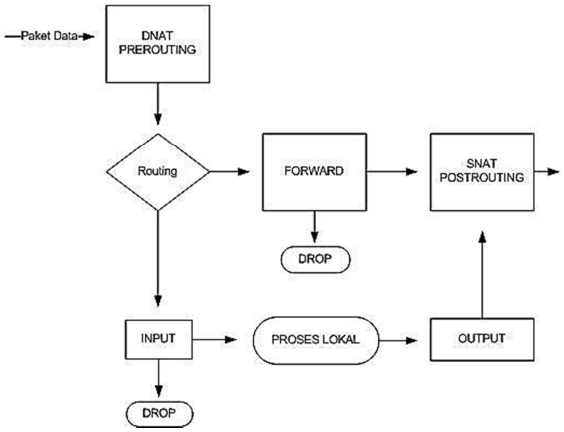
3.1 Analisa Metode *Packet Filtering*

Pada tahap ini akan di analisa metode firewall yang sering digunakan secara umum dalam pemfilteran satu layer, salah satunya adalah menggunakan metode *Firewall Packet Filtering*, firewall jenis ini memfilter paket data berdasarkan alamat dan opsi-opsi yang sudah ditentukan untuk paket tersebut. Metode ini bekerja dalam level IP paket data dan membuat keputusan mengenai tindakan selanjutnya (diteruskan atau tidak diteruskan) berdasarkan kondisi paket tersebut. metode ini di desain untuk mengontrol aliran paket berdasarkan alamat asal, tujuan, port dan tipe informasi paket yang dikandung di dalam tiap paket. Ip firewall sangat aman namum dapat mengabaikan sejumlah log yang mungkin penting.



Gambar 4.1 : Skema Paket Filtering

Network Filter memiliki lima rantai utama yang dapat digunakan, yaitu PREROUTING, POSTROUTING, INPUT, FORWARD, dan OUTPUT. Hubungan kelima rantai tersebut dapat dilihat di bagan berikut :



Setiap paket yang tiba di 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 POSTROUTING sebelum akhirnya paket benar-benar meninggalkan host.

3.2 Hasil Analisa Paket Filter

Analisa dibawah ini merupakan hasil dari pengujian metode paket filter dengan teknik *port scanner* menggunakan tool *nmap*.

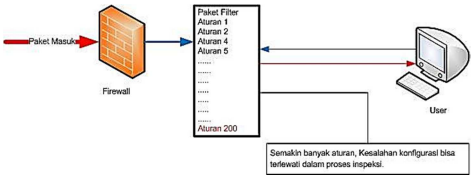
```
Nmap scan report for 192.168.1.1
Host is up (0.0045s latency).
Not shown: 991 filtered ports
PORT     STATE  SERVICE         VERSION
22/tcp   open   ssh?
23/tcp   closed telnet
25/tcp   closed smtp
139/tcp  closed netbios-ssn
256/tcp  closed fw1-secureremote
1720/tcp closed H.323/Q.931
3306/tcp closed mysql
5900/tcp closed vnc
8080/tcp closed http-proxy
MAC Address: 00:0C:29:EC:CB:5C (VMware)
OS fingerprint not ideal because: Didn't receive UDP response. Please tr
No OS matches for host
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   4.49 ms 192.168.1.1

NSE: Script Post-scanning.
Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report any incorrect results
Nmap done: 1 IP address (1 host up) scanned in 449.29 seconds
           Raw packets sent: 2300 (107.200KB) | Rcvd: 119 (22.542KB)
```

Gambar 4.5 : Hasil Analisa *Scanner Packet Filter*

Berdasarkan hasil analisa diatas, seharusnya pake filter sudah mampu melakukan filtering terhadap port scanner, akan tetapi hasil dari output diatas menunjukkan bahwa dengan metode paket filter diatas masih terdapat kesalahan dalam konfigurasi, sehingga kebocoran yang terjadi pada firewall ini bisa terjadi pada *port-port* lainya ketika sedang dilakukan *port scanner*. Berikut merupakan gambaran kenapa bisa terjadi kebocoran yang di akibatkan karena terlalu banyak *protocol* yang di inspeksi dan rule yang terlalu panjang.



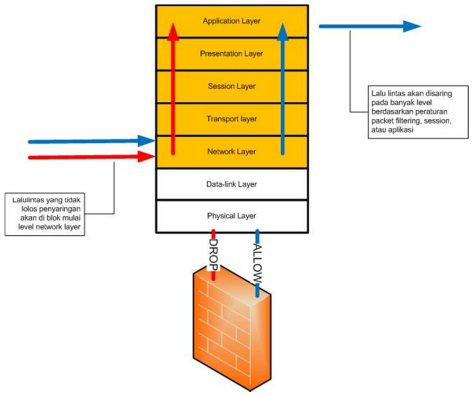
Gambar 4.6 : Gambaran Proses Filtering

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.

3.3 Pemecahan Masalah

Berdasarkan permasalahan diatas, dapat di simpulkan bahwa dengan menggunakan metode penfilteran paket filtering, kemungkinan besar akan meloloskan paket data yang sebenarnya membahayakan segmen

jaringan *local area network*, dengan demikian walaupun menggunakan metode *firewall packet filtering* sudah baik, tetapi dilihat dari metode inspeksi yang digunakan, masih terdapat kekurangan dalam melakukan inspeksi terhadap paket data pada lalulintas jaringan, sehingga perlu dilakukan pemfilteran secara slektif, agar dalam pemfilteran paket yang melalui lalu lintas firewall, akan benar-benar terinspeksi secara selektif, disamping menghasilkan sisi kemudahan dalam membaca informasi *log* dan fungsionalitas sistem firewall, baik itu dilihat dari metode ataupun sistem yang digunakan, maka perlu ditingkatkan lagi yaitu dengan menggunakan metode *Stateful Multilayer Inspection* pada sistem yang mudah dipahami, dalam hal ini memanfaatkan *Router OS Mikrotik* sebagai firewall dan menerapkan metode multilayer di satu sistem.

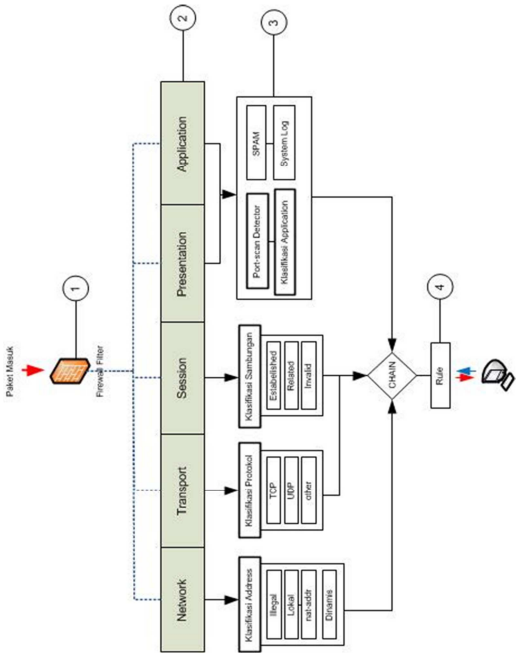


Gambar 4.7 : Pemecahan Masalah

Pada gambar diatas, ketika paket masuk melalui firewall, paket akan di kelompokkan berdasarkan klasifikasi protokol dan elemen-elemen yang sudah di sesuaikan dengan keadaan paket pada saat masuk, kemudian setelah paket di klasfikasi, paket akan di berikan tanda terhadap koneksi yang terbentuk, sehingga akan teridenfikasi secara jelas paket yang sedang berjalan di dalam router merupakan paket apa, setelah paket terindetifikasi dengan tanda sesuai klasifikasi, maka paket akan di inspeksi berdasarkan kategori layer protol mulai dari *layer network* hingga sampai *layer application*, setelah itu paket akan di filter melalui rantai rule yang di tentukan oleh administrator, apakah di ijinkan atau tidak. Kelebihan dari metode ini adalah proses inspeksi secara selektif dan rule yang tidak begitu panjang. Karena apabila terlalu banyak rule yang diterapan dapat menyebabkan salah konfigurasi, sehingga dengan metode ini kebijakan yang di terapkan dapat bekerja dengan baik dan selektif.

3.4 Implementasi Metode

Pada tahap ini metode *Stateful Multilayer Inpection* akan diterapkan pada *Mikrotik Router OS*. Sebelum menerapkan metode ini dengan menggunakan mikrotik berikut konfigurasi pada aspek-aspek jaringan yang akan di buat :



Gambar 4.10 : Arsitektur Stateful Multilayer Inspection

Penjelasan arsitektur firewall *Stateful Multilayer Inspection* :

1. Paket masuk melalui firewall.
2. Pemfilteran masuk berdasarkan masing-masing kriteria layer pada layer protokol jaringan, *network, transport, session, presentation, Application.*
3. Inspeksi masuk kedalam kriteria-kriteria paket, mulai dari klasifikasi *Address*, klasifikasi Protokol, klasifikasi sambungan, klasifikasi aplikasi.
4. Pada proses terakhir paket masuk kedalam kebijakan-kebijakan yang mengatur firewall sebelum paket sampai ke user.

4. Kesimpulan dan Saran

4.1 Kesimpulan

Berdasarkan uraian-uraian permasalahan dan pembahasan pada bab-bab sebelumnya, maka penulis dapat mengambil kesimpulan dari tugas akhir sebagai berikut :

Berdasarkan hasil analisa dan penerapan *firewall* yang telah di buat, dengan menggunakan metode *Stateful Multilayer Inspection,* paket yang masuk melewati firewall akan di inspeksi secara selektif dengan cara mengklasifikasikan protokol-protokol dan menandai sambungan yang terbentuk dan kemudian paket tersebut didaftarkan pada kelompok daftar kriteria paket, dengan demikian paket akan benar-benar terinspeksi pada layer-layer protokol jaringan secara efisien dan selektif.

4.2 Saran

Adapun saran yang penulis usulkan untuk melanjutkan pengembangan sistem ini adalah:

Metode *Stateful Multilayer Inspection* yang diterapkan pada *Mikrotik Router OS* ini masih memerlukan pengembangan keamanan untuk menangani keamanan pada segmen aplikasi dengan menggunakan ekternal proxy supaya kinerjanya dapat berjalan optimal. sekaligus menambahkan alat bantu berbasis web untuk monitoring keamanan, khususya sebagai alat bantu bagi administrator dalam monitoring *firewall*.

5. Daftar Pustaka

[1] Chu-Hsing Lin, Jung-Chun Liu, Chien-Ting Kuo, Mei-Chun Chou, Tsung-Che Yang, 2009. “Safeguard Intranet Using Embedded and Distributed Firewall System”. *International Journal of future Generation Communication and Networking.* Vol.2,Vol.1, 9-15.

[2] http://id.wikipedia.org/wiki/Tembok_api#Stateful_Firewall, diupdate tanggal 11 juli 2013.

[3] http://wiki.mikrotik.com/wiki/Firewall, diupdate tanggal 5 April 2013.

[4] http://wiki.mikrotik.com/wiki/Dmitry_on_firewalling, diupdate tanggal 5 Mei 2009.

[5] http://www.forummikrotik.com/general-networking/15268-about-firewall.html, diupdate tanggal 24 Oktober 2010.

[6] Imam. C (2013). *Linux Networking*, Penerbit Jasakom, Jakarta.

[7] Janner Simarmata (2008). *Pengamanan Sistem Komputer*, Penerbit Andi. Yogyakarta.

[8] Jusak. (2013). *Teknologi Komunikasi Data Modern*, Penerbit Andi. Yogyakarta.

[9] Onno W. Purbo (2008). *Keamanan Jaringan Internet*, Penerbit PT Elex Media Komputindo. Jakarta.

[10] Shaymaa W. Abdulatteef, 2012. “An Implementation Of Firewall System Using Mikrotik Router OS”. *Journal of university of anbar for pure science* Vol.6,Vol.2 , 8-11.