Keamanan Jaringan Dengan Firewall Filter Berbasis Mikrotik Pada Laboratorium Komputer STIKOM Bali

I Gusti Komang Oka Mardiyana,
STMIK STIKOM Bali
Jln. Raya Puputan Renon no.86 Denpasar - Bali
e-mail: moka@stikom-bali.ac.id

Abstraksi

Laboratorium komputer difungsikan sebagai sarana pembelajaran mandiri, karena masing-masing komputer yang ada sudah terkoneksi ke Internet. Penggunaan komputer tidak dapat dipantau secara detail, bisa jadi komputer tersebut di gunakan untuk hal-hal yang tidak semestinya. Oleh karna itu harus ada sebuah upaya untuk mengelola pemakaian komputer pada laboratorium salah satunya dengan menerapkan konsep firewall. Permasalahan tersebut dapat diatasi menggunakan MikroTik sebagai pengatur lalu lintas data Internet serta melakukan pemfilteran beberapa aplikasi yang dapat mengganggu konektifitas jaringan komputer sesuai dengan aturan yang disepakati sebelumnya. Pada penelitian ini menggunakan perangkat dari MikroTik, dengan harapan hasilnya dapat memenuhi kebutuhan sistem khususnya dalam menerapkan konsep firewall untuk mengatur lalulintas paket data bagi para pengguna komputer dengan memanfaatkan firewall filter berbasis MikroTik.
Kata Kunci: Firewall, MikroTik

1. Pendahuluan

Laboratorium sebagai sumber pembelajaran di sebuah perguruan tinggi dalam hal ini adalah laboratorium komputer, laboratorium yang mana isinya adalah seperangkat komputer, tentunya akan digunakan oleh banyak pengguna, baik itu dari kalangan mahasiswa, dosen dan petugas kampus tentunya dengan berbagai kepentingan yang berbeda.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. Untuk menyikapi keamanan tersebut dipandang perlu untuk menerapkan kebijakan teknis yang digunakan untuk mengelola user, mencegah akses yang tidak perlu yang nantinya dapat membebani jaringan.

Segala bentuk ancaman yang datang baik langsung maupun tidak langsung akan mengganggu kegiatan yang sedang berlangsung dalam jaringan di laboratorium 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.

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 "KEAMANAN JARINGAN DENGAN FIREWALL FILTER BERBASIS MIKROTIK PADA LABORATORIUM KOMPUTER STIKOM BALI" akan dibahas bagaimana merancang 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 tempat penelitian yaitu pada Laboratorium Komputer STIKOM Bali.

2. Metode Penelitian

2.1. Tempat dan Waktu

Penelitian dan penulisan ini berlangsung pada Januari 2015 sampai dengan April 2015 yang akan dilakukan di STIKOM Bali dengan alamat Jl. Raya Puputan No. 86 Renon, Denpasar – Bali.

2.2. Alur Analisis

Alur analisa dalam pengerjaan penelitian ini adalah terdiri dari beberapa tahapan, yaitu:

1. Pengumpulan Informasi
   - Studi Literatur

Pengumpulan data dengan cara mengumpulkan literatur, jurnal, paper dan bacaan-bacaan yang ada kaitannya dengan perekayasaan sistem jaringan komputer.

- *Site Survey*
  Kegiatan dalam Site Survey mencakup observasi dan wawancara secara langsung kelokasi dimana kita akan melaksanakan penelitian yaitu pada Laboratorium Komputer STIKOM Bali. Dalam proses Site Survey, dilakukan pendokumentasian hal-hal penting yang berkaitan dengan proses analisa rekayasa sistem jaringan komputer seperti:
  - Lokasi fisik dari peralatan
  - Bagaimana peralatan tersebut saling terkoneksi
  - Pemanfaatan media transmisi
  - Skema untuk IP Address
  - Akses Internet
  - Hak akses ke internet
  - Kebijakan pemakaian internet

2. Analisis
   Dalam tahapan ini dilakukan proses analisa terhadap system yang sudah ada (current system) dimana hasil analisa tersebut akan digunakan acuan untuk membuat perancangan system yang baru termasuk didalamnya memilih perangkat yang akan digunakan untuk rekayasa sistem jaringan computer ditinjau baik dari segi *hardware* maupun *software.*
3. Perancangan / *Selection and Design*
   Dalam tahap ini juga dilakukan perancangan sistem jaringan dengan membuat desain jaringan yang lebih mutakhir meliputi topologi fisik dan topologi logical. Pembuatan *prototype* menggunakan aplikasi *Virtual Box*.

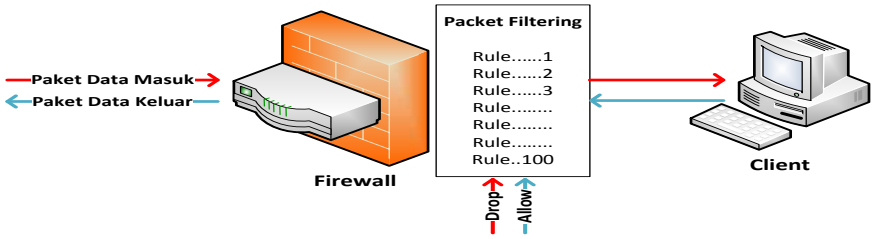
Dari penjelasan diatas, berikut adalah gambaran tentang tahapan yang digunakan dalam pelaksanaan penelitian ini.

3. Pembahasan

Perancangan dilakukan untuk membuat suatu bentuk rancangan jaringan komputer yang sesuai untuk diterapkan sistem *gateway* sekaligus sebagai firewall yang menerapkan packet filtering dimana metode packet filtering akan mengatur semua packet baik yang menuju, melewati atau akan dituju oleh packet tersebut. packet tersebut akan diatur apakah akan di terima, diteruskan atau di tolak.

3.1. Firewall

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 didalam tiap paket.



Gambar Iustrasi Aliran Data Firewall

3.2. Konfigurasi Mikrotik

1. Pengamanan Router

Pengecekan terhadap semua konesi yang akan masuk dari jaringan internet (public) ke router. Tutup semua koneksi yang sifatnya tidak valid, izinkan semua koneksi yang sifatnya Established dan izinkan koneksi dengan protocol ICMP untuk masuk ke router. Dijelaskan dengan beberapa baris perintah berikut:

/ip firewall filter

add chain=input connection-state=invalid action=drop comment="Drop Invalid connections"
add chain=input connection-state=established action=accept comment="Allow Established connections"
add chain=input protocol=icmp action=accept comment="Allow ICMP"
Jaringan yang berasal selain dari internet (public) adalah dari jaringan internal Laboratorium dianggap terpercaya, maka semua jaringan yang berasal dari Laboratorium diizinkan untuk mengakses router MikroTik.

Tabel Jaringan Laboratorium Komputer STIKOM Bali

NO	CHAIN	SRC-ADDRESS	ACTION	IN-INTERFACE	COMMENT
1	INPUT	172.16.1.0/26	ACCEPT	Lan1	Lab Database
2	INPUT	172.16.2.0/26	ACCEPT	Lan2	Lab Mobile Technology
3	INPUT	172.16.2.64/26	ACCEPT	Lan3	Lab Multimedia
4	INPUT	172.16.2.128/26	ACCEPT	Lan4	Lab Robotic
5	INPUT	172.16.3.0/26	ACCEPT	Lan5	Lab Web Technology
6	INPUT	172.16.3.64/26	ACCEPT	Lan6	Lab Programing
7	INPUT	172.16.4.0/26	ACCEPT	Lan7	Lab Business Inteligence
8	INPUT	172.16.4.64/26	ACCEPT	Lan8	Lab Networking

2. Pengamanan Client Jaringan Laboratorium

a) Melakukan pengecekan terhadap semua koneksi yang akan melewati (forward) router dari jaringan internet (public) ke jaringan Laboratorium.
/ip firewall filter
add chain=forward protocol=tcp connection-state=invalid action=drop comment="drop invalid connections"
add chain=forward connection-state=established action=accept comment="allow already established connections"
add chain=forward connection-state=related action=accept comment="allow related connections"

b) Untuk meminimalkan potensi serangan dari beberapa IP Address tersebut makan dilakukan blokir terhadap IP BOGON.

c) Konfigurasi jumps to new chains untuk masing-masing protocol yaitu tcp, udp, icmp.
/ip firewall filte
add chain=forward protocol=tcp action=jump jump target=tcp
add chain=forward protocol=udp action=jump jump-target=udp
add chain=forward protocol=icmp action=jump jump-target=icmp

d) Meminimalkan TCP Port dan UDP Port yang terbuka sebagai salah satu cara untuk meminimalkan potensi serangan ke dalam jaringan

Tabel Drop TCP Port

NO	**CHAIN**	**PROTOCOL**	**DST-PORT**	**ACTION**	**COMMENT**
1	TCP	TCP	69	DROP	TFTP
2	TCP	TCP	111	DROP	RPC Portmapper
3	TCP	TCP	135	DROP	RPC Portmapper
4	TCP	TCP	137 - 139	DROP	NBT
5	TCP	TCP	445	DROP	CIFS
6	TCP	TCP	2049	DROP	NFS
7	TCP	TCP	12345 - 12346	DROP	NetBus
8	TCP	TCP	20034	DROP	NetBus

Tabel Drop TCP Port

NO	CHAIN	PROTOCOL	DST-PORT	ACTION	COMMENT
1	UDP	UDP	69	DROP	TFTP
2	UDP	UDP	111	DROP	PRC Portmapper
3	UDP	UDP	135	DROP	PRC Portmapper
4	UDP	UDP	137	DROP	NBT
5	UDP	UDP	9204	DROP	NFS

e) Izinkan hanya yang ICMP diperlukan saja, dengan tujuan untuk meminimalkan ICMP Codes yang terbuka untuk client.

Tabel Accept ICMP Codes

NO	CHAIN	PROTOCOL	ICMP-OPTIONS	ACTION	COMMENT
1	ICMP	ICMP	0:00	ACCEPT	Echo reply
2	ICMP	ICMP	3:01	ACCEPT	Net unreachable
3	ICMP	ICMP	3:04	ACCEPT	Host unreachable
4	ICMP	ICMP	8:00	ACCEPT	Echo request
5	ICMP	ICMP	11:00	ACCEPT	Time exceed
6	ICMP	ICMP	12:00	ACCEPT	Parameter bad

4. Simpulan dan Saran

4.1. Simpulan

Adapun kesimpulan yang dapat diambil dari penelitian ini adalah:

1. Keamanan jaringan dengan firewall filter berbasis mikrotik yang dihasilkan masih berupa perancangan penerapan system keamanan.
2. Sistem yang dirancang dapat memenuhi kebutuhan sistem khususnya dalam melakukan packet filter sesuai dengan kebutuhan pada Laboratorium Komputer STIKOM Bali mampu mengamankan jaringan pada Laboratoium Komputer dengan melakukan filter terhadap lalu lintas data yang melewati router sesuai dengan ketentuan yang telah rancang

4.2. Saran

Adapun saran untuk pengembangan keamanan jaringan berikutnya adalah:

1. Menambahkan alat bantu berbasis web untuk monitoring firewall.
2. Dilakukan implementasi secara langsung pada Laborarorium Komputer STIKOM Bali sehingga dapat diketahui efektifitas dari penerapan system keamanan dengan firewakll filter berbasis MikroTik.

Daftar Pustaka

[1] Melwin Syafrizal. (2005), Pengantar Jaringan Komputer, Penerbit Andi, Yogyakarta.

[2] Aidil Chendramata, Adhityo Priyambodo. (2006) INTEGRASI KEAMANAN SISTEM INFORMASI BERBASIS *OPEN SOURCE*, Direktorat Sistem Informasi, Perangkat Lunak Dan Konten Direktorat Jenderal Aplikasi Telematika Departemen Komunikasi Dan Informatika, Jakarta.

[3] Eksan Wahyu Nugroho. (2006), Implementasi Waktu Pencarian *(Time To Live)* Alamat Internet Protokol (*IP* Address), JURNAL SISTEM DAN INFORMATIKA Volume2, Edisi Pebruari, 2006, Denpasar

[4] Rachmat Rafiudin, (2009), IP Routing dan Firewall dalam Linux, Penerbit Andi, Yogyakarta.

[5] Anjik Sukmanji, Rianto. (2008), Jaringan Komputer Konsep Dasar Pengembangan Jaringan dan Keamanan Jaringan, Penerbit Andi Yogyakarta

[6] Hardana. (2011), Konfigurasi Wireless RouterBoard Mikrotik, Penerbit Andi Yogyakarta

[7] http://www.mikrotik.co.id/index_lihat.php?id=1

[8] http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml#icmp-parameters-codes-0